



Security Operations Management

Third Edition

Robert McCrie

Professor of Security Management
John Jay College of Criminal Justice/CUNY



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier



Acquiring Editor: Tom Stover
Editorial Project Managers: Hilary Carr, Emily Thomson
Project Manager: Punithavathy Govindaradjane
Designer: Victoria Pearson

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

Copyright © 2016, 2007, 2001 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

ISBN: 978-0-12-802396-9

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data

A catalog record for this book is available from the Library of Congress

For information on all Butterworth-Heinemann publications
visit our website at <http://store.elsevier.com/>



Working together
to grow libraries in
developing countries

www.elsevier.com • www.bookaid.org



Acknowledgments

A book of this sort is long in the making and incurs many debts along the way. In a general sense, the 450 or so authors of the papers of *Security Journal*, which I edited from 1989 to 1998, provided inspiration for much of the content of this book. Additionally, the readers and news sources of *Security Letter*, which I have written since 1970, have informed me of topical operational issues of concern to them. And readers of the first two editions, particularly students and faculty at John Jay College, contributed to content found in this new volume with their helpful critiques.

This book draws from many papers from *Security Journal* as well as criminal justice and management-oriented publications. Additionally, findings and recommendations from the Academic/Practitioner Symposia sponsored by the ASIS Foundation in earlier years have been helpful for identifying material for inclusion. These symposia were chaired by David H. Gilmore; Carl T. Richards was vice chair.

Many talented security practitioners and academics have provided me with inspiration – knowingly or unknowingly – over the years. Surely, that list is long. Those who must be included are as follows: J. Kirk Barefoot; James Calder; Kevin Cassidy; Ronald V. Clarke; John G. Doyle, Jr.; Anthony L. Gentile; Eva Giercuskiewicz; Joseph Gulinello; Martin Gill; David Haas; William J. Kelly; Charles Nemeth; Keith Oringer; Hans Öström; Joseph Ricci; Richard D. Rockwell; Joseph S. Schneider; Bo Sørensen; Tom Winn; and Jeffry Zwirn. Thanks also to those who read parts of the manuscript and provided guidance on how to improve them. These have included Gerald L. Borofosky, Paul DeMatteis, John Friedlander, Walter A. Parker, and Peter Tallman. Thanks also to so many unnamed others who contributed to the effort.

My associate, Luis A. Javier, tirelessly saw to numerous production and fact-checking details in preparing all editions. And above all, deepest appreciation goes to Fulvia Madia McCrie, without whom this book would *never* have been realized and who has been of inestimable importance to getting this out. At Elsevier Butterworth-Heinemann my warmest thanks go to Hilary Carr for her patient nurturing of this edition and Punithavathy Govindaradjane and team who meticulously saw to the copy editing and final preparation of the third edition.

—R.D. McC.

Security Operations in the Management Environment

Security management is ready and eligible to be considered as a management science.

—Charles H. Davidson in *Security Journal*

To achieve optimal protective goals, security executives, directors, and managers must operate successful programs. The results are consequential. The contention of this book is that adequate security is not merely a best practice, but rather that it is an essential characteristic for every organization. Without appropriate security the organization is at risk for failure. Vulnerability eventually will be exploited. As that occurs, the entire enterprise will face decline and failure as the natural consequences.

This book will provide insights to assess security risks and manage operations to protect assets from loss. The very words used on a routine basis help explain what security practices are all about. The word “operate,” for example, is derived from the Latin *operatus*, the past participle of the verb “to work”; hence, operations are concerned with exerting power or influence in order to produce a desired effect. Security operations, therefore, are the processes whereby the protective aims of the organization are to be achieved. Success does not depend on good intentions alone, although thoughtful analysis always should precede definitive action. The security practitioner must correctly assume and passionately advocate that his or her appropriate involvement is consequential in achieving what needs to be done.

Operating security programs is not easy. Surely protection is an inherent factor in success and continuity of an operation. Because of this, one might assume – falsely so – that efforts to protect assets (and to do one’s job well) would receive broad, largely uncritical support from senior management and ownership. That’s not necessarily the reality. Some senior managers support security programs assiduously; others fail to understand the criticality of security or, for their own reasons, choose to constrain programs to the minimum level possible.

Security managers must constantly strive to communicate relevance within the world of work. A paradox exists within the workplace: freedom results in creativity and spontaneity, and may foster innovation and economic development. At the same time too much freedom makes abuses within the organization easier to occur. Therefore, controls that decrease possibilities of loss are implemented. However, these same controls may also decrease creativity and efficiency. The art of the security practitioner is to find a sweet balance: to encourage creative expression and achievement, while concurrently making the

control mechanisms reasonably unburdensome to employees, visitors, vendors, and the public at large. The result is that the organization may function without undue burden of constricting security operations.

This book considers the tasks of operating security loss prevention programs for every type of contemporary organization. The principles involved are applicable for both for-profit private sector enterprises and the public sector – not-for-profit (NFP) corporations and government at all levels.

Generally, the management principles and practices discussed in this book are not exclusively applicable for security programs. They are relevant for any organization that requires management. A security manager can migrate with these same principles into other workplace endeavors, drawing from lessons learned through experience. Countless readers and users of earlier editions have done exactly that. Yet the study of this topic is recent. Early governments, military activities, and trade or marketplace commerce required organizations to maximize return on investment. As the scale of activities grew, management skills were required. In particular, only in the past century have management principles been scientifically evaluated, and then only in limited applications. For security management practices that gestation has been even shorter. We shall review some of those antecedents and see how they have helped guide effective operations in the twenty-first century.

Organizations and Managers

To understand what a manager does, it is essential to consider the ways in which organizations have evolved in modern public and private institutions. Management must be rational in order to achieve long-term success. Therefore, the creation of organizations and their successful achievement of desired objectives must be understandable both to those within and outside the organization and to those within and outside a particular functioning unit. This is true for security departments as well as for every other operating division of an organization.

What Is an Organization?

The word “organization” is derived from the Greek *organon*, meaning organ, tool, or instrument, and is akin to something that performs work. Organizations are composed of groups of people bonded by a purpose: a systematic scheme to achieve mutually agreed-upon objectives. Typically, organizations might be divided into a bifurcated scheme: administrators (leaders and planners) and functional members (followers and processors). These roles may be interchangeable according to different circumstances. For example, a security officer without supervisory responsibilities might suddenly be transformed to a leader to deftly protect others when an emergency occurs.

This role migration is possible because management envisioned such a possibility of an emergency and selected and trained personnel to function well in unanticipated

circumstances. Organizations are created, therefore, in order to achieve objectives deemed desirable by leaders and planners of the organization, by those who carry out tasks, or in some cases by both.

Who Is a Manager or Director?

The word “manage” is derived from the Gaelic *mano*, related to hand, and was first linked to the handling or training of a horse in graceful or studied action. Thus, the word suggests the concept of controlling, directing, or coping with challenging and constantly diversifying circumstances. A manager is a person who controls or directs an organization in a desired, purposeful direction. The title of director usually outranks that of manager and refers to the person who directs the work of managers and their subordinates.

What Is Security and Who Is a Security Manager?

Security is defined today as “the protection of assets from loss.” Each word in this definition carries its own implications. The word “protection” means to cover or defend. The term “assets” encompasses numerous possibilities of tangible and intangible resources of value. Yet the most important assets in any operation are people. Clearly, cash and cash equivalents and physical property are considered assets, and knowledge-related activities (intellectual property) and the opportunity to achieve desired goals due to particular circumstances similarly are also assets. An earlier definition of security was “private people protecting private property.” This definition has become dated as private security activities even in private locations have extended also to include “public” protection in a larger context. Also, the earlier definition of security is unsatisfactory because it cites “property” and not people as the assets of greatest significance. “Loss” is clear enough as a term, meaning decrease, impairment, dissipation, or forfeit.

A security manager (or director or chief) is a person who protects identified assets through personnel, procedures, and systems under his or her control. The goal is to achieve objectives – agreed upon with senior management – that also produce minimum reasonable encumbrances to overall operations.

Titles within organizations can change according to fashion. For most of the twentieth century, the titles “president,” “executive,” “chief,” “director,” “manager,” and others had specific meanings. They connoted a hierarchy well understood by those within and outside the organization. Such a hierarchy still exists, but titles may be neither clear nor consistent and can vary from one organization to another. Often an executive (or manager) creates new titles for structural or motivational purposes (see Chapter 5). Thus, words such as “deputy,” “associate,” “assistant,” “managing,” “acting,” “senior,” and “junior” can be parts of some titles that may serve to provide the level of significance of the position to the internal hierarchy and the outside communities. Titles have considerable importance within organizations. Ultimately, the value of a title is linked to the amount of power that is associated with it.

What Is the Purpose of an Executive?

Executives and those with executive tasks – regardless of their titles – are responsible for the planning and analysis of required programs. They are further responsible for implementation of such programs, and executing them. Planning and execution go together. Ultimately, the challenge to organizational leaders is to be effective in achieving or surpassing the reasonably set goals of the organization. Peter F. Drucker (1910–2005) in *The Effective Executive* argues that the primary strategy of work is measured not in the brilliance of its conception, but in how well the desired goals were actually achieved. The nature of work changes constantly, he observes.

According to Drucker, “knowledge workers” are the human capital through which objectives are achieved. Knowledge workers are members of an organization whose effectiveness is realized through the use of information often accessed and partially analyzed through technology. Drucker posits that effectiveness is not simply necessary as a managerial attribute; it is vital and can be learned through concerted effort, leading to still greater effectiveness. Drucker writes:

I have called “executives” those knowledge workers, managers, or individual professionals who are expected by virtue of their positions or their knowledge to make decisions in the normal course of their work that have significant impact on the performance and results of the whole. They are by no means a majority of the knowledge workers. For knowledge work too, as in all areas, there is unskilled work and routine. But they are a much larger proportion of the total knowledge workforce than any organization chart ever reveals.¹

The effective security executive or manager is a person who identifies the problems and opportunities facing the organization, makes plans to resolve them, organizes resources so that the mission may be successfully achieved, deputizes others to follow through on his or her behalf, and then supervises the continuing operation. This is the essence of the American concept of management. It is spelled out further in the next section.

What Is the Strategy of Management?

Management refers to the way in which members of an organization make key decisions on how goods and services are produced. It can also refer to the process by which such goals may be achieved.

Throughout contemporary organizations, the strategy of management is accomplished via a process of identifying, analyzing, planning, organizing, deputizing, and supervising activities common to the attainment of these goals. This process is systematic in that order and conduct is required to achieve objectives by members of the organization. The

BOX 1.1 THE HOLY GRAIL OF CONTEMPORARY MANAGEMENT

Managers use a simple, logical linear process to achieve desired goals. The problem or opportunity may differ in significance, and the time required to adequately analyze and plan it also may vary widely. The manager or director possesses or has received authority and responsibility to resolve a major problem, plan to commence a new program or facility, or resolve a substantial programmatic failure that has engulfed the organization. Once having the assignment, the director/manager gets busy as discussed in the text. A major problem or opportunity may require weeks or months to resolve, but the sequence of events remains the same. Here's the outline used broadly in American management circles:

1. *Analysis and planning.* Once the problem has been identified, the management team will seek to amass all relevant information. It is then used to form a plan that is intended to achieve the desired objectives. This is the longest and usually the most critical step in the process.
2. *Organizing.* This step is a detailed extension of planning. Issues such as personnel required, physical and electronic resources needed, operating protocols, and budget will be completed.
3. *Deputize.* Somebody may be needed to operate the new or improved program. The head planner will deputize someone to manage it going forward.
4. *Supervise.* As the new manager takes over the program, the director or senior manager now oversees the subordinate, assuring that agreed-to objectives are being met.
5. *Criticize.* Constant critical analysis and improvement normally accompanies the implementation of the plan. Conditions constantly change. Therefore, the original plan evolves with dynamic circumstances. Perpetual quality improvement and troubleshooting on unexpected developments continue in the process as results are measured and compared with expected objectives.

A mnemonic helps recall these points: *analyze, organize, deputize, supervise, criticize.*

manager sees to this process in each link of the chain (see [Box 1.1](#)). Specifically, the concatenation of managerial tasks is as follows:

1. *Problem identification: collecting relevant information.* The first organizational step identifies the need that requires some consequential managerial action. This need may be to commence a new program or initiative, to revise an old program faltering for some reason, to solve a newly created problem, to seize an opportunity, to expand or contract operations, or to handle still other options. The management process begins by asking the question: "What needs to be accomplished and why?" It then grapples with the clarified requirements that emerge from the following stages.

Assume that the organization is expanding and must create a new facility to achieve the desired increase in production. This new facility will require a security program to protect its assets. What will the security program look like? Early in the process of planning for such a facility, the security director assumes change of the

security-related aspects of the project. He or she collects pertinent information so that an optimal security program may be achieved on time and on budget. The size, condition, employment, production requirements, environmental issues, potential problems, and other issues will be considered, and the most problematic matters will be isolated. Then the director, often aided by others, completes additional tasks until the program is fully implemented. The process is as follows:

- a. *Analyzing and planning.* Analyzing is the process of separating something into its constituent parts or basic principles. This allows the nature of the whole issue to be examined methodically. To analyze a security problem, the practitioner seeks to collect all pertinent information, which then becomes the basis of planning – or formulating – a means to achieve the desirable goals. These are the critical next parts of the managerial process.

Wise managers do not proceed generally to the next step in the sequence until the previous one is reasonably completed. *How much planning is enough?* A manager is never likely to have all the knowledge and facts necessary to comprehend every relevant facet to analyze fully and then plan comprehensively without ever looking back. Further, conditions change constantly and create situations with which the manager must contend. Yet at some point the analysis must be summarized and assessed when a reasonable quantity of information has been collected and a plan for action evolved. That process of working with finite knowledge and resources is what is fascinating and challenging about the art and method of management. The security director might collect and analyze the following information about the new facility being planned:

- Function of the new facility (what it does, its size and significance)
- Site selection (for protective and risk-averse features of the topography)
- Architectural and engineering firm involvement
- Local conditions where the facility is to be located (e.g., recent crime and development patterns that can be analyzed spatially)
- Local resources available (police, fire, emergency-oriented)
- Legislative or regulatory requirements relevant to the project
- Special security features likely to be required at such a facility

This process involves fact-finding in which the manager, or a surrogate, visits the site to determine its potential risks and opportunities so that these may be incorporated into the formal plan. Relevant data and studies are collected. The security planning team prepares the physical security plan for the new facility.

Needs and expectations are shared and discussed on a preliminary basis with the architects and engineers involved in the process. Planning for security measures required by the facility once it begins operating is also undertaken at this time. The manager discusses the analysis and planning with senior management.

- b. *Organizing.* After the need has been determined, its critical parts have been identified, and a plan has been established to respond to the need, resources must

be organized – that is, created or accumulated in order to achieve the objective. Money and personnel must be committed. Technology and software strategies may be required and must be allocated. Impediments must be resolved. Commitments must be assured. Then the plan can be implemented by selecting subordinate managers. The plan must now be approved by relevant decision makers throughout the organization. Resources required for the security program at the new facility are then mobilized. The steps taken may include:

- Consulting with architectural and engineering personnel about specific security design needs
- Issuing a request for proposal (RFP) for the system (Chapter 9)
- Establishing qualified bidders for the security project
- Reviewing submissions and awarding the contract
- Supervising the project's installation
- Assuring adequate training and support materials
- Testing the system under normal and adverse circumstances

At this point, a complex system has been created for the new facility.

Meanwhile, a security staff must be hired and procedures for both security and nonsecurity personnel must be prepared and reviewed. The next step assures these goals are met.

- c. *Deputizing.* A manager does not achieve the objectives of the plan solely by his or her actions: a manager works in the company of others. In the management process, the problem has been analyzed and a plan to deal with it has been agreed upon. Resources have been committed firmly. Now the process of assuring that the plan achieves its objectives is shared with persons who will follow through – hopefully to realize the intended goals. Persons deputized to achieve these ends on behalf of the planning managers are themselves managers who are now transferred the responsibility for assuring that the plan will be carried out. The senior planning manager is now free to supervise this person or persons. The new security system is designed, approved, and becoming operational. A manager must be appointed to operate the enduring, ongoing satellite security program. It is not likely to be the senior security executive. Consequently, someone is deputized to assume this responsibility on behalf of management at headquarters. He or she will administer the plan of the new facility.
- d. *Supervising.* The planning manager next supervises the manager who has been given responsibility for achieving the goals set by the plan. Through this process, the manager can assure that goals are reached in the face of constantly changing circumstances. Thus, the principal manager is engaged in controlling the work of others and the allocation of resources in pursuit of the desired objectives. The supervising manager in the hierarchy remains available to critique, and supports and guides the manager deputized to carry out the plan. The supervising manager now has time to concentrate on other matters, such as identifying another need and planning its resolution or supervising other

operating programs. The central manager's time commitment for the new facility gradually lessens as the deputy assumes control. That deputy reports regularly on developments. The central manager maintains quality control over the physical and procedural process involved in creating the plan for the new facility. At this point, the managerial process for the new location has been completed. The time it takes to complete the process varies considerably depending on particular problems to be managed. The process is dynamic; circumstances change constantly, often in ways that could not have been anticipated early in the planning period even by the most conscientious and rigorous planners. Therefore, the manager must be prepared to constantly refine the plan to new circumstances, seizing fresh opportunities for further gains in programmatic objectives whenever possible.

- e. *Criticizing results.* Constant critical analysis and change are normal experiences. (The word *criticizing* is not usually meant in a negative sense, but rather is used to imply commenting, interpreting, and judging.) At this point, the planning process has been completed from inception to realization. The sequence may take as little as a few hours by a single individual or as much as months of concentrated effort by a devoted managerial team. Such a team could include internal managers, contract personnel, and independent consultants retained for the project. However, although the program may be functional, the process is never complete. Circumstances change constantly, often in ways that could not have been anticipated even by the most conscientious and rigorous planning process. Therefore, the manager must refine the plan to fit the new circumstances, seizing new opportunities for further gains in programmatic objectives whenever possible to meet the needs of a contemporary workplace.

Characteristics of Modern Organizations

Contemporary organizations of size and complexity must possess a pertinent structure to achieve operational success. Civilization is about 5000 years old, but the industrial age arrived in Europe only in the eighteenth century, arriving decades later in what would become the United States. The demands of constantly competing, expanding industrialization – coupled with growing urbanism – created pressures for greater effectiveness on organizations. This process attracted the attention of seminal early observers who first described evolving characteristics of the operational processes. These observations created the basis for methodological observers who sought science-based ways of improving industrial output. Much later still, security practitioners emerged as a cadre of managers to protect organizations in specific and distinctive ways.

Pivotal individuals in this process may be divided into three categories: classical management theorists, scientific management proponents, and recent distinctive contributors to security management practices.

Classical Management Theorists

Industrialization flourished following principles of expediency and common sense. In time, the processes of production came under scientific analysis and subsequent improvement. The first significant and comprehensive codification of management principles was provided by a French mining engineer, Henri Fayol (1841–1925). He observed workplace processes, which he then categorized into logical and distinct descriptive terms. They have endured well with broad applications and significance:

- *Division of work.* In an organization of any size, labor is divided into specialized units to increase efficiency. Work within the organization tends to become increasingly specialized as the organization grows in size.
- *Hierarchy.* Organizations disperse authority to managers and employees according to their formal position, experience, and training.
- *Discipline.* Good discipline exists when managers and workers respect the rules governing activities of the organization.
- *Unity of command.* No individual normally should have more than one supervisor. Work objectives concerning tasks should relate rationally among supervisors and subordinates. (Fayol derived this point from his observations of military structure.)
- *Chain of command.* Authority and communication should be channeled from top to bottom in the organization. However, communication should flow from bottom to top as well.
- *Unity of direction.* The tasks of an organization should be directed toward definable and comprehensible goals under the leadership of a competent manager.
- *Subordination of interests.* The goal of the organization should take precedence over individual desires. When personal agendas become paramount, the goals of the organization cannot be achieved effectively.
- *Remuneration.* Pay and the total benefits package should be fair.
- *Equity.* Managers should be just and kind in dealing with subordinates.
- *Stability of tenure.* Management should plan so that positions are stable. Reduction of positions (downsizing; “rightsizing”) may be necessary under times of market and production downturn, but often the reduction of previously budgeted positions reflects the failure to plan and execute wisely.
- *Order.* The workplace should be orderly.
- *Initiative.* Employees should be encouraged to show personal initiative when they have the opportunity to solve a problem.
- *Teamwork.* Managers should engender unity and harmony among workers.
- *Centralization.* Power and authority are concentrated at the upper levels of the organization. The advantages of centralization versus decentralization are complex and may be regarded as a cyclical phenomenon in management fashion; that is, despite a penchant for centralization of organizational power, there may be times when production is best achieved by decentralization of planning and much

decision making. (Do organizations operate best centrally or regionally operated? It's a debate. French preference, following Fayol's culture, espouses centralized planning and management. In the United States, many decisions evolve on the operating units.)

Fayol offered common sense observations that have not been substantially revised over time. His list of 14 descriptives remains as fresh and pertinent today as it was a century ago. Yet, he made other observations. According to Fayol, all managerial activities can be divided into six functions:

1. *Technical* (engineering, production, manufacture, adaptation)
2. *Commercial* (buying, selling, exchanging)
3. *Financial* (searching for an optimal use of capital)
4. *Accounting* (stock taking, balance sheets, cost analysis, statistical control)
5. *Managerial* (goal setting, analyzing and planning, organizing, deputizing, supervising)
6. *Security* (protecting physical assets and personnel)

These six functions are always present, regardless of the complexity and size of an organization. Thus, all organizational undertakings involve an interlinking of functions. Security is correctly included as one of these fundamental activities of general management. Fayol observed that the security function “involves exposure identification, risk evaluation, risk control, and risk financing.”² In a remarkably insightful observation for its time, he also added:

Quite frankly, the greatest danger to a firm lies in the loss of intellectual property, a loss that the firm may attempt to prevent through patent protection, trade-secret protection, signed agreements (nondisclosures) with key personnel, and access to its innermost secrets on a strictly “need to know” basis.

Fayol's prescient views hold that security of know-how and opportunity take precedence over physical assets. Many contemporary security practitioners readily would agree.

Fayol is regarded as a classical administrative theorist. Other pioneers of his genre include Max Weber (1864–1920) and Chester Barnard (1886–1961). Weber developed the term “bureaucracy,” which he described as the most rational form of an organization.³ According to Weber, large-scale tasks could be pursued by organizing human activity as follows:

1. Activities directed toward meeting organizational goals are constant and officially assigned.
2. Activities are controlled through a hierarchical chain of authority.
3. A system of abstract rules ensures that all operations are treated equally.
4. Bureaucratic officials remain emotionally uninvolved while fulfilling their formal duties.

Barnard, an executive for New Jersey Bell Telephone, emphasized that a “cooperative system” generally is necessary for an organization to reach its goals. In *The Functions of the Executive*, Barnard advanced a concept known as acceptance theory, concluding that subordinates would follow the leadership of supervisors and managers when four conditions were met:

1. They could and did understand the communications they received.
2. They believed that the communication was consistent with the purpose of the organization.
3. They believed that it was compatible with their own personal interest.
4. They were mentally and physically capable of complying with the communication.⁴

Weber underscored the importance of managerial involvement to achieve desirable goals. Barnard espoused the principle that clear, reasonable communications could result in workers accepting the demands of a bureaucracy.

Scientific Management Pioneers

Early exponents of scientific management sought to use data collection and analysis to improve workers’ performance. The costly and time-consuming efforts required to save a few minutes or seconds might seem like a frivolous activity to some; however, improved techniques, when applied to a repetitive process on a large scale, pay generous rewards over time by improving efficiency. Furthermore, the same process of job analysis could offer improvements in safety and comfort for the worker.

Frederick W. Taylor (1856–1915) was a self-taught engineer who became chief engineer of a steel company by the age of 28. His impressive early climb up the career ladder was related to his ability to study work scientifically and then to apply the results directly. His contributions had enormous influence on the workplace throughout the twentieth century. He was called the father of scientific management.⁵ Taylor’s principles were generated at a time when skilled workers were in short supply and the workplace needed to develop best practices to enhance industrial productivity. His ideas are summarized as follows:

1. *Determine what’s important in a task.* Managers must observe and analyze each aspect of a task to determine the most economical way to put that process into general operation. The use of time studies helps to establish what works best.

Example: Federal Express couriers delivering or picking up packages knock on a door before ringing the bell. Their studies have revealed that customers respond faster to the knock-first-then-ring sequence. Perhaps regular FedEx customers also are conditioned to faster response because they know who is at the door. Similarly, security officers responding to an incident can be more productive and thorough by following a developed protocol they have learned that sequentially prompts them to direct employees and members of the public to take actions that will protect their well-being during the emergency.

2. *Select personnel scientifically.* Taylor believed that all individuals were not created equal. Training could help modify differences in behavior and performance, but still some persons would be more effective than others in performing the same tasks. It stands to reason, therefore, that operations will be improved when managers concentrate on selecting only those who show the best capacity to perform the job required.

Example: Security personnel are often the first people visitors and others meet when entering a workplace. Some people have better communication skills than others in interfacing with the public. Still others are prized because they have good visual memories and can remember individuals who have been terminated for cause long ago and may be returning for no good reason. Furthermore, security personnel are frequently first responders in times of emergencies. Concerning circumstances like these, some individuals are clearly more effective than others. As part of the screening process, personnel can be selected who have the characteristics most needed for a particular application.

3. *Offer financial incentives.* Selecting the right worker for the right task does not by itself assure optimal effectiveness. Workers need motivation, and hourly pay and benefits alone may not be sufficient to achieve that goal. Taylor ascertained that providing a differential piece-rate form of incentive can produce higher worker output than what would ordinarily be expected.

Example: The manager of an investigative department provides incentive payments for those staff investigators who are able to complete more investigations than the baseline expectation. Quality control assures that such investigations meet or exceed expected standards of quality for the assignments undertaken so that investigators seeking to achieve additional payments may not sacrifice standards to achieve higher benefits.

4. *Employ functional foremanship.* Taylor argued that responsibility should be divided between managers and workers. Managers primarily would plan, direct, and evaluate the work; the individual worker was responsible for completing the designated tasks. This permitted a worker to take orders from a functional foreman regardless of the stage of work because all managers and foremen would understand the same work processes.

Example: Assume that a new security supervisor replaces another normally responsible for a work unit. The goals of the workers being supervised are identical. Since procedures to achieve these objectives are understood by all workers, a new supervisor reasonably should be able to achieve the same objectives with the workers as the regular supervisor would have.

Frank Gilbreth (1868–1924) and Lillian Gilbreth (1878–1972) were a husband and wife team who translated Taylor's scientific management approach and applied it to specific tasks, much as Taylor had done. The Gilbreths further sought to increase the speed of attaining production objectives by eliminating useless motions. They noted that efficient procedures also led to less fatigue and chances of error by workers.⁶ Their research underscores the importance of designing systems and tasks that support them carefully. As a result, errors are less apt to occur or may be less frequent

and serious after such analysis than in systems that are not established with empirical methods.

Example: On March 28, 1979, at Three Mile Island, near Harrisburg, Pennsylvania, a near meltdown of a nuclear power facility almost occurred. It resulted in a limited evacuation of the area. As a result of the fear generated by this emergency, the nuclear industry in the United States was stigmatized, and additional construction of nuclear power facilities ceased for years to come. In subsequent investigations, many factors explained why the nuclear accident at Three Mile Island occurred. One significant issue was that critical gauges and controls were not within the line of sight of engineers at the control consoles. An investigation of the Three Mile Island facility by the Nuclear Regulatory Commission determined that an inadequate quality assurance program to govern construction and monitor quality “resulted in the construction of a facility of indeterminate quality.”⁷ Failure to design a facility properly may explain why losses occur; conversely, good design system may be more important than marginal differences in human competency in explaining the achievement of desired effects.

Likert’s System 4 Categories

Rensis Likert (1903–1981) was an organizational psychologist who began his career at the US Department of Agriculture and then at the Institute for Social Research at the University of Michigan. After retirement he established the Institute for Corporate Productivity (i4cp). Likert is remembered for two intellectual contributions. One was research-based, the Likert Scale that evaluated activities on a scale from 1 to 7 and that continues to be used widely in social science research comparative scales.

His other contribution was the concept of System 4 that divided organizations into four categories.⁸ These were intended to describe the characteristics of management styles under different circumstances:

- *System 1: exploitive authoritative.* Management operates by fear. Communication comes from the top down. Responsibility is held tightly by senior managers who do not trust subordinates. Workers do not feel comfortable about discussing job-related issues with those higher in the hierarchy.
- *System 2: benevolent authoritative.* Management controls are shared more widely in the organization. Subordinates again do not feel comfortable about sharing views with higher-ranking personnel, but the feeling is less extreme than in System 1. Team work is not a feature. Motivation is linked to rewards.
- *System 3: consultative.* Communication travels in both directions, but upward relationships are cautious. Confidence in subordinate employees is stronger than in System 2 but is not complete. Some discussions about aspects of the workplace are discussed between supervisors and subordinates.
- *System 4: participative group.* Communications are natural and frequent in both directions. Teamwork is encouraged. The supervisor has considerable confidence in subordinates, and the reverse is also true. Responsibility for achieving organizational goals is widely dispersed.

BOX 1.2 SWOT ANALYSIS	
Strengths 1. Market share is high 2. Widely regarded as best in class 3. Leader in innovation within its industrial sector	Weaknesses 1. Gross profit is tight with price increases difficult to achieve 2. Foreign competition is growing with fresh marketing approaches 3. Income is too cyclical with no strategy to deal with troughs
Opportunities 1. Can build on growth using eCommerce better 2. May expand into new foreign markets 3. Monetization of assets through partnerships with noncompetitive organizations	Threats 1. Substantial competitors are poised to be entering the market 2. Execution risk with growth plans untested for market expansion 3. Regulatory environment changing that could impinge on profit and operations
SWOT analysis or matrix was used by Albert Humphrey in the 1960s and 1970s and has been popularized by management writers such as Michael Porter.	

The SWOT Matrix

Ways of thinking about marketplace problems and opportunities evolve over time. In the past market planners were taught that every problem also presented an opportunity, or vice versa. In the serious activity of allocating limited resources, managers more recently have turned to strengths, weaknesses, opportunities, and threats (SWOT) as a more nuanced approach at planning. While not based on pure research, SWOT analysis evolved using data from Fortune 500 companies and presented at a conference held by Stanford Research Institute (now SRI International). The technique is meant to force managers to confront weaknesses or threats and turn them into strengths or opportunities. [Box 1.2](#) provides an example that might be used for general organizational planning. But an individual security department could create its own SWOT analysis with pertinent programmatic differentiation. The matrix has been credited to Albert Humphrey (who denied being the originator).

Security Management Precedent Setters

The craft of operating security programs effectively is a recent one, when judged by contemporary standards. The principal professional association in the field, ASIS International (ASIS; formerly the American Society for Industrial Security), was founded in 1955. The Security Industry Association began in 1967, the National Council of Investigation and Security Services in 1975, and the International Security Management Association in 1976. Surely, informal private security operations existed prior to the founding of these groups, and thousands were employed in security positions in the nineteenth century and the first half of the twentieth century. But only in the last half of the twentieth century did security



FIGURE 1.1 Ronald V. Clarke: crime mitigation researcher. Ronald V. Clarke and others proposed a theory that underlines crime reduction: situational crime prevention. In 2015, Clarke and Patricia Mayhew won the prestigious Stockholm Prize in Criminology for their contributions to loss reduction theory and practice. (Source: Ronald V. Clarke.)

emerge as a defined, usual, respectable, and visible part of management. In the process, security operations have been enhanced by the writings and practices of those who have directed successful programs. In particular, five persons are mentioned here who have contributed notably to the conceptual and operational framework of the discipline. They are Ronald V. Clarke, Charles H. Davidson Jr., Eduard J. Emde, J. Kirk Barefoot, and Bonnie S. Michelman.

- *A theoretical basis for security practices.* Although his research career largely has been rooted in studies aimed at aspects of community crime mitigation and funded by various governmental agencies, Ronald V. Clarke has contributed exceptionally to the philosophical and research basis of private sector security practices ([Figure 1.1](#)). Clarke, a professor at the Rutgers University School of Criminal Justice, was an early social science researcher who helped develop the field of situational crime prevention. Other pioneers in this field include Paul and Patricia Brantingham, L.E. Cohen, D.B. Cornish, and Marcus Felson. These researchers have established situational crime prevention and opportunity theory as a philosophical basis for identifying risks and means of reducing them. These factors are a motivated offender, a suitable reward or goal for the offender's actions, and the absence of appropriate controls that could check such action by the offender (see [Box 1.3](#)). A fourth component, often mentioned, is the potential creation of shame or image problems for a perpetrator.

BOX 1.3 SITUATIONAL CRIME PREVENTION: KEY ELEMENTS, POSSIBLE CONTROLS, OR MITIGATING FACTORS

Key Elements	Possible Controls or Mitigating Factors
A motivated offender	Deny access to sensitive areas Warn of punishment for illegal behavior Prosecute apprehended offenders
A suitable reward or goal	Decrease available assets that might be stolen from a potential victimization site Render vulnerable assets less attractive to thieves or alter behavior of potential victims so that they might be less likely to be victimized Make vulnerable assets difficult for thieves or other offenders to benefit from
Absence of appropriate control	Assign security officers (“place minders”) to protect a location or increase their numbers Install or upgrade a security system Educate nonsecurity employees and others to participate willingly in loss prevention strategies

Note: Situational crime prevention posits that all three elements may be assessed to determine the crime vulnerability of a location or situation. A fourth element sometimes mentioned relates to image risk to the perpetrator by shame or embarrassment. By changing any one element, the possibilities of increasing or decreasing violent or property crime change.

By intervening with any one of these three primary factors – which is often possible at low or no substantial cost – measurable crime should decrease. Situational crime prevention does not envision situations in which an environment will entirely be free of crime. Rather, it seeks to engineer practical measures that will permit a normal pattern of human and commercial activity while reducing violent acts and property offenses to a tolerable level.

- *Providing support for research and its dissemination.* ASIS evolved from its founding as a small, narrow interest group into a global professional and trade organization. Charles H. “Sandy” Davidson Jr. (1910–1994) joined the organization in 1985, as director of research and development and staff liaison with the ASIS Foundation (Figure 1.2). During his tenure Davidson raised research grants to support original studies in security-related matters. He helped found *Security Journal*. Davidson organized the Annual Academic/Practitioner Symposia that began in 1997, and attracted leading security directors and security faculty members to develop curricula and standards. After the attacks of 9/11, with ASIS executive director Michael J. Stack, Davidson helped reshape the organization to better respond on global issues of terrorism.⁹ Retiring as a two-star Army general, Davidson is remembered by named scholarships in the graduate degree in business and organizational security management degree program of Webster University.
- *Expanding security’s global influence.* With increasing globalization, security has become a transnational vocation. All presidents of ASIS embark on a year-long schedule of greeting members at various local chapters and at national and



FIGURE 1.2 Charles H. Davidson: security research advocate. Charles “Sandy” Davidson provided a shift in focus for ASIS International when he served as director of research and development. Working through the ASIS Foundation, Davidson supported original research, brought academics and practitioners together, and helped found *Security Journal*. After his career with ASIS, he returned to military duties where he retired as a major general. (Source: *ASIS International*.)



FIGURE 1.3 Eduard J. Emde: reflecting globalization of security. Eduard J. Emde exemplifies how security practitioners have expanded beyond “gates and guards” to encompass problem solving on a global level. A Dutch national, he holds degrees from two countries and has consulted on security matters in many countries. Beginning as a student member of ASIS, he became chair in 2015. (Source: *ASIS International*.)

international meetings. All men and women elected to the prestigious position of president have acquitted their office with enthusiasm (often at great personal cost). Eduard J. Emde, a Dutch citizen and principal consultant for BMKISS Europe, became the first internationally based president of ASIS in 2012 (Figure 1.3). He exemplifies how peer-to-peer education and networking and global security consulting have become an enduring dynamic of increasingly global security problems and responses.

- **Emphasizing internal investigations and risk management.** Investigations are an important technique for organizations, for both external and internal loss control and management purposes. Failure to institute a fact-finding inquiry may result in unchecked losses or other vulnerabilities. J. Kirk Barefoot, with Rickard K. Paterson, removed the mystery of undercover operations by establishing a school that trained students to be effective and ethical fact-finders for internal and external deviance (Figure 1.4). The process encouraged managers, in appropriate circumstances, to consider the regular use of undercover operations as an ethical, reasonable, and efficient means of detecting and deterring crime victimization and the flouting

of recognized performance standards. Barefoot further detailed the process in *Undercover Investigations*.¹⁰ Barefoot, a security director for a Fortune 500 company, also became the organization's risk manager, demonstrating the linkage between loss prevention and use of insurance to off-load risks.

- *Women providing diverse leadership.* Initially, security was an employment mostly reserved for males, and remained that way as other vocations opened opportunities for women. However, security by necessity came to include women throughout the ranks and at highest positions. Darlene Sherwood became the first female president of ASIS in 1985. Since then women have served the vocation at a national level including Bonnie S. Michelman, president in 2001, who meanwhile directed security operations at one of the nation's leading medical campuses (Figure 1.5).



FIGURE 1.4 J. Kirk Barefoot: the importance of investigations. J. Kirk Barefoot illustrates the many facets in which a security practitioner may serve his or her organization. Educated in criminal justice and polygraph examination at Washington State University, he segued into corporate loss investigations, becoming the first president of the American Polygraph Association. In his corporate positions, Barefoot extended his duties to manage security, investigations, risk management, and aspects of human resources. (Source: Scott Barefoot.)



FIGURE 1.5 Bonnie S. Michelman: growing presence of female leadership. Women have played a growing role in security leadership since the 1980s. An example is Bonnie S. Michelman, Director of Police, Security, and Outside Services of Massachusetts General Hospital (MGH). She also serves as a security consultant to MGH's owner organization that supports 13 additional hospitals with 100,000 employees. Michelman was president of ASIS International, one of five women since 1985 in this position. (Source: Bonnie S. Michelman.)

Organizations and Security

Fayol stated that a formal structure naturally evolves over time to achieve efficiency. This view was new when it was first propounded. Yet organizations have always used ranks, grades, classes, or other categorizations to reflect significance and authority. While ranks and titles may change and considerable variation may exist within characteristics of the organization, the structures of modern corporations and institutions fit general patterns. A review of the two major types of nongovernmental organizations will illustrate where security management may be found.

For-Profit Corporations

Most corporations are established at the behest of private investors who seek a return on their invested capital; that is, they are for-profit corporations. This sector is responsible for an estimated 85% of the gross national product, according to the 9/11 Commission.¹¹ Such corporations are considered perpetual entities performing the activities described in their charters. Corporations issue common stock to investors, who hope to generate a profit (through dividends and growth of value) from the capital they put at risk (Figure 1.6).

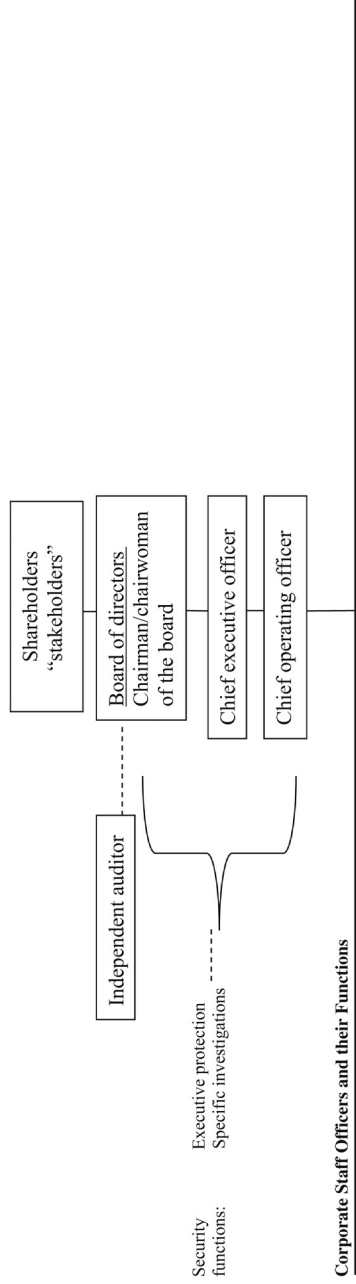
Individuals or institutions that purchase common stock are termed the corporation's shareholders or stakeholders. These shareholders own the corporation, and their degree of ownership (equity) depends on the number of shares they own relative to the total number of shares authorized to be outstanding in the organization. Large corporations with thousands of shareholders are not democratic organizations. They are in no position to hear from all shareholders individually on corporate matters, and modern shareholders expect to have no voice in routine operations or planning. However, shareholders are not without representation. The board of directors legally represents total ownership – that is, the shareholders of common stock. Figure 1.7 shows a corporate organizational chart showing related security functions. In publicly held corporations, in which shares are traded on public stock exchanges, investors exercise their factual ownership by casting votes for directors annually and approving any major changes in the financing, structure, and governance of the entity. A chairman or chairwoman of the board heads the board of directors. This person may also hold other executive duties within the corporation or has held such responsibilities in the past.

The board may be composed of two classes of directors. One category is inside directors, who are currently employed by the corporation. This will include the chief executive officer (CEO; who may also hold other titles). The CEO's role is self-evident: he or she is the person most concerned with executive responsibilities, being in charge of all planning, growth, and operations. Usually immediately subordinate to the CEO is the chief operating officer (COO), who is the main officer concerned with managing day-to-day operations and who reports to the CEO. Formerly, the title of president was equivalent to CEO, but that is no longer the case in most large, complex organizations. The board may also include one or more vice presidents (sometimes titles of executive or senior vice president

Type of Impact and its Effects	Impact Descriptors and Event Categorization			
	Catastrophic	High	Medium	Low
Financial				
Loss of revenue				
Loss of value after insurance recover				
Loss of shareholder value				
Penalties				
Bad debts				
Additional operating				
Costs				
Non financial				
Reputational loss				
Loss of operational opportunity				
Customer service				
Regulatory/legal				
Loss of market share				
Loss of quality				
Brand tarnish				
Environmental				
Contractual				
Staff moral				
Political				

FIGURE 1.6 Identifying key assets and what their risks are. Early in the continuity process, key assets and critical business processes are identified. They can then be categorized according to likelihood of occurrence and level of control possible. This grid can be used for different types of untoward events, emergencies, and disasters with their collateral effects estimated. (Source: *Control Risks Group*.)

are used). These vice presidents may be responsible for a variety of corporate tasks, including financing, manufacturing and production, marketing, legal affairs, and research and development. Other functions can include information (data operations), human resources, and international operations. Most vice presidents will not be members of the board. They often are referred to in large corporations as senior staff officers. They constitute the



Activity	Finance	Human Resources	Marketing	Operations	Counsel	Research	Technology
Title	Chief	Director	Director		Chief	Chief	Director or chief
Tasks	Financial planning Controlling Internal auditing Compensation studies Financial public relations Real estate	Recruiting and vetting Training Affirmative action Discipline and discharge	Market research Advertising Public relations Promotion	Administration Manufacturing Purchasing Traffic Quality control Engineering	Litigation Contracts Regulatory affairs	Planning Competitive analysis	Systems management
Security functions	Internal investigations Assets protection	Employee vetting	Competitive information	Physical security Emergency planning	Investigations	Competitive information	Data security Computer audits

FIGURE 1.7 Corporate organizational chart showing related security functions. All organizations divide responsibilities according to specialized tasks. Security may report to different units depending on the nature of the industry.

executive cadre in large for-profit businesses and variously have responsibility for finance, human resources, research and development, legal affairs, and information systems.

Other staff officers may be included as board members, depending on the nature of the corporation. Outside directors also may be included as board members. Although they are not employees of the corporation, they do possess skills and experience believed to be valuable in directing the strategic affairs of the corporation. Sometimes, an outside director represents, or is personally, a major shareholder, or such a director may own or represent significant debt obligations of the corporation. Other outside directors may be executives of other noncompeting corporations. They may thus be enlisted for board membership because of the experience they may offer to business decision making. Still other outside directors may be academics, public figures, or diverse leaders with insight and professional connections that can aid board decision making.

The commitment the “C-suite” has toward a security program varies widely according to type of industry, history of losses, regulations, and other factors. A security director to thrive needs to comprehend the motivations and priorities of senior for-profit corporate officials. [Box 1.4](#) provides a list of 10 points that will be familiar to many CEOs, COOs, and

BOX 1.4 TEN CONVICTIONS OF EFFECTIVE MANAGERS

1. *Make a profit, or else.* All resources of the organization must be geared directly or indirectly at making a profit. Further, the profit achieved must be sufficiently attractive to the capital providers (investors). If not, they will remove their investment and will reallocate their funds to other presumably more attractive investment options elsewhere. If loss of capital begins and can't be stanchd, the organization then faces inevitable decline. (In governments and in not-for-profit corporations, the goal is not profit-driven but is related: to manage finances astutely.) Any manager who cannot control expenses and work with a budget eventually will be gone.
2. *Constantly drive down the cost of production and operations.* This helps achieve the goal of earning a reasonable profit and keeping the providers of capital happy. Meanwhile
3. *Persistently strive to improve quality.* The organization must be directed implacably toward constant quality improvement in products and services. Otherwise, competition in the private sector, which is always present and searching for fresh opportunity, will seek to acquire market share at the expense of the attractive, profitable, and complacent market leader (“eating the competitor's lunch”) by finding strategic weaknesses in products or services and exploiting them. The public sector equally should be focused on constant quality improvement.
4. *Incentives drive programs.* Earliest management theorists knew the power of incentives. Normally they are used to motivate individuals to perform better. But incentives also may be structured to block desired goals, a perverse reality. Understand how to use incentives to achieve the greater good.
5. *Spend money to save money.* That is, be willing to take risks and search for additional capital, operational resources, or both to invest in technology, better procedures, outside

assistance (consultants), expanded operations, or whatever. If the return on investment is faster than alternative uses of capital, the increased expenditures will pay off. Money almost always will be forthcoming for launching new promising ventures, increasing quality, reducing cost, and producing more profit. Managers are encouraged and rewarded (incentivized) to risk capital this way.

6. *Identify relevant activities, count them, and then analyze them.* What you don't count, you can't manage. Managers should develop "metrics" that help measure principal activities so they can be analyzed and improved. Years of experience doing something certainly matter. But procedures that have been honed from science-based analysis of data rigorously collected and analyzed likely will produce better results – a more efficient, goal-oriented workplace. A related point is the following: constantly assess how goals are being reached and change course if the path being taken is not productive.
7. *Design jobs to link authority with responsibility.* Managers may seek authority (the ability to be boss) while concurrently shirking responsibility for the end results, thereby diverting blame to others for any failure. Therefore, senior managers must design jobs to link authority with responsibility. After that the performance of managerial subordinates needs to be independently reviewed. Performance reviews and independent verification of results are not options. People often lie. Therefore, constant verification must be built into human systems. This is also to make sure that mutually agreed-to goals are being pursued thoroughly and honestly. Success follows after hiring the best people available, setting reasonable objectives, providing needed staff and resources, and providing appropriate incentives for success down the chain of command for achieving the desired results.
8. *Prevention pays.* Prevention always trumps brilliant response. That is, avoiding problems that are reasonably foreseeable distinguishes the clever manager from the subperformer. The manager who has responded splendidly to an emergency garners attention and often admiration in the short term. But if that emergency could have been prevented or mitigated by reasonable preventative measures, such attention and admiration is hollow. Hindrance to losses or emergencies is a mark of a distinguished and valuable managerial leader.
9. *Change or die!* Enterprises at all times have entropy built within them. The most successful enterprises have sown within them the seeds of their future obsolescence and destruction. Every brilliant plan eventually becomes obsolete. This malaise as it develops is hard to spot and diagnose. The leader must have the vision to see when the time has arrived for substantial and fundamental – even radical or revolutionary – reorganization. Then she or he must possess the courage to execute these changes in the opposition provided by the entrenched defenders of the *status quo*.

Finally, I offer students a personal observation for their consideration:

10. *Relationships and integrity are everything.* Success depends on working well with others. Therefore, build positive rapport with coworkers at all levels. Be courteous and respectful with everybody always. Support your supervisor above all else, but don't slight your coworkers. Take criticism positively as a cue to improve performance. As a supervisor yourself, emphasize the positive by extending your hand to a subordinate when appropriate and praising him or her publicly: "I appreciate you for what you just did." Unimpeachable personal integrity must guide and sustain the manager every day in all her or his endeavors.

Chief Financial Officers (CFOs). These points are profound as they are part of the mind-set of the vast majority of decision makers. Security practitioners will communicate value to the organization within these points.

The for-profit corporation has a formal organizational chart. [Figure 1.7](#) displays a chart with familiar categories of senior management titles. An understanding of the dynamics of a corporation begins at the top with a consideration of the board of directors.

Boards meet with the frequency set in the bylaws of the corporation. In addition to full board meetings, members often serve on committees, which conduct deliberations on specific issues and make recommendations to the whole board. Typically, the board committees include executive (daily operations), public affairs, executive compensation, and audit committees. In large, publicly held corporations, executive compensation and audit committees usually are composed exclusively of outside directors. This particular composition of the board committees enables fiscal or ethical irregularities at the senior level to reach independent fact-finders for evaluations.

The audit committee receives prepared financial reports from the independent auditor, an external firm of accountants that audits financial records of the institution and reports on their soundness to the board. While serving the interests of the shareholders and corporate operations, the audit report also meets reporting requirements of the Securities and Exchange Commission. From the security standpoint, should dishonesty or ethical deviance be occurring by a senior staff officer or officers, a whistle-blower – defined as an employee who reports illegal activities of his or her employer or fellow employees to outside authorities – can contact the independent auditors, who would have a legal duty to evaluate the charge. Often, whistle-blowers have already condemned the illegal activities inside their organization, but to no avail. Thus, they turn to outside authorities as a last resort. In other cases, the whistle-blower may be motivated to reveal information for personal or financial reasons.

The highest-ranking executive concerned with security may interact with the board and senior corporate officers in several ways, one of which is shown in [Figure 1.8](#). In some organizations, security directors present periodic reports to the board on significant protection issues and their implications for the organization. Additionally, the security director is likely to supervise executive protection measures, if relevant, and efforts to safeguard proprietary information at the board level, as well as elsewhere in the organization. Finally, security may be involved in specific investigations at the request of the board or in cooperation with the auditors or other senior corporate officials.

The organizational chart of a large for-profit corporation reflects the relationship among the corporate staff at headquarters. It may be described as hierarchical and somewhat like a pyramid, as suggested by Fayol's earlier observations. The trend in recent decades has been to shrink the headcount at headquarters. The senior executive cadre in such organizations sets policy and objectives and often provides internal consulting. Daily operations management is less frequently found at headquarters. Large and diversified corporations may replicate the headquarters hierarchy with various operating units possessing a similar pyramidal management structure to the parent corporation. An example of such a hierarchy is shown in [Figure 1.9](#).

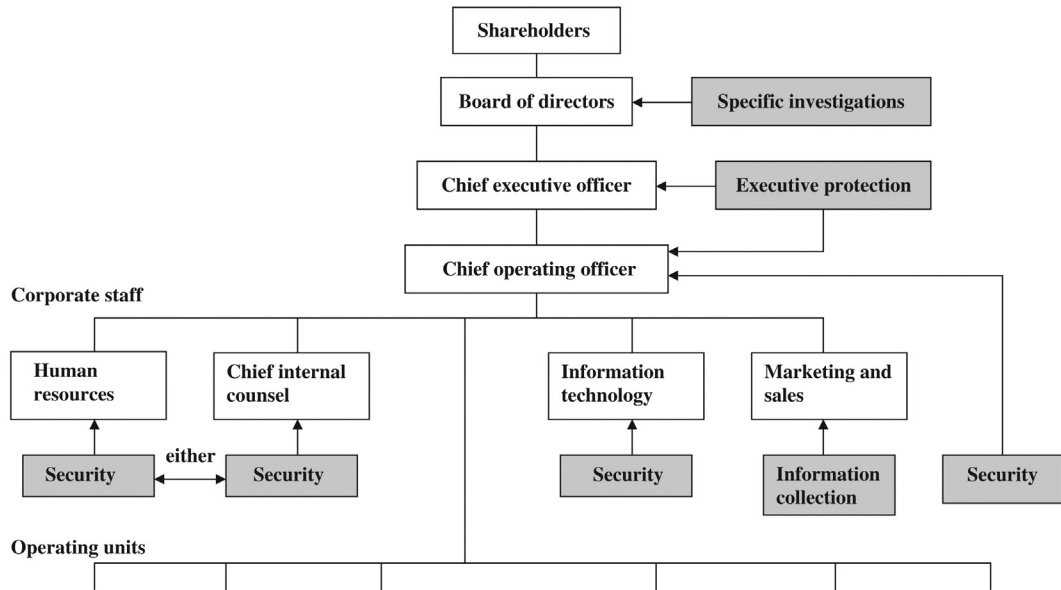


FIGURE 1.8 Possible reporting structures for a security director in a large for-profit corporation. Organizations may have separate security departments with different skills, resources, and purposes. This scheme shows how security units at a staff level in a complex, for-profit corporation could report at different senior management levels. Operating units also could have their own security staffing and function.

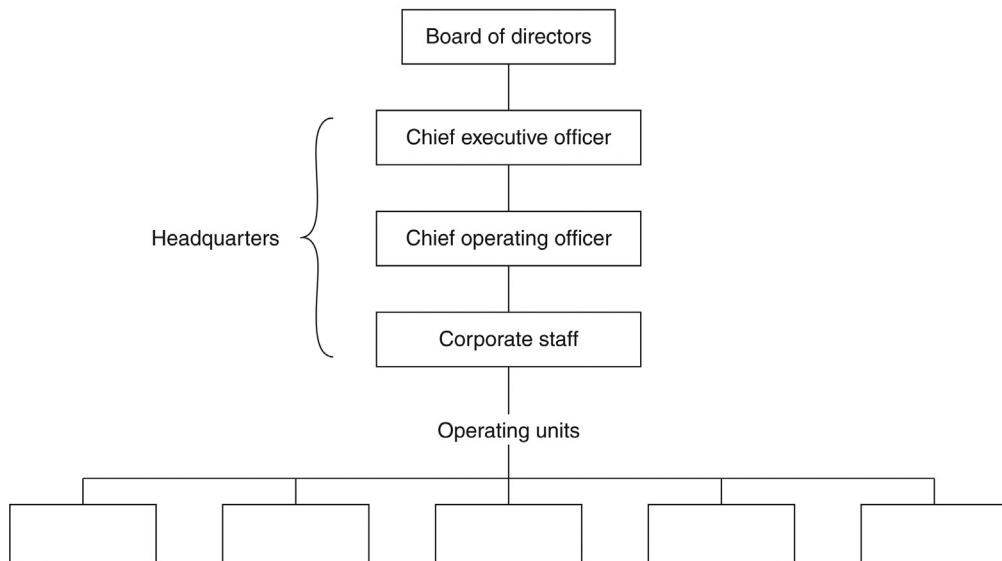


FIGURE 1.9 How corporate staff relates to operating units. The corporate staff is small in many large contemporary operations. A corporate security director may or may not exist at the corporate level. Operating units may be divided into subordinate divisions or subsidiaries based on the nature of their work or geography. These divisions or operating units will have their own staffing requirements met, possibly with separate security developments for each one. (Source: Moore, T., 1987. *Managing: goodbye, corporate staff*. *Fortune*, December 21, p. 65.)

These subordinate corporations or companies are called operating units. The operating units function independently of headquarters to achieve their goals, although headquarters may retain a planning, monitoring, and consulting role. Thus, a diversified corporation may have a board, a CEO, a COO, and other senior staff officers at headquarters, but also numerous operating companies within the structure, all of which may replicate the hierarchical structure at the staff level. This structure of a small headquarters senior staff followed by member operating units with varying degrees of independence from staff operations constitutes the usual situation currently encountered in large for-profit entities.

Not-for-Profit Corporations

For-profit corporations generally are what the public thinks of when reflecting on the nature of corporate structure. Many organizations do not have as their goal the necessity of returning dividends and increased value to their shareholders. These are NFP organizations. They include educational, healthcare, and research institutions, as well as charities and professional associations. NFPs possess much of the same hierarchical and reporting structure as for-profit organizations. However, titles may differ; instead of a president or CEO, the leader might be called a director or administrator. The board of directors may be equivalent to a board of trustees, governors, or supervisors. No shareholders exist because the board represents the public at large, which the nonprofit corporation is chartered to serve through its endeavors.

Many NFP groups are large, diversified, and well known to the public, and operate with the same reporting structures and operating practices as for-profit businesses. While profit is not the motive for NFPs, the accumulation of losses is not an objective either. In reality, NFPs face most of the same kinds of management issues common to for-profit organizations. Therefore, a director of security possesses analogous responsibilities and creates similar types of programs in NFPs as in for-profit entities.

Government Security Operations

Government has an obligation to the public to operate effectively. This includes reducing losses, waste, error, and risks to the lowest practicable level. Above all else, government has a duty to protect the public. Depending on the size and complexity of such units, government may achieve its goals with a variety of resources. These may include law enforcement personnel delegated to internal protective functions or independent police or security units. Large police organizations and small ones may also turn to the private sector to contract out for security services to supplement their own activities that do not require a sworn law enforcement officer. Further, many large government units possess inspectors general to investigate internal allegations of improper behavior.

Layers of Management

The management structure of large organizations appears on paper like a pyramid. This reflects the hierarchical structure of the organization. For operations to operate efficiently, management often is divided into several categories: senior management (includes the staff officers most concerned with strategy, planning, and consolidation of results from subordinate units), middle management (includes numerous support roles with more restricted planning and strategizing, while operational tasks are greater), and first-line management (includes those most concerned with the daily work product of the organization and who have diminished planning activities).

Security in the Organizational Hierarchy

In a large, diversified organization, the highest officer concerned with protection of assets from loss may have the title “vice president” or a variant. He or she is usually categorized as working within middle management while closely connected to higher, lower, and parallel management. This security manager reports directly to a senior officer, who may differ by title according to the type of industry involved. For example, in research-oriented businesses, the security chief generally reports to the chief internal counsel; in manufacturing firms, reporting tends to be with the function concerned with operations or production; in service businesses, reporting generally occurs to the director of human resources. These reporting relationships are not fixed, and other reporting structures are common.

While the top corporate security director usually is classified in middle management, this categorization should not be regarded as inconsequential or unimportant. Security directors frequently provide reports to the board of directors and may routinely interact with all senior officers of the corporation in providing pertinent services. However, in many organizations, particularly those with numerous divisions, global reach, and large scale, a chief security officer (CSO) may be at the C-level; he or she may report directly to the CEO, COO, or other senior administrator or officer in such circumstances.

Structure of a Complex Security Department

Security or loss prevention departments can possess considerable variation. Further, the structure of such departments is likely to change over time. For example, if security officer services are contracted out, supervision of the contract is still required, although the total number of proprietary employees required will be reduced considerably by the out-contracting process. A typical security department is apt to oversee propriety personnel, contract staff, and internal consulting services, as shown in [Figure 1.10](#).

A security department may incorporate considerable breadth and diversification in its resources and duties. It reflects the guarding, alarm monitoring, and asset moving and

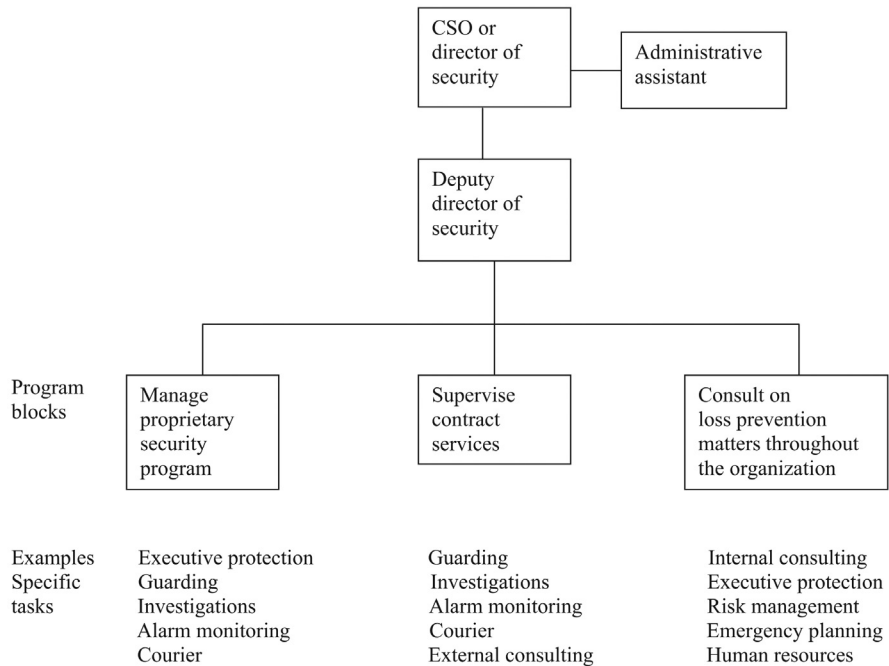


FIGURE 1.10 Work relationships of a security program. Considerable variation exists in the way security units are organized. In this example, two managers aided by an administrative assistant are responsible for proprietary (in-house) staff and supervising contract security services. They also act as internal consultants for other management issues where their skills could be valuable.

protection found in most organizations, as shown in [Table 1.1](#). Additionally, it reflects the internal consulting, risk management, data protection, investigation, and human resources tasks often performed or involving participation by security departments. Security operations also audit programs to determine how loss prevention efforts can be improved.

Related to this function is risk management, which is concerned primarily with property, casualty, and liability insurance of an organization. In this case, as risks are reduced, the organization may benefit from lower insurance premiums, the capacity to increase self-insurance, and benefits in coverage achieved through improved security operations. The CSO may have an ongoing role in interfacing with the risk manager and occasionally in working directly with insurance brokers serving the organization in loss reduction context.

Ethics and Security Operations

Ethics relates to moral actions, conduct, motive, and character. It is professionally the right or befitting action within its context. While a criminal act generally is also a breach of moral conduct, ethics includes numerous behaviors that fall short of breaching criminal or civil laws. The widely heard cliché is that “ethics start at the top” in any organization. As

Table 1.1 Types of Services Potentially Offered by Large, Complex Security Programs

Services	Frequency
Alarm monitoring	High
Computer security	High
Competitive intelligence	Low
Emergency planning	Moderate/high
Ethics	Moderate
Executive protection	Moderate
Facilities management	Moderate
Guarding-propriety or contract	High
High security courier	Low/moderate
Information technology	High
Internal consulting	High
Investigations	High
Loss prevention consulting	Moderate
Polygraph	Low
Regulatory compliance	Low/moderate
Preemployment screening	High
Risk management	Low/moderate
Safety audits	Low/moderate
Security training awareness	High

Ira Somerson, an industry consultant, noted: “When busy CEOs take time to discuss ethical issues in their work, the message soon filters down.”¹²

Seminal research on workplace deviancy was conducted by academics John P. Clark and Richard C. Hollinger.¹³ Over 9500 employees at all levels were queried in three geographical areas, representing numerous types of public and private workplaces. Results from the Clark–Hollinger study show that the level of self-reporting workplace deviance differs widely and generally is not related to income. Surely not all protection employees are above reproach ethically or criminally. Indeed, a rare few seek employment in the field because it affords them the opportunity to exploit opportunity. Yet security personnel were assessed in all three employment segments in this study and ranked among the highest in ethical standards. This finding may be due to the fact that security personnel tend to be selected for having higher personal ethical standards. Another explanation could be that security practitioners have less opportunity for workplace deviance due to the nature of the job design.

In many organizations, operational security personnel are regarded as ethical arbiters. That is, they are expected to be the individuals who understand the culture and regulations fully, are presumed to do the right things themselves, and can be turned to for guidance on general ethical matters. Moreover, security managers – usually in coordination with human resources, the chief internal counsel, and others – are likely to be involved in setting, promoting, and managing ethical programs. They may:

- Draft a corporate ethics policy and disseminate it broadly.
- Emphasize the importance of ethical standards at new employee orientations.

- Provide new employees with a workplace ethics statement they may sign.
- Establish mechanisms whereby someone with an ethical concern may be heard confidentially and nonjudgmentally.
- Investigate promptly and thoroughly all allegations of unethical behavior and refer the results of such efforts to appropriate authorities.

The motivation for the growing emphasis on ethics has many bases. Some executives claim that ethical behavior is morally proper and that is why they believe in it. Others would agree and discreetly add that voluntary ethical standards decrease public censure and chances of unwelcome litigation and legislation. But more than this is at stake. Perhaps the biggest factor behind the wave of ethical enlightenment is that such behavior is simply a good practice. Put differently, if only one part of an organization is perceived as being unethical, the entire organization can be and will be tainted and potentially devastated in the process. See [Box 1.5](#).

ASIS promulgates a Code of Ethics (see Appendix B). Violators who come to the attention of the ASIS Ethical Standards Committee are given the opportunity to explain their perceived misconduct. Expulsion from ASIS is one of the consequences for those persons who deviate from the code and whose cases are considered by the Ethical Standards

BOX 1.5 PENN STATE AND ITS ETHICAL FALLOUT

Police arrived at the home of Jerry Sandusky, former Penn State assistant football coach, in November 2011, and arrested him on multiple counts of child sexual abuse. Four days later either Penn State's board of trustees dismissed its president, Graham Spanier, or he resigned first. Spanier was beginning his 17th year as president and had "led the university as it grew from a remote outpost of American higher education into a top-tier public university." He was charged with eight criminal counts, including child endangerment, perjury, and conspiring to cover up Sandusky's crimes. As of this writing, he has not been tried.

Spanier wasn't the only one charged. Two other former high-ranking Penn State administrators are also awaiting trial. The revered football coach of 46 seasons, Joe Paterno, was fired. Several other Penn State employees, including the head of campus police and security, left the university. Huge repercussions followed, including a university fine of \$60 million paid to the N.C.A.A. and \$60 million in compensation to Sandusky's victims. The board commissioned a report for a group led by former FBI director Louis J. Freeh, now a consultant. The harsh report charged that a "culture of reverence" for football permitted overlooking the behavior of a single former member of the football coaching staff.

The perception of brushing sexual assault under the rug led to an extensive attack on the university. A single lower-level coach, retired when he committed some of these acts on university property, put the reputation of thousands on the line.

Sources: Sokolove, M., 2014. The shadow of the valley. *New York Times Magazine*, July 20, p. 24; Wilson, R., 2012. As students return, Penn State begins the year under a cloud. *Chronicle of Higher Education*, September 7, p. A8.

Committee and found in violation of established practices. The Ethical Standards Committee does not issue annual reports; therefore, its activities and significances are a conjecture.

Other professional and trade organizations concerned with loss prevention also possess codes of ethics and good conduct. Some of these are the Academy of Security Educators and Trainers, the Business Espionage Controls and Countermeasures Association, the International Association for Healthcare Security and Safety, the National Burglar and Fire Alarm Association, and the National Council of Investigation and Security Services. An MBA Oath began at Harvard Business School in 2009 to foster responsible value creation (Appendix C). Business students at over 250 schools around the world have signed it. It is included because the issues cited have relevance for managers concerned with risk reduction. This list of organizations with ethic is not meant to be comprehensive. The point is that security practitioners generally take ethics as a serious, profound reflection of their responsibilities to their colleagues, employees, and clients – and to society as a whole. Such ethical structures usually permit censure, suspension, and expulsion as possible sanctions for errant members. Normally, the person accused of unethical behavior has an opportunity to respond to the charges at a specially convened board to hear charges and responses. The appointed group then collects and assesses the facts in the situation, arrives at a conclusion, and may report its findings to the full group for a final consideration.

Summary

Organizational concerns of corporations became the object of research only in the mid-twentieth century. Security operation as a discipline arrived later and continues to evolve. Successful security operations are critical to the growth and stability of organizations of any size and complexity. While usually a part of middle management, security operations are concerned with performance throughout the entire organization. In some large, complex, globally oriented organizations, the CSO is considered a senior officer and reports appropriately in the organization. The functions of the executive charged with security operations are diverse and subject to change according to the primary operation of the organization. The ethical nature of the chief executive often influences the behavior of subordinate employees and others concerned with the operation. Security practitioners generally are viewed as exponents of an organization's ethical policy and program and frequently are involved in establishing and managing the policy.

Discussion and Review

1. What is the essence of “the art” of contemporary security practice?
2. When did the era of modern management emerge? When did protection management appear as a distinct managerial function?
3. Briefly describe the purpose of an executive within contemporary organizations in contrast to that of managers.

4. The managerial process involves a sequence of interrelated activities. What are they and why does each have significance?
5. What are the similarities on Henri Fayol's categorizations of the workplace and a typical operation today? How are Fayol's descriptives similar to contemporary organizational structure and activity? What differences exist between his observations and the present place of work?
6. What were the contributions of scientific management to the contemporary workplace? In particular, how is the security function significant?
7. How does "outsourcing" affect current security practices?
8. Describe the connections between situational crime prevention and research applications for loss problems or concerns.
9. Explain how the structure of the organization permits recourse to investigate and respond to allegations of improper behavior, even at the highest level.
10. Describe the role of security managers in establishing policies and maintaining standards in ethical issues within the workplace.

Endnotes

- ¹ Drucker, P.F., 1985. *The Effective Executive*. HarperBusiness, New York, NY, p. 8. Also: Stone, N. (Ed.), 1998. *Peter Drucker on the Profession of Management*. Harvard Business School, Cambridge, MA.
- ² Fayol, H., 1984. *General and Industrial Management*. Institute of Electrical and Electronics Engineers, New York, NY, p. 11 (revised by Erwin Gray).
- ³ Weber, M., 1947. *The Theory of Social and Economic Organization* (A.M. Anderson, T. Parsons, Trans., Parsons, T., Ed.). Free Press, New York, NY.
- ⁴ Barnard, C.I., 1938. *The Functions of the Executive*. Harvard University Press, Cambridge, MA. Also: Hill, L.A., 1992. *Becoming a Manager*. Harvard Business School Press, Boston, MA.
- ⁵ Taylor, F.W., 1911. *Principles of Scientific Management*. Harper & Brothers, New York, NY.
- ⁶ Gilbreth, F.B., 1972. *Motion Study*. Hive Publishing Company, Easton, PA.
- ⁷ Tomain, J.P., 1987. *Nuclear Power Transformation*. Indiana University Press, Bloomington, Indianapolis, IN, p. 36.
- ⁸ Likert, R., 1961. *New Patterns of Management*. McGraw-Hill, New York, NY.
- ⁹ McCrie, R.D., 2012. Progress and problems of security in Millennium Society: an essay for the 25th volume of *Security Journal*. *Secur. J.* 25 (1), 1.
- ¹⁰ Barefoot, J.K., 1995. *Undercover Investigations*, third ed. Butterworth-Heinemann, Boston, MA.
- ¹¹ National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*, 2004. W.W. Norton & Company, New York, NY, p. 317. A section states: "The 'first' first responders on 9/11, as in most catastrophes, were private-sector civilians. Because 85 percent of our nation's critical infrastructure is controlled not by government but by the private sector, private sector civilians are likely to be the first responders in any future catastrophes."
- ¹² Cunningham, W.C., Strauchs, J.J., Van Meter, C.W., 1990. *Private Security Trends 1970 to 2000: The Hallcrest Report II*. Butterworth-Heinemann, Boston, MA, p. 49.
- ¹³ Clark, J.P., Hollinger, R.C., 1983. *Theft by Employees*. Lexington Books, Lexington, MA.

Additional References

- Brown, P.B., 2006. Don't plan too much. Decide. *New York Times*, January 28, p. C5.
- Criscuoli, Jr., E.J., 1988. The time has come to acknowledge security as profession. *Ann. AAPSS* 498, 99.
- Davidson, C.H., 1989. Toward a new discipline of security management: the need for security management to stand alone as a management science. *Secur. J.* 1 (1), 3–13.
- Davidson, M.A., 2004. *The Gold Standard: ASIS Celebrates 50 Years of Advancing Security*. ASIS International, Alexandria, VA.
- Gladwell, M., 2011. *Outliers: The Story of Success*. Little, Brown and Company, New York, NY.
- Harowitz, S.L., 2005. The very model of a modern CSO. *Secur. Manage.* 49 (4), 42–51.
- Hudson, M., 2014. Espousing equality, but embracing a hierarchy. *New York Times*, June 23, p. BU3.
- Lepore, J., 2009. Not so fast: scientific management started as a way to work. How did it become a way of life? *The New Yorker*, October 12, p. 84.
- McCrie, R.D. (Ed.), 2002. *Readings in Security Management: Principles and Practices*. ASIS International, Alexandria, VA.
- Shearing, C.D., Stenning, P.C., 1983. Private security: implications for social control. *Soc. Probl.* 30 (5), 503–504.
- Yothment, J., 2014. Uncovering smart solutions. *Secur. Manage.* 58 (7), 58–62.
- Zalud, B., 2013. Security officer success: define expectations up front. *Security*, February, p. 14.

Further Reading

- KPMG Forensic: Integrity Survey 2013, <<http://www.kpmg.com/us/en/services/advisory/>>.
- National Business Ethics Survey 2013, <<http://www.ethics.org/nbes/download-reports/>>.
- Standards for Internal Control in the Federal Government, September 2014. Comptroller General of the United States, Washington, DC, GAO-14-704G.

Core Competencies to Create Effective Protection Programs

Private security is more than twice the size of federal, state, and local law enforcement combined.

—The Hallcrest Report II

Security activities for an organization are often centered within a department dedicated to delivering value to the organization through services. As the previous chapter indicated, much flux occurs in the nature of organizations themselves and within various departments providing such services. Still, some generalizations can be made that will be appropriate for various types of managerial situations. This chapter examines the means whereby organizations with dedicated security departments are organized to serve the entire operation. It further looks at the relationship between organizations that contract out for routine security services. We begin by examining core competencies of security operations.

Core Competencies of Security Operations

Core competencies refer to the fundamental abilities a protective program needs in order for it to deliver services effectively. These needs will vary according to the type of organization, its size and geography, recent history, criticality of resources, vulnerability to losses, and other factors. No single executive is expected to be competent in all demands required of the position, but the subsequent subsections serve as a means of generating thought as to what a protective operation's value to the organization is or could be. This list is dynamic and reflects the changing nature of the requirements of security programs and of the expectations of people heading them.

Initiating and Managing Security Programs

As discussed in the previous chapter, problems and opportunities require appropriate response.

The circumstance might be minor, requiring brief intervention. Or it could be a situation requiring the creation of new managerial protocols. That is, a program needs to be developed. The identification of these situations, their analysis after fact-finding, the organizing of an appropriate program, the appointing of a deputy to operate the new program, and its supervision and constant improvement are reasonable expectations. Three skills

reflect the core competencies executive management expects from the senior security personnel:

1. *Initiating new programs.* Organizations are never static. New issues require fresh responses. Assume that in 5 or 7 years the organization will be considerably different than it is today. Security management programs change in parallel with other activities in the workplace.
2. *Operating existing programs.* The ability to initiate a successful program is a strategic skill, whereas the operation of existing programs is less challenging. Nonetheless, this is the basis of most daily work and includes opportunities for creativity and constant program improvement, much as what occurs in the initiating of such activities. Another core skill is the ability to collect information that is critical to the operation and assess the success of ongoing programs (see [Box 2.1](#)). The manager or director for such operations normally manages the budget for these activities (see Chapter 8).
3. *Handling personnel administration.* The recruiting, screening, hiring, training, supervising, promoting, disciplining, terminating, and conducting of other personnel-related activities are expectations of high-performance security operations (see Chapters 3–7).

BOX 2.1 COLLECTING AND MEASURING WHAT'S IMPORTANT

Once goals are set, data are needed to evaluate how successfully aims are being reached. Relevant data collection can also point to other issues that require more attention than what was initially apparent. Managers believe that data – the metrics – are indispensable in creating a sensible program. Much of the burden of collecting systems inputs can be collected through automated systems. The data can then be analyzed, sometimes with the use of computer programs that can produce extensive reports, nuanced to the issues that are important. Analysis is improved. This is partially why security operations have provided greater measurable value over the years. Criminal incidents must be collected for legal and risk management purposes and also so that they can be measured for any relevant trend. Services performed by security personnel may be collected and measured for the same reasons. The following reflects the information a security department might collect to assess programmatic developments.

Number of criminal incidents, including:

- Robbery
- Aggravated assault
- Other assault
- Burglary
- Larceny (theft): employee
- Larceny: nonemployee
- Motor vehicle theft

- Forgery and counterfeiting
- Fraud and embezzlement within the facilities
- Vandalism on or near property
- Trespassing
- Other

Network interfaces (computer crime), including:

- Virus and worm incidents
- Computer system crashes (utilities problems)
- Flooding or denial-of-service (DoS) attacks
- Spoofing (appropriation of an authentic identity by nonauthentic users with the attempt to cause fraud or attack critical infrastructure)
- Intellectual property infringement
- Other

Number of noncriminal emergencies, including:

- Accidents (within the facility)
- Accidents (automotive)
- Accidents (in the proximate area)
- Dangerous behavior
- Fires and smoke conditions
- False alarms
- Losses of utilities
- Malfunctions of critical equipment
- Slips and falls
- Water and flood damage
- Wind damage
- Other

Number of service activities, including:

- Complaints and miscellaneous
- Compliance – regulatory
- Employee records checks
- Escort services
- Executive protection detail
- Information provided
- Investigations (internal)
- Investigations (personnel-related)
- Investigation (external)
- Key runs
- Lock or key service
- Lost and found
- Visit by inspectors or regulators

Initiating new programs, operating existing ones, and dealing with personnel issues are expectations of all managers, not just those concerned with asset protection. However, some tasks are specific to loss prevention staff:

- *Contract services management.* Since a large portion of security services nationwide is provided by contract personnel, operations must be able to select, motivate, supervise, and discipline contract vendors and their personnel so that goals are met (Chapter 9).
- *Private investigations.* Investigations within the workplace may be managed internally or contracted to outside investigators or consultants. But the security manager in charge is likely to monitor the assignment to assure that objectives are pursued diligently.
- *Assess security technology.* Security practitioners are not expected to be engineers. However, they are required to be familiar with current technologies to serve the protective objectives of the organization. They should further be able to procure such technology and services under favorable terms for management (see Chapter 10).
- *Other expectations.* As indicated above, security programs have considerable variations in their operational goals. Therefore, some organizations will have such core competency objectives as executive protection, international affairs, risk management, competitive intelligence, data security, emergency planning and response, and other topics.

Some general personal characteristics are also critical for all high-performance executives in protection positions:

- *Communications.* Security leaders and their programs obtain and retain support by successfully serving various “customer bases” (senior management, various operating departments, employees, visitors). Those responsible for security programs constantly must enunciate what security does and why it is relevant, without being repetitious and boring.
- *Leadership.* Security programs often require various groups to take – or not take – actions against their will. Personal leadership by persons responsible for the program helps retain the credibility and support such programs require (see Chapter 11).

A Brief History of a Growing Field

Security has always been essential for the protection of people and property. Indeed, security is required for the establishment and growth of nations, communities, nonprofit organizations, and commercial enterprises. Broadly considered, external security is provided by military resources, internal security by law enforcement, and private assets are taken care of by proprietary security. Without security, an organization is vulnerable and vulnerability is eventually exploited.

In England during the eighteenth century, independent maritime police and for-hire detectives, the Bow Street Runners, heralded the beginning of a private security industry.¹ The security industry itself emerged as a modern business activity within the United States in the second half of the nineteenth century.² During this period, investigations, guarding, executive protection, consulting services, alarm monitoring and response, and armored courier services all had their origins. By the mid-twentieth century, large corporations had established proprietary security programs that initially were concerned narrowly with loss prevention and order maintenance. Managers for these programs in industrial applications often reported to engineering, maintenance, and general administrative or operational units.

At the end of the 1950s, a resurgent economy and the implications of Cold War protectionism vastly increased the importance of security as an organized business practice. Industry was serving the needs of military preparedness and expanding commercial inventiveness: both required adequate security measures, though of differing sorts. Such diverse interests in proprietary security were met, in 1955, with the founding of the American Society for Industrial Security, now ASIS International.³

Early members of ASIS were employed usually as loss control directors serving for-profit and institutional organizations. Typically, they would be concerned about physical security, emergency response planning and coordination, and internal investigations. Members who worked for industrial corporations that provided products, systems, services, and research for government, especially the military and intelligence community, faced extensive compliance requirements to protect information and production know-how from possible compromise. ASIS members in those early years included many retired military officers. Membership also consisted of retired police officers, special agents of the Federal Bureau of Investigation and other law enforcement organizations, and persons who became responsible for security without having had any previous formal preparation in the military or law enforcement.

Security directors in these organizations sometimes were responsible for identifying and assigning security classification to information and materials requiring protection in the national interest.* With the fall of the Berlin Wall in 1989, the military threat between the superpowers in the East and West diminished rapidly. The need for protection of intellectual property and of physical developments related to military requirements declined, but did not disappear. Meanwhile, other security priorities and duties emerged.

The modern origins of professional security are related to earlier military and industrial needs. Yet protection was needed in other organizations where theft, vandalism, and employee safety were issues. Retailing, distribution, general manufacturing, and many types of service businesses – especially financial institutions – added security services at the place of work. Most security programs in the 1950s and 1960s concentrated on anti-theft and information protection measures. But by the late 1970s, some security programs

* The specialized nature of information identification and assignment of security classifications produced a group of managers who founded the National Classification Management Society in 1964. Classification management may be part of the responsibility of a security operative.

began to absorb other management and administrative duties, including safety. In the 1990s, data security, emergency planning, and organizational ethical concerns became significant management issues. In the twenty-first century, a variety of issues emerged without any reduction in the significance of earlier protective mandates. Antiterrorism, protection of intellectual property, and rapid recovery from untoward incidents (contingency planning) became paramount issues for management attention.

Today, the security industry is not one entity but a series of internal and external commercial activities that sometimes overlap each other but which generally are distinct. These activities include services such as guarding, investigations, alarm monitoring, escorting, and consulting; electronics (including companies that manufacture, distribute, and add value to systems); cybersecurity technology and software; and hardware (encompassing nonelectronic, high-quality products and materials that serve above-standard protective needs).

Additionally, government at all levels – federal, state, and local – has become a major consumer of security services and products. This is true even for government units that provide criminal justice or emergency response services to the public. These services and products vendors are numbered in the tens of thousands and constitute the security industry.

How Contemporary Security Services Have Evolved

Licensed security guard companies and investigators have been on the scene for decades. But by the late 1960s, no independent critical analysis of this growing security industry had taken place. That changed. In 1970, contemporary security practices in the United States were described and evaluated by the scathing and influential *Rand Report*. This document represented the first time the burgeoning security industry received a systematic analysis from a disinterested research group. With a grant from the Law Enforcement Assistance Administration (LEAA), the Rand Corporation began, in 1970, a 16-month investigation of “private police” in the United States. The authors, James S. Kakalik and Sorrel Wildhorn, were lawyers trained as policy analysts and employed by Rand in Santa Monica, California. Their task was to assess private security businesses and personnel with an eye to how private security might be a concern of public policy.

For starters, the *Rand Report* impugned, correctly, the level of employment standards then common for private security personnel. The authors observed:

The typical security guard is an aging white male, poorly educated, usually untrained, and very poorly paid. Depending on where in the country he works, what type of employer he works for (contract guard agency, in-house firm, or government), and similar factors, he averages between 40 and 55 years of age, has had little education beyond the ninth grade, and has had a few years of experience in private security ... He often receives few fringe benefits; at best, fringe benefits may amount to 10 percent of wages. But since the turnover rate is high in contract agencies, many employees never work the 6 months or 1 year required to become eligible for certain of these benefits.⁴

The *Rand Report* continued with its litany of harsh observations of private security practices, largely concentrating on guard and investigative services. Cited were the following: weak preemployment screening, high turnover in the industry, poor hourly compensation, and a lack of meaningful licensing standards. Times have changed. Much evidence indicates that security practices have improved, although the persistence of numerous substandard protection service providers and programs remains a reality. In the decades following publication of the five-volume *Rand Report*, considerable advancement in the industry occurred, though at a measured, slow rate.

The next significant official scrutiny of private security services also emanated from LEAA funding and had been recommended by the *Rand Report*. In 1972, LEAA created the National Advisory Committee on Criminal Justice Standards and Goals. This group undertook a number of detailed, analytical reviews of various issues connected with criminal justice. For each review a varied group of specialists was convened, supported by research and support staffs, and encouraged to look at a problem critically and prospectively. One such group was the Private Security Task Force (PSTF). Following a series of discussions and inquiries stretching over 18 months, the PSTF issued its comprehensive report in 1976.⁵ Drafters and authors of the PSTF were individuals representing law enforcement officials, corporate security directors, and an executive of a major security services company. The report identified almost 80 goals and standards for private security. The list encompassed such areas as licensing, regulations, consumer services, personnel training, crime prevention systems, hourly compensation, and conduct and ethics. The *Report of the Private Security Task Force* was not intended as an impetus to achieve federal legislation to regulate aspects of the security industry; rather, its intention was to identify significant issues that would stimulate local and state laws and codes to be passed or strengthened. Also, it would serve as an industry guide to improvement in procedures. An outline of these standards and goals is included (Appendix C) because, despite the passage of these codes, so many of these modest proposals have yet to be enacted by states or the federal government.

These two documents – *Rand Report* and the *Report of the Private Security Task Force* – served to inform legislators, regulators, general management, the security industry, the media, and the public at large about issues relating to private security. In some ways, changes have occurred in almost all aspects of security services delivery; in other aspects, change has been barely discernable. Yet the industry and the performance of security services – both proprietary and contract – have experienced steady growth from a period beginning at least since the end of World War II to the present. Why? Several reasons exist for the growth of private security. Senior executives do not accept their subordinates' recommendations for increased security expenditures – or any other kinds of financial allocation – without rational justification. Such asset allocations are generally predicated on defined needs that the organization has identified and that, therefore, make the existence of security expenditures an informed imperative, rather than a capricious decision.

What Drives Security Operations?

Security operations normally do not exist within an organization for a single reason. Typically, numerous factors interweave to justify commitments to fund protective operations. These will vary in significance according to a wide variety of factors relating to the degree of risk appetite, demand for internal services, and the value of assets to be protected in the workplace. The leading elements that underpin the reason for being of contemporary security programs and that drive their growth and vitality today are as follows:

- *Cost savings.* An operating security program may reduce losses to an organization that will in turn offset the apparent cost of the security services. For example, employees may be unwilling to work certain shifts because they feel unsafe at or near the workplace. Their replacement could be costly. The presence of access control and a security patrol could make the perilous shift a possibility.
- *Risk mitigation.* Security is a fundamental necessity for corporate endurance and success. Lack of adequate protection could lead to devastating results. Security programs identify weaknesses and seek to reduce risk (see [Box 2.2](#)).[†]

BOX 2.2 A CASE OF INADEQUATE SECURITY: THE DEMISE OF PAN AM WORLD AIRWAYS

The advertisements proclaimed: “Pan Am Makes the Going Great!” And it did. Pan Am World Airways was the first transatlantic carrier to provide regularly scheduled flights. For most of the twentieth century, Pan Am possessed its own distinctive cachet. Pilots, flight attendants, ground crew, and passengers were attracted to the carrier for its élan and quality services, and the airline prospered. In fact, one of the major midtown skyscrapers constructed in Manhattan in 1960s was named for the airline (now the MetLife building) as its headquarters.

In the late 1960s, airlines became aware of their vulnerabilities to breaches of security. Numerous planes were skyjacked, and preboard screening became a requirement instituted by the FAA. The impetus for international air carriers to improve security had become a priority. Almost all international air carriers saw the loss of some business as a result of travelers’ fears of potential skyjacking, rare as it might be.

Most airlines developed passenger and luggage preboarding programs to provide for their own needs. The attractiveness to contract out proprietary services to other airlines became a consideration. One of these that acted on the opportunity was Pan Am, which created, in 1986, a wholly owned subsidiary, Alert Management Systems, Inc., to provide services to Pan Am and other airlines. The new security service was financed, in part, by a surcharge of \$5 per ticket on each transatlantic flight.

Pan Am’s Alert Management Systems was positioned as a high-visibility service provider and revenue generator for the parent company. Yet the security “was more for show than genuine security,” according to Steven Emerson and Brian Duffy, authors of *The Fall of Pan Am 103*. When Alert Management Systems began operations at New York’s John F. Kennedy Airport, for

[†] The goal of security management programs generally is not to reduce risks as low as possible. That would be excessively burdensome and costly. Rather, it is to reduce risks to an acceptable or practicable level.

example, Alert personnel paraded dogs throughout Pan Am's check-in counters for the media's cameras. However, according to Alert's first president, Fred Ford, they were not dogs trained to sniff for bombs; they were merely "well-behaved German shepherds."

Pan Am retained the services of a security consultancy, Ktalav Promotion and Investment Ltd. (KPI), to critique its performance and to review operations at Frankfurt and 24 other airports. Isaac Yeffet, a former security chief for El Al Airlines, then with KPI, wrote to the airline that: "Pan Am is highly vulnerable to most forms of terrorist attack," despite the existence of their own Alert Management, and that "a bomb would have a good chance of getting through security" at the Frankfurt Airport. Yeffet concluded: "It appears, therefore, that Pan Am is almost totally vulnerable to a mid-air explosion through explosive charges concealed in the cargo." But Yeffet's report and Ford's request for more resources for Alert Management were ignored by Pan Am's senior management. The price of inadequate security would be high. On December 21, 1989, Pan Am flight 103, a Boeing 747 jet, was blown apart over Lockerbie, Scotland, killing all 259 people aboard and an additional 11 on the ground.

Pan Am's decline as a viable business did not begin with Lockerbie, but instead started in 1973 when the Arab oil embargo pushed up fuel prices at the same time as a sharp recession began. From then to the 1980s, Pan Am lost over \$2 billion and only survived by selling its Pacific routes to United Airlines in 1986. But Lockerbie substantially sealed the fate of Pan Am. By 1994, the airline was bankrupt. A jury held that Pan Am and its Alert Management Systems, because of the numerous security deficiencies, were guilty of "willful misconduct" in permitting a security breach that allowed a bomb to be placed aboard the craft.

Sources: Emerson, S., Duffy, B., 1990. *The Fall of Pan Am 103*. G.P. Putnam's Sons, New York; Stuart, R., 1986. Pan Am ads touting security plan stir a debate. *New York Times*, June 10; Greenwald, J., 1991. Fallen emperors of the air. *Time*, January 7, p. 71; Sullivan, R., 1994. Court upholds Pan Am 103 awards. *New York Times*, February 1, p. D2.

- *Income generation.* A security program is often thought by managers not involved with protection to be a "cost" to the operation, not a source of "profit." This is an unacceptable characterization for security endeavors. However, in some circumstances, security departments perform services that can generate fresh income for the organization that would otherwise be unavailable. For example, some workplaces share their own security services with other businesses or institutions and charge for them accordingly. Hence, they can become a true profit center for the parent organization (see [Box 2.3](#)).
- *Crime.* Violent and property crime that could occur within or near a facility or property can be deterred by the presence of security personnel, the installation and functioning of an alarm and closed circuit/Internet Protocol television (CC/IPTV) system, and good security design. This is supported by research from situational crime prevention studies, which confirms that pertinent measures may reduce losses from crime and other risks.
- *Fear.* The presence of trained security personnel and state-of-the-art systems makes employees, vendors, and visitors feel safer at the workplace. For example, the availability of a parking lot security patrol may reduce users' trepidation while it

BOX 2.3 MAKING SECURITY A PROFIT CENTER

Profit centers are workplace activities that bring income to the enterprise from activities that are not traditionally part of the department's mission.

Profit centers may provide security services to noncompetitive organizations for fees. Such activities include guarding, investigations, alarm monitoring, computer backup services, parking lot management, and consulting. Such activities can be profitable for the organization providing them. The customer or client derives benefits from resources with demonstrable performance characteristics and ongoing management attention. Not all security operations can or should possess profit centers of this sort, but for some opportunities exist and may be pursued to strengthen the security program and the parent organization simultaneously.

lowers actual risk. In this sense, security provides a desirable service to those who use the parking lot.

- *Litigation.* The failure to have an adequate security program may leave the owner and operator of a facility vulnerable to a successful tort action for negligent security in the event that a crime or related loss occurs. The burden for the defendant is greater if the facility has a weaker protective program than do comparable operations within the region. The existence of a security program by itself, however, does not protect the facility from successful litigation in the event an actionable offense for negligence takes place.
- *Insurance against liabilities or negligence.* Organizations often are required to provide security services and systems for themselves because their property and casualty liability insurance coverage – or other specific insurance policies – mandate certain minimum protective measures.
- *Legal mandates.* In some cases, specific litigation directly requires the presence of security operations. For example, financial institutions face general obligations to maintain a security program subsequent to the Bank Security Act of 1968 and as subsequently modified.
- *Bureaucratic requirements.* Numerous governmental agencies create regulations that mandate the existence of security programs. Usually, these are the outgrowth of federal laws that contain broad language and leave the specifics to be developed by a designated federal agency. For example, the Federal Aviation Administration (FAA) requires airport managers and airlines to institute a variety of protective measures, including preboard screening of airline passengers and personnel and vetting of checked luggage. These regulations were developed to protect the air-traveling public.
- *Accreditation requirements.* Institutions that meet the general standards of their appropriate accreditation body sometimes also face the specific demands for the provision of general security measures from such an accrediting association. For example, the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) promotes high-quality patient care through a voluntary process of accreditation, encompassing thousands of healthcare organizations. JCAHO has

no specific security standards at present; however, in practice, the desirability of an appropriate security program is expressed through the “Plant, Technology, and Safety Management” section of the JCAHO’s (2000) *Comprehensive Accreditation Manual for Hospitals*, which requires a safe environment for institutions desiring to meet the criteria of JCAHO.

Clearly, the need for security programs and services in commerce and institutions is not derived from a single requirement, but rather from a combination of factors. The individual reasons for having a particular level of security are affected by geography, time, financing, available personnel, legal precedents pending legislation and litigation, and other considerations. Ultimately, security programs exist due to the conviction that any vulnerability eventually will lead to unfavorable consequences. This explains why security services continue to grow.

Laws That Affect Growth of Security Service

In the past two generations federal and state laws have come to impact the characteristics of security operations. For example, the Occupational Safety and Health Act (OSHA) of 1970 (29 USC 651 *et seq.*) was passed to develop and promulgate occupational safety and health standards. It required and established a bureaucracy to develop and issue regulations, conduct investigations and inspections to determine the status of compliance with safety and health standards and regulations, and issue citations and propose penalties for noncompliance with safety and health standards and regulations.[‡] Many security directors also serve as OSHA compliance officers at their workplaces.

Other specific laws calling for increased commercial security measures were passed. Notable among these was the Bank Security Act of 1968.[§] This law was passed because bank crimes had grown steadily during the decade. The increased incidence of bank robberies, burglaries, and extortions prompted Congress to require all federally chartered banking institutions to undertake particular security measures to reduce the risk of successful criminal acts. In retrospect, the measure in itself did not reduce the growing pattern of violent and property crimes against financial institutions covered by the Act: in fact, they kept increasing for years after passage of the law.[¶] This Act was significantly

[‡] An Assistant Secretary for Occupational Safety and Health reports to the Secretary of Labor. OSHA regulations do not pertain to the federal or state governments or to mining. A separate act, the Federal Coal Mine Health and Safety Act of 1969 (30 USC 801 *et seq.*), is concerned with safety and health issues in that industry.

[§] The Bank Protection Act of 1968 (PL 90-389) embraced the jurisdiction of four federal banking supervisory agencies: the Comptroller of the Currency, the Board of Governors of the Federal Reserve Systems, the Federal Deposit Insurance Corporation, and the Federal Home Loan Bank Board. Nothing requires a bank to install a surveillance system. However, if it is installed, it must meet Title 12 of the US Code.

[¶] Bank crime has fluctuated over the years. In 1932, there were 609 holdups across the country. By 1943, it had declined to 24, following passage of the 1934 Bank Robbery Statute (Cross, R.F., 1981. *Bank Security Desk Reference*. Warren, Gorham & Lamont, Boston, MA, pp. 1–4). In 1968, the year the Bank Protection Act passed, 1769 bank robberies occurred. The following year, this number was 1793. In 2011, bank robberies reached 5014. That year 60 burglaries and 12 larcenies occurred (Federal Bureau of Investigation, 2012. *Bank Crime Statistics, Federally Insured Financial Institutions*. Federal Bureau of Investigation, Washington, DC).

modified years later to make requirements more reflective of changing circumstances. For example, the original law of 1968 produced regulations for Minimum Security Devices and Procedures (12CFR21). These included specific language related to antitheft technology, which became less relevant with the introduction of new and better cameras and recording media. By the 1990s, bankers possessed greater latitude with regards to designing security systems most appropriate for their needs. While the Bank Security Act is not directly associated with decreasing bank crime patterns, common sense argues that such institutions must implement reasonable security measures to protect employees and the public. Perhaps without the vigorous measures that were instituted by this law, bank crime would have increased. This act is an example of the federal government passing a measure that demands a distinctive private sector security response. In the process this law aided the role of security management to grow as a management practice in a particular sphere, in this case financial industries. Other federal measures would follow.

Another – and demonstrably more successful – example of how a legislative initiative causes the creation of security strategy relates to skyjacking, or the criminal highjacking of commercial airplanes.** This type of crime became an issue on November 24, 1971, when a man who called himself Dan B. Cooper commandeered a Northwest Orient flight from Portland, Oregon, en route to Seattle. The passengers were released in Seattle and a ransom and parachutes were taken aboard. Cooper ordered the flight to take off for Reno and to fly at a minimum speed and at low altitude. When the plane landed in Reno, Cooper, some parachutes, and \$200,000 in small, used bills were gone. The skyjacker and the cash were never recovered. Within 6 months, six other attempted skyjackings with parachute demands occurred. Most were unsuccessful, but the crime pattern threatened the air transportation industry.

Historically, Cooper's offense was not the first skyjacking: that occurred in Peru in the 1930s. Yet from 1930 to 1967, only nine incidents of air piracy occurred, of which only four were successful. Then, in 1968, 17 skyjacking incidents took place, of which 13 were successful. The next year, the total jumped to 40 incidents, of which 33 were successful. For the next 3 years, as the private and public sectors fought the trend, the number of attempted skyjackings on United States–scheduled aircraft held steady, while the number of successful incidents dropped from 17 in 1970 to 11 the next year, and then 8 in 1972. With implementation of control measures, skyjacking attempts dropped for the period 1973–1979 to 31, with only 3 being successful. The measures succeeded in reducing the risks of air piracy and restored confidence in travelers. This is a convincing example of how a coordinated security policy can reduce an international problem. However, risks to scheduled airport/airliner security had not been fully analyzed and reduced.

** The Federal Aviation Act of 1958, as amended. Section 315(a) required the FAA to report on the effectiveness of the Civil Aviation Security Program to Congress on a semiannual basis. In the 1980s domestic airline security measures were supplemented with assessments of foreign airports, conducted pursuant to the International Security and Development Cooperation Act of 1985 (public law 99–83).

9/11 and its Consequences

In the years following the institution of federally mandated preboard screening program for scheduled airlines, security practitioners and the general public continued to complain about security. Dissatisfactions were registered in letters to the editor and articles in the general press attesting to the extent to which security measures were easily defeated and, therefore, inadequate. How inadequate these measures really were did not become apparent until the morning of September 11, 2001, when four groups of Islamists commandeered two planes at Boston Logan Airport, one at Newark International Airport, and one at Reagan National Airport in Washington, DC. The terrible events of 9/11 indicated that vulnerabilities would be exploited by some willing to give up their lives for a cause.

In the aftermath of 9/11 two major pieces of federal legislation were passed. The first was the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT) Act of 2001 (PL 107-56). This Act was signed into law just 6 weeks following the attack. The main objectives of the USA PATRIOT Act were to enable law enforcement agencies to obtain intelligence on suspected terrorists, to deter terrorists from entering and operating in the United States, and to limit the ability of money-laundering activities that support terrorist actions. Much of this work was accomplished by cooperation with the private sector. The USA PATRIOT Act expires after a set number of years. It has been renewed with modifications since its incipience and is up for renewal in 2015.

More far reaching for security operations management was the Homeland Security Act of 2002 (PL 107-296). This Act created the most significant change in government structure since establishment of the Department of Defense through the National Security Act of 1947. The Department of Homeland Security (DHS) resulted from the merging of 22 federal agencies with a mandate to establish a safe and secure homeland. The impact on security operations didn't end at the federal level. Additionally, Homeland Security Presidential Directive/HSPD-5 tasked DHS to develop and administer a National Incident Management System (NIMS) and a National Response Plan (NRP). The private sector was to participate in the process. Within a few years following 9/11, every state government and the District of Columbia established an entity to find ways to protect communities from terrorist risks. This structure also facilitated a practical objective: state governments were now able to receive funding from DHS and other entities concerned with protection. The net effect of DHS was to channel billions of dollars for security products, services, systems, and research throughout the nation. Furthermore, agencies within DHS encouraged and mandated changes in security practices in the private sector.

Soon after its founding, DHS created a National Infrastructure Protection Plan (NIPP). The developmental process identified 17 critical infrastructure sectors encompassing both public and private interests. These 17 sectors were considered "so vital to the United States that their incapacity or destruction would have a debilitating impact on national security,

BOX 2.4 SEVENTEEN CRITICAL INFRASTRUCTURE SECTORS

Agriculture and food
 Banking and finance
 Chemical
 Commercial facilities
 Commercial nuclear reactors, materials, and waste
 Dams
 Defense industrial base
 Drinking water and water treatment
 Emergency services
 Energy^a
 Government facilities
 Information technology
 National monuments and icons
 Postal and shipping
 Public health and healthcare
 Telecommunications
 Transportation systems

NIPP promotes a partnership model to create government and private security efforts to protect critical infrastructure in the 17 sectors.

^a The energy sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

national economic security, and national public health of safety, or any combination of these matters” (Box 2.4). While terrorism served as an impetus for the creation of the NIPP, public/private cooperation has been enhanced through more efficient responses to major emergencies such as hurricanes. NIPP initiated voluntary private sector councils to advise on how to strengthen security in the sector by cooperation and the institution of best practices. The private sector participates in all the national infrastructure partnerships, except those exclusively concerned with government issues.

These changes all resulted from the attack on the morning of September 11, 2001. The South Tower of the World Trade Center imploded less than 1 hour after being struck. About 0.5 hour after that the North Tower collapsed. The final tally would be 2801 fatalities, of whom 418 were first responders from services in the City of New York, and 157 were occupants of the two planes involved in the attack.^{††} (Meanwhile, 188 died in a separate attack on the Pentagon: 124 in the building and 64 from the plane involved in the attack. Additionally United Airlines Flight 93, leaving Newark, New Jersey, heading for San Francisco, was skyjacked and then commandeered by passengers resulting in a

^{††} www.september11victims.com (accessed October 13, 2014). The total number of fatalities has risen over the years from the effects of morbid conditions created by rescue operations.

crash near Shanksville, Pennsylvania, killing 44 including the terrorists.) In the situation within New York City, the startling reality is that perhaps 15,000 lives were saved by the prompt actions of alert, trained floor fire marshals and also by security officers – the true first responders – who personally assisted countless masses of terrified office workers rushing out of the Towers in a true life and death struggle. That day hit the contract security guard industry hard. Twenty-nine security officers from four providers died in the process. Other proprietary security personnel also were lost. This tragic event with response from security services missed the attention of the National Commission on Terrorist Attacks on the United States where only a brief mention of private security is found in the commission’s report.⁶

However, the process did recognize the importance of the private sector in contributing to national security. The *9/11 Commission Report* states:

*The “first” first responders on 9/11, as in most catastrophes were private-sector civilians. Because 85 percent of our nation’s critical infrastructure is controlled not by government but by the private sector, private-sector civilians are likely to be the first responders in any future catastrophes.*⁷

Police chiefs across the nation saw the advantages of better cooperation with the extensive resources of the private security sector. In the ensuing months law enforcement reflected on how an era of growing terrorist countermeasures would strain resources. In an unprecedented 2-day National Policy Summit in 2004, police, private security, researchers, and academics convened to find ways where public/private cooperation could work more effectively. The summit was sponsored by International Association of Chiefs of Police (IACP) and Community Oriented Policing Services (COPS), a unit within the Department of Justice (DoJ).⁸ The final report advised several action items:

1. Leaders of major law enforcement and private security organizations should make a formal commitment to cooperation. The goal will be for “the implementation of sustainable public–private partnerships” to mitigate terrorism, public disorder, and crime.
2. DHS or DoJ or both should fund research and training on relevant legislation, private security, and law enforcement in public security cooperation.
3. DHS or DoJ or both should create an advisory council to oversee day-to-day implementation issues of law enforcement/private security partnerships.
4. DHS or DoJ or both, plus other organizations, should convene key practitioners to move this agenda forward.
5. Local partnerships should set priorities and address key problems as identified by this summit.

The report notes: “In reality, in many crises, security officers ... are the first responders.”

The action items from the summit will require support if they are to make a difference. Perhaps further summits will be needed. But domestic and global crime, terrorism, and

environmental emergencies are too great for the public sector to handle alone. Liking it or not, private security is being drawn into a new uncharted phase that demands greater professionalism and reliability. In turn, private security deserves something back, for example, better and faster intelligence on issues that affect them from law enforcement at all levels.

Cooperation between law enforcement and the private security sector differs according to local conditions. ASIS International fosters cooperation between police and security practitioners at chapter meetings across the nation. The New York City Police Department has precinct community councils in which the business community can participate in monthly meetings. A more pertinent program is NYPD Shield in which police and private security executives can meet to discuss current issues of significance, leading to more productive cooperation in dealing with crime patterns or local emergencies. Still imperfect, but improved public/private cooperation between law enforcement and private security has resulted from 9/11.

The Sarbanes–Oxley Act

The Sarbanes–Oxley Act (SOX) 2002 empowers the Securities and Exchange Commission to increase regulations of publicly held companies. Section 404: Management Assessment of Internal Controls is a key section. It requires each annual report of the issuer to include an “internal control report” that reports on the responsibility of management to establish and maintain an adequate internal control structure and procedures for financial reporting of the enterprise. Additionally, the report assesses the effectiveness of the internal control structure and procedure for financial controls. The Act was passed following the financial debacles of Enron, Global Crossing, WorldCom, and others that included substantially false financial reporting and contentions by senior officers that they were unaware of such rampant irregularities.

The onus of the Act is on the chief executive officer (CEO) at the time of the filing, or the person who is performing duties of the CEO. Similarly, the CFO signs documentation at the time of filing and shares major responsibilities for such filings. Most of the burden to meet the Act falls to internal auditors and the outside independent audit firm. However, security directors are likely to be involved in conducting fact-finding to assure that compliance is in order or that irregularities can be understood better.

The Patient Protection and Affordable Care Act

The cost of worker benefits can have a direct impact on resulting services. With passage of the Patient Protection and Affordable Care Act (PPACA), widely called ObamaCare, workplaces faced employer mandates to provide healthcare benefits beginning January 1, 2015. In 2016, employers must report on a monthly basis their compliance with the law. The net effect of the measures is to increase costs for employers and employees for healthcare benefits, while increasing health insurance availability. Workplaces will

evaluate the cost requirements to meet the law. Security services will cost more generally for personnel services due to high healthcare costs. Organizations will have to see how higher costs can be justified or how costs can be contained by adjusting personnel requirements.

Other Legal Measures Affecting Security

While loss clearly helped increase the formation of security programs in banking and aviation, many other industries were developing security programs without the force of directive legislation. For example, no legislation requires the retail industry to engage in security measures; however, substantial measurable losses in retailing have produced a cadre of managers who evaluate losses and forcefully seek to mitigate them. The same holds true for other aspects of commerce and industry – public, private, and not-for-profit sectors alike. Nonaviation transporters, distributors, mining and processing facilities, and a myriad of service organizations have all enhanced their security policies and systems.

These factors stimulated the growth of proprietary security programs. In the process, this trend stimulated the emergence of the contemporary security industry, which expanded to fill the growing services required by this commercial impetus. Meanwhile, many proprietary organizations partially or fully shifted security activities to outside services and contractors. We examine this issue next.

The Role of Unions in Security Operations

Large contract security guard companies with broad client bases typically serve some clients that require union representation for some of their employees. These businesses are not unionized nationally, but are likely to deal with numerous union contracts throughout the markets they serve, in accordance with demands of their local customers. Smaller contract security companies normally also are not unionized or, if they are, employees are represented by small “pure” unions dealing only with security guard companies. One reason why the security guard industry has been refractory to inroads from unions is a presumed legal impediment that makes the issue of unionizing security officers somewhat complicated.

As part of New Deal legislation in 1935, the National Labor Relations Act prohibited unfair labor practices against unions and granted organized labor the right of collective bargaining. The Act, also known as the Wagner Act, established the National Labor Relations Board (NLRB), Title 29, Section 159, the US Labor Code. This measure was intended to help settle union–management disputes over unfair labor practices. This Act was amended in 1947 by the Taft–Hartley Act. The Taft–Hartley amendment passed during a time when strikes were a national concern. It provided for an 80-day cooling-off period if a strike could cause a national emergency. The effects of such a strike obviously would be exacerbated if unionized security guards joined their coworkers on the picket line. Therefore, Taft–Hartley Section 9(b)(3) provides that the NLRB may not certify an employment

unit that includes guard and nonguard employees and, further, the NLRB may not, as a result of an election, certify as a representative of a unit of guards a union that admits nonguards to membership. Thus, unions exclusively for guards were created. These tended to be small and regional.

While most of these “pure guard” unions appeared to be run for their members’ benefits, a few were not. In the 1970s the Allied International Union numbered 700 security guards as members. The union was purchased for \$90,000 by a rogue Daniel Cunningham. The union’s constitution and bylaws permitted the incoming president to elect his own officers and appoint a successor; therefore, members had no right to vote or state any opinion authoritatively on relevant issues.⁹ Cunningham demanded and received indirect payoffs from local and national security guard companies. During this time he organized the guards in industries where the loss of security personnel could be critical: casinos and nuclear power plants. Meanwhile, the venal labor boss stole from funds in the union’s treasury. Eventually, Cunningham was convicted on several labor racketeering charges brought by the New York State Organized Crime Task Force.¹⁰

Unions that admitted guards and nonguards to membership (mixed unions) were not prohibited if the employer voluntarily agreed to recognize such a union. This has occurred throughout the country and over many years. NLRB Section 9(b)(3) limits mixed unions from representing both workers generally and security personnel, unless the employer has no objection. Otherwise during a union organizing process, the NLRB cannot direct an election in a unit that includes guards and nonguards. But nothing prevents guards from filing unfair labor practice charges against employers with the NLRB. Further, future elimination of the section is conceivable legislatively that would ease possibilities for large employers to recognize large unions in the same workplace.

The huge number of security guards and their potential for unionization has become apparent. Meanwhile, most security guard companies view with considerable mistrust and discomfort the prospect that their employees would become members of any powerful and prominent national union. This would seem to add an additional complication in the relationship with their customers for contract guard services. Yet such a relationship could be in the best interest of guard employees and owners and operators of security guard companies. On one hand, the fears of contract guard company operators could be allayed with specific language in agreements with the union that limits or prohibits disruptive practices.

Security managers generally resist the concept of unionization, because a union could intervene in the disciplining or termination of a unionized security worker, thus harming a long-established management prerogative. Further, the union would be involved in benefits issues. Yet in some cases unions provide benefits directly to members as part of the membership dues. Organized labor could reduce management’s fears by providing a catalyst for improving compensation, wages, guard standards, and security company operating profits at the same time. A strong national union would be a natural ally with the security guard industry in achieving needed federal and state legislative goals. The evidence is also persuasive in that unions have been able to raise wages for nonsecurity building

service personnel where market-wide prevailing agreements occur. Such compacts do not place one building operator at a disadvantage over another since all parties to the agreement meet identical requirements.

The Growth of the Modern Protective Industry

Most organizations direct security operations through a proprietary department. This implied that the organization “owns” the unit that provides its security services. Workers are regular employees of the enterprise. Proprietary security directors and associates remain central to the planning, organizing, and management of such services. However, as the previous chapter observed, security departments have been diminished in terms of proprietary personnel as more resources have been contracted out to outside service suppliers. The proprietary organization became the client, customer, or contractor of the supplier.

The security industry emerged from its mid-nineteenth century origins to develop as a group of specialized services and product sources. While not generally classified as a growth industry, security services and products could be considered. Components have grown and continue to expand steadily during the past century in response to demands of the marketplace. During the last quarter of the twentieth century, the US security industry surged at a rate considerably exceeding that of the nominal gross domestic product (GDP) for the same period of time. (The GDP is the aggregate measure of economic activity excluding income from foreign investments.)

For example, for the years 1987–1989, the US security industry grew at a rate of more than 11% annually, compared with an average annual growth rate of 7.5% for the GDP during the same period. During this period, gross revenues from security services – security guarding and related services, central station monitoring, and armored car services – grew from \$11.1 billion to \$13.8 billion, an increase of 24.3%. Between 1992 and 1996, growth of the industry continued, but at a slower rate. Total revenues increased about 8%, from \$29.1 billion to \$39.3 billion. Meanwhile, the nation’s GDP grew at an average annual rate of 4.2%. Therefore, this increase actually represented an improvement relative to the period 1987–1989. Indeed, security revenues as a percentage of GDP grew from 0.39% in 1992 to 0.44% in 1996, to 0.47% in 2000, and 0.56% in 2006.

The appetite for security services and systems has continued, although growth is never a straight line. External purchases of security services and products are related to general economic activity, technological innovations, and changes in regulations that can affect purchase decisions. Another market research firm finds that growth of private security revenues for the period 2014–2019 are projected to increase at a compound annual growth rate of 4.2%, as shown in [Table 2.1](#). This will result in revenues for services of \$66.9 billion in 2019 and \$80.3 billion by 2024 if the same growth rate continues.

Security products and systems are measured separately from services. These products are closely tied to new construction trends. In times of economic growth, this sector participates. Further, the growth of security technology has clearly been an impact on the long-term decrease in crime within the workplaces, in government facilities, and in communities.

Table 2.1 Private Security Services Demand (in Millions of Dollars)

Factor	2014	2019	2024	% Annual Growth 2014/19
Guarding	19,400	23,500	27,000	3.9
Alarm Monitoring	17,100	20,500	24,350	3.7
Private Investigations	4,800	6,350	8,200	5.8
Correctional Facilities Management	3,250	3,950	4,600	4.0
Systems Integration & Management	2,810	4,000	5,640	7.3
Armored Transport	2,600	2,700	2,950	0.8
Security Consulting	2,110	2,900	3,890	6.6
Pre-Employment Screening	1,320	1,670	2,040	4.8
All Other	1,110	1,330	1,630	3.7
Total	54,500	66,900	80,300	4.2%

Source: Freedonia Group, Inc., June 2015.

Electronic systems have received considerable attention in the past and have far surpassed mechanical locks. However, this sector also continues to grow robustly, as seen in [Table 2.2](#).

US security spending exceeded \$410 billion in 2014, according to research from ASIS International and the Institute of Finance and Management.¹¹ This represents total expenditures for private sector, nongovernment organizations, and government at all levels.

Security Services

Three out of \$4 expended for purchased protection needs are allocated for personnel-based services. These activities require the support of equipment and technology, but the

Table 2.2 Electronic and Mechanical Security Products and Systems (in Millions of Dollars)

Factor	2011	2016	2021	% Annual Growth, 2011/2016
Electronic				6.3
Access controls	3,610	5,550	7,900	9.0
Alarms	2,890	3,700	4,610	5.1
Video surveillance	1,295	1,620	1,990	4.6
Contraband detection	1,205	1,640	2,180	6.4
Vehicle security	1,190	1,480	1,760	4.5
Electronic article surveillance	545	590	670	1.6
Other	165	220	290	5.9
Mechanical				6.3
Locks	2,235	3,300	4,330	8.1
Other	1,480	1,750	2,020	3.4
Net imports subtracted	2,565	4,400	6,400	—
Total	14,615	19,850	25,750	6.3

Source: The Freedonia Group, Inc., 2012.

bulk of the expenditures are for direct compensation and benefits of personnel and their support.

Personnel-based services may be divided into seven categories:

1. *Security guard services.* This category absorbs a number of protection workers with varying responsibilities, including extensive public service contact (“officers”), asset protection specialists (“guards”), receptionists, patrol officers, executive protection personnel, watchmen, timekeepers, and others. These personnel provide both the important “visible security” presence required by many protective objectives and the less apparent, behind-the-scenes securing of physical assets by deterring, detecting, and reporting activity related to threats to people or property.
2. *Central station services.* The computing revolution has permitted organizations to monitor people, places, and events with efficiency and accuracy. Originally, central stations provided burglar alarm, fire notification, and messenger-requesting signals. Today, burglar and fire alarms remain the core of such services, but numerous other monitoring functions are also available, such as remote visual monitoring. Expenditures for such services have grown steadily in the past 25 years, and have surpassed, or are about equal to, the amount contracted out for security guard services.
3. *Private investigation services.* In the past, investigators were linked to the resolution of specific losses. That’s still true, but assignments faced by contemporary investigators are broader. Investigators today are much more likely to conduct evaluations to make sure that corporate policies are maintained, such as by assuring that licensing fees and payments are properly documented. Investigators are frequently integral in due diligence fact-finding (i.e., the vigilant care needed in a given situation) prior to acquiring an asset or related to litigation involving the organization. This category of contracted service continues to grow in importance for proprietary security programs.
4. *Armored car services.* Ever since Washington Perry Brink started his transport business with a horse and a wagon in the nineteenth century, customers have turned to outside organizations to physically move assets. In addition to transporting cash, these services may provide activities such as the servicing of automated teller machines (ATMs) and the transporting of high-value noncash assets such as jewelry and computer tapes and documents. They also handle aspects of cash management for financial organizations removing such services from traditional bank services.
5. *Consultant and other services.* When particular problems emerge, security operations managers often turn to consultants with special expertise in particular activities. Most major industries and most types of specific security concerns – for example, data protection and financial investigations – can retain the services of such persons or their organizations for a defined period of time to achieve the desired goals. Due to the shrinking of central staff management in the past 25 years, managerial resources

were reduced and the use of outside consultants replaced in-house management capabilities on an as-needed basis. Meanwhile, other services are equally significant to organizations. For example, in the event of a loss of computer processing capability, an organization may turn to facilities that have compatible hardware that may be commandeered for immediate use.

6. *Electronic security equipment and systems.* To provide more control at less cost, managers turn to electronic security equipment, which can augment, supplement, and verify the actions of security personnel. Though smaller than personnel-intensive services, capital outlay for such equipment is growing steadily. The ways these funds are allocated are given as follows:
 - a. *Intrusion detection equipment.* These devices and systems indicate the unauthorized passage of individuals into a protected area.
 - b. *Vehicle security systems.* These products deter and detect the theft or removal of cars, trucks, vans, and other mobile conveyances.
 - c. *Computer security equipment.* Because of the importance of data protection, systems to protect information assets are growing at a substantial rate and play an important role in loss deterrence for data systems.
 - d. *CC/IPTV equipment.* Security operations increasingly use CC/IPTV systems to monitor, analyze, and record activities. (This is also called video surveillance technology.)
 - e. *Fire detection equipment.* Facilities are required to use fire detection systems by codes, standards, insurance requirements, or common sense.
 - f. *Electronic article surveillance (EAS) systems.* These systems are primarily used to control the losses of retail merchandise. However, EAS systems also may be applied to broader applications of assets control.
 - g. *Access control equipment.* Systems to efficiently allow or deny entrance make an important contribution to operating a secure facility. This category is closely related technically to intrusion detection equipment.
 - h. *Secure telephone equipment.* This equipment protects telephone and data transmissions from unauthorized interception.
 - i. *X-ray inspection equipment.* X-ray impressions may identify the presence of weapons or contraband material hidden in packages or on persons.
 - j. *Metal detection equipment.* These systems identify metal content hidden within packages or on persons. Wide applications are found at airport preboard screening and the checking of people and hand parcels entering at-risk locations.
 - k. *Biological, nuclear, and chemical detection.* Still another way of identifying contraband is the use of technology to identify the chemical signatures of such materials. These may result in an alarm being sounded or in a security officer setting aside a suspicious object for further evaluation.
7. *Mechanical security hardware.* In addition to personnel and electronic devices, systems, and software, security operations often require the purchase and use of

particular products and materials. Hence, any object or material that is not electronic is categorized as mechanical security hardware. This category also is substantial, and projected to grow along with construction needs. While electronic products and systems are in the spotlight, mechanical locks continue to have sufficient applications to assure their continuance. This category includes safes, vaults, glazing, and other products specifically marketed for their protective features. A door that is required to be intrusion-resistant would be included in this category; a normal door would not be. Locking devices including door locks, padlocks, deadbolts, latches, as well as security storage equipment such as safes and vaults and fire extinguishers, and related products are also included in this category.

Security Services and Products as a Global Business

All enterprises require security. Therefore, security is a universal business. The United States is the largest producer and consumer of security services and products at present, representing over one-fourth of global market demand. Areas apart from North America and Western Europe are growing more rapidly and the need for security services and products is at a greater level. For example, Brazil is the world's second largest market after the United States, but China will surpass both within the decade. See [Table 2.3](#). More than half of the market is for guarding.

Additionally, global demands for security products and systems match services in increased demand. Issues affecting security demand in different countries include rising crime rates, expanding economies, new business formation, investment from abroad, growth in demand for better residential security, and privatization of formerly state-owned businesses.

Part of the growth in the security market is related to steady increases in population. In 2013, the global population was 3.771 billion. Growing at a compound annual growth rate

Table 2.3 World Security Services (in US\$ Billions)

Nation or Region	2013	2018	2023	Change, 2013–2018
North America	59.2	74.7	93.0	4.8
United States	51.9	63.5	76.5	4.1
Canada and Mexico	7.3	11.1	16.5	8.9
Western Europe	40.3	47.4	55.4	3.3
Asia/Pacific	37.8	60.9	93.3	10.0
China	6.6	13.8	24.3	15.9
Japan	9.2	11.6	14.1	4.7
Other Asia/Pacific	22.0	35.5	54.9	10.0
Other regions				
Central and South America	27.1	44.3	68.7	10.3
Eastern Europe	9.1	13.1	18.7	7.6
Africa/Middle East	17.1	26.2	38.4	8.9
World Security Services Revenues	190.6	266.6	367.5	6.9

Source: Freedonia Group, October 2014.

of 1.9%, by 2018, global population will be 4.15 billion and 4.535 billion by 2023. Since different parts of the world grow at different rates, geography relates to market activity. However, a much more significant factor is modernity itself – the sense that security is both a need and a desire in urban life. This forms a variable but expanding worldwide need for security services, products, and technology.

Managers of global security operations need to understand foreign cultures before imposing solutions that seem logical in the homeland. Security trends and technology differ among countries and regions. Issues such as fraud and prevention, the concept of privacy, business continuity management, civil unrest, and terrorism present variations. The relationships between managers and subordinates also differ.

How Security Executives Rank Priorities

Security practitioners deploy proprietary and contract services and electronic security systems in order to achieve a wide range of objectives. Principally, tasks relating to personnel matters, budgeting, training, and program planning and administration comprise most of the time available in a manager's week. However, in addition to routine program management, numerous security-related threats require consideration and action. These change with the times, geography, and the nature of particular industries.

The security threats and management issues listed by respondents to a Fortune 1000 study are various, as shown in [Table 2.4](#). (These issues are discussed in greater detail in the final chapter of this book.) The following is a list of the top 26 security threats and management issues:

- *Computer/communications security (e.g., Internet/intranet security)*. Protecting assets relating to attacks on information resources and misuse of information technology (IT) is a large task. It has grown in significance for managers and currently ranks highest among 26 concerns. Computer attacks against an organization can be on a scale from minimal to catastrophic.¹²
- *Business continuity planning/organizational resilience*. Emergencies in organizations can be due to nature-based, people-based, design-based, and technology-based factors, among others.¹³ The crisis or contingency manager seeks to avoid a crisis from occurring by establishing contingency plans.
- *Workplace violence prevention/response*. For most people, the workplace is a safe place. But occasionally, violence intrudes into an otherwise nonviolent environment. Despite such events being uncommon, the issue cannot be dismissed by managers; indeed, it is at or near the top of any list of workplace concerns.¹⁴ Diligent managers must take measures to make employees feel safe on the job, and at the same time deter disgruntled employees, terminated workers, enraged customers or clients, and others from untoward action.
- *Employee selection/screening*. Security directors frequently are involved in directing, assessing, and improving ways by which new employees may be

Table 2.4 Most Important Security Threats and Management Issues

Rank	Security Threat
1	Cyber/communications security (e.g., Internet/intranet security)
2	Business continuity planning/organizational resilience
3	Workplace violence prevention/response
4	Employee selection/screening
5	Environmental/social: privacy concerns
6	Property crime (e.g., external theft, vandalism)
7	General employee theft
8	Crisis management and response: domestic terrorism
9	Identity theft
10	Unethical business conduct
11	Environmental/social: pandemics (e.g., Ebola virus)
12	Crisis management and response: political unrest/regional instability/national disasters (evacuation potential)
13	Litigation: inadequate security
14	Fraud/white-collar crime
15 (tie)	Litigation: negligent hiring/supervision
15 (tie)	Substance abuse (drugs/alcohol in the workplace)
17	Business espionage/theft of trade secrets
18	Environmental/social: robberies
19	Intellectual property/brand protection/product counterfeiting
20	Global supply chain security
21	Executive protection (including travel security)
22	Insurance/workers' compensation fraud
23	Crisis management and response: international terrorism
24	Bombings/bomb threats
25	Labor unrest
26	Crisis management and response: kidnapping/extortion

See also Chapter 11.

Source: Securitas Security Services USA, 2015. Top Security Threats and Management Issues Facing Corporate America. Securitas Security Services USA, New York, NY.

screened (vetted) before an offer of employment or a significant promotion is made (see Chapter 3).

- *Environmental/social: privacy concerns.* The word “privacy” does not appear in the Constitution. However, invasion of one’s personal information has grown to be a risk that can result in legal action if harm occurs that could have been avoided.
- *Property crime (e.g., external theft, vandalism).* An omnipresent concern for security practitioners is minor and major larceny against the assets of the organization. Security operations seek to decrease the opportunity for such acts by instituting appropriate, cost-effective controls.
- *General employee theft.* Despite the best efforts to screen-in the most productive and honest workers, experience shows that employees represent serious risks. Generally, employee deviance represents only a few within the workforce. However, due to their

understanding of the security vulnerabilities, these few can cause substantial losses of assets.

- *Crisis management and response: domestic terrorism.* Risk exposures can occur at home and abroad. The security practitioner has the duty to qualify and manage threats and vulnerabilities.¹⁵ Organizations that operate in nations where there are risks to employees and assets require constant monitoring. Optimal security operations must seek to assess the risks in various nations. They must further stay abreast of any changing conditions that could lead to threats to employees or expropriations of assets. In the event of an emergency, security planners must attempt to remove employers safely from harm's way.
- *Unethical business conduct.* In many circumstances, one of the tasks for security operations is to play varying roles in drafting, monitoring, and enforcing an organizational code of ethical conduct.¹⁶
- *Identity theft.* In a recent year almost 12 million persons were victimized by the effects from identity theft in the United States. The crime has no borders, so victims are found globally. Workplaces are impacted when merchandise is transported to perpetrators or their agents.¹⁷
- *Environmental/social pandemics (e.g., Ebola virus).* Ebola, severe acute respiratory syndrome (SARS), and other viral attacks impact the workplace, although immediate risks are few. Typically, organizations plan on how to conduct operations as close to normal as possible in the unlikely event that a pandemic hits close to home. In 2014, security directors of global organizations prepared contingency plans in the event that operations or supply chain activity was interrupted by the Ebola virus.
- *Crisis management and response: political unrest/regional instability/national disaster (evacuation potential).* The supply chain can be shut down if a key material, part, or assembly cannot be delivered due to an interruption. Security practitioners have roles in assuring that, as far as possible, alternative resources are available. Similarly, some security programs have 24/7 active monitoring of global conditions where the organization operates.
- *Litigation: inadequate security.* The reality or fear of legal action for negligence is one of the driving features in security management today. Security program operators are involved in a variety of activities related to these risks, including instituting procedures and controls to reduce such risks and preparing actions or defenses for legal cases.¹⁸
- *Fraud/white-collar crime.* The term "white-collar crime" was coined by the sociologist Edwin Sutherland, and signifies unlawful, nonviolent conduct committed by corporations and individuals. It includes theft, fraud, and other violations of trust, including embezzlement. Embezzlement is the fraudulent appropriation of property by one lawfully entrusted with its possession. Frequently, this crime is committed by someone with a fiduciary responsibility within the organization, which he or she then abuses. The investigation and prevention of fraud (i.e., false representation or intentional perversion of truth to induce another to part with something valuable) is an important task in any organization.

- *Litigation: negligent hiring/supervision.* Under the doctrine of *respondeat superior*, the employer may be held responsible for negligence by an employee. Training that informs workers on what they can and cannot do can mitigate claims. Risk analysis further lowers workplace vulnerability to lawsuits.¹⁹
- *Substance abuse (drugs/alcohol in the workplace).* Employee drug testing is widely used in industry. Policies, procedures, consent forms, checklists, and training materials are needed for such programs.²⁰
- *Business espionage/theft of trade secrets.* For many organizations, the loss of crucial information is of greater importance than the fraudulent disappearance of products or supplies. These transgressions include espionage or theft of trade secrets, including developmental procedures and know-how.
- *Environmental/social robberies.* Robberies are categorized as the third most significant crime in the hierarchy of the FBI's *Uniform Crime Reports*. Robbery is the taking or attempting to take anything of value from the care, custody, or control of someone. Force or threat of force of violence and putting the victim in fear is a characteristic of this crime. Robbery mitigation is likely to succeed when risk mitigation is put into place.
- *Intellectual property/brand protection/product counterfeiting.* The brand, product, and information of an organization are precious assets. Intellectual property can walk out the door or be accessed through a few keystrokes. Security practitioners are interested in preventing this loss and also investigating possible incursions early on to lessen the damage.²¹
- *Global supply chain security.* The stealing of goods that are being transported or stored is an ongoing concern for product manufacturers and distributors.²² Outright theft requires prompt investigation and response. Broad transportation issues include container tracking and transit point security.
- *Executive protection (including travel security).* The protection of senior officials from risk has become a highly evolved skill that draws upon management planning and analysis.²³ Protection choreography, advance security preparations, domestic and international travel assessment, and physical training are all involved in the process.
- *Insurance/workers' compensation fraud.* Organizations that provide workers' compensation insurance sometimes encounter abuse, which requires investigation and response. A security program is generally tasked with investigating other incidents concerning insurance claims.
- *Crisis management and response: international terrorism.* The bombings of the World Trade Center, the Boston Marathon, the Oklahoma City federal building, and public and private assets in various locales domestically and globally suggest the importance of measures to deter such attacks.²⁴ As a global activity, security planners look at risks from unstable parts of the world, and political risks from groups such as ISIS (or ISIL) that could destabilize the world and affect conventional operations.
- *Bombings/bomb threats.* Bombings in the workplace are rare. Bomb threats are frequent. Security practitioners devise strategies to analyze and deal with threats as they are received.

- *Labor unrest.* Currently, labor–management relationships remain adversarial, as always, and as they are supposed to be. This does not necessarily lead to unrest. However, when issues flare, the matter becomes a security priority.
- *Crisis management and response: kidnapping and extortion.* Kidnapping (i.e., the forcible abduction of a person from his or her residence or business) for profit via ransom payment is rare in the United States. Extortion (i.e., obtaining property by threatening to injure or commit any other criminal offense) is more common and sometimes involves features of kidnapping. Organizations operating in kidnapping-for-profit countries make broad preparations to protect employees from victimization.

Other security threats occur in the workplace. For example:

- *Sexual harassment/Equal Employment Opportunity Commission (EEOC).* Complaints of harassments by coworkers or others at the workplace have been recurrent in recent years. Similarly, alleged violations of the EEOC guarantees have affected security operations. Both types of allegations require investigation and response.
- *Product diversion.* Sometimes, products are sold abroad at a lower price than what is charged to distributors and retailers in other markets. The manufacturer loses revenues when these products intended to be sold into the lower-priced market are surreptitiously sold back into the domestic distribution channels by a third party. Security operations must seek to prevent such transshipment and to investigate any suspected incidents that may be encountered.
- *Product tampering or sabotage.* The integrity of a product is vital to its maker. Sometimes, however, products are intentionally adulterated. In extreme situations, this willful and malicious destruction of property can lead to injury and death. Additionally, the organization can have its valuable market position threatened by the results.
- *Organized crime.* Criminal activity that is perpetuated by individuals who are systematized and concerted to common goals is defined as organized crime. It is not solely a law enforcement problem but also directly of importance to any organizations affected by it.

Specific Concerns for Different Industries

The security threats and management concerns listed in the preceding sections reflect responses from managers in numerous types of industries. Naturally, when responses from a particular industry are disaggregated from the total, the rank and pattern of priorities change. The following sections present four large industry groups from the sample as well as their respective top five concerns.

Manufacturing

Security directors of Fortune 1000 manufacturing firms cite the top two concerns mentioned above as their primary management concern. The distinctive variance from the overall profile was seen in the high rank accorded to the security of intellectual property.

This reflects the importance of safeguarding proprietary technology and processes that create a competitive difference.

Top Security Threats: Manufacturing

1. Cyber/communications security (e.g., Internet/intranet security)
2. Workplace violence prevention/response
3. Business continuity planning/organizational resilience
4. Employee selection/screening
5. Business espionage/theft of trade secrets

Finance and Insurance

Business services and insurance in the survey included computer and data service firms, financial institutions, and insurance companies. This segment placed two computer-related security concerns among the top five. The theft of personal computers (PCs) and laptops, for example, can represent a loss of current value and future opportunity. The loss of information can far exceed any physical disappearance of hardware.

Top Security Threats: Finance and Insurance

1. Cyber/communications security (e.g., Internet/intranet security)
2. Business continuity planning/organizational resilience
3. Workplace violence prevention/response
4. (Tie) Employee selection/screening
4. (Tie) Environmental/social: privacy concerns

Retail Trade

Like other major industry groups, retailers and related companies in the Fortune 1000 group placed cyber-communications security as their paramount concern. Previously property crime and general employee theft ranked at or near the top. Employee screening concerns also ranked higher with this group than with other industry groups, which reflects the concerns that security executives in the retail trade industry have about obtaining and managing ethical employees.

Top Security Threats: Retail Trade

1. General employee theft
2. (Tie) Cyber/communication security (e.g., Internet/intranet security)
2. (Tie) Identity theft
4. (Tie) Workplace violence prevention/response
4. (Tie) Employee selection/screening

Utilities

Consistent with the broad survey group, the utilities industry placed workplace violence as its top concern. Also, computer-related security issues rank high for this group, while terrorism has declined as a top five concern for this industrial sector.

Top Security Threats: Utilities

1. Cyber/communications security (e.g., Internet/intranet security)
2. Business continuity planning/organizational resilience
3. Employee selection/screening
4. Workplace violence prevention/response
5. Crisis management and response: domestic terrorism

Summary

Security operations must possess competence in a “core” set of skills in order to run successfully. These skills include program initiation, ongoing monitoring, and constant endeavors to improve performance. Corporate security endeavors are still new, having been the focus of independent research only in recent decades. Yet the reasons for the growth of such services involve diverse psychological, legal, social, and financial requisites. Politics and federal and state laws have helped shape security services. The horrific events of 9/11 and legislation passed since then have provided a reshaping of what the public sector expects from private security. The changing priorities of security practitioners in large corporations focus on workplace violence, crisis management, and executive protection, although the nature of those concerns differs according to the particular industry of the corporation.

Discussion and Review

1. Why are some operational contingencies considered “core?” What would be an example of a noncore competency?
2. Why was the *Rand Report* so influential on security practices? Is it pejorative to refer to private security services as “private police?”
3. What factors are most important in driving the growth of security services and programs?
4. Describe federal laws that have helped form security practices.
5. How have the events following 9/11 reshaped private security?
6. What are the differential rates of growth of security services, electronics, and hardware? Why would these grow at different rates?
7. Corporate security managers place workplace violence at or near the top of their concerns. Is this likely to change? What factors could influence different types of industries to report different security priorities?

Endnotes

¹ Beattie, J.M., 2012. *The First English Detectives: The Bow Street Runners and the Policing of London, 1750–1840*. Oxford University Press, Oxford, New York.

² McCrie, R.D., 1988. The development of the U.S. security industry. *Ann. AAPSS* 498, 23–33.

- ³ McCrie, R.D., 2005. ASIS International. In: Encyclopedia of Law Enforcement, vol. 2. Sage Publications, Thousand Oaks, CA, p. 547.
- ⁴ Kakalik, J.S., Wildhorn, S., 1972. Private Police in the United States: Findings and Recommendations, vol. 1. Government Printing Office, Washington, DC, p. 30.
- ⁵ National Advisory Committee on Criminal Justice Standards and Goals, 1976. Private Security: Report of the Task Force on Private Security. Government Printing Office, Washington, DC.
- ⁶ 9/11 Commission, 2004. Final Report on the National Commission on Terrorist Attacks Upon the United States. W.W. Norton & Company, New York. The reference: "Many civilians in the South Tower were initially unaware of what had happened in the other tower Many people decided to leave, and some were advised to do so by fire wardens. In addition, Morgan Stanley, which occupied more than 20 floors of the South Tower, evacuated its employees by the decision of company security officials," p. 287.
- ⁷ *Ibid.*, p. 317.
- ⁸ IACP, COPS (2004). National Policy Summit: Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder. IACP, Alexandria, VA.
- ⁹ Cook, J., 1983. Brother Cunningham and the guards. Forbes, February 14, p. 107; Top security union official on trial for extortion, manipulation of union funds. Security Letter, May 17, 1982, p. 2.
- ¹⁰ President's Commission on Organized Crime, 1985. Organized Crime and Heroin Trafficking. U.S. Government Printing Office, Washington, DC.
- ¹¹ ASIS International, 2014. U.S. Security Industry Growth Projection. ASIS International, Alexandria, VA.
- ¹² The literature on IT security is extensive. Examples: Chang, L.Y.C., Grabosky, P., 2014. Cybercrime and establishing a secure cyberworld. In: Gill, M. (Ed.), The Handbook of Security. Palgrave Macmillan, New York, p. 321; Workman, M., Phelps, D.C., Gathegi, J.N., 2013. Information Security for Managers. Jones & Bartlett Learning, Burlington, MA; Thermos, P., Takanen, A., 2008. Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures. Addison-Wesley, Upper Saddle River, NJ; Smallwood, R.E., 2012. Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets. John Wiley & Sons, Hoboken, NJ.
- ¹³ Elliott, D., 2014. Disaster and crisis management. In: Gill, M. (Ed.), The Handbook of Security, second ed. Palgrave Macmillan, New York, p. 791.
- ¹⁴ Kelleher, M.D., 1996. New Arenas for Violence. Praeger, Westport, CT. Also: Mattman, J.W., Kaufer, S., 1997. Complete Workplace Violence Prevention Manual. James Publishing, Costa Mesa, CA; Southerland, M.D., Collins, P.A., Scarborough, K.E., 1997. Workplace Violence. Anderson Publishing, Cincinnati, OH.
- ¹⁵ Wheeler, E., 2011. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Syngress, Waltham, MA.
- ¹⁶ Adams, A.A., 2014. Security Ethics: Principled Decision-Making in Hard Cases. In: Gill, M. (Ed.), The Handbook of Security, second ed. Palgrave Macmillan, New York, p. 959.
- ¹⁷ Pontell, H.N., Geis, G., 2014. Identity theft. In: Gill, M. (Ed.), The Handbook of Security, second ed. Palgrave Macmillan, New York, p. 302.
- ¹⁸ Imbau, F.E., Farber, B.J., Arnold, D.W., 1996. Protective Security Law, second edition. Butterworth-Heinemann, Boston, MA.
- ¹⁹ Nemeth, C.P., 2012. Private Security and the Law, fourth ed. Butterworth-Heinemann, Waltham, MA.
- ²⁰ Fay, J., 1991. Drug Testing. Butterworth-Heinemann, Boston, MA.
- ²¹ Post, R.S., Post, P.N., 2008. Global Brand Integrity Management: How to Protect Your Product in Today's Competitive Environment. McGraw-Hill, New York; Burwell, H.P., 2004. On line Competitive Intelligence: Increase Your Profits Using Cyber-Intelligence. Fact on Demand Press, Tempe, AZ.

- ²² Tyska, L.A., 1989. Transportation–distribution theft and loss prevention. In: Fennelly, L.J. (Ed.), *Handbook on Loss Prevention and Crime Prevention*, second edition. Butterworth-Heinemann, Boston, MA.
- ²³ D’Addario, F.J. (Contributing Ed.), 2014. *Personal Safety and Security Playbook: Risk Mitigation Guidance for Individuals, Families, Organizations, and Communities*. Elsevier, Security Executive Council, Waltham, MA. Also: Gonzalez, D., 2014. *Online Security for the Business Traveler*. Butterworth-Heinemann, Waltham, MA.
- ²⁴ Johnson, R., 2013. *Antiterrorism and Threat Response: Planning and Implementation*. CRC Press, Boca Raton, FL.

Additional References

- Chaiken, M., Chaiken, J., 1987. *Public Policing – Privately Provided*. National Institute of Justice, Washington, DC.
- D’Addario, F.J., 2013. *Influencing Enterprise Risk Management*. Elsevier, Security Executive Council, Waltham, MA.
- Johnston, L., 1992. *The Rebirth of Private Policing*. Routledge, London, New York.
- Milakovich, M.E., 1995. *Improving Service Quality*. St. Lucie Press, Delray Beach, FL.
- Pastor, J.E., 2003. *The Privatization of Police in America*. McFarland & Company, Jefferson, NC.
- Shearing, C.D., Stenning, P.C. (Eds.), 1987. *Private Policing*. Sage Criminal Justice System Annuals. Sage Publications, Newbury Park, CA.
- Smith, E.N., 2014. *Workplace Security Essentials: A Guide for Helping Organizations Create Safe Work Environments*. Butterworth-Heinemann, Waltham, MA.
- South, N., 1988. *Policing for Profit: The Private Security Sector*. Sage Contemporary Criminology. Sage Publications, Newbury Park, CA.
- U.S. General Accounting Office, February 1990. *Report of the National Advisory Commission on Law Enforcement*. U.S. General Accounting Office, Washington, DC.

Further Reading

Cybersecurity: evolving threats, evolving solutions. <gcn.com/cdwgcybersecurity>.

Staffing to Meet Protective Goals

It is imperative that those exercising supervisory authority over security guards (whether contract or proprietary) initiate affirmative actions to ensure that the guards are physically, mentally, and morally capable and qualified to perform their assigned duties.

—Jennifer F. Vaughan, *Avoiding Liability in Premises Security*

Staffing relates to the recruiting and preemployment screening (vetting) of individuals required for protective activities. This process is critical for all managers concerned with security operations. Indeed, chief security officers, security directors, and their deputies normally spend considerable time and effort on the topics discussed in this and the next three chapters. Failure of any organization to make such screening a priority can lead to regrettable developments ([Box 3.1](#)).

The staffing process must balance the requirements of the organization with the abilities provided from a finite pool of potential employees. The requirements further change depending on the position needing to be filled. This chapter discusses staffing matters relating to entry-level, supervisory, and managerial issues; however, the emphasis will be on entry-level employment. Hiring personnel for security positions is like hiring persons for any other position within the organization; nevertheless, security positions are distinctive in some ways and require a level of background screening that extends beyond the scope adequate for most other employees. This vetting is required due to the high level of trust expected in such positions. The means of ascertaining the levels of confidence in new hires are discussed later in this chapter.

At all employment levels, with security being no exception, complex concerns influence the process of personnel selection. These relate to the size of the employment pool, geographical considerations, time of the year, legal constraints, reputation and industry of the potential employer, and other factors affecting the choices an employer is likely to have.

Personnel Planning

In order to achieve optimal performance, organizations must plan to fulfill personnel needs for three basic requirements. First, ongoing programs require personnel to replace those who retire, resign, or leave for cause. Next, personnel may be needed on a temporary

BOX 3.1 THE PERILS OF POOR PREEMPLOYMENT SCREENING

The failure to vet prospective employees in a comprehensive manner increases the risks that dangerous and dishonest employees may be hired. Employers frequently learn that applicants for employment fail to reveal significant facts of their work or personal history. At BellSouth, for example, approximately 15–20% of new applicants conceal a secret.¹ Serious error and omissions in corporate and professional résumés should be identified by a diligent review of “facts” provided on the application form. Lack of appropriate preemployment screening has led to the following situations:

- The vice president for corporate communications at Walmart was forced to resign after it was discovered that he lied about receiving an art degree from the University of Delaware. He was about to be promoted to senior vice president when a review of his employment file discovered the lie in his education history.²
- In Rio Linda, California, a substitute custodian after working at a high school for 3 days was charged with the death of an 18-year-old female student. The school board hired the custodian before his background check was verified. The custodian had a prison record following a manslaughter charge for his part in a store holdup that left a customer dead. He also had served time for parole violation in beating his wife.³
- The Yahoo board fired its new CEO who falsely claimed on his résumé that he held a computer science degree. An activist investor discovered that the executive had lied. An outside executive placement firm failed to uncover the inaccuracy.⁴
- A medical doctor serving as an intern at University Hospital of the School of Medicine at the State University at Stony Brook, New York, failed to disclose on his application that he had spent time in prison for sprinkling arsenic-laced ant poison on coworkers' donuts and coffee while working as a paramedic in Illinois. During his internship at Stony Brook, the doctor treated 147 patients, 1 of whom lapsed into a coma shortly after the doctor's treatment.⁵
- An American woman was accepted to a selective British law firm's training program with credentials from Georgetown Law School and recommendations from a prosecutor for the Manhattan district attorney among others. She was busy handling criminal cases and was almost about to be named a barrister. However, a clerk reviewing her application believed that the listed age was wrong. A further inquiry revealed forgeries and bogus credentials errors.⁶
- The CEO of RadioShack resigned when it was learned that he had no college degrees, whereas he claimed he had two. He was also facing a trial on his third arrest on charges of driving while intoxicated.⁷

These examples involve nonsecurity professionals. The same dangerous deception occurs among security personnel. In one example, a security guard working at the civic auditorium in Albuquerque, New Mexico, was employed to maintain order during a wrestling match. A bystander claimed he was observing a disturbance, but the contract security officer concluded otherwise. The guard handcuffed the observer, removed him to a separate area, and beat him. At trial, the guard's earlier conviction for violent crime was revealed. An appellate level decision found that the security contractor was negligent. The court ruled, in part, that the security

firm did not adequately investigate the background and character of individual guards prior to hiring them.⁸ Law enforcement officials arrested 104 airport workers from 3 airports in the Washington, DC, area for fraudulently obtaining security badges that allowed them to work in restricted areas. That sweep increased to 356 the nationwide total of people who had been arrested for supplying false information to obtain security badges or jobs over the previous 9 months.⁹

References

1. Robinson, E.A., 1997. Beware – job secrets have no secrets. *Fortune*, December 29, p. 285.
2. Abrams, R., 2014. Walmart vice president forced out for lying about degree. *New York Times*, September 17, p. B3.
3. Suspect in student's killing has prison record. *New York Times*, May 19, 1997, p. A12.
4. <http://latestnews.thefiscaltimes.com//2012//05/13/yahoo-ceo-steps-down>.
5. McQuiston, J.T., 1993. Lawyer ties man's coma to intern Stoney Brook dismissed. *New York Times*, October 28, p. B7.
6. Buettner, R., 2013. Falling far short of the whole truth. *New York Times*, February 14, p. A21.
7. <http://www.nytimes.com/2006/02/21/business/21radio.html>.
8. Vaughan, J.F. (Ed.), 1997. *Avoiding Liability in Premises Security*. *Strafford Publications, Atlanta, GA*, p. 157.
9. Wald, M.L., 2002. Officials arrest 104 airport workers in Washington area. *New York Times*, April 24, p. A13.

basis to staff a short-term requirement. And finally, personnel may be needed to staff new programs. The processes involved in this planning activity are as follows:

1. *Identify personnel resources.* The number of employees required for current operations as well as any new organizational goals must be assessed. Further levels of skilled and experienced personnel needed for any internal growth or contraction or new venture must be estimated. This process is critical because it relates to substantial ongoing obligations the employer will have toward the worker. The security planner will estimate the number of employees needed at fixed points, those who will patrol, and their relief personnel. In planning a schedule for an entire year, vacations and personal time must be taken into consideration. Control of costs is never far from the mind of the manager. However, goals must be accomplished and these are impossible without adequate staffing.
2. *Monitor current internal personnel resources.* At least some personnel required for a new venture may be found among existing employees. Therefore, management benefits from having a database of existing personnel to draw upon when openings arise.
3. *Estimate labor resources available for a particular market.* The characteristics of the workers available (quantity, skills and educational level, wage rates, and unemployment trends) need to be identified for each particular market.

4. *Analyze future personnel requirements.* The program planner should be reasonably assured of the capacity of the market to meet needs in the foreseeable future for the variety of staffing demands to be encountered.
5. *Create personnel strategies.* Likely as not, a security staffing program of any size can feature proprietary and contract security personnel. Personnel needs will vary with the cycle of the organization – seasons, growth or contraction, and special events or untoward incidents.

In commencing a new program, often employees are phased in, rather than being added as a group. This pattern has implications for the use of funds required to finance the program or project. Software-based programs greatly aid efficient use of cash to fund what has to be done. (For more on budgeting, see Chapter 8.)

Job Descriptions

The number of security personnel needed for the project or program and when they are to be phased in must first be determined. Specific tasks and ranks must be set. Then job descriptions for these positions are prepared. These are summaries of the basic tasks required for the position. They serve to establish minimum desired criteria for persons who will be recruited and vetted for the available positions. Job descriptions may include title, tasks to be performed, work conditions, positions reported to, assigned hours, and wages.

Wages and benefits are usually determined by the compensation office, which is usually located within the finance department in large organizations. Wages are set based on numerous factors. These are relative to local pay scales, ranges found nationally for the positions described, corporate pay policy, the capacity of the workplace to compensate hires, and the urgency with which the positions must be filled. Compensation advisory services are often retained to provide pay and benefits advice based on industry norms.

Job descriptions clarify organizational structure and briefly summarize the key performance standards required for the position. The job description also is a basis of comparing the eventual performance of an employee with the original written expectation. Job descriptions vary markedly according to the position. For an entry-level position, they emphasize the minimum skills required (Box 3.2), while those for supervisory positions attempt to identify persons who have had sufficient experience and personnel skills to supervise the work of others even if they previously were employed in a nonprotective position.

Job descriptions for managerial posts normally emphasize years of experience and the nature of responsibilities and career achievements emphasized (Box 3.3).

The preparation of job descriptions is not an idle process. If they are too demanding, the number of individuals in the preemployment pool will be reduced. Further, these terse descriptions might be construed to serve as a basis of an agreement between the worker and the workplace. Job descriptions must always allow for flexibility so that an employee might refuse an assigned task complaining, “That’s not on my job description.”

BOX 3.2 EXAMPLE OF A JOB DESCRIPTION FOR A SECURITY OFFICER

Title: Security Officer

Grade level: (employer may set different grades according to skill and pay)

Hours: (day, evening, night shifts indicated)

Salary range: (usually quoted on an hourly basis for this position)

Major duties and responsibilities:

Working with people:

- Works harmoniously with the public; able to obtain cooperation from persons who are initially difficult
- Able to take prompt, reasonable action to mitigate injuries or risks to members of the public from unexpected events
- Provides necessary and timely assistance to the public in case of injuries or emergencies
- Deters unauthorized persons from entering restricted areas by ensuring that all entering such areas display proper identification
- Provides information and supportive assistance courteously in all contacts with employees and the public
- Is trained or trainable in cardiopulmonary resuscitation and emergency first aid

Working with systems:

- Operates a computer terminal and able of entering new data; writes own coherent and complete reports
- Can use commercially available data-inputting systems
- Monitors access control, alarm, and closed circuit/Internet Protocol television (CC/IPTV) system
- Can be trained to operate a fire alarm command system
- Issues temporary identification documents to visitors

Routine procedures:

- Patrols assigned areas in accordance with procedures and instructions located in the post orders
- Conducts periodic inspections of facilities to identify hazards and prepare reports
- Investigates incidents observed and reported and prepares concise factual written incident reports

Qualifications required:

- Communicates orally in English clearly and courteously
- Writes reports factually and grammatically correctly
- Possesses minimum 5 years' experience in law enforcement, fire safety, or with private security where systems experience was included; or minimum of 2 years higher education from an accredited academic program, preferably in security management, criminal justice, communications, or related fields
- Meets physical standards necessary to perform assigned duties such as:
 - Responding to emergencies, including assisting a person or persons to safety
 - Carrying and operating a fire extinguisher weighing 30 lb
 - Restraining someone psychologically or physically and assisting in removing a disruptive person from the premises (if policy requires such intervention)
 - Driving a vehicle (must have a driver's license)

- Stands, walks, or sits without relief for 2 hours
- Possesses no record of felony convictions or convictions for relevant misdemeanors
- Passes a medical examination including, but not limited to, blood and urine analysis to detect presence of any illegal substances; passes a behavioral screening reflecting the absence of psychopathology

Job descriptions are like contracts with employees and must be prepared with discernment. The above provides an illustration of issues to be considered for an operational security position with considerable public contact.

BOX 3.3 JOB DESCRIPTION FOR A CRISIS MANAGEMENT CENTER CONTROLLER

Summary: Crisis Management Centers monitor 24×7 external events and are the focal points for managing and coordinating responses to incidents that may put employees, visitors, facilities, and the reputation of the organization at risk. The Crisis Management Controller will assume primary responsibility for monitoring global events using news feeds and intelligence. He or she will collate and update risk-relevant data to form ongoing risk assessments and to support decision making in a crisis. He or she will assist with crisis response, ensuring relevant events are escalated and responded to in an effective and timely manner.

Responsibilities:

- Assume primary responsibility for monitoring global events via specified information sources.
- Provide routine reporting based on security issues such as high-risk travel, event-related risk, and other topical threats.
- Manage and update the Crisis Center's risk-relevant data.
- Assist in analyzing the impact of events or threats to the organization.
- Provide ongoing support to the crisis coordinator.
- In a crisis, take responsibility for logging and reporting on the sequence of events and the response of the organization.
- Draft and disseminate crisis communications.
- Respond to and field enquiries from firm-wide stakeholders in a crisis.
- Support the assessment of external information sources.

Skills/experience:

- Excellent written and oral communication skills
- The ability to work well under pressure
- Knowledgeable about world events
- Good organizational skills, with the ability to coordinate multiple requests for information and prioritize accordingly
- Highly responsive and proactive, able to own tasks from start to finish
- Relevant work experience in a risk/security-related field
- Additional language skills preferable
- Problem-solving skills and analytical skills a must

Source: Goldman Sachs.

Negligent Hiring Litigation

The primary reason to implement excellent staffing programs is to attract and retain a cadre of competent, motivated, and productive employees. Another important factor influencing such programs is the fear of a lawsuit resulting from an untoward personal action. Personnel procedures that are not scrupulous could result in hiring a rogue employee whose behavior, for example, could hurt another person or result in loss of assets. This could lead to a charge of negligent hiring. Prudent operational management can reduce the possibility of such a plaintiff's action from succeeding. Such an action is usually lodged in civil courts against the employer-defendant. The action can be based on constitutional principles, case law, common law, or federal or state statutes.

The pressure to take shortcuts in an effort to save money and time can result in the wrong person being hired and then retained into the future. Most employment errors take place because the organization has not created a rigorous human resources (HR) vetting program in the first place. Regardless of the cause, organizations must take a reasonable degree of care in selecting employees and determining if they are fit for the positions for which they are being recruited.¹ If any actionable occurrence results, the specific charges against the defendant-employer may be negligent hiring and negligent retention, which are separate causes of action based on employer negligence.² Negligent hiring occurs when the employer knew or should have known of the employee's unfitness prior to offering that individual a position within the organization. Negligent retention takes place when the employer becomes aware of the employee's unfitness for duty and does not terminate the employee promptly.

In addition, an employer is responsible for certain acts of the employee under the doctrine of *respondeat superior*. This is a concept of vicarious liability in which the employer assumes responsibility in certain cases for wrongful acts of the employee acting on behalf of the employer. However, if the employee acts outside of the course and scope of his or her employment—even when on the job and being compensated at the time—such an incident may not necessarily result in a judicial verdict against the employer. A judge could make a *summary judgment* in favor of the defense in such circumstances. This would permit the trial to proceed with this allegedly errant employee as the sole defendant. By contrast, if the employer could have determined something about the employee from a routine background investigation that would have prevented hiring the person, but did not conduct such an investigation, the employer may be held liable for negligence in hiring.

Other reasons for vetting employees are to assure that certain frequently occurring hiring-related problems do not occur.³ Some examples of these are as follows:

- Hiring people who have too much in common with their interviewers
- Hiring friends of current workers without the connection being made clear in the vetting process
- Employing someone to repay a favor
- Settling for mediocre candidates because of the pressure to fill positions
- Hiring someone for political reasons or for the feeling that one cannot afford the best candidate

- Not probing for limitations, lies, or the lack of relevant details in the prospect's work or education history
- Talking instead of listening while conducting preemployment interviews
- Overselling the position

For whatever reasons, the consequences of failing to vet employees properly prior to making an offer of employment can lead to substantial losses by the employer in a trial (see [Box 3.4](#)). The legal principles pertaining to negligent hiring are not fixed and are thus subject to change, from court decisions and appeals to changing conditions and new laws. Generally, the main requirements of a plaintiff to establish civil liability in which an allegation of injury or damage occurred are as follows:

1. The existence of a *legal duty* by the defendant to protect the plaintiff
2. A *breach* (failure) of that duty
3. *Damage*, harm, or injury as the proximate (direct) cause of that breach

BOX 3.4 NEGLIGENT HIRING: VERIFYING INDICATIONS OF INTEGRITY

The burden of appropriate vetting is incumbent on both proprietary employers and employers of contract workers. In such cases, an employer is obliged to conduct a reasonable investigation into the employee's work experience, background, character, and qualifications. The standard of care does not vary, although the greater the risk of harm, the greater the degree of care necessary to constitute ordinary care.

This is demonstrated in the case *Welch Manufacturing, Division of Textron, Inc. v. Pinkerton's, Inc.* [474 A.2d 436 (1984)]. Welch Manufacturing sued Pinkerton's for losses sustained due to three major thefts connected to a Pinkerton's security guard. Welch claimed that Pinkerton's was negligent in the hiring, training, supervising, and assigning of a guard who was later found to have been a coconspirator in such losses, and that the negligence was proximate cause to the losses. A Rhode Island civil court returned the verdict in favor of Welch. Pinkerton's appealed. The appeals court reviewed Pinkerton's contention that insufficient evidence existed relative to the theories of liability raised in the lower court. The security firm requested that the lower court's decision should be set aside.

THE BACKGROUND

For 30 years, Pinkerton's had a contract to provide security services for Welch, which manufactured gold sunglasses frames for the US military. The Welch manufacturing complex contained sizeable quantities of gold required for these manufacturing purposes. Pinkerton's personnel were aware that gold was stored on the premises. Pinkerton's assigned a 21-year-old part-time employee to patrol the Welch premises during the night shift. The guard had worked in security for Pinkerton's less than 6 months at the time of the assignment. Over the next 45 days, during the night shifts, three thefts occurred at Welch's facilities, resulting in a loss in excess of \$200,000.

An investigation soon identified the new guard as the culpable thief in two of the larcenies. He had resigned by the time the third crime occurred but testified later in the civil suit against Pinkerton's that he provided vital information to parties who robbed the facility of

another \$180,000. In that third crime, the former Pinkerton's guard put a gun to the head of a replacement guard. At trial the erstwhile guard made the astounding admission that he sought the position with Pinkerton's in order to steal from Welch's. He felt that eventually he would be assigned there as he indeed was. But was Pinkerton's negligent in its duty to Welch?

THE DEFICIENT PREEMPLOYMENT PROCESS

Pinkerton's application for employment requested the names of former employers and of three character references. Pinkerton's did not contact the character references. The company did forward reference forms to the applicant's high school principal and to a hospital where the applicant had worked for about 1 month. The forms did not address questions relating to the applicant's honesty and trustworthiness. The hospital provided an employment termination form in which a supervisor checked a box indicating the worker was deemed "good" for "honesty." The supervisor also noted that the worker had failed to report for work on two occasions. Pinkerton's also telephoned someone who had been the applicant's superior officer in the navy for about 2 months, who said that he would recommend the applicant for a job with Pinkerton's.

Pinkerton's lost the case in a lower court and appealed. The appellate court ruled that "Pinkerton's cursory investigation prior to [the applicant's] employment provided it with little current intelligence on him and could well support an inference of negligence in hiring for such a sensitive assignment as the guarding of gold." The court further noted that the applicant had no prior working experience similar to Pinkerton's business. His prior assignment before being assigned to Welch did "not evidence ascending levels of sensitivity." The appeals court dismissed Pinkerton's appeal and affirmed the judgment of the lower court.

THE LESSON

At the time of this incident, which happened in 1973, vetting standards were lower than the levels reached in later years. Indeed, Pinkerton's procedures appeared to reflect the norm of the time. What the case establishes, however, is that an ordinary duty of care requires a reasonable investigation of a security applicant's background, including his or her character. In this case, Pinkerton's did not offer in its defense a single affirmative statement of the candidate's probity from a supervisor or other independent person. If such statements were obtained, an employee nonetheless might steal on the job. But the employer in such a circumstance would have demonstrated good faith in meeting this appellate court's standard.

Source: Maxwell, D.A., 1993. *Private Security Law: Case Studies*. Butterworth-Heinemann, Boston, MA.

In various cases, appellate courts have established criteria for negligent hiring and training. They further identify issues in the failure or omission to take reasonable measures to reduce these risks. Frequently in plaintiffs' actions, the loss prevention director and other individual employees involved in the case may be charged personally as defendants, in addition to the employer. Even if the loss prevention director is defended by attorneys for the employer, such an individual may need to consult independent counsel to protect his or her own interests. Thus, a lawsuit for negligent hiring can require corporate and individual response, involving financial costs, unwanted publicity, and misuse of time, which could have been mitigated by the exercise of reasonable vetting measures. The remainder of this chapter will concern such measures.

The Vetting Process

Hiring the right people can be costly, slow, and frustrating. But highly performing security operations personnel are not deterred from their goals. Even when employment challenges are great, the process must succeed. The astute manager will persevere to obtain the best employees as possible under any circumstances. Organizations thrive or fail based on employee selection.

The entire vetting process can be costly. For entry-level and supervisory employees, vetting involves expenditures to recruit candidates, perhaps to pay personnel agencies, costs of staff time allocated to review applications and conduct interviews, and outlays for background investigations and preemployment testing. Only then can the additional cost of training be contemplated. For managerial or executive positions, costs may involve management recruiters who bear some of the responsibility of vetting. Ancillary expenses are incurred to interview and eventually relocate the successful applicant at the managerial and executive level (Box 3.5).

The personnel process can be partially analyzed according to productivity costs, that is, determining what means of attracting candidates produces the best long-term results. This can vary widely in organizations. One means of attracting candidates for employment can be exhausted or become less efficient with time. The vetting process in security-oriented employment contains a number of distinct phases, as shown in Figure 3.1. The first step is

BOX 3.5 FEDERAL CONTRACTOR SCREENS IN HASTE AND LAPSES RESULT

Positions in the federal government demanding secret or top secret clearances should be beyond reproach, although perfection is not realistic either. Yet the principal federal contractor for screening proprietary and contract employees has come under withering criticism for failure to raise red flags for National Security Agency secret leaker Edward Snowden and Washington Navy Yard shooter Aaron Alexis.

Each year the Office of Personnel Management (OPM) processes about 2.3 million investigations. As part of President Clinton's "reinvent government" initiative, a unit for security and investigations was transferred to an employee-owned company, USIS. This corporation handled around 45% of all federal government checks for OPM. USIS quickly became a lucrative service business employing 7000 with revenues from government contracts of \$344 million in a noncompetitive contract.

Operational-level employees complained that they were pushed to complete investigations quickly, 10 cases due in a single day, according to one investigator. One procedural lapse was the difficulty in obtaining mental health records. The USIS investigators had to drive to the facility where the applicant was treated. Someone there – not necessarily a person who had treated the applicant – would be asked to review the file and sign a form attesting to whether the person posed a threat to national security.

Source: Yang, J.L., 2013. Security vetting fixated on speed, insiders say. Chicago Tribune, September 22, p. 29.

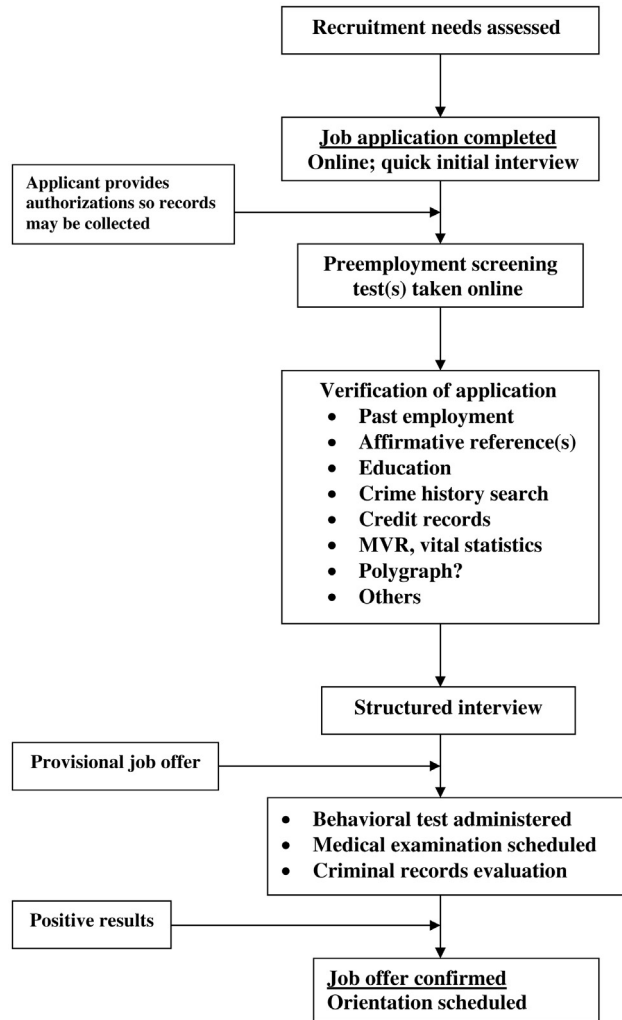


FIGURE 3.1 Stages of the security-oriented vetting process. From initial job recruitment to scheduling the successful applicant for orientation is a linear process. To speed selection and obtain the best candidates for the available jobs, systems are used.

to obtain as large a pool of prospects as possible at a reasonable cost. This process often involves recruiting.

Recruiting

For entry-level positions, most managers desire to attract many candidates to be considered. This is called the applicant pool. The deeper the pool, the greater the choice is. In cases where specific and demanding criteria are established as a requirement for employment, the number of qualified candidates will be fewer. Recruiting expenses hopefully

Table 3.1 Security Recruitment Productivity Worksheet Comparison

Recruitment Method	Completed Applications	Recruitment Cost (\$)	Cost Per Application (\$)
Web site inquiries	—	—	—
Fee-paid Web search	—	—	—
Classified advertisements			
Daily newspaper A	—	—	—
Daily newspaper B, etc.	—	—	—
Sunday newspaper	—	—	—
Display advertising	—	—	—
E-mail responses	—	—	—
Incentives to current employees	—	—	—
Job fair attendance	—	—	—
Personnel agencies	—	—	—
Radio spots	—	—	—
TV spots	—	—	—
Drop-in recruiting office	—	—	—
State employment service	—	—	—
Other	—	—	—

Managers constantly evaluate procedures to determine which ones have the best payoff. In this table, a comparison of different means to recruit new employees is cited. The results can identify recruiting means that bring in the most completed applications and their costs. Other analyses can determine which type of recruiting results in employees who remain with the organization longest or which produce the best results.

should produce a commensurate return with their outlays. That is because better employee selections will result in lower turnover, better performance, and less long-term cost.

A manager is likely to experiment with different means of attracting applicants and determining which methods produced the most desirable results. For example, [Table 3.1](#) shows a simple security recruitment productivity worksheet whereby different recruiting methods can be analyzed for their cost-effectiveness. It identifies cost per completed application, but the final criterion of successful recruiting is the number of successful applicants who are screened and offered a position that is accepted. In addition, it is important to take into account whether the worker makes a positive contribution over an extended period of time. The recruitment method that produces the most acceptable applications may be different from the one that produces the most acceptable employees on a long-term basis. Analysis can help identify the most effective recruitment medium for an employer.

Security program managers must attract applicants so that they can have a large enough pool to select the best candidates for the position. For security guards, a rule of thumb is to receive about 10 applications of interest for every job opening. Apparently higher costs in processing such applications do not deter management because unsuitable candidates easily may be screened out in the process where expenditures are low. Meanwhile, the open hiring process may attract spectacular candidates who otherwise would be missed. If a reasonable number of candidates cannot be found, some employers will opt for filling the available positions with temporary workers and relaunch the job search later. If that's

not the case, the comparative study divides the dollar cost of acceptable applications by the number of applications received. This yields a cost per application, which can lead to a ranking of the most productive means of recruiting. While this sample report is concerned with measuring completed applications, other analyses could identify actual hires, or those employees who remain on the job for 90 days or more. Such results may differ from those based only on applications completed.

Employers of security personnel use a number of strategies to attract applicants. The following are means used for entry-level and supervisory personnel:

- Employer's own Web site
- Internet employment sites
- Personnel agencies
- Classified advertisements in daily or weekend newspapers
- Display advertisements
- Radio or television advertisements
- State employment services
- Incentives to current employees
- Job fairs
- Police benevolent organizations
- College placement services
- Military or Veterans Administration employment services
- Association job placement services such as on ASIS International chapter website
- Health club or community center member recruitment

If some types of recruitment sources begin to pale in effectiveness, high-performance managers turn to other means of obtaining needed applicants. Flexibility on management's part may achieve the desired goal. For example, offering part-time or flexible schedules and unusual incentives may draw applicants who might otherwise not consider applying for full-time work. Similarly, making prospects feel welcome, valuable, and engrossed in interesting and relevant work – like security – may produce qualified applicants who might otherwise pass on the opportunity to work for the organization. Employers may find at times that they must aggressively and imaginatively lure individuals to apply for the positions they have available.⁴

In analyzing the effectiveness of different recruitment sources, a manager may later determine that one type of source is better than another. The results may differ according to the type of security assignments involved and the culture of the employer. For example, a study of newly hired marketing representatives found that employees recruited through college recruitment efforts had better initial levels of performance than did those recruited from newspaper advertisements.^{*,5} The analytical security executive is likely to identify

*Vetting sources must also be aware of the Drivers Privacy Protection Act (PL 103-322) designed to protect personal information of drivers and their vehicles that could be released by any state department of motor vehicles.

which recruiting sources are most productive for the short and long term by monitoring performance of different recruiting sources over time.

The employer's Web site and in-house application workstation are likely to be the most effective means of obtaining successful results. The informative screens should contain job descriptions. A well-developed site will appeal to many applicants. Prospective employees may attach their résumés, a personal statement, samples of achievements, lists of references, and other pertinent information to Internet-based job applications. For the employer, this method of obtaining informative submissions is efficient and low cost, and speeds the review process for the applicants.

The early screens of the site welcome the applicant, provide some general information about the job, identify minimum requirements, and discuss what the process is before a position is filled. As the applicant completes the early part of the application, the process can come to a polite end when it is clear that the applicant does not possess the minimum qualifications. A message thanking the applicant for his or her interest and assuring that the information will be kept for use if a suitable position occurs is given.

For those who do meet the criteria, the applicant might be invited next to take an on-line test that can identify attitudes toward honesty and other personal attributes. Following this details in the application or résumé may be verified.

Applicants for managerial and executive positions may be recruited by outside personnel recruiting firms. These share some of the burdens of vetting candidates during their search before they propose candidates to the prospective employer. Management and executive recruiters usually charge the employer a percentage of the successful applicant's beginning annual compensation; in other cases, a flat fee may be charged, regardless of success.

In-Person Prescreening

Anyone who physically presents himself or herself to a personnel office and requests an application for work should be provided one readily, even if no positions are currently available or are likely to be in the foreseeable future. To do otherwise could risk the perception of discrimination and subject the organization to a civil action for employment discrimination. However, if no positions are currently available or likely to be in the foreseeable future, a posted notice or a receptionist may inform potential applicants of this situation. At their option, job-seekers may then complete electronically or physically an application that can be filed for possible future consideration when positions become available.

On the receipt of a completed application from such a candidate, a clerk or manager may conduct a brief interview to provisionally ascertain the facts of the application and to inform the applicant of the subsequent steps in the employment process. The brief informal interview also helps establish the communication skills of the applicant.

The Application

The application is management's opportunity to obtain information needed to determine whether the applicant should be considered for further background screening and

BOX 3.6 THE EMPLOYMENT APPLICATION: HOW MUCH IS ENOUGH?

Some employers of security personnel use simple application forms that require directory-type information and little more. This is not a wise practice for security positions. The application process provides the organizations with the ability to inform the applicant about the philosophy, activities, and culture of the company. To obtain verification of background information, a consent form needs to be signed and dated. If the workplace desires educational verification and records, separate authorization forms are usually necessary for each institution. Applicants are informed that they must successfully pass drug and criminal background checks prior to a final offer of employment. In some cases a polygraph examination might be a requirement for which a release is included in the application.

a possible offer of employment. For most of the past century, applications were completed on paper forms. However, organizations increasingly enable the applicant to enter information directly into a computer terminal within a personnel office or complete the application on the company's Web site. The quantity of information required from the applicant on the employment form differs widely based on the strategy of the employer. The degrees of detail and the thoroughness of the evaluation process also reflect the employment philosophy of the employer (Box 3.6). Long applications discourage some applicants from completing the process due to their arduous nature. However, some security and HR managers believe that a lengthy and detailed application produces stronger applicants who are more likely by extrapolation to be careful and detail-oriented on the job. Clearly, longer applications also provide the workplace with more information with which to make an informed decision on the applicant.

Vetting methods from the application process to the point of finally offering a position of employment involve aspects of privacy as well as questions of fairness and accuracy. A balance between the rights of the applicant and the needs of the employer must be maintained. This is particularly true for employers of protection personnel. For security-related positions, more information generally is requested of applicants than in other types of employment. Regardless of the length of the application, some minimum information is required. Directory-type data – current address, phone, and Social Security number (SSN) – are required, as well as work and educational history. The specific questions asked of new prospective employees on applications have been shaped in recent years by various federal laws. The main federal laws affecting preemployment standards are as follows:

- The Fair Labor Standards Act (FLSA) of 1938 *et seq.* requires certain employers to pay their workers a minimum hourly wage and to pay time-and-a-half for hours worked more than 40 in a given workweek.
- Title 7, Civil Rights Act of 1964, as amended by the Equal Employment Opportunity Act of 1972, prohibits employment discrimination on the basis of race, color, national origin, sex, and religious practices.

- The Occupational Safety and Health Act (OSHA) of 1970 (29 USC 651 *et seq.*) created an administration to develop and promulgate occupational safety and health standards, to develop and issue regulations, to conduct investigations and inspections to determine the status of compliance with safety and health standards and regulations, and to issue citations and propose penalties for noncompliance with safety and health standards and regulations.
- The Rehabilitation Act of 1973 (29 USC 701 *et seq.*) prescribes discrimination against individuals with disabilities by the federal government, federal contractors, and recipients of federal financial assistance (see also the Americans with Disabilities Act (ADA) below).
- The Employee Retirement Income Security Act (ERISA) of 1974 is the federal law that sets minimum standards for most voluntarily established pension and health plans in the private sector. In the past employees and would-be workers have sued employers on drug-related and wellness requirements.
- The Vietnam Era Veterans' Readjustment Assistance Act (VEVRAA) of 1974 (38 USC 4212) requires that employers with federal contracts or subcontracts provide equal opportunity and affirmative action for Vietnam-era veterans and others on active duty.
- The Pregnancy Discrimination Act of 1978 prohibits sex discrimination on the basis of pregnancy by amending Title VII of the Civil Rights Act of 1964.
- Executive Orders 11246 and 11375, and Revised Orders 4 and 14 (Affirmative Action) bar discrimination on the basis of race, color, religion, national origin, or sex in federal employment and in employment by federal contractors and subcontractors.
- Title 42, United States Code, Section 1983 (Civil) guarantees citizens of the United States or other persons within its jurisdiction from the deprivation of any rights, privileges, or immunities secured by the Constitution and its laws.
- Title 18, United States Code, Section 242 (Criminal) protects citizens and others from discrimination by reason of color or race and allows for criminal penalties against offenders.
- The Fair Credit Reporting Act (FCRA) of 1971, as amended, restricts certain credit information about individuals. Some states have enacted even more restrictive legislation than the federal act. (By contrast, credit information about businesses is not restricted and is available to anyone willing to pay for it from commercial services.) A credit report contains two parts – a credit header and a credit history. A credit header is frequently important for employment purposes as it provides the SSN, age, phone number, recent addresses, and any known aliases. Credit header information – or full reports – may be obtained only after receiving written permission from the individual involved.
- The Immigration Reform and Control Act (IRCA) of 1986 requires that employers verify the eligibility of each employee to work by completing INS Form I-9.
- The Employee Polygraph Protection Act (EPPA) of 1988 prohibits the use of polygraph examination in the private sector, unless excluded by terms of the Act.
- The ADA of 1990 (42 USC 12101 *et seq.*) provides broader coverage than the Rehabilitation Act. It prohibits employers with 15 or more workers from

discriminating against qualified persons based on their disabilities. Some states also have enacted similar state statutes on the basis of disability. It is important to recognize that knowing what constitutes a disability is not always clear and can change over time (Box 3.7).

- Genetic Information Nondiscrimination Act (GINA) of 2008 prohibits the use of genetic information in health insurance and employment. The Act makes it illegal to deny group health plans and health insurers solely on the basis that a person has a genetic predisposition to develop a disease in the future.
- The Employment Nondiscrimination Act (ENDA) has not been passed but has been introduced almost every year since 1994. It prohibits discrimination in hiring or employment on the basis of sexual orientation or gender identity.

BOX 3.7 DEFINING WHAT IS A DISABILITY

The Americans with Disabilities Act (ADA) of 1990 defines a disabled person as someone who has a physical or mental impairment that substantially limits one or more major life activities, has a history of physical or mental impairment, or is regarded as having a physical or mental impairment. The nature of specific disabilities is in a constant flux related to court decisions that modify what employers may or may not exclude in considering the applicant. The Equal Employment Opportunity Commission (EEOC) is the principal agency that regulates ADA and certain other employment laws. Sometimes the concerns about excluded positions have led to searching questions for security and human resources managers. For example, does wearing glasses constitute a disability? Or may security employers be forced to hire convicted felons because they are in a protected class?

The ADA modifies the hiring process, but guidelines are compatible, nonetheless, with the desire of achieving a competent and effective workforce. The employer must be aware, however, of the ADA's context. Applicants who are "qualified" and able to perform "essential functions" of a position with or without "reasonable accommodation" may be in a protected status to receive employment consideration. The employer may insist on the following guidelines:

1. The disabled individual must satisfy the prerequisite of the established position. Certain levels of experience and education are typically permitted prerequisites.
2. The individual must be able to perform essential job functions with or without reasonable accommodation. A key factor is whether a particular job function is essential. For example, a position requiring a security officer to communicate with the public verbally could exclude a candidate who is mute. However, if verbal communication was not an essential job function, the employer might make "reasonable accommodation" by permitting a mute employee to work in other tasks where verbal skills are not required and communication by other means could be used. Historically, if an applicant for a security position had a conviction for a misdemeanor or felony, he or she would be automatically screened out for the position. Today, in some states, "qualifying" misdemeanors may be means of automatically rejecting a candidate, but not others.
3. In terms of defining "reasonable accommodation," employers only have to provide accommodation if it does not present the organization with "undue hardship." This is further defined as "requiring significant difficulty or expense." The employer is held to ADA

standards that are related to size of the corporation, number of employees, and the cost of the accommodation necessary to render the disabled person capable of performing the required work to established standards. That is, the larger the organization, the greater the expectancy is that the employer will be able to absorb the difficulty or expense of adjusting to such accommodations.

Source: Greenhouse, L., 1999. Justices wrestling with the definition of disability: is it glasses? False teeth? New York Times, April 28, p. A26.

Existing measures may be further strengthened by subsequent modifications in rules and regulations. Also, state measures may expand on federal coverage. As a result of these proscriptives, application forms are limited in what they may or may not ask. Such limitations may change at any time based on new rulings in case law and passage of federal and state legislation. These have evolved by making employers more attuned to nuances of questions that could prevent denial of opportunities to a spectrum of the population that has experienced employment discrimination in the past.

The employer has a legal obligation to verify essential information in the application, particularly for security-related positions. This is a vital process because applicants may deliberately or inadvertently provide incorrect or misleading information in their applications and résumés. Verification of references and other relevant information should be completed substantially or fully before a formal interview is scheduled.

Social Media

In recent years the use of social media in the vetting of prospective employees has been a much discussed topic. If information on someone is available on the Web, no expectation of privacy exists. Therefore, why shouldn't a security or HR worker check social media for insights to the applicant that are valuable?

The problem is that information gleaned from social media collection may be biased or incorrect. The prospective employer could draw deleterious conclusions if assumptions were not verified by independent means. Social media can be positive for an applicant, revealing characteristics that were not apparent from the vetting process. Despite the ambiguous legal basis for integrating social media checks into a vetting process, many workplaces find the process valuable and irresistible.

Ban the Box

For much of the past century employers would include check-off boxes as part of the employment application. Many still use these in the electronic format. However, one venerable question concerning arrest is now illegal in over a dozen states. The Equal Employment Opportunity Commission (EEOC) has conducted a national campaign to inform employers that the box asking about past arrests should be eliminated. Some people are

arrested in the exercise of their political rights; many others are arrested for charges that are dismissed at the police station or the court house.

What concerns management is the hiring of someone who has a criminal record of convictions that should have screened out this person before being hired. But the EEOC concludes that many persons are adversely affected early in the application process if they are asked about arrests. Convictions are another matter. The employer can and should ask about misdemeanor or felony convictions as part of the application process. A separate criminal record check can confirm the matter. This line of questioning is best saved for near the end of the vetting process so no discriminatory references can be drawn.

Security employers have higher standards than for other employment sectors concerning past criminal convictions. Any felony convictions may serve to exclude an applicant for consideration in security employment. Misdemeanor convictions may or may not be the basis for exclusion, depending on the nature of the offense, the age of the offender at that time, the extent of the punishment, and how long ago the incident occurred.

E-Verify

About 11 million unauthorized immigrants are living in the country and about 70% of them are in the workforces. Congress and some states require that employers take appropriate steps to safeguard jobs for authorized employees. Employment eligibility verification process must be in place. E-Verify is a free Internet-based system operated by the Verification Division of the Department of Homeland Security's US Citizenship and Immigration Services (USCIS) and the Social Security Administration (SSA).

The federal government and many states require verification for the right to work as a matter of law. According to a US Government Accountability Office study, about 2.3% of employees screened received nonconfirmation of status to work. This was based on a study of 14.9 million queries from nearly 222,000 employers.⁶

References

Most applications request references of applicants. Generally, these may be of two types: employment-related or personal. Of these two, employment-related are more significant in that they relate to workplace attitude and proficiency. Personal references tend to be biased and are usually not job-oriented; therefore, most employers place emphasis on job-related sources for information about the applicant. Some employers request personal references but never act upon them. However, government and private sector positions requiring a high level of integrity in their hires may request character references in addition to those linked to past or present employment. Self-serving personal references from applicants' mothers and best friends are not convincing. Employment verifications and confidential references from applicants' former supervisors, however, carry much weight.

References may be vetted by clerks telephonically, by written requests, or by a combination of both. Letter of recommendation should come from persons who have a defined relationship with the applicant. Preferably, the applications are submitted on professional

stationary. However, formatted letters of recommendation sent via a protected Internet link are satisfactory. Employers give highest credence to letters that speak about the relevant experience of the applicant and the sense of unbiased comment on his or her character and ability. Questions on interpersonal and communication skills are important for most security positions. Questions on leadership are relevant for those seeking management and executive positions. Applications should be signed – even electronically – by the letter writer.

Some organizations turn to investigators or contract services to aid them in their reference checking, or turn most of the process over to such organizations. As noted earlier (Box 3.4), the failure to obtain a single affirmative statement of probity concerning a candidate can lead to a charge of negligence in hiring. This would occur in the event that an employee had a relevant personal history experience, capable of negating consideration for employment that was not revealed on the application but that a reasonable effort on the employer's part would have discovered. See also discussion on SSN below.

Employment Verification and Continuity

References and employment evaluations from an applicant's previous direct supervisors are valuable, perhaps critical, to employers in making a decision on whether to hire that person or not. Some employers are reluctant to permit their supervisors and managers to share candid insight on a departed worker's performance and personal behavior. They fear possible civil suits for slander or liability from workers who may be denied an employment offer based on such negative statements. However, supervisors and managers who speak truthfully and without malice about a former worker, even while revealing negative aspects about the worker's employment history, rarely are targets of litigation that is sustained by the court.

Astute security-conscious employers look carefully for any gaps in employment in the applicant's work history. These are not necessarily red flags of trouble. Employment gaps may reflect time needed to find new employment after one job has ended, or it can reflect time off for education, training, relaxation, or healthcare. Such a gap also could reflect jail or prison time or other involvement with the criminal justice system. Careful evaluation should determine why employment gaps have occurred.

In addition to personal and employment references, verification of other information in the application should be undertaken. Such inquiries generally require the approval and sometimes cooperation of the applicant. Managers should always be aware that information derived from commercial services requires careful evaluation. Errors occur despite best intentions. A decision not to hire someone on the basis of a single negative finding cannot be justified, and is unfair. Commercial services greatly expedite the cost of conducting a comprehensive, relevant, and generally accurate collection of the applicant's records. However, the employer is able to accomplish the same objectives in collecting information by in-house investigators or personnel staffers using available credentials checking manuals, directories, and Internet databases.⁷ Such information includes the following:

- *SSN verification.* Congress never intended SSNs to become national identifiers, but they are. Once issued, an SSN is permanent and is only changed under extraordinary

circumstances. A genuine SSN remains one of the most important indicators that the applicant is who he or she says he or she is. Guides to understanding the SSN explain the information revealed in the distinctive numbering sequence.⁸ SSN verification can indicate the state and approximate year of issuance.

The importance of SSN as an identifier remains. Therefore, all employers – and individuals – have an obligation to take reasonable efforts to protect the privacy of such numbers. Employers in many cases have stopped using SSNs as internal identifiers since this process is gratuitous and provides a private bit of information to a large audience without justification. The SSN remains vital for both credit checks and criminal record searches. However, an applicant may be victimized by another person who is currently using or has used that person's SSN for unauthorized purposes, an example of identity theft. This crime could occur without the victim-applicant's knowledge. Hence, problematic information revealed through an SSN check should not be the sole basis, without further confirmation, of eliminating a candidate for employment consideration.

- *Credit history checks.* The use of credit reports may be important as part of conscientious preemployment verification. In most cases, the employer is not concerned with the applicant's level of debt or credit use information. (The exception is for employees working in the financial industry and those with fiduciary duties.) Employers rather wish to obtain factual directory-type information from an independent source. Therefore, employers or their data brokers usually request only "header information" or "credit header" on the applicant, rather than the full credit report. Major credit bureaus deliver reports instantly to authorized data brokers and, due to the automated nature of the business, costs for such reports are low. However, prospective employees must specifically authorize the employer to undertake a credit search. A statement of the applicant's rights must be provided that the applicant should read before authorizing the search by signing the release. Three major credit bureaus are supported by hundreds of independent local and regional credit collection businesses. Both credit bureaus and their customers should be familiar with terms of the FCRA as amended. The full text of the FCRA and notices of rights are available on www.ftc.gov/bcp/conline/edcams/fcra/index.html.
- *Military history.* Employers generally are not allowed to ask about the nature of discharge of applicants with military service history. However, asking whether the applicant is registered for Selective Service or if the applicant was a member of a branch of the armed forces is acceptable. The applicant may obtain a standard form (DD214) detailing his or her personal military service history. It provides information on training specialties, ranks achieved, dates of service, and type of discharge (although this may not be requested specifically). Locations and dates of foreign service, awards, and distinctions received are cited. Disciplinary information may be revealed. However, offenders have the opportunity to appeal to a military court, subsequent to the time any punishment has been discharged, and request that the

court seal the records of any criminal or other charges. In this situation, the potential private sector employer would not be aware of such potentially troublesome factors in the applicant's military background.

Employers may help their applicants obtain a DD214 by providing them with form SF 180, Request for Military Records Form. This may be downloaded from www.nara.gov/regional/mpsrf180.html.

- *Motor vehicle reports (MVRs).* Even if the applicant is not expected to drive a vehicle in the course of his or her intended employment, an MVR check may be wise. The record provides directory-type information and may also reveal other facts about the candidate that could be important in arriving at an employment decision. For example, the MVR may reflect an address different from the one that appears on the application. The employer would wish to determine the reason for this difference during the interview process. Further, if the applicant must or could potentially drive in the process of employment, the logic of an MVR search at the onset of employment consideration is apparent. MVRs contain directory-type information but also data on height, weight, eye and hair color, date of birth, and when the license was issued. Violations, recent convictions if authorized to be collected, accident data, and other factors also are provided according to regulations of many states. Employers may use the services of a professional records verification service (see below) or contact state motor vehicle agencies directly to obtain such information. Each state maintains its own separate databases of licensed drivers, vehicle registrations, ownerships, accident reports, and other information such as title history and liens. No national, all-inclusive database on MVRs is in existence. States must comply with the federal Driver's Privacy Protection Act that limits personal information that can be included on a record.
- *Civil record searches.* While filling a management position, an employer may wish to evaluate the civil records of the applicant. Such searches can identify possibly concealed information about the candidate, including other names used, addresses, former employers, and the existence of judgments, lien bankruptcies, and pending litigation. Although many types of liens and Uniform Commercial Code filings are available free of charge, an information broker or a commercial records checking service would expedite the process. In addition, the expertise and time required to retrieve them explains why many larger employers farm out this task. In some states and cities, telephone queries are answered, while such information is increasingly available over the Internet. For a list of state and local sites with free Internet access, visit www.brbpub.com.
- *Criminal history.* Employers in protective services are eager to determine, and rightly so, whether prospective employees have a criminal history that would render them unsuitable for a position of trust. The applicant's fingerprints are checked against those of known criminals or wanted persons. Currently about 20 states and the District of Columbia perform such vetting as part of the guard licensing process. States may require such vetting for other categories of employees

such as teacher, child care workers, medical personnel, and numerous other positions as defined by state or local statutes. The state may conduct a search only through its own criminal justice database. This would identify convictions for felonies and misdemeanors and open arrest warrants known only to that state. A better strategy would be for the search to involve the FBI's national database of offenders and wanted persons as discussed below. State legislation can make this possible.

In the past, employers often believed that *any* arrest or conviction for a criminal offense should automatically lead to a rejection of the candidate. However, today many factors have changed employers' way of thinking about this issue, reflecting the position that certain types of arrests or convictions should not necessarily block a person from obtaining employment for a security position. The key factors are the relevancy of the candidate's offense to the nature of the security work anticipated and the particulars of the offense. Relevant details include the age of the offender at the time of the crime, how long ago it occurred, its severity, and the presence or absence of subsequent illegal behavior since the offense originally took place.

Criminal records are public documents. However, since states keep their records in different locations and have their own procedures for releasing them, access can be frustrating for security or HR personnel unfamiliar with the process. Most criminal records are retained at the county as well as the state levels. Over 5000 locations exist within the United States where such criminal records may be found. Depending on the locality, such records may be obtained by mail, fax, commercial service, the Internet, or in person. Fees for providing copies of the records and supporting documents often are charged. Usually, search information requires the person's full name, date of birth, years to be searched, and SSN.

Potential employers are advised to consider relevant felony and misdemeanor records only in evaluating the candidate's total credentials for employment. That is, currently many counties also provide arrest records that did not lead to conviction. For the sake of employment consideration, such information must not be considered. However, sometimes in the process of conducting a background investigation, an employer may discover an open arrest warrant for the applicant, often in a distant jurisdiction. Under such circumstances, the employer should contact local law enforcement immediately.

The obtaining of criminal history records is highly desirable for comprehensive background investigations of a new candidate. A potential employee may sign a criminal background check release form, including SSN, date of birth, any aliases used, and a driver's license number to expedite the search. This form should be witnessed and may need to be notarized. Alternatively, an employer may ask an applicant to obtain a Certificate of Good Conduct from police departments of the communities in which the applicant has lived. This should not be considered a definitive record since the applicant may have committed a crime and been convicted and punished in a different jurisdiction from the one in which the

applicant is currently residing and from which he or she is supplying good conduct documentation.

Employers of security personnel can satisfy their needs for criminal records in communities in which state security guard registration exists and in which the state vets all such applications through the National Crime Information Center (NCIC) database maintained by the Federal Bureau of Investigation. The NCIC collects and organizes records provided to it by state criminal justice agencies. Thus, if an NCIC check does not reveal the presence of a criminal record, an employer may have a high level of confidence that the applicant has not been convicted of a crime that makes him or her unfit for security employment, as defined by the offenses cited as relevant in the states that require NCIC screening for security personnel. Such information is not available instantaneously. Fingerprint checks for criminal cases are processed by NCIC within hours. But nonpriority record searches require several weeks to complete. Unless prevented by law, most private sector employers will allow employment to begin before results of the NCIC fingerprint check have been completed. This may not be advisable. (For further discussion, see Chapter 9.)

Is it possible for the applicant to possess a criminal conviction and yet not have it revealed by comprehensive police record checks? Yes. One way is by an error in the record-keeping process, such as the failure of authorities to receive such information from the state or local level. Another way is for the applicant to appeal to a court for a certificate of relief to be granted after discharge from incarceration or termination of parole. This certificate seals the offender's record from public scrutiny. An exception is for certain government jobs in which the applicant must agree to have records of the offense unsealed temporarily for scrutiny by government employment background investigators. Additionally in some states youthful offenses are sealed automatically by the court after a period of time has passed in which no further offenses have been recorded by the youth.

In some employment situations, even a "clean" police record does not necessarily mean that the applicant does not have a past felony conviction. However, a diligent review of the applicant's work history dates should reveal any unexplained time gap that could reflect jail time or other reasons to give the employer pause.

- *Educational records.* Over 4000 postsecondary academic institutions and programs exist in the United States. About four out of five of such institutions will verify degrees received and years of attendance of past students and graduates. Some educational institutions will confirm such requests by phone, mail, and fax, usually without charge. The employer can provide a Request for Educational Verification signed by the applicant for those institutions that do not readily provide such information.

If the employer desires a transcript of academic records, a release generally is needed, including the student's name, year graduated, campus attended, and SSN. At some institutions, e-mail requests by students for transcripts are accepted. The student's signature is required in order to release a transcript to a third party. The student may request that the transcript be mailed directly to the prospective

employer, in which case the envelope should be retained and be considered part of the document. The transcript normally will include an embossed (raised) institutional seal attesting to the authenticity of the document. Institutions usually charge modest fees for providing transcripts.

The trend in recent years is for educational institutions to be tighter in providing data on an applicant's educational experience than in earlier years. The reason for this is the Family Educational Rights and Privacy Act (FERPA) that protects the privacy of student education records. Workplace experience confirms that 25–35% of all job applicants falsify information concerning educational background. Higher institutions have blocked or deterred release of student records because they claim they fear penalties from FERPA violations. However, an expert states: “Zero times in the history of FERPA has a college been penalized for violating the law.”⁹

- *Other records.* Prospective employers may scrutinize other information provided by the applicant. Some examples are vital statistics, workers' compensation records, and licenses. Verification of such data may help raise the confidence level the employer has in the applicant. Such information also sheds light on the applicant that might otherwise not come to the attention of the employer. Professional licenses and certificates may reveal such information as the date of issuance, current status, expiration date, and field of certification. A license and a certification are strong indications, but not a guarantee, of competence.

Prospective employers have a right to ask candidates to bring in their actual diplomas and certificates to be scrutinized, photocopied, and returned to the applicant. Copies of the records are stored in the applicant's dossier. While these can be counterfeit, experienced HR and security personnel usually can separate the original from copies by inspection. An Internet search can quickly identify if documents provided by applicants derive from genuine institutions, subject to recognized accrediting organizations, or are bogus diploma mills.

Nowadays most certifications expire after a period of time, typically 3–5 years. It is the duty of the applicant to keep a certification up to date. Similarly, the workplace should verify that the license or certification is current. Disciplinary information from candidates usually is not available from the granting authorities. In many cases, a person disciplined by an organization responds by resigning from it. Nonetheless, it is reasonable to document credentials offered by a potential worker prior to offering him or her employment.

The Polygraph

Efforts to determine individual honesty go back a long time. Many of the techniques developed to identify honesty were crudely related to observations that psychological stress modifies behavior and physiology. The early Chinese gave suspects rice powder to take into their mouths, respond to a charge, and then ordered to spit the rice powder out a few moments later. If it was dry, then the person was believed to be dishonest. This was based

on the premise that lying affected emotion, which, in turn, had a measurable physiological effect. In this case, deception was believed to lower saliva production.¹⁰ In other cases, truth seekers used methods to detect lies that were hardly reliable or based on scientifically established criteria. These included the Ordeal of the Red-Hot Stones and the Ordeal of the Red-Hot Iron.¹¹ If the suspect survived the walk on the coals or the touch of the iron, he or she was deemed to be innocent of the charges.

Determining what constitutes a lie and what constitutes the truth is not always clear. Deception in many applications is a normal part of life. Not surprisingly, it frequently occurs when a person wishes to obtain employment or some other benefit and suppresses information that could damage that opportunity. But in employment circumstances, the nature of the information required tends to be specific. A prospective employer might desire unequivocal responses to certain questions, such as “Are all the facts in your application for employment true?” or “Have you ever stolen any item from a previous employer valued at more than \$25?” The answers to such questions, if reasonably obtainable by some objective measurement, can be valuable in an employment decision. This was an expectation of polygraph examinations widely administered in the United States until the late 1980s.

Polygraph examinations originated in the nineteenth century, when Cesare Lombroso, an Italian criminologist, invented a blood pressure recording device that recorded pulse and blood pressure changes occurring as subjects were being questioned. William Multon Marston, a US lawyer who also studied psychology, publicized the possibilities of using Lombroso’s device to aid in distinguishing truth-telling from deception.¹² The first practical use of a polygraph was undertaken under the leadership of August Vollmer, police chief in Berkeley, California. Vollmer assigned John A. Larson and later Leonarde Keeler to develop the modern device. The instrument collects human physiological responses to various yes or no questions. The device measures and records minute blood pressure changes as questions are posed. The recorder graphically displays changes in pulse, respiration rate, and galvanic skin response (otherwise known as perspiration).

Prior to the data collection phase of a polygraph examination, examinees usually are put at ease and are informed on how the examination will be conducted. The examiner endeavors to convince the examinee of the reliability and certainty of findings from the examination that follows. Sensors then are attached physically to the subjects. They are asked a series of relevant questions about substantive matters, usually interspersed and contrasted with irrelevant ones. The polygraph examiner establishes a baseline from physiological responses to irrelevant questions and uses the points of comparison of relevant questions to irrelevant ones. Deviation in the pattern may indicate deception. This is called the relevant/irrelevant technique.

Experience of the examiner is critical in arriving at a deceptive/not deceptive/inconclusive determination. Examiners will spot an anomaly, stop the recording, inform the examinee that the indication suggests deception, and ask the examinee to provide an explanation. Some examiners in recent years use computer analysis of responses received in an attempt to identify deception.

Over most of the twentieth century, many law enforcement units, government, and private industry in the United States used the polygraph as a means of determining deception in preemployment vetting, criminal investigation, and for other purposes. But given the relativity of truth itself, is the polygraph reliable for such use? In 1984, a Department of Defense research report summarized 42 scientifically based studies concerning the polygraph under varying circumstances. The report observed that the polygraph could create two kinds of errors.

False-negative errors are erroneous decisions that an individual is not speaking falsely when he or she is actually deceptive. *False-positive errors* are erroneous decisions that a person is being deceptive when he or she is being actually truthful. These are the most frequent types of error likely to be committed by an examiner. Nonetheless, the report concluded cautiously: “Used with prudence, and a full knowledge of its limitations, the polygraph will continue to play a role in our criminal justice system and counterintelligence operations.”¹³ But what of the private sector?

A year later, the Office of Technological Assessment (OTA), the research arm of the US Congress, conducted its own review and assessment of scientific evidence on the validity of polygraph testing. The review occurred at the request of the House Committee on Government Operations.¹⁴ OTA’s findings underscored the broad utility of polygraph examination in numerous applications, but concluded that unanswered questions remain about the validity of polygraph use in some circumstances, especially preemployment screening.

By the mid-1980s, according to an estimate based on a survey conducted by the American Psychological Association (APA), as many as 5 million polygraph examinations were administered in the private and public sectors, mostly concerning private sector employment.¹⁵ Most polygraph examiners at the time believed that this estimate was far too high. A Congressional report put the number of polygraph examinations at “over a million” a year – 300,000 of them for employment purposes alone in the private sector.¹⁶ About 20,000 federal polygraph examinations also were administered each year. But Congress, facing pressure from unions, passed the EPPA of 1988 (29 U.S.C. 2001 *et seq.*).

This Act sought to discourage the widespread use of polygraph testing in noncriminal investigations and it succeeded in that regard. EPPA prohibited most private employers from using polygraph examinations either for preemployment screening or during the course of employment to detect any unreported workplace theft. With the passage of this law, use of the polygraph decreased substantially in the private sector. However, federal, state, and local government retained the right to use the polygraph as part of their employment decisions, and some governmental units, particularly in intelligence, continue to do so.

Nonetheless, the polygraph was not totally excluded for use in preemployment circumstances. The Act permits polygraph tests to be administered in the private sector, subject to restrictions, to certain prospective employees of security service firms. These include security guards and armored car and alarm monitoring and response employees. Specifically, Section 2006 of the EPPA does *not* provide blanket exemption

on the use of preemployment polygraph testing for uniformed and plainclothes security personnel. The exceptions are if personnel are being engaged in facilities, materials, and operations concerned with production, transmission, or distribution of electric or nuclear power; public water supply facilities; shipments or storage of radioactive or other toxic waste materials; and public transportation of currency, negotiable securities, precious commodities or instruments, or proprietary information.

EPPA does not elaborate on what constitutes “precious commodities or instruments” or “proprietary information.” Most security service providers, large and small, routinely have not required polygraph screening since the passage of EPPA. Conceivably employers meeting conditions of EPPA could request that prospective security employees be vetted by a polygraph examination. This request is most likely to be relevant in a specific incident investigation when a small number of individuals have access to critical information in a loss. It would be up to the security services provider to consider this request. Like other factors in employment decisions, polygraph examinations have limitations (Box 3.8). Other measures have grown in use and are discussed in the next section.

BOX 3.8 BEATING THE POLYGRAPH: THE ALDRICH AMES CASE

Use of the polygraph by the military, law enforcement agencies, and national security staffs has provided such success that government received exemption from the polygraph limitations cited in the Employee Polygraph Protection Act (EPPA) of 1988. However, nobody claims that results from a polygraph examination are infallible. Spies have been trained to overcome the skills of an experienced polygraph examiner by using tranquilizers, biofeedback techniques, or pressing toes down at critical points during questioning.

The most serious breach of security in the US intelligence system occurred despite the fact that the convicted traitor, Aldrich Ames, was given routine polygraph tests by the Central Intelligence Agency over an 11-year period. During his nefarious work for the Soviets, Ames was able to identify to the KGB at least 11 clandestine CIA agents, 4 of whom were executed.

How was Ames able to overcome a system that appeared to have worked well in the past? Ames, a veteran CIA case officer, seemed to do nothing more devious than act in a friendly way with his polygraph examiner. Ames first started working with the KGB in 1985 for cash payments that eventually totaled about \$3 million. The year after he began spying, Ames was recorded as deceptive on a polygraph question related to his personal finances. In 1991, deception also was reflected on a question as to whether he had ever worked for the Soviet Union. In both circumstances, Ames was given 4 days to rest and then retake the polygraph examination, which he then passed. The deception on Ames's 1991 relevant question as to possible spying was not forwarded to the FBI until 2 years later. Hence, it might be said that Ames did not “beat the polygraph,” but that he “beat the system” of evaluating such readings.

Sources: Waller, D., 1994. How Ames fooled the CIA. *Newsweek*, May 9, p. 24; Stein, J., 1995. Lie detectors lie (tell the C.I.A.). *New York Times*, February 15, sec. 4, p. 13; <http://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames>.

Despite the low scientific basis for polygraph testing, the process continues as part of vetting for certain federal security positions. The process is considered valuable because the questioning allows the examiner to elicit admissions stemming from fear of the process. In some cases, examiners will ask the individual to return for a second session.

Preemployment Testing

Applicants for employment may be screened by a variety of standardized objective instruments. These “tools” are designed to measure personality, aptitudes, interests, and achievements of potential employees. Test anxiety should be minimized and coaching on how to achieve the desired results should be considered unethical. Different types of test instruments are available to employers, which will be discussed in the following sections.

Psychological or Behavioral Stability

For some positions, prospective employers will wish to be assured that all reasonable efforts have been made to identify and assess relevant psychopathology in the applicant. Such testing is complex and invariably involves collaboration with a licensed psychologist trained in psychometric testing methods. The potential employer normally is not interested in classification, etiology (causation), methods of diagnoses, and other facets of abnormal psychology, as interesting as they may be. The employer's goal is to authorize relevant tests that can identify abnormal traits that could lead to dangerous or otherwise unacceptable work performance from such employee. For example, an employer might be considered unethical if candidates for employment as armed officers or for executive protection work are not screened for mental disorders.

A licensed psychologist with experience in personnel selection typically has many psychological instruments from which to choose as part of a behaviorally oriented screening process. Two widely used include the Minnesota Multiphasic Personality Inventory (MMPI-2) and the Sixteen Personality Factor Questionnaire (16PF).

The MMPI-2 (the ‘2’ indicates a major new version introduced in 1982) is a self-report test of 567 true–false questions. The MMPI was developed in the 1940s to assess psychological adjustment problems in mental health settings. It evolved empirically by establishing true–false questions that separated groups of individuals: one with known psychiatric problems (e.g., anxiety, depression, and schizophrenia) and the other “normals.”¹⁷ Uses of the MMPI include preemployment screening, evaluation for promotion, performance assessment, disability evaluation, and return-to-work evaluation. MMPI is also used experimentally to explore how personality factors are related to job success.

An individual taking the MMPI answers true–false questions, which are assigned T-score values on different scales (e.g., scale 1, hypochondriasis; scale 2, depression; and so on). Profiles are then drawn for comparisons to normals; these profiles can be created for highly specific employment circumstances. The MMPI-2 includes an updated normative

sample for seven regions of the United States, eliminates gender and sexual orientation language, and is balanced for demographic characteristics.

The value of the MMPI-2 as a screening instrument has been widely recognized. The psychologists J.N. Butcher and S.A. Coelho describe the scales that are valuable in evaluating candidates for law enforcement and protection employment:

Thus, it appears that common personality problems to be wary of in selection of police and security personnel include applicants who are impulsive, superficial, overactive, manipulative, easily frustrated, and immature. These personality traits are likely to show up in pre-employment screening as elevation on scales 9 (mania), 4 (psychopathic deviate), 3 (hysteria), or 1 (hypochondriasis).¹⁸

Under the ADA, MMPI-2 is considered to be a medical test and, therefore, should be administered only after a conditional job offer has been given to the applicant. MMPI-2 test results should not be placed in an employee's personnel file due to ethical requirements mandating confidentiality of psychological and medical information. They should be filed separately and securely. MMPI-2 results should not be used solely as a basis to deny individuals employment consideration. Proper interpretation – conducted by a licensed psychologist – requires a review of the results in the context of an individual's life history and assessment of current behavioral functioning.¹⁹

A newer MMPI-2-RF was published in 2008, and contains only 338 true-false questions. This newer psychological instrument was developed to shorten the time required for completion (usually 30–50 min). As a newer test, the research literature on its validity is evident. The employers' professional psychologists will likely describe the strengths and weaknesses of the newer form.

A person taking the MMPI (or any psychological instrument) may decide to overreport (exaggerate) or underreport (deny) a behavior being assessed by the test. MMPI-2 includes four validity scales intended to measure a person's test-taking attitude and tendency to fake results. One validity scale tests for lies, another identifies a quality of randomly selecting answers, a third scale identifies randomness only in the last half of the test, and the fourth identifies people with profiles in the normal range but who actually have signs of psychopathology. This design of the MMPI has made it attractive in numerous workplace applications.

Another psychological personality test used extensively for security employment in the United States and Canada is the 16PF; currently in its fifth edition. The 16PF has been the subject of more than 4000 published research articles. Like the MMPI-2, the 16PF requires professional users to have had graduate training in psychological test interpretation. Also like the MMPI-2, the 16PF is considered part of a "screen out" assessment strategy for psychopathological potentials. The state of California currently requires it in the selection of all state police officers. The 16PF, which is composed of 185 items, is faster to administer than the MMPI-2. Testing can be self-administered through a reusable booklet or via computer interface.

But such psychological tests are only part of a screening process. J.M. Fabricatore, a psychologist who critiques such psychological instruments, emphasizes the importance of considering testing results as only one factor in an employment decision:

*Every security administrator/selection executive/chief of police would dearly love to have a 10-min. unfakable psychological test that costs \$3, can be scored in 30 seconds, be interpreted by a non-professional, is ADA/EEOC invulnerable, and has a predictive validity of 0.99. The difficult and complex truth is that selecting applicants for security/law enforcement assignment is always a human judgment.*²⁰

The 16PF questionnaire has 185 questions that usually can be answered in 25–35 min. Many employers schedule prospective employees to take a personality assessment online. Results are analyzed by an interpretative report.

The Clear Purpose Test

In contrast to personality psychological tests, another type of test is much more widely applied in preemployment screening for security personnel. Many security employers – large and small – screen all prospective employees with a test instrument that identifies specific personality and behaviorally oriented traits, particularly concerning attitudes toward honesty. Unlike the MMPI-2, the 16PF, or others of the genre, these “clear purpose” tests may be administered before an offer of employment is contemplated. Indeed, a version may be offered to the applicant when he or she enters the employment office for the first time or accesses the employer’s online employment application process.

The term “clear purpose” refers to testing goals that focus on specific qualities of importance to a security program employer. Such factors as integrity, propensity of drug or alcohol use, potential for using safe practices at work, and likelihood of being terminated from employment for cause are obviously significant issues on the minds of employers. A clear purpose test may signal the presence of one or more undesirable workplace traits. For most of their history, these tests have been called paper-and-pencil instruments, and were often self-administered with a pencil and booklet. But increasingly, the test-taking process involves interface with a computer, in an employment office or over the employer’s Web site. Results are scored instantly. Other test-scoring variations exist, including mailing, faxing, or e-mailing answer sheets to the test publishers for scoring and providing results.

Because of the importance of employee honesty, employers have been eager to embrace objective preemployment testing as part of the evaluative process. Tests that focus on integrity traits have grown in importance for entry-level employees in certain industries. These preemployment screening instruments have achieved substantial support among security-conscious employers for a number of reasons (see [Table 3.2](#)). Test publishers have issued two types of measurements, either one of which – or both – may be included in the same test. The first type is referred to as an overt integrity test and measures theft attitudes. This type of test includes questions about frequency and extent of theft and

Table 3.2 Preemployment Integrity Screening Methods Compared

Screening Methods	Convenience Issues	Main Problems	Main Advantages
Integrity tests (also called “clear purpose” tests)	Can easily be made part of the usual screening procedure, even in initial electronic applications	Company representative(s) must be trained to appropriately use test scores Not all integrity tests are thoroughly validated Should not be confused with clinical personality testing	Validity evidence exists Generally nonoffensive No adverse impact (meet EEOC guidelines) May discourage dishonest applicants from applying
Personal interviews	Usually part of hiring procedure and are often time-consuming	No evidence of validity with theft criteria Difficult to determine applicant’s truthfulness in discussing theft and counterproductive activity Can lead to charges of bias or discrimination	Inexpensive (already part of hiring procedure) Structured interviews show more promise than traditional interviews
Reference checks	Are often time-consuming	Little evidence of validity Most misconduct is undetected Previous employers reluctant to give negative information	May increase truthfulness of applicants Verifies information provided on application forms and résumés
Criminal background checks	Commonly available through services, yet lengthy turnaround no longer required	Not all criminals are on record Likely to exhibit adverse impact Information obtained must be job-relevant Many states are introducing restrictive legislation	Complete, reliable, verifiable data can be obtained (although the process may be burdensome)
Credit checks	Quick but somewhat costly	Relevance to theft not clear May not meet EEOC guidelines	Obtain information relevant to financial need and fiscal responsibility. Header data can be compared with what the applicant provides

Source: Adapted from Jones, J.W., Terris, W., 1989. Selection alternatives to pre-employment polygraph. *Recruitment Today*, May/June, pp. 24–31.

counterproductive activity in general, one’s punitiveness and rumination about theft, the perceived ease of theft, and an assessment of one’s personal integrity.²¹ The second type of test asks applicants to self-report their frequency and amount of theft and other illegal or counterproductive activity.

Other Tests

Another type of test, labeled as “disguised-purpose” or “covert,” is linked to normal-range personality devices. These are broader in scope and are not explicitly aimed at theft. The

items do identify other desirable features in employment such as dependability, conscientiousness, social conformity, thrill-seeking, trouble with authority, and hostility.²²

Still another preinterview questionnaire is created from a pool of true–false items. The instrument identifies a set of questions that, it is believed, are related to specific aspects of reliable and productive work behavior and can differentiate against a population with contrary responses.²³ These criterion-keyed true–false questions plot the test takers' responses for numerous scales, including emotional maturity, trustworthiness, conscientiousness, and safe job performance.

Other areas to consider with regards to preemployment personality tests include those given in the next section.

Testing the Tests

Employers can select from numerous test publishers. These publishers should meet certain criteria so that their tests follow legal and privacy considerations, including:

- *Reliability (consistency)*. Tests should produce the same results from individuals who are retested. Publishers demonstrate this quality by retesting and determining coefficients of agreement between the original test and the retest.
- *Validity (accuracy)*. Does the test deliver what it is supposed to? Test publishers use a variety of research strategies to establish validity. These include correlation with polygraph test results, correlation with anonymous admissions, the use of a time series to examine aggregate rates of inventory shortage before and after the introduction of a test program, and the comparison of test performance by groups hypothesized to differ in integrity (e.g., felons compared with test takers without criminal records).²⁴
- *Legality*. The testing instrument must follow federal and state statutes relating to preemployment screening. If an applicant is denied employment in part because of scores from a preemployment test and institutes a legal action against the would-be employer, the test publisher must be prepared to demonstrate how its test conforms with such laws.
- *Utility*. Assuming that a test meets the criteria of validity, reliability, and legality, its utility to the workplace must also be established. Major reviews of integrity tests were undertaken by the OTA in 1990²⁵ and by a panel from the APA²⁶ in 1991. The OTA report was critical about integrity testing, but neither called for legislative remedies nor suggested alternatives. The APA report supported the validity of such testing, but generally criticized test publishers for their failure to cooperate with independent researchers to enhance knowledge of such measurements.

The OTA report found no studies conducted by independent researchers in which detected theft was used as the criterion. However, a few years after the OTA report was released, H. John Bernardin and Donna K. Cooke, at Florida Atlantic University, studied a group of 111 employees hired by a major retail convenience store chain over a 3-year period.²⁷ The

researchers found that a test designed to detect deviant/nondeviant characteristics successfully predicted theft for a group of convenience store employees. No significant differences on the test emerged as a function of race, gender, or age. Other studies have identified the value of such tests in reducing counterproductive behavior in the workplace.²⁸

Finding Applicable Test Instruments

Hundreds of test publishers exist and thousands of tests are on the market. How does a manager narrow the candidates for consideration? Since 1992, the Association of Test Publishers (ATP) has been a nonprofit organization representing sources for tests and assessment tools concerning selection and screening instruments. ATP is committed to advance best practices in testing. The organization maintains a list of test publishers from which details on individual tests and services may be obtained (www.testpublishers.org).

The Buros Institute of Mental Measurements and the Buros Center for Testing, both associated with the University of Nebraska at Lincoln, provide services to users of commercially published tests. These include analytical reviews and information, available online, on almost 4000 tests, covering all aspects of applied instruments (<http://buros.org>).

Job-Related Skills Testing

Employers know from experience that prospective workers differ in terms of personal abilities and behavioral characteristics. Apart from integrity and counterproductive behavior, prospective employers can identify specific minimum levels of skills required for the workplace. For example, security employees who must write concise, coherent reports can be tested on their writing abilities. Or those who interact with the public routinely can be evaluated on their interpersonal problem-solving traits. Employers may learn from experience that certain personal characteristics are the marks of high-performing employees in their industry and can obtain standard tests to use as a means of identifying the presence of these desired characteristics. A vocationally oriented psychologist can aid employers in selecting such tests.

Fitness for Work

Some positions require physical fitness in order to adequately perform them. For example, the employer may determine that security personnel need to be able to carry a portable fire extinguisher for a given distance and use it. Or the position may require the worker to be on his or her feet for a certain period before relief. Further, in nonsecurity employment physical wellness is vital. Simple and reasonable tests can identify the employees' fitness to work. In some cases annual physical examinations may be required, for example, for workers in transportation who have control of a train, bus, truck, or plane. It is the duty of management to ascertain what kinds of physical tests, if any, are required at the minimum for a position being filled.

Another aspect concerns psychological fitness. Employees have committed suicide, taking the lives of others in the process, because they were depressed and suicidal



FIGURE 3.2 For certain kinds of employment, workers must possess physical and mental wellness. Security, human resources, and operational personnel need to assure fitness for service in risky jobs. Andreas Lubitz (a) was copilot in 2015 of a commercial jetliner that he deliberately crashed, resulting in 150 deaths (see debris in 'b'). He had growing vision problems and also was depressed. Two physicians informed him that he was too ill to work. But his employer, the airline, did not receive this information.

(Figure 3.2). In such low-frequency, high-consequence events, management needs to examine if it has taken all reasonable steps to keep the public and its employees from performing in tasks that could result in suicide, harming others. Similarly, workers who have extended hours of employment and are at risk of accidents or injuries to others present risks. Management needs to be reasonably assured that workers are fit physically, mentally, and by alertness to perform the functions for which they are employed.

Reviewing the File

In an ideal situation, at this point in the vetting process, a candidate for employment might have had a brief interview, completed the detailed application, and have taken a clear purpose preemployment screening test online. Meanwhile, personnel have used the time to verify information contained in the application. This method has saved costly assets of the organization – especially, interview time – from being deployed wastefully in interviewing candidates who do not meet the requirements. An applicant may be scheduled for an interview as the applicant's employment folder is being completed.

The Final Employment Interview

Due to the time required, this is the most costly aspect of preemployment screening. Nonetheless, interviews are fundamental in evaluating prospects for security employment before making a final decision. Many reasons exist for this widely used selection procedure. First, written and verbal references are valuable in providing insight into the applicant's fitness for the particular position, but can be incomplete. A personal interview can help elucidate missing information from references. Next, the information collected prior to the interview often contains details that are divergent with responses provided by the applicant on the application form. The interview provides an opportunity for these

uncertainties to be explained. Finally, the interview process may help the employer to determine the ability of the applicant to explain why she or he is interested in the position and why he or she would or would not perform the job well.

The interview has many flaws. The applicant may be coached to answer questions in a certain way in order to please the interviewer, although it fails to reveal the true motivations behind seeking the position. Also, some interviewers have biases that prevent them from objectively identifying the best candidates for the available position. Indeed, computer-based interviews might accomplish the same goals as face-to-face integrity interviews, with greater objectivity and speed as well as less cost.²⁹ In addition, the face-to-face interview presents an opportunity to examine a candidate's nonverbal communication skills, something that a computer-based employment screening system cannot yet accomplish at this point of development. Also, some candidates might not accept a position in an organization in which they were not offered the opportunity to be interviewed personally. Finally, in positions of critical importance, the opportunity to raise probing questions and ascertain how the applicant deals with critical possibilities is afforded by the interview process. Just as the application form – paper or electronic version – must avoid discriminatory-type questions, the face-to-face interview must do the same (Box 3.9).

BOX 3.9 FAIR AND UNFAIR PREEMPLOYMENT INTERVIEW QUESTIONS	
State and federal employment regulations guide what may or may not be asked on applications and during interviews. The employer's labor lawyer or state and local human rights officials can direct employers to variations in prohibited questioning or screening practices. Questions related to race, religion, and ethnic or national origin is prohibited. The following are other general topics of what is fair or unfair to ask:	
Unfair Inquiries	Fair Inquiries
Name: maiden or spousal	Have you ever used a different name while employed? Does your spouse or a close relative work here?
Address: own one's home	What is your current address?
Age of applicant	Will you be older than a certain age, say 21, at the time the job will begin?
Height or weight	Not to be asked
Religion	Not to be asked
Citizenship	Will you be able to complete an I-9 form (to prove his or her right to work in the United States)? Are you a US citizen?
Arrests	Have you ever been convicted for a felony or for (specified) misdemeanors?
Marital status or dependent children	Does the applicant have any reason why he or she might not be able to work certain hours if the job ordinarily would require it?
Military discharge	Request a DD214 as part of the screening process
Medical history	Require medical tests before a final offer of employment is extended
Submit a photograph	May be taken once a job offer has been made

Interviews might be in the form of a single individual session, several sessions over an extended period of time, a panel involving two or more interviewers with the interviewee at the same time, or a combination of these. The trend at the entry level is to conduct more than one brief interview so that a variety of candidates can be compared by different interviewers. At the management and executive level, the trend is toward multiple contacts over an extended period of time with different persons involved, all of whom eventually pool their observations before a decision to offer a position is made.

The interview may last from a few minutes to over 1 hour. The interview process itself can be construed to be a test. Therefore, interviewers should assure that the questions raised relate to requirements of the job. Typically, interview types are divided into several categories:

- *Structured.* The questions follow a progression and often are prepared in advance. The interviewer may ask each of the prepared questions to every candidate.³⁰ This is the most frequently used interview style, although aspects of other types may be included. Interviewers take this opportunity to ascertain technical and interpersonal skills of the applicant. Interviewers are likely to ask a series of open-ended questions that require the applicant to respond at length, rather than with a yes or no answer. An example of an open-ended question is: “Tell me about a problem you encountered in your previous position and how you overcame it.” Open-ended questions are most pertinent for individuals seeking management-level positions.
- *Unstructured.* This type of interview is freer in form and often seems random, with features of an informal friendly conversation. Information about the applicant, nonetheless, is likely to be copiously provided by the candidate, but it may not be adequately job related to serve the interests of the skillsets for the position to be filled.
- *Depth.* This style is used for careful evaluation of the candidate’s fitness for a particular critical position. It will review carefully contents of the application form and raise hypothetical situations calling for on-the-spot problem solving by the applicant.
- *Panel.* To the applicant, interviews by two or more people at the same time may seem more stressful, but this is not necessarily so. Panel interviews permit several interested persons within management to make a collective decision and to permit the same verbal responses and nonverbal cues to be evaluated by more than one person from the same interaction with the applicant.
- *Stress.* This type of interview is similar to the structured type except that it introduces difficult and sometimes challenging questions to the applicant to ascertain how he or she might react. In some cases, this interviewing format poses questions for which no plausible answer is available or for which the applicant is highly unlikely to possess the information required in order to properly answer the questions. During such an interview procedure, questioners are unlikely to signal to the applicant if his or her response is satisfactory. This type of interview is not popular with private sector applicants and is more likely to be encumbered in screening for high-stress law enforcement, military, and intelligence positions.

Interviews are more art than science. The interviewer seeks to project an atmosphere that leads to candid responses that will help the workplace make an informed decision (Box 3.10).

BOX 3.10 PREEMPLOYMENT REFERENCE SHEET

Opening the interview:

- Develop rapport.
 - “Tell me a little bit about yourself.”
 - “What are three words that describe you?”
 - Note if the interviewee is mirroring behavior.
- Establish a behavioral norm.

Honesty and integrity:

- Inform the interviewee what areas will be covered.
- Applicants will disclose deleterious information if they:
 - Believe past indiscretion will be discovered
 - Are allowed to rationalize behavior
 - Minimize the seriousness of actions
 - Are allowed to feel bad about previous actions

Rationalizations:

- Shows understanding
- An assumptive question: “Some people leave a few jobs off their résumé because they only worked there for a few days. How many jobs did you leave off your résumé?”

Types of questions:

- Assumptive:
 - Best used if believed there is derogatory information
 - Gets closer to the truth: “In the past year, how many times were you written up?”
- Enticement:
 - Used to challenge a statement by the applicant and assess commitment to answer: “Is there any reason why a past employer would have anything negative to say about you?”
- Behavioral questions:
 - Seek to identify critical incidents likely to arise on the job
 - How will the candidate respond: “Tell me about the time you had to bend the rules?”
- Probing questions:
 - Designed to elicit more information of a specific nature
 - “How did you react to that pressure?”
- Paraphrased questions:
 - Use the applicant’s response in the form of a question that requires the applicant to expand upon an earlier response
 - “You called the manager?”
- Open-ended questions:
 - Tend to invoke a more lengthy description or narrative from the applicant
 - “What was your primary challenge at your previous company?”
- Closed-ended questions:
 - Used to confirm facts through yes or no responses
 - Do not encourage the applicant to speak freely: “You have had four jobs since college?”

- Leading questions: not advisable normally:
 - Should be avoided because they indicate the answer that the interviewer desires
 - “Don’t you think it’s important to be detail-oriented in this position?”

Source: Wicklander-Zulawski, 2014.

Promising research years ago suggesting that interviewers might be trained to spot “microexpressions” and draw useful conclusions from them has not panned out.³¹ However, government guidelines and liability protection force employers to screen out potentially dangerous applicants. The interview is an important part of the process that cannot be omitted. Tech-savvy workplaces may conduct the interview via two-way video, but distance from the workplace site is no excuse for eliminating this step.

Assessing the Candidates

With the completion of the preemployment screening process, management must now decide which candidates should be offered positions. All the information that has been collected will be assessed. This may be conducted by HR or security managers who have met the candidates or by an independent reviewer within the organization who has not personally met the candidate. The latter option is meant to prevent bias or lapses in the screening process from affecting a balanced employment offer decision.

To determine whether the employer discriminates against a protected class in its testing or screening process, data should be retained on who passes the process and who fails. If the pass ratio of the percentage in the protected group is less than four-fifths of the majority group, the employer may be creating an adverse impact, according to the law.³²

Example:

Percent passing from the protected group: 50

Percent passing from the majority group: 75

Ratio = $0.50/0.75 = 0.667$ or 67%

However, four-fifths = 0.8 or 80%

Therefore, this hypothetical test does not meet requirements of the “four-fifths rule” and would not be in compliance with EEOC guidelines. The employer would be advised to reevaluate the screening process, determine why some groups are being excluded, and revise the screening process in accordance with the findings.

Preemployment Drug Screening

Many workplaces have a preemployment drug testing policy. Such screening may be required as a matter of law. Drug and behavioral testing occurs after a conditional offer of employment has been made. All applicants should be informed in writing of the

organization's substance abuse policy and drug screening procedures. In cases in which the potential employer conducts work on behalf of the federal or state government, such a policy is a legal requirement. For example, Title V of the Omnibus Drug Initiative Act of 1988 includes a provision with the short title of the Drug-Free Workplace Act of 1988 (PL 100-609) that all businesses contracting with the federal government and all grantees receiving federal financial assistance must certify that they have in place policies directed toward the creation and maintenance of a drug-free workplace.³³ The Act does not specifically require preemployment drug screening. However, many organizations establish such a procedure as a policy to conform to the objective of the Act. Drug test policies may go beyond preassignment. If the policy is administered uniformly, drug test usage may be random, for reasonable suspicion, for cause, following treatment, prior to promotion, and postaccident.

Prospective employees should be requested to sign an informed consent form to permit substance abuse testing. This notice may state that a confirmed positive test result may lead to a rejection of an employment offer. The form may also state that the failure to consent to the test will result in the application process being incomplete, hence not leading to a final offer of employment.

Screening test samples are usually analyzed in clinical laboratories experienced in such procedures. The usual technique is an enzyme multiplied immunoassay technique (EMIT), which analyzes the urine sample of the prospective employee. (Saliva tests may also be selected for identifying a wide variety of drugs.) The lab process determines the presence of a drug or drug metabolite by comparing a test sample of urine with a reference solution. The test requires about 90 s to produce a reading. A positive reading for the detection of substances tested requires an additional confirmatory test before results are shared with the applicant or a decision about employment should be made by management. A second test, with greater specificity than that of the initial procedure, then is conducted before a final determination about rescinding the provisional offer of employment.

An example of this type uses test technology such as gas chromatography/mass spectrometry (GC/MS). Preferably, the test is conducted on the initial urine sample. Organizations should engage the services of clinical laboratories meeting high professional standards to minimize false-positives and to assure test accuracy while minimizing cost of the tests. Employers and their drug-screening laboratories know that some prospects who use illegal substances will try to "beat the test." They may dilute their urine by drinking excessive water or substances such as vinegar that sometimes confuse the test result. (Test-adulterating substances are sold over the Internet.) Also, simply avoiding consuming illegal substances a few days prior to a urine test can be sufficient to result in no adverse finding. For example, alcohol is cleared in 10–12 hours, amphetamines in 1–2 days, cocaine in 2–30 days, and prescription drugs in 1–6 weeks.

Hair testing can identify a drug history going back up to 90 days. Results produce twice as many positives as urine or saliva. However, the process is more intrusive requiring 100–120 strands of hair from the crown of the donor's head. (If necessary, usually hairs

from other parts of the body may be analyzed.) Hair testing for drugs of abuse requires only about 24 hours, plus another 24–72 hours if the sample must be retested.

Medical Test

The employer may decide that a medical examination for general health determination also might be required after a conditional offer of employment. This may occur when the applicant has had physical disabilities in the past and the employer requires a medical opinion on the potential for recurrence of the problem.

The Final Offer of Employment

Following the collection of all relevant information on the applicant, including behavioral measurements and drug and medical documentation, a final offer of employment is extended. The individual is welcomed and transferred to HR to commence work. In the case of certain managerial positions, the new employer may wish to assure that no violation of a noncompete agreement signed at a previous employment exists. The next step in the employment process is orientation and training, subjects of great concern to successful security operations management.

Summary

The secret of success in many organizations is to hire and retain the right people. Reliable preemployment screening is at the core of successful operations management. This is particularly the case for protection programs. Security personnel are selected in much the same way as other workers in an organization; however, higher standards for determining applicants' previous legal, moral, and ethical behavior guide employment decisions.

Discussion and Review

1. Why is it incumbent on employers of security personnel to vet prospective employees more thoroughly than in nonsecurity positions?
2. In a civil action, how can a claim of negligent hiring have a greater chance of succeeding?
3. What is the risk to security operations managers if they are personally cited in a civil action involving a claim of negligent security?
4. What are the inherent risks of personal references? What are the desirable reasons for retaining such procedures despite their limitations?
5. How have technology and the Internet changed preemployment screening?
6. Several federal acts protect the privacy of individuals. If an employer in the process of screening an application discovers an open arrest record for an applicant, what is the recommended course of action?

7. Does the EPPA make an exception for certain employers? If so, who are they? Under what circumstances would it “make sense” for an employer to require certain employees to be vetted by a polygraph examination?
8. Explain the difference between reliability and validity in preemployment tests.
9. Under what circumstances might a test for psychological stability be highly desirable in employing security personnel?
10. Explain how the “four-fifths rule” serves as a means of identifying employment bias.
11. To what extent should the workplace peruse applicants through social media sites? At what point is the prospective employer invading the privacy of an applicant?

Endnotes

- ¹ Service, J.G., 1988. Negligent hiring: a liability trap. *Security Management*, January, p. 65.
- ² Chuvala, J., Gilmere, J.A., 1992. Legal consequences for negligent retention, supervision, and training of employees. *Secur. J.* 3 (2), 87–90.
- ³ Fischer, R., quoted in *ibid.*
- ⁴ Rhodes, S., Springen, K., 1997. Economy: yup: help wanted. *Newsweek*, January 13, p. 52.
- ⁵ Werbel, J.D., Landau, J., 1996. The effectiveness of different recruitment sources: a mediating variable analysis. *J. Appl. Soc. Psychol.* 26, 1337.
- ⁶ US Government Accountability Office, 2011. Employment verification: federal agencies have improved E-Verify, but significant changes remain. US Government Accountability Office, Washington, DC, GAO-11-330T, February 10.
- ⁷ Rosen, L.S., 2008. *The Safe Hiring Audit*. Facts on Demand Press, Tempe, AZ.
- ⁸ *Ibid.*, pp. 184, 186.
- ⁹ LoMonte, F.D., Student Press Law Center, quoted in Kelderman, E., 2014. Privacy laws: boon for students or shield for colleges? *Chronicle of Higher Education*, October 31, p. A8.
- ¹⁰ Kleinmutz, B., Szucko, J., 1984. Lie detection in ancient and modern times: a call for contemporary scientific study. *Am. Psychol.* 39, 766–776.
- ¹¹ Barefoot, J.K. (Ed.), 1994. *The Polygraph Story*. American Polygraph Association, Washington, DC.
- ¹² Lykken, D.T., 1981. *A Tremor in the Blood: Uses and Abuses of the Lie Detector*. McGraw-Hill Book Company, New York, NY.
- ¹³ Department of Defense, 1984. *The Accuracy and Utility of Polygraph Testing*. Department of Defense, Washington, DC.
- ¹⁴ U.S. Congress, Office of Technology Assessment, 1983. *Scientific Validity of Polygraph Testing: A Research Review and Evaluation – A Technical Memorandum*. U.S. Congress, Office of Technology Assessment, Washington, DC.
- ¹⁵ American Psychological Association, 1991. *Questionnaires Used in the Prediction of Trustworthiness in Pre-Employment Selection Decisions: An A.P.A. Task Force Report*. American Psychological Association, Washington, DC.
- ¹⁶ See Endnote 14, pp. 3, 25. Also see Hearings on S. 1815. Senate Committee on Labor and Human Resources (Prohibited Use of Lie Detectors), 99th Congress, 2B Session, April 23, 1986.
- ¹⁷ Butcher, J.N., Coelho, S.A., 1997. The Minnesota Multiphasic Personality Inventory-II (MMPI-2). *Secur. J.* 8, 121–124.
- ¹⁸ *Ibid.*

- ¹⁹ Sumpster, G.F., 1997. Review of the Minnesota Multiphasic Personality Inventory 2. *Secur. J.* 8, 125–127.
- ²⁰ Fabricatore, J.M., 1997. The Sixteen Personality Factor Questionnaire (16PF). *Secur. J.* 8, 162.
- ²¹ Sackett, P.R., Wanek, J.E., 1997. Integrity testing: an overview. *Secur. J.* 8, 11–18.
- ²² *Ibid.*
- ²³ Borofsky, G.L., 1997. The Employee Reliability Inventory (ERI). *Secur. J.* 8, 55–60; Rain, J.S., 1997. Review of the Employee Reliability Inventory (ERI). *Secur. J.* 8, 61–63.
- ²⁴ Sackett, P.R., Wanek, J.E., 1997. Integrity testing: an overview. *Secur. J.* 8, 11–18.
- ²⁵ Office of Technology Assessment, 1990. The Use of Integrity Tests for Preemployment Screening. Office of Technology Assessment, Washington, DC.
- ²⁶ Goldberg, L.R., Grenier, J.R., Guion, R.M., Sechrest, L.B., Wing, H., 1991. Questionnaires Used in the Prediction of Trustworthiness in Pre-Employment Selection Decision: An APA Task Force Report. American Psychological Association, Washington, DC.
- ²⁷ Bernardin, H.J., Cooke, D.K., 1993. Validity of an honesty test in predicting theft among convenience store employees. *Acad. Manage. J.* 36 (5), 1097–1108.
- ²⁸ Kuhn, R.A., 1990. The attack on employer's rights. *Secur. J.* 1, 74–80; Borofsky, G.L., Klein, H.J., Davis, W., 1993. Pre-employment screening for unreliable work behaviors: an opportunity to work cooperatively with human resource managers. *Secur. J.* 4, 185–192.
- ²⁹ Jayne, B.C., 1997. The utility of a computer interview to screen for positions of public safety. *Secur. J.* 8, 205–208.
- ³⁰ Shea, C., 2014. The liar's 'tell.' *The Chronicle Review*, October 17, p. B6.
- ³¹ Still, D.J., 1997. High Impact Hiring: How to Interview and Select Outstanding Employees.: Management Development Systems, Dana Point, CA, p. 139.
- ³² *Ibid.*
- ³³ Fay, J., 1991. Drug Testing. Butterworth-Heinemann, Boston, MA, pp. 23–24.

Additional References

- Abrams, S., 1977. *A Polygraph Handbook for Attorneys*. Lexington Books, Lexington, MA.
- Arnold, D.W., Jones, J.W., 2002. Who the devil's applying now? *Security Management*, March, p. 85.
- Black, I.S., Yeschke, C.L., 2014. *The Art of Investigative Interviewing*. Butterworth-Heinemann, Waltham, MA.
- Carlson, J.F., Geisinger, K.E., Jonson, J.L., 2014. *The Nineteenth Mental Measurements Yearbook*. University of Nebraska Press, Lincoln, NE, (new editions every 2 years).
- Fields, G., 2004. Security Vetting of Employees Is Highly Prized. *Wall Street Journal*, February 24, p. B1.
- Gale, A. (Ed.), 1988. *The Polygraph Test: Lies, Truth and Science*. Sage Publications, London.
- Hetherington, C., 2007. *Business Background Investigations*. Facts on Demand Press, Tempe, AZ.
- Hetherington, C., 2015. *The Guide to Online Due Diligence Investigations: The Professional Approach on How to Use Traditional and Social Media Resources for Investigators*. Facts on Demand Press, Tempe, AZ.
- Hinton, D., 2002. *Criminal Records Book*. Facts on Demand Press, Tempe, AZ.
- Leeds, J.P., 1997. Security and law enforcement pre-employment testing. *Secur. J.* 8 (1–2), 1–208, (special issue).
- Lykken, D.T., 1974. Psychology and the lie detector industry. *Am. Psychol.* 29 (10), 725–739.

- Rosen, L.S., 2012. *The Safe Hiring Manual*, second ed. Facts on Demand Press, Tempe, AZ.
- Sankey, M., 2008. *The Public Research Records Tips Book*. Facts on Demand Press, Tempe, AZ.
- Sankey, M.L., Hetherington, C., 2008. *The Manual to Online Public Records*. Facts on Demand Press, Tempe, AZ.
- Sawyer, D.C., 2014. Line Up a Screening Strategy. *Security Management*, March, p. 64.
- Spies, R.A., Plake, P.S., 2005. *The Sixteenth Mental Measurements Yearbook*. University of Nebraska Press, Lincoln, NE.
- Vaughan, J.F., 1999. *Avoiding Liability in Premises Security*, fourth ed. Strafford Publications, Atlanta, GA.

Further Reading

Employment test publishers. <www.testpublishers.org>.

Workplace test reviews, information, and psychometric counseling. <<http://buros.org>>.

Training and Development for High Performance

Training is everything. The peach was once a bitter almond; cauliflower is nothing but cabbage with a college education.

—Mark Twain, *Pudd'nhead Wilson*

The training of employees and the development of their skills and careers are critical and time-consuming activities within security operations. Successful training is directly linked to high performance on the job. High standards are more likely to be achieved with a relevant, engaging period of learning. Successful training ensures that employees meet the short-term needs of the employer, while further development enhances their long-term skills and career paths. Training and development also provide the organization with employees who better absorb the corporate culture and who are prepared to meet future needs of the workplace. In organizations of all sizes, the chief security officer (CSO) or senior security manager is likely to maintain a close interest in training and to devote considerable time to this activity.

Numerous approaches regarding training and development have been applied throughout the history of management. The organization needs to establish the training and development resources required and how to teach new employees their tasks.

Security practitioners at all levels must constantly learn more about their trade craft. Training and education not only helps work become more satisfying for individuals but also produces direct benefits to the employer.

Security as a vocation is constantly changing. Skills need to be kept up to date. Relevant knowledge must be shared with workers as soon as its criticality becomes apparent. Unlike a skilled craft in which a period of apprenticeship is expected, security knowledge and procedures at the operational level can be taught much more quickly than in an apprenticeship. Nonetheless, security personnel in the United States generally are undertrained relative to their growing public expectations and duties.

Why Train Anyhow?

Training provides employees with skills and information needed to do the job safely and effectively. However, additional factors underscore the importance of security training. The following are the factors why training is essential in high-performance security programs:

Table 4.1 Statutory Requirements of Security Guard Regulations (*N* = 51)

	1998		2010	
	<i>N</i>	%	<i>N</i>	%
Any security guard regulations	43	84	46	90
Minimum age requirement for unarmed guards	21	41	43	84
Proof of citizenship or permanent residency	14	27	35	67
Fingerprint check and full-face photo	24	47	30	59
Formal written application used	–	–	34	67
An application fee charged	–	–	35	69
Minimum level of education required	3	6	15	29
Background check required	20	39	43	84
Denial for past misdemeanor related to security	–	–	4	8
Unarmed training required	8	16	23	45
Armed training required	3	6	14	27

Security guard employment in the United States has increased in recent decades. Since 9/11, requirements for security guards have risen in all areas, as this table shows, although they still remain at a low level relative to law enforcement.

Source: Nalla, M.K., Crichlow, V.J., 2014. Have the standards for private security guards become more stringent in the post 9/11 era? An assessment of security guard regulations in the US from 1982 to 2010. *Secur. J.*

1. Local and state statutes require security training in many states. The basic requirements in these states generally remain low, but the trend to expect more continues. Preassignment or initial training is required in a number of states, and the trend for such state-mandated learning is continuing. In 1986, 12 states required preassignment training for unarmed security officers. By 2000, that number had grown to 18 and in 2006 21 states required preassignment or initial training before being placed on assignments. Requirements for armed security officers are broader. From 22 states in 1986, mandated training requirements increased to 33 states in 2000.¹ Since the attack of September 11, 2001, pressure for preassignment and postassignment training of security personnel has grown further. By 2010, 46 states and the District of Columbia had at least some security guard regulation. Background checks had grown from 20 in 1998 to 43 twelve years later (Table 4.1).
2. A few states also require in-service or refresher training for security guards. According to a survey of the industry, 23 states require training of unarmed or armed security officer or both.² Some cities enforced statutory requirements for security guards. For example, applications for guards in Los Angeles must undergo a fingerprint check and full-faced photo and meet physical requirements, while Glendale does not. Whereas Glendale denies security guard employment for past misdemeanors related to security and imposes uniform requirements, Los Angeles does not.
3. Armed security officers historically have had more required or expected training than nonarmed personnel. The vast majority of security officers are not armed. No trend seems in place to increase armed personnel since the events of 9/11. However, some assignments reasonably require an armed presence and state-mandated training

is a public policy. Even if a state or city does not require training for armed security personnel by statute, reasonable training including regular refresher training is a logical policy.*

4. Many security positions require more training than the legal minimum of a few hours prior to the initial assignment. Security officers who deal extensively with the public or work within the nation's critical infrastructure are expected to respond appropriately and effectively in emergencies. Security officers who interact with complex technology require more training than the minimum. The length of such training and education is determined according to the actual need. For example, in schools where Peace Officer Standards of Training (POST) exist, school security officers usually are required to complete typically a minimum of 40 hours preassignment training with annual refresher training included.³

In some cases, training of security officers can last weeks. For example, 3 weeks of preassignment training, following 8 hours of state-mandated training, have been required by New York City's Health and Human Resources Administration before security personnel are assigned to homeless shelters. In Sweden, security officers for a private security services company are trained almost 6 months before being assigned to certain government-contracted assignments where they serve in lieu of civil service security.

5. Training and retraining produce important measurable benefits. Training reduces risk and loss. Research by Liberty Mutual Insurance Company indicates that a mere 2% of industrial accidents occur because employees didn't know how to perform the task safely or properly.⁴ Only 6% of accidents are due to equipment failure. The vast majority of industrial accidents – 92% – occur because workers failed to perform their tasks properly. Performance deficit is diminished by training and refresher retraining.
6. Lack of adequate training may be the basis of a successful tort action. The failure to provide adequate training for security personnel can lead to a successful plaintiff's action for negligent security and would no doubt be upheld at an appellate level. David A. Maxwell, a lawyer and educator specializing in protective matters, writes: "Employees should be subjected to training prior to assignment When the role at hand involves a potential for harm or injury, the standard for training rises to the risks."⁵ Courts have held that when employees are not trained on how or how not to use weapons and an injury results, the employer may be negligent. But in far less grave circumstances than one involving weapons, an organization and specific managers may face accusations that subordinate personnel were inadequately trained.
7. Requiring security officers to be trained is a reasonable public policy. In the 1950s and 1960s, the average police officer possessed a high school education and was trained in a police academy for only a few weeks. Today, police officers in most cities and industrialized states often must possess a minimum of 60 college credits. Still other states require a 4-year academic degree in order to be considered for a law

*The report *Guards with Guns* (<https://cironline.org/hired-guns/>) provides state by state basic and firearms training for security personnel as of December 9, 2014.

enforcement position. (Military or other government service may be accepted in place of some or all postsecondary education.) Meanwhile, police academy training averages 5–6 months for urban and state police forces.

8. Workers value employers who provide meaningful training. Many workers are attracted to employers who provide training programs and educational benefits. This self-selection enhances the quality of the pool of prospective employees for such works. Once hired and trained, employees are likely to remain longer with such organizations, returning to the workplace the benefits of the training and education they have achieved.

The analogy between public police and private security services is awkward and debatable on many points. Yet it is apparent that many similarities also exist between the two. Private security personnel “protect and serve” in much the same way as police officers on patrol do, albeit on private property and for private interests. Therefore, it is reasonable as a public policy that security officers be trained to a level at which they can do their jobs effectively, while understanding the legal responsibilities and limitations of their roles. This was made apparent with the summit organized by International Association of Chiefs of Police (IACP) and Community Oriented Policing Services (COPS), a unit of the Department of Justice, which convened in early 2004. The conclave was cosponsored by ASIS International, the International Security Management Association (ISMA), the National Association of Security Companies (NASCO), and the Security Industry Association (SIA). Final recommendations that were approved at the IACP annual meeting in November 2004 call for a formal commitment to cooperation between major law enforcement and private security organizations. The recommendations further called on support for “institutionalized partnerships” to aid greater public–private cooperation and facilitation. The recommendations called upon the Commission on Accreditation for Law Enforcement Agencies (CALEA) and state accreditation bodies “to require public–private partnerships as an accreditation standard.”

The Training Manager

High-performance security training programs are headed by training managers or supervisors who excel in their tasks and have an affinity for training others. Their responsibilities include consulting on training policy and subject content with senior managers and others involved in establishing training goals. They further seek to ensure that training objectives are achieved. The training manager organizes internal training courses and may teach some or all of them. Typically, the training manager is closely involved in the orientation of new employees and newly promoted supervisors.

The training manager is expected to remain informed on the latest issues, materials, regulations, and technologies to ensure effective instruction of all those who complete training. This person may also be involved in the evaluation of training programs, although analysis of training results may occur elsewhere in the organization.

In smaller organizations, the security manager may also be responsible for training, as well as other responsibilities. Large organizations may have several staff members assigned training responsibilities and produce their own curricula, visual aids, and training materials that are available through numerous forms of content delivery. Trainers may be obliged to use whatever space can be assembled or they may use a specially designed and dedicated learning facility.

Planning Training and Development Requirements

Security-oriented programs require different types of training for various purposes. In most organizations, entry-level training receives the greatest attention. This is a reasonable policy. However, programs cannot become static and training must never be thought of as something *only* for new hires. Training programs require periodic review and renewal so that programmatic content remains fresh and pertinent.

Changes in the workplace and society make good training and development important. Many executives think of training as a cost burden. However, the training process should provide precise, desired results for management, with measurable changes in workplace performance. Training methods welcome experimentation in order to improve results and reduce costs. For example, technology-based learning can decrease the cost and enhance learning effectiveness for new workers.⁶ Students remain with the program until all critical elements can be tested and passed with full comprehension. Web-based programs permit training managers to follow progress of individual workers in each part of the lesson. Those who have difficulty with particular points of learning can be re-retrained by a supervisor. Further, systems-based training allows managers to identify specific segments of instruction as problematic for trainees. Such training material can be reworked to facilitate learning comprehension.

While a large number of vocations require some preassignment training, that obligation is particularly evident for security positions. The *Report of the Task Force on Private Security* refers to training as “a vital determinant of job performance” and proposes standards that should be monitored by state boards.⁷ Several states have mandated specific requirements for training for security personnel: proprietary and contract workers by law must meet a prescribed curriculum possibly involving preassignment training, postassignment training, and periodic retraining. Security management is obliged to keep details of individual training achievements for use in potential civil litigation for alleged inadequate training.[†] Further, such records are fundamental to enhancing designs for learning.

In today's Information Age, the need for training and personal development must be continuous. Some managers think of work as having two major components: doing the actual work and training or learning on how to do it better. Management, or training managers, must be alert for specialized training that is required, including short sessions on new laws, technologies, or strategies, especially following major security incidents, such

[†] Plaintiffs' lawyers frequently include “negligence in training” in civil actions when it is alleged that a tort to the plaintiff would not have occurred had the security employees directly involved been trained better.

as a terrorist attack, which may require either reemphasis on fundamental principles or innovative protocols and procedures.

Training is thus defined as a process of learning specific skills and knowledge required by the employee to carry out an existing job or to complete a new one. The process is mostly aimed at operational-level workers, both proprietary and contract. Training merges with development, which, combined, advances the informational, critical, and analytical skills of persons in preparation for managerial and executive responsibilities. Development will be discussed later in this chapter. For now, we will look at the initial contact of a new employee with the formal organization.

That Critical Phase of Orientation

Orientation introduces new security employees to the history, culture, objectives, and available resources of the organization. In large organizations, orientation and training programs may be in the hands of dedicated personnel frequently drawn from human resources, security, and other departments. However, operational-minded managers generally are involved closely with the training process. They or surrogates are likely to appear at orientation sessions to make new employees feel welcome and to emphasize the personal concerns uppermost in the mind of the director.

Orientation provides a variety of information to new employees. The process serves as more than a welcome to new employees; it has a serious objective of impacting performance of new employees. Usually the following elements are part of a new employee's formal introduction:

- The history and ethical basis of the organization
- What management expects from all employees
- What employees can expect from management
- What the organization does; its trends, prospects, products, or services
- Characteristics of the department where the employee will be assigned
- The reporting structure (an organizational chart may be provided)
- The purpose of security in the organization and the value management places on it
- Security and safety policies in the workplace

The orientation covers certain fundamentals so that all new employees will become familiar with the same organizational requirements and expectations as those who have gone before them. Orientation also covers practical information, such as keys and identification documents to be assigned, hours to be worked, payroll procedures, the restroom locations and use policy, the alcohol and drugs policy, the firearms policy, the personal telephone use policy, personal use of the computer and access to the Internet, and the policy regarding personal visitors. Some employers request that new employees sign a statement that they have heard and understood policies discussed during the orientation process.

At such an orientation, new workers complete forms required for tax, healthcare, insurance, and other organizational requirements. The company handbook is distributed and may be reviewed in depth with new employees by the orientation leader. At the conclusion of the orientation phase, new workers typically feel upbeat about achieving employment from the organization and are now eager to learn specifically how they are expected to perform.

The orientation occurs after the employee has formally been offered and has accepted a position with the security program. The orientation itself need not be long and can either precede or follow the training process.

Training Content for New Security Employees

Prior to beginning the training process, the operating manager will identify what information will be relevant for new employees. No two workplaces are likely to be identical in their training objectives, protocols, and needs. Content of the training program will emerge from the ethos and needs of particular employers. Still, some subjects related to security services are likely to be found in most programs. For example, fires in the workplace are not frequent occurrences, but they are emergencies when they do occur. Therefore, adequate time should be provided for the worker to learn about procedures when a fire occurs and fire suppression equipment is used.

The content of the training material should be related to the job description created for the position being filled.

The following are specific training factors for certain types of security personnel:

Preassignment training. Security personnel require training, subsequent to orientation, before being posted to a position. The number of hours devoted to this phase of training is variable. For example, the State of New York currently requires 8 hours of preassignment training followed by 16 hours of basic training within the first 90 days of employment.[‡] The Task Force on Private Security in 1976 had recommended a minimum of 8 hours formal preassignment training with a minimum of 32 hours of basic training within 3 months of assignment. In the Task Force's standards, a maximum of 16 hours could be supervised on-the-job (OTJ) training. Many employers, however, combine preassignment training with basic training before the employee is posted. The number of hours that organizations actually train security employees differs widely. Most train for the minimum number of hours required by law; however, some programs have determined that extensive additional training is necessary due to the nature of the employment.

[‡] The New York State Security Guard Act of 1992 (Article 7-A of General Business law), as amended in 1994, provides a state registry of security officers including their current license status. Potential security guard employees are fingerprinted by licensees or other designated persons or entities. The fingerprint cards originally were screened by the Federal Bureau of Investigation's National Crime Information Center. The law was later amended that reduced the criminal records check to the state database. However, as of May 2005, the state law again was amended to require the FBI background check. Other states continued to use the FBI database.

The trend in the United States and in other industrial nations is to increase the level of initial training required before personnel are assigned to posts of responsibility. This is because of the growing legal burden to train security personnel so that they are aware of their minimum legal obligations in dealing with the public. Failure to understand such principles could lead to a charge of inadequate security in a tort action. Employers may increase the quantity of training because their security employees often interact with complex systems or because further job-specific training is necessary.

Security officers generally require training even if they come to the job with previous experience in police departments, the military, other private security companies, or proprietary security departments. This is because the employer wants new employees to share a common denominator with other employees, the uniform curriculum. An exception to this policy is usually made for temporary security employees who work under close supervision and for active police officers who are working temporarily, moonlighting, in security positions.

The 8-hour preassignment training course, proposed by the Task Force for entry-level security personnel, is divided into four segments: orientation, legal powers and limitations, handling emergencies, and general duties, as shown in [Box 4.1](#). The course is to be used in classroom instruction, in conjunction with audiovisual (AV) aids, and concludes with a test to assure that the content has been understood and

BOX 4.1 PRIVATE SECURITY 8-HOUR PREASSIGNMENT TRAINING COURSE

Section I: orientation: role of a security guard (2 hours):

- Functions, duties, and responsibilities:
 - Being proactive in prevention
 - Methods of functions: policy, procedures, and rules
 - Related functions: access control, patrol, and inspections
- Public relations:
 - Deportment and appearance
 - Conflict resolution/management
 - Providing assistance to employees and the public
 - Proper notifications under different circumstances
 - Liaison with law enforcement and public agencies
- Security guard's responsibilities (partial):
 - Detect
 - Deter
 - Report orally and through written documents
- Role of public law enforcement

Section II: legal powers and limitations (2 hours):

- Arrest/custody procedures
- Justification in the use of force
- When use of deadly force may be justifiable
- Penal law offenses encountered by security guards

Section III: handling emergencies (2 hours):

- Nature of emergencies encountered by security guards
- Emergency and disaster response and notification
- Appropriate hazardous materials incident response
- Security guard safety

Section IV: communications and public relations (1 hour):

- Communications duties and strategies
- Sensitivity and interpersonal communications awareness
- Media and public information

Section V: access control (1.5 hours):

- Access control
- Security surveys
- Identification systems
- Other forms of identification
- Benefits of access control
- Documentation

Section VI: report writing review (0.5 hour):

- Introduction
- Reports: providing information and sequence
- Preparing the report

Source: Based on a model originally prepared by the Private Security Advisory Council, included in their Model Private Security Licensing and Regulatory Statute. This is not an endorsement of the program by the author or the publisher as the 8-hour preassignment training by itself is considered as insufficient preparation for contemporary security guard services.

mastered. This is a *de minimis* recommendation from four decades ago, and still not adopted in most parts of the country. It is included here to reflect the barest minimum proposed by a task force when security training needs were less complex.

Basic training. As previously mentioned, many employers combine orientation with preassignment training and basic training. However, some employers prefer to provide basic training in modules over time for new security officers. The Task Force on Private Security recommends a minimum of 32 hours of basic training in addition to the preassignment phase, as shown in [Box 4.2](#). This training should be completed over a 3-month period and may include a maximum of 16 hours OTJ training.

Each of the topics mentioned in [Boxes 4.1 and 4.2](#) represents a subject of considerable importance. Some require more time than others. The training manager will decide on the time allocation appropriate for the particular workplace.

The growth of training required for security personnel is similar in some ways to the increased training for public law enforcement officers. In 1973, the National Advisory Commission on Criminal Justice Standards and Goals recommended 400 hours training for sworn police officers. Since then, most urban police departments require police

BOX 4.2 PRIVATE SECURITY 32-HOUR BASIC TRAINING COURSE

Note: A minimum of 4 classroom hours and a maximum of 16 classroom hours should be allocated in each of the following sections, and a maximum of 16 hours of supervised on-the-job training should be permissible.

Section I: prevention/protection:

- Patrolling
- Checking for hazards
- Personnel control
- Identification systems
- Access control
- Fire control systems
- Types of alarms
- Law enforcement/private security relationships

Section II: enforcement:

- Surveillance
- Techniques for searching
- Crime scene searching
- Handling juveniles
- Handling mentally disturbed persons
- Parking and traffic
- Enforcing employee work rules/regulations
- Observations/description
- Preservation of evidence
- Criminal/civil law
- Interviewing techniques

Section III: general emergency services:

- First aid
- Defensive tactics
- Fire fighting
- Communications
- Crowd control
- Crimes in progress

Section IV: special problems:

- Escort services
- Vandalism
- Arson
- Burglary
- Robbery
- Theft
- Drugs/alcohol

- Shoplifting
- Sabotage
- Espionage
- Terrorism

Source: National Advisory Commission on Criminal Justice Standards and Goals, 1976. Private Security: Report of the Task Force on Private Security. Government Printing Office, Washington, DC, p. 103.

cadets to successfully pass requirements in a program that is approximately 6 months in length. Smaller departments also require academy training, but the time allocated is closer to 400 hours proposed in 1973. In policing and security, instruction on legal issues, public relations, and new technology add to the quantity of time required to be fully effective in these jobs.

Extensive basic training. Some organizations train new security employees far more than the minimum required by standards in those states where training is mandated. This is a salutary development. While a state might have a minimum requirement, no state has a maximum one. Some employers design extensive curricula for security officers and their supervisors to meet their considered requirements. For example, healthcare facilities frequently require security guards to be trained 1 to several weeks before being placed alone on a major post. Training security officers for casino environments, for example, demands selecting personnel who can deal with challenging environments ([Box 4.3](#)).

BOX 4.3 TRAINING SECURITY FOR CASINOS

Casinos need security personnel to maintain order and enforce rules, while working effectively with the clientele, “many of whom expect to be treated as VIPs because of their celebrity or their financial status.” Security officers at Circus Circus Reno in Reno, Nevada, are required to write a short essay as part of the application process. Physical fitness is also emphasized. Officers must be able to administer CPR or remain beside sick customers lying on the ground. Therefore, they must be able to kneel for extended periods and then rise again.

Following ASIS International’s Private Security Officer Training Guidelines, basic training is at least 48 hours total, with 8 hours of general job training, 16 hours of training about the site and security duties, and 24 hours of OTJ training.

Circus Circus Reno has a 4-week training period for new officers. The first week is classroom based. Then 3 weeks are spent in the field with a training officer. They also take a 2-day defensive tactic class and a 1-day CPR and first aid course. They also receive training on the use of pepper spray. Emphasis on managing aggressive behavior and alcohol awareness is also provided. Officers are trained to spot guests who are lost and need directions in contrast to suspicious individuals who might not have the right to be in certain areas.

Source: Ricci, J., Longmore-Etheridge, A., 2013. A winning team. *Secur. Manage.* 57,63.

BOX 4.4 TRAINING FOR ARMED SECURITY GUARDS*Classroom-based training:*

Topic I: legal and police restraints (3 hours):

- Rights of private security personnel to carry weapons and the power of arrest
- Statutory references
- Policy restraints

Topic II: firearms safety and care and cleaning of the revolver (2 hours):

- Nomenclature and operation of the weapon
- Performance of cartridge
- Safety practices on duty and at home
- Range rules
- Care and cleaning of the weapon

Topic III: successful completion of written examination (1 hour):

- At least 20 min on the above topics with a minimum passing score of 70%
- Should be designed so that persons with other or prior experience can demonstrate competence in the subject areas

Range-based training:

Topic I: principles of marksmanship (2 hours)

Topic II: Single-action course (8 hours):

- A silhouette target with a distance of 25 yd is used with 30 rounds fired under different circumstances for qualification of which the minimum passing score is 18 hits (60%).

Topic III: double-action course (8 hours):

- The distance and target are the same, but trainees operate from a crouching position under different circumstances and must score 43 hits out of 72 attempts (60%).

Firearms training. The vast majority of private security personnel are not armed in the course of their employment; however, some are. Security officers who are expected to carry firearms in the course of their employment invariably face additional minimum requirements for training. The Task Force on Private Security recommends that security personnel be required to complete successfully a 24-hour firearms course that includes legal and policy requirements, or submit evidence of competency and proficiency, prior to assignment to a job that requires a firearm. The course of training is divided into classroom and range components, as shown in [Box 4.4](#).

Weapon proficiency requirements should be met on an annual basis if the employee continues to require the weapon as part of his or her duties. State and local requirements for the possession and use of firearms provide specific regulations about firearms retraining and range experience for that particular jurisdiction. Instructors are recommended to be qualified through the National Rifle Association or other comparable qualifications program. Whether guards should be armed or not is a management policy issue. (It is discussed further in Chapter 9.)

The armored car industry, which requires most service employees to carry firearms, has created its own set of standards. The Training Committee of the National

BOX 4.5 FIREARMS TRAINING FOR ARMORED CAR PERSONNEL

- Company and industry policy on use of weapons
- Legal limitations
 - Firearms safety
 - Care in firearms cleaning
 - Basic revolver training
 - Combat firing
 - Use of gunports
 - Use of shotgun
 - Qualification and certification

Source: Training Committee of the National Armored Car Association.

Armored Car Association has proposed an outline of basic firearms training for its employees, as shown in [Box 4.5](#).

Training for Investigators. Investigators, also called fact-finders and other titles, have an important role in security services. Their exact duties vary widely according to their assignments. Usually, a combination of classroom, home study, and OTJ training is provided. For example, the May Corporation, a major retailing chain, has produced a 60-day training program for undercover operatives. Much of this time is spent observing the performance of highly proficient security investigators. This field experience is supported with study of a proprietary manual. After considerable observation and discussion, the store detective is ready to make his or her own stops of shoplifters with the instructor continuing to act as a coach.

Investigators usually enter this type of work with specific interests in this type of work. Many are college graduates with degrees in security, criminal justice, forensic science, and police science. In some organization, retired police officers migrate to corporate or not-for-profit investigative positions. Nonetheless, all require orientation and training on how to do their jobs well.

Ongoing training. This refers to flexible, continuous, individualized programs to ensure that private security personnel are kept informed of pertinent developments in the field. This information is provided in numerous ways and formats. These include roll call training, visits from supervisors to security personnel on post, mailed or distributed training bulletins, formal correspondence programs, and teleconferencing and DVD and Web-based interactive training. Refresher training or security alerts may be provided through cell phone messages, e-mail, printed bulletins, telephone messages, and smartphone conferencing that can inform security personnel of important subjects that are not related to the day-to-day routine. All training resources serve to emphasize best practices. Security procedures should be reviewed and emphasized with testing.

Training Techniques

Training may be achieved by using a number of techniques that are adaptable to specific needs. Most of these approaches are suitable for entry-level operational personnel, but can be used successfully at other employment levels as well for postemployment training.

The Venerable Classroom Style with More Learner Participation

Classroom-style training of individuals has many advantages. One instructor can provide training to many learners at the same time. In addition, numerous learning aids (lectures, discussions, films, PowerPoint™ presentations, videotapes, computer-aided demonstrations, role-playing) can be used during the same training process. For these reasons, classroom training is efficient, effective, uniform, and economical. Furthermore, this method promotes bonding among new employees who come to know each other as fellow learners in a supportive setting. As students are learning, the instructor remains alert to how the lesson is being received. Ambiguous material can be reviewed, clarified, and retaught quickly. Classroom instruction is valuable for all tiers of learning.

Classroom training has undergone an evolution in the twenty-first century. The trainer's dry pontification reading from yellowed notes for the edification of nodding learners is passé. Today the trainer is more likely to identify problems that stimulate further questions and animated discussion. Often, learning will be enhanced by breaking a group of learners into separate units. They will work as a team to resolve the issue the trainer has presented to them. After a period of work, representatives from different teams will share their findings with the entire group. This process allows the trainer to provide positive feedback to the groups and to critique their results at the same time.

At the management level of training, the case history method is often employed. This introduces a hypothetical or an actual unresolved organizational problem, with the management options then considered. Often, groups of managers work in teams to compete with each other in identifying strategic solutions, which become the basis for discussion among the training leader and members of all the teams.

Case histories have been an integral part of training and education for over a century. Christopher Columbus Langdell introduced the case history method to students at Harvard Law School in the 1880s. This method replaced the previous technique of law school professors slowly reading their notes to students, who would copy them and later commit their points to memory. The case history method extended from law schools to other educational venues, including graduate education in business and management.[§] Participants in case history learning experiences absorb considerable information about a situation and are asked to analyze the material and present their own recommendations to help the organization resolve its identified problem. This helps participants enhance their understanding of specific

[§] The case history method in professional schools presents the student with detailed and accurate facts about a situation as the basis of classroom discussion. A possible security-oriented case history: a department faces reorganization due to a merger. How should the new structure operate?

circumstances while at the same time hone their decision-making skills. In less challenging circumstances, hypothetical case histories are used to replace extended real-life examples for edification and discussion. Leaders often pose questions for students such as “How could the developments in this situation have been avoided?” or “What other circumstances does this circumstance remind you of?” or “What are the hidden losses in this case scenario?”

The disadvantage of the classroom method is that it may be too passive. Learners are present physically and may appear to participate in the learning process, but actually some may tune out or not comprehend the necessary information. Further, classroom instructors vary considerably according to their effectiveness. While most truly desire to help students learn, some cover material inadequately, inadvertently providing ineffective or incorrect information for new employees. Additionally, classroom training is not hands-on training. Lecturers may discuss procedures and share illustrative or personal experiences to make points clearer. If the learner needs to interact with technology or others, he or she may need direct exposure to these circumstances, guided by the instructive presence of an experienced colleague. This process is described next.

The Popularity of On-the-Job Training

This type of training occurs while security officers in training learn from experienced officers who are performing actual job-related activities. They are neither in a classroom nor in another type of learning facility, although the former may be incorporated later in the process. The learner is in an actual work location guided by experienced, competent, and reliable security professionals who serve as supportive instructors. For example, novice store detectives learn the craft of making successful apprehensions or – “stops” – by observing and shadowing experienced detectives. The detective trainees do not make apprehensions, but observe them, participate in interrogations, and witness the signing of apprehension reports. In time, the OTJ instructor will determine when the apprentice is prepared to conduct his or her own apprehensions, and at this point the new employee will be encouraged to do so under supervision. If the apprehension is conducted satisfactorily, it will signify that the OTJ training process has achieved its objectives and the store detective will begin to work under less direct supervision.

Managers who must allocate the training budget are generally positive about OTJ training because the learning process is direct, relevant, and under experienced supervision. Instructors may describe the desired performance and then observe the apprentice learning the new skills. Errors can be quickly identified and corrected on the spot. Desired behavior can be supported by immediate praise, reinforcing the desired actions. One disadvantage of OTJ training is that it duplicates manpower commitments. While the trainer and learner are conducting useful work during the training process, the quantity of work achieved is no more than what a single experienced worker alone would perform. Furthermore, OTJ training depends on the availability of motivated experienced instructors who nurture the learning of others. Not all of the most highly qualified workers are able to meet these requirements.

The Flexibility of Computer-Aided Interactive Instruction

Computer-based learning has had a substantial influence on the training process in recent years. Unquestionably, this dynamic process is continuing and aids learning by increasing interactivity. Program enrichment and dramatic special effects make the material memorable. The cumbersome requirement of tying a learner to a computer in a laboratory or office has now dimmed in importance. With intelligent phones and, better, laptops and iPads widely available and often owned and carried by the learners themselves, new skills can be acquired at any time and at any place.

The subject material is logically created, presented in programmed format, often enlivened with realistic animation and audio materials, and designed to elicit responses to assure comprehension of the material. When the learner answers a question correctly, the program acknowledges it – often with personal references that may be part of the programming: “Good work, Joseph!” or “That’s your fifth correct answer, Tina!” If the learner presents an incorrect answer to a question, the program will suggest “try again” and await the correct answer to provide the expected praise. In some cases, the learner will be referred back to earlier materials in the learning sequence where the critical information was initially presented. By this looping back process, the learner will review and presumably comprehend the desired instructional material before being able to proceed further with the lesson. Unlike conventional learning, where some students will have full comprehension and others “passable” but incomplete learning, computer-aided instruction allows full achievement by all participants. Further, the training manager will have details on what questions in the testing sequence a particular student failed to grasp. These wrong answers may suggest the need for additional training by the learner. However, they may also indicate that the teaching material was not sufficiently clear or compelling for learners to understand what was to be comprehended.

The disadvantages of computer-aided instruction relate to complexity and cost. The learning process is connected to specific facts, policies, and procedures. The time and effort required to create a learning segment of this type of instruction is extensive, although computer techniques have reduced the overall costs in the past and promise increasing future efficiencies. Still, the programming activity often has a designed rigidity that makes the student less able to deal with unexpected occurrences, so frequently part of security experience. That is why computer-aided learning is rarely the sole way trainers have employees learn new material. And although computer learning gives all participants a full understanding of the key points in the subject material, retention of such information will differ among learners.

Computer-aided instruction may supplement other modes of training. Such instruction may be delivered at workstations as part of instructor-led courses, at commercial learning centers, within a corporate or security department training center, or wherever the learner has access to a computer with an Internet connection. Some programs may be self-paced and delivered via laptops. Programs are available for different levels of complexity – from entry-level basic patrol instruction to advanced systems and data security ([Box 4.6](#)).

BOX 4.6 OUTLINE OF AN ADVANCED SECURITY PROGRAMMING COURSE: POLICY, ADMINISTRATION, AND FIREWALLS

Numerous programs provide learning on information technology skills. Some of these programs are formal in academic settings lasting one or more semesters. Others are brief courses to help practitioners gain skills needed for emerging workplace needs. The following is an outline of a 3-day course offered by a training company at numerous locations. The course may also be taken virtually or by self-paced learning on the Web.

Attack methods:

- How attackers think
- Information gathering
- Unauthorized access
- Software bugs
- Denial of service
- Ransomware

Security assessment:

- Risks: what to protect
- Who are the hackers
- Legal issues

Security implementation policy:

- Architecture
- Services and access
- Vulnerability detection and audit
- Incident response planning

Firewall architecture:

- Perimeter definition: depth of defense
- Demilitarized Zone (DMZ)
- Firewall advantages

Firewall components:

- Bastion host
- Packet filters (advantages and disadvantages)
- Proxy servers
- Stateful inspection
- Firewalls: hybrid and host
- Content filtering

Authentication:

- Reasons to authenticate
- Passwords
- Tokens and keys
- Common auditing scenarios
- Biometrics
- Authentication placement and enhancement

Intrusion detection and response:

- Detection methods and processes
- Centralization and placement
- Intrusion Detection Systems (IDS) issues

Cryptography:

- Secret-key and public-key cryptography
- Message digest algorithms
- Digital signatures
- Certificates and certificate authorities
- Public key infrastructure (PKI)
- Cryptographic applications
- Secure Sockets Layer (SSL)

Source: Global Knowledge.

The Attraction of Audiovisual Materials and PowerPoint

Nothing beats grabbing the attention of a learner than dramatic streaming images. Security management facilities may possess rich resources of films and tapes for training and educational purposes. AV resources can enliven classroom learning and may be incorporated into computer-aided instruction. AV resources are valued because they can draw upon dramatic situations, actual images from past crimes or incidents, and the use of corporate officials or professional actors to convey desired messages. AV materials use voice, action, and special effects just like any Hollywood production.

AV materials have an initial high cost for acquisition, but they can be used and reused for future training iterations. Some AV programs for security use include a manual for instructors and student handouts. AV material can be exciting and informative when well produced. A few productions, however, fail to achieve their desired goals and are boring, while other films can quickly become dated and obsolete. The trainer should preview such materials and select those that best meet the needs of the workplace. Often site-specific AV materials may be developed internally on videotape or digital format at moderate cost. This has particularly been the case since the availability of camcorders and digital editing and production techniques.

PowerPoint is an immensely popular software program to quickly and easily create slideshows. First offered only on Mac in 1987, the software was purchased by Microsoft in 1990 for MS Office. The program possesses many useful applications, including training and education. PowerPoint has been described as the “best and worst thing to ever happen to meetings.” This is because good ideas have slick presentations, whereas those “spurious, obvious, ill-conceived, or poorly thought out can be presented with a professional polished look.”

Programs can be created with graphics, animations, and multimedia segments. If desired, the training manager can copy PowerPoint slides onto a thumb drive or CD to share with other trainers. In some learning contexts – for example, executive briefings – PowerPoint slides might be considered inappropriate, although use of computer-aided learning is an effective and well-accepted mode of learning.

The Drama of Demonstrations

Often following the acquisition of new products, systems, and software programs, staff must be trained in their use. Such training may be provided with demonstrations of the actual materials acquired and intended to be used in the workplace. (Occasionally, such products may be “demoed” prior to their purchase to obtain critical feedback from workers.) Demonstrations may be incorporated into OTJ training and classroom training as well. For new products and services that are acquired, initial demonstrations may be given by vendors, although some vendors have computer-based instructions to aid in the process.

Demonstrations are important because they represent the most efficient means by which new corporate investments in hardware or software can be disseminated to persons most likely to use them on a daily basis. Generally, employees enjoy learning by being part of a demonstration and peppering the demonstrator with questions as the process unfolds.

“T” Groups (Sensitivity Training) When Human Emotions Must Be Engaged

These highly participatory learning methods are intended as one means of improving the learner’s skills in working with other people. This is achieved by increasing their ability to understand how others react to behaviors encountered in the workplace. T (for training) groups are small sessions that may take place without a leader present. The group is given a task, and members create working relationships with each other to achieve the goal. “T” group members eventually may see the subtleties of their verbal and nonverbal communications with each other. A manager may use such a technique to explore feelings of sexism, racism, and other sensitivity issues that might hamper workers from interacting productively and harmoniously with each other. For example, if concern for harassment in the workplace exists, “T” groups can evaluate the nature of how people feel differently about remarks and behaviors that might seem like normal communication or joking to some, but which are offensive to others. Such a process generally leads to greater sensitivity on the part of those who might be the cause of objectionable behavior.

Role-Playing – Bringing Out Dramatic Issues

A leader or coach may describe a particular situation to a group and then ask members of the group to improvise the scenario. For example, the trainer may wish to instruct a new

group of retail security personnel on how to apprehend a shoplifter. One volunteer would play the shoplifter's role and others would act as security agents intent on apprehending the offender. The remaining learners would observe and critique the process. Role-playing usually involves learners who have not completed the training but already have learned basic principles. The object now is to act out a mini-drama in which the principle to be learned is examined.

The unrehearsed acting by the participants provides an opportunity for the leader or coach to stop the action at different points and ask trainees what they think is right or wrong about the action they witnessed. The use of unstructured drama in role-playing can aid trainees substantially in understanding procedural and behavioral lessons that need to be learned. For example, a security manager who is responsible for healthcare or social service facilities may determine that "T" groups are valuable in helping trainees understand the nature of their patients' or clients' emotional status, which could be fragile or dysfunctional. Role-playing scenarios are mini-dramas that are usually enjoyable for instructors and participants alike, leading to a stimulating learning experience.

Other Techniques

Numerous other types of training also exist, but are less frequently found in security training programs. These include apprenticeship, behavior modeling methods that provide immediate feedback, and skill analysis, in which relevant workplace behavior is assessed for weaknesses.

The Criticality of Firearms Training

The need for firearms training is generally codified by state and local regulations. At least 32 states and the District of Columbia require initial training for armed security personnel. Of these, 24 also require refresher training, on an annual basis. Generally, specific training on firearms by a certified firearms instructor is needed prior to registration. In some cases, employers may operate where no statewide requirement exists for initial training of armed personnel. However, local requirements on a county or city level may be in existence. Even if this is not the case, the workplace is advised to assure that any armed security agent be trained to the minimum standards of those states with such requirements.

Managers of security programs and operators of security service businesses have depended less on armed employees than in earlier years. Further, at the time of the Rand research, only 19% of private security personnel actually carrying firearms had job-related training on use of the firearms they carried. The *Rand Report*, released in 1970, stated that 49% of private security personnel carried firearms. By the year 2006, that percentage was under 5%, excluding consideration of law enforcement officers who work part-time in security programs.

The decline in the arming of private security personnel is mostly related to the increased liability from accidental or unintentional injury from the use of firearms. Most

security directors have determined that they can design security programs that meet their objectives without arming security personnel. Further, an armed security worker creates a different tone at the job that might conflict with the dynamics of the workplace.

Nonetheless, numerous examples exist where security officers probably should be armed. In such cases, responsibility for assuring that armed security personnel are initially trained and maintain their annual training requirements is a responsibility of both the individual security officer and the employer. Software programs can keep track of completed training and provide reminders when annual refresher firearms training should be scheduled.

The *Report of the Task Force on Private Security* proposed a standard of a 24-hour firearms course – or its equivalent – prior to assignment to a position requiring a firearm. The proposed standard further required requalification annually as long as the security officer continued duties requiring use of a firearm. In New York State, for example, security guards who carry firearms must first complete requirements for an *unarmed* guard license (also known as a “registration card”). The applicant then must obtain a valid New York State pistol permit that requires a background check and the demonstration on why the pistol permit is required. Then additional 47 hours of initial training and 8 hours of annual training on top of the basic training is required by the Security Guard Act of 1992, as amended.

Training for armed security personnel is offered by schools that include tactical training and knowledge of relevant sections of the state penal law. Training facilities have instructors who have completed courses offered by the National Rifle Association and other organizations.

Ongoing “In-Service” Training

Most high-performing security programs require formal training on an annual basis for all security personnel. This training maintains the basic skills, knowledge, and judgment employees need to perform their assigned duties. Such training helps keep performance levels high as the relearning counteracts the tendency of skills – once learned but not used – to decline in their reliability. Additionally, it is presented to keep employees informed on issues such as changes in corporate directions, legal issues, criminal and loss-related patterns and trends, and technological advancements.

Other training courses may be considered for proprietary employees or contract employees engaged as executive protection or celebrity security agents. A defensive driving course is a separate kind of training linked to executive and celebrity protection. These courses require periodic retraining.

Security employees involved in interviewing should consider a course or courses that teach interviewing techniques. These are for in-house and contract investigators whose work includes interviewing witnesses and suspects.

Ongoing training can be presented using didactic techniques described earlier in this chapter. For emphasis on a current concern, personnel may receive a briefing

before the start of a shift. This is widely incorporated into law enforcement programs. The same technique can be applied when security officers congregate before leaving for their posts. Lectures, handouts, and brief AV presentations can emphasize the importance of a point in the training agenda. For security officers who are few in number or who work at dispersed locations, training can be provided by phone-in messages, through contact with supervisors, and from printed material left for or mailed to such employees.

Ongoing training is flexible and draws upon the resources most pertinent to the workplace environment. This type of training is needed for several important reasons. First, existing skills become obsolete and need refocusing. Further, employees need to learn more so that they can absorb other tasks within the organization during downsizing. Cross-training is often beneficial, keeping workers alert on complex matters where frequent application of the skills involved does not normally occur. The director of training is likely to identify trainable issues that can be offered in a cycle over an extended period of time.

Many employers encourage self-paced development and education by providing partial or full tuition reimbursement for employees who attend institutions of higher learning on a part-time basis. This encourages employees to pursue degree programs that will enrich their lives and their careers. Workers may also learn by taking management-sponsored correspondence courses on subjects of relevance to the workplace (Box 4.7).

BOX 4.7 CORRESPONDENCE AND ONLINE COURSES

Security training, as well as professional contacts, normally occurs during conferences, symposia, meetings, and courses. But learning can also occur on an ongoing basis through lessons delivered by mail or by the Web.

One of the time-tested ways to learn is through correspondence courses. In such courses, learners can proceed at their own pace and may select courses that are of great interest or importance to them as well as to their employer. AlliedBarton Security, a national security services firm based in King of Prussia, Pennsylvania, offers a home study course for all employees. Coordinated by the AlliedBarton Academy, the program includes 15 self-study modes similar to a correspondence course. The final five units are delivered in a classroom setting. Participants must pass examinations as they ascend from stage to stage through five levels. At the fifth level, the participant earns the Master Security Officer (MSO) designation.

Postsecondary education has moved into a new era of online options. For example, John Jay College of Criminal Justice offers undergraduate courses in security management, emergency planning, and other relevant topics. The same institution offers a master's degree in security management, totally obtainable online. The student misses the back-and-forth exchanges of the classroom. But he or she gains in convenience. Without an online option, students with difficult working schedules or who live far from an academic center would never be able to achieve a diploma.

The Importance of Reducing Risk in Confrontations

Specific topics have become important to security practitioners growing out of public discussions and concerns. An example of a current topic of importance to managers of security personnel is how to deal effectively with the public. In particular, what might a security officer do to de-escalate a tense situation with a member of the public?

A concept captured by law enforcement a generation ago is sometimes used in security guard training. Training in verbal judo enables the learner to remain calm outwardly and under control during disagreements.⁸ This usually involves finding solutions to particularly resolve difficult situations. The learner appreciates how to empathize with an agitated member of the public while not losing self-control. Training enables the learner to understand that an irate member of the public is not angry against the security guard personally, but rather verbal attacks are directed toward, in this case, the guard as a symbolic focus of that public person's ire.

Since security personnel are normally the organization's "first face" a visitor encounters, courtesy and sensitivity are valuable traits. Respecting the public appropriately aids security personnel to achieve their goals with aplomb.

Emergency and Fire Prevention Training

In a time of job expansion, many security practitioners require training in fire safety and emergency response. These are significant learning areas unto themselves. But few people are better prepared for this kind of training than those in security. Many cities take the goal of fire safety seriously and have state-mandated requirements for training, some of which requires passing of a test of comprehension and future retesting.

Personnel trained in fire safety measures must engage in a scheduled series of fire alarm communications system testing. This includes daily (visual inspection that the fire command station is online and that trouble signals are investigated, and a lamp test), monthly (transmit alarm to verify transmission to central station alarm company and conduct tests of elevators equipped with firemen's service operations), and semiannual (including check of manual pull stations, public address system, alarm/strobe signal operation, functioning of floor warden phones, and verification that fail-safe release on reentry doors equipped with fail-safe release doors is operational).

As an example, the City of New York mandates that personnel in major commercial and industrial buildings be trained in specific topics by a curriculum previously approved by the Fire Department of the City of New York (FDNY). The following are some courses widely required in this endeavor:

- *Fire guard.* This course prepares participants for responding to impairments of fire alarm systems, standpipe systems, and sprinkler systems in all types of buildings.
- *Supervision of fire alarm systems.* This course teaches the operations and types of fire alarm systems and other related installed in all properties.

- *Sprinkler systems.* The FDNY administers a 75-question Certificate of Fitness Examination for Sprinkler Systems Citywide. The certification is not premise-related.
- *Standpipe systems.* This course also prepares persons for the 75-question FDNY Certificate of Fitness Examination for Standpipe Systems.
- *Construction site fire safety manager.* FDNY offers a Certificate of Fitness in all aspects of fire prevention and protection in buildings being constructed or demolished.
- *Coordinator of fire safety and alarm systems in homeless shelters.* Coordinators in homeless shelters, both public and private, are required to complete a course for the safety of employees in fire emergencies and emergencies other than fires for this environment.
- *First aid, cardiopulmonary resuscitation/automated external defibrillator (CPR/AED) course.* The American Red Cross has a curriculum on this topic. The course takes 0.5 day and should be refreshed annually.
- *Fire safety director (FSD).* This course discusses actions to be taken by FSDs when fire/smoke emergencies occur. In the City of New York, FSDs are required for business/commercial office buildings and hotels/motels/hostels. Applicants must satisfactorily complete (attend and pass) a training course for an FSD given by a school or organization accredited by the FDNY. The certification is a two-step procedure. The first is the general qualification for FSD given as a written test. The second is a specific qualification for the building where the applicant is employed. A representative from FDNY conducts an on-site test to ascertain the applicant understands fire command procedures pertinent to that location. Candidates failing the on-site test will not be permitted to maintain their Certificate of Completion and will not be permitted to perform as an Acting FSD.
- *Emergency Action Plan (EAP) director.* Business and commercial office buildings and hotels, motels, and other buildings require someone trained as an EAP.

Security Training for Nonsecurity Personnel

Everybody in the organization should be part of the process to protect people, property, and intellectual assets. Security needs are too great for any department alone. The number of security personnel budgeted might not be adequate to achieve the level of staff coverage desired by protection planners. Even if this is not the case, the strategy in most organizations is to involve all employees in the protective process at some level. Therefore, the security manager, or the security training manager, will enlighten nonsecurity personnel in the rationale and methods of workplace security and safety issues. In large proprietary organizations, security managers routinely speak about relevant security issues at orientations for new employees. They are also available to reemphasize protocols or introduce new ones according to the circumstances. It is strategically important for security to be visible and available to all employees. Being part of the new employee orientation program is part of this.

Training for Trainers and Supervisors

In recent decades, attention has been devoted to training the trainers as well as aiding supervisors and managers to be more effective in their positions. Such efforts improve the quality and performance of the services provided. Specific training-for-trainers courses are available at trade and educational institutions throughout North America. While not specifically related to security training, the brief courses do expose trainers to principles that can be applicable to loss prevention and physical security needs.

Development and Education for Managers and Executives

Managers and executives must mature in their positions. Because of the knowledge-based content of managers' work, the term "development" is applied for the ongoing cognitive and skills growth of managers and executives. Development is fostered by education, which can be provided in a variety of settings. Attendance and participation at programs provided by specific security-related and general management organizations can serve personal developmental needs. Examples of specific programs include those offered at symposia, conferences, and exhibits of the ASIS International, the International Security Conferences, and meetings held by other industry-specific groups that support security training and education. These can serve local, regional, or international practitioners.

General management organizations that offer courses include the American Management Association, the Conference Board, and numerous academic institutions found throughout North America and abroad with programs and courses in management and organization. Additionally, graduate and undergraduate institutions provide continuing education courses in security management and business administration, criminal justice, and industrial/occupational psychology that can provide valuable information and insight to security personnel.

Distance learning is a learning mode in which the student is not present in a classroom with the instructor, but learns via a closed-cable television link. The term also refers to self-paced learning that may or may not be monitored by an educational institution. Distance learning helps students come in contact with instructors and resources not available in the learner's immediate area. It permits self-motivated individuals to study where they are and when they can. However, most academicians believe that, while distance learning has much value, its impact has not met the test of time like conventional group learning.

Certifications for Loss Prevention

Certification is a process whereby an individual is awarded a designation after having demonstrated competence through education, pertinent experience, and independent verification. Certification is usually established through testing. Generally, certification requires proof of ongoing growth through confirmed attendance at continuing education activities, participation in research projects, teaching in the field, and other means.

Recruiters and employers generally view certification of managers positively, since the process provides an independent indication of relevant capability. Senior managers often encourage managers to obtain professional certification, and to keep it once earned. Among security practitioners, several certifications have stood the test of time:

The *Certified Protection Professional*[™] (CPP) designation is awarded by the Professional Certification Board of the American Society for Industrial Security. The CPP program began in 1978, and over 5500 individuals around the world currently meet CPP requirements. Recertification requires proof of continuing education and growth and must be verified every 3 years. The CPP exam consists of 200 multiple-choice questions covering tasks, knowledge, and skills in those areas, including test questions in the following areas: security management, 38%; investigations, 15%; legal aspects, 7%; personnel security, 9%; physical security, 19%; and protection of sensitive information and emergency management, 6% each. In 2003, the ASIS International Professional Certification Board initiated two additional programs.

The *Physical Security Professional*[™] (PSP) certification has awarded 500 certifications following successful passage of the exam. The PSP covers the following subject areas: physical security assessment, selection of integrated physical security measures, and implementation of physical security measures.

The designation *Professional Certified Investigator*[™] (PCI) has been achieved by more than 100 persons. Subject areas included in the exam are case management, evidence collection, and case presentation.

Another main certification in the protection field:

Certified Fraud Examiner[™] (CFE) is issued by the Association of Certified Fraud Examiners, Austin, Texas. The CFE program began in 1988, and numbers over 75,000 practitioners, often with auditing and investigative responsibilities. CFEs must earn minimum continuing professional education credits in order to maintain annual CFE compliance. Information: www.acfe.com.

In the sphere of information technology security credentials have gained broad support:

Certified Information Systems Security Professional[®] (CISSP) designation. Since 1989, approximately 90,000 persons in 143 countries have earned this certification. To qualify for the examination, a candidate must pass the CISSP exam and possess 4 years' experience in 1 or more of the 10 domains of the common body of knowledge of the field. Information: www.cissp.com.

Certified Healthcare Protection Administrator (CHPA) is intended to identify leaders in healthcare organizations concerned with security or police, safety, emergency management, and risk management. To participate in the examination, the individual is a person who directs the team, has an influence on hiring/firing, holds budgetary responsibilities, and establishes business strategies. Information: www.iahss.org.

Certified Institutional Protection Specialist (CIPS) is available for officers, supervisors, and other frontline personnel concerned with cultural property protection. Training for the certification is available live, through DVD, and through online formats.

Information: www.ifcpp.org.

Certified Forensic Interviewer (CFI) from the Center for Interviewer Standards & Assessment. Information: <http://certifiedinterviewer.com>.

For engineering technicians working in the fire alarm industry:

Certifications in Fire Alarm Systems and Inspection and Testing of Fire Alarm Systems from the National Institute for Certification in Engineering Technologies. Four levels of certification are offered. Information: <http://www.nicet.org>.

Measuring Effectiveness

Security training is too important not to be validated and evaluated. Yet all forms of training cannot be completely and objectively or quantitatively assessed. This is a difficult issue for quantitatively oriented managers: it is not possible to prove that by providing a certain number of hours of instruction on a particular topic a measurable effect in workplace performance can be determined. Nor is it always possible to see that this effort will have a definable economic impact. Still, certain fundamental questions can be raised, as suggested by Leslie Rae⁹:

Has the training satisfied its objective?

Has the training satisfied the needs of the clients or workplace?

Are people operating differently at the end of, and as a result of, the training?

Did the training contribute directly to this behavior?

Is the learning achieved being used in the real work situation?

Has the learning contributed to the production of a more effective and efficient worker?

Has the training contributed to a more effective and efficient (hence, more cost-effective) organization?

The first three questions relate to the nature of training itself, while the last four are concerned with the effect of training on the work. According to Rae, questions arise in validation and evaluation that are subject to assessment. These include the following:

- *Content of training.* Is it relevant? Is it up to date?
- *Method of training.* Were the methods used the most appropriate ones for the subject? Were the methods used most appropriate for the learning styles of the participants?
- *Amount of learning.* What was the material of the course? Was it new to the learner or merely a rehash of information previously learned? Was it useful, although not new to the learner, as confirmatory or revision material?

- *Trainer skills.* Did the trainer have the necessary skills to present the material in a way that encouraged learning? Did the trainer have a positive attitude about learning?
- *Length and pace of the training.* Was the learning of the essential material of appropriate length and pace? Were some aspects too extensively covered? Were others provided insufficient time to adequately learn?
- *Objectives.* Did the training achieve its desired objectives? Did the learner have the opportunity to try to satisfy personal objectives?
- *Omissions.* Were any essential points omitted from the learning process? Was material included that was not essential to the learning?
- *Learning transfer.* How much of the learning is likely to be put into action on return to work? If it is to be a limited amount or none at all, why is this so? What factors will deter or assist in the transfer of learning?
- *Accommodations.* If the training facility is within the control of the trainer, was it relevant to the type of training provided? Was the learning in a facility suitable to the occasion? Were adequate refreshments and comforts available?
- *Relevance.* Was the course/seminar/conference/workshop the most appropriate means of presenting the learning activity undertaken?

After a period of time, learners may be questioned about their reflections on the material they had learned. Such issues as the following then may be assessed:

- *Application of learning.* What aspects of your work now include elements that are a direct result of the learning event? What new aspects of work have you introduced as a result of your learning? What aspects of your previous work have you replaced or modified as a result of your learning?
- *Efficiency.* How much more efficient or effective are you as a result of the training? Why or why not?
- *Retrospective analysis.* With the passage of time and attempts to apply learning, are there any changes you would wish to make to your outcome answers?
- *Ongoing evaluation.* The assessment of learning can be conducted by providing questionnaires to learners asking them to rate their experiences. For example, learners can be asked to evaluate the relevance of their training on a scale. One scale frequently used is the Likert Scale, which has seven levels, where 1 represents the lowest score, 4 represents neutral or the midpoint, and 7 represents the highest score. Gradations between the extremes and the midpoints allow variations of feelings to be identified. Such questionnaires can be scored quickly by management, although interpretation will take longer. Many managers prefer to evaluate training shortly after it is completed by a group and then again at some point in the future when the lasting effects of the training may be assessed.

Questionnaires may also include open-ended questions about the content and process of the learning experience. Examples of such questions include the following: "What did you most like about the training you received?" "What did you least like?"

“Do you believe others in your position should receive this training program in the future?”

In addition to questionnaires, managers may wish to establish control groups in which the performance of those who undergo training is contrasted with the performance of those in a control group. Clearly, control group research is not desirable for situations in which it is necessary to train all workers about critical skills or knowledge.

Another way to evaluate training is through direct observation, in which training evaluators or supervisors report on the performance of workers following the completion of training. (Presumably, these evaluators would have had experience observing these employees prior to the training process and are thus in a position to note performance differences.) Training or human resources personnel may also conduct in-depth interviews with trained workers to assess what they achieved during the learning process. Questions tend to be specific, asking workers what is different about the workplace processes since the training concluded. Additionally, trained individuals may wish to keep journal accounts of the ways in which their training has affected their behavior and performance.

Training assessors collect such questionnaires, research data, interview notes, and journal accounts in an attempt to evaluate the effects of training and determine the value such training has to the employer. The training evaluator also is likely to speak informally over time to those who have been trained and to those who supervise or manage those who have been trained and obtain useful subjective information on how the training has been beneficial or has failed to meet its objectives.

Summary

With the complexity and diversity of security management tasks today, adequate initial training for security personnel is expected. This may be supplemented by ongoing in-service training for operational workers. Managers and executives also require further development through education at conferences, seminars, and academic courses. Such training sometimes seems costly to managers who do not understand its benefits. Training should be planned to achieve or exceed the objectives of the employer. A variety of training methods can be considered to meet the requirements of cost-effective learning. Workplace training requires validation and review as well as long-term evaluation and follow-up.

Discussion and Review

1. What are the salient arguments for training new security personnel?
2. How has the Information Age affected content and delivery of training programs?
3. What appears to be the main emphasis on the 8-hour preassignment training course proposed by the Task Force on Private Security? What is the reasoning behind preassignment training? Three decades later are those educational goals still relevant?
4. Define ongoing training and compare it with in-service training.

5. What are the strengths of the case history method for training? What are its weaknesses?
6. Under what circumstances would management provide T group in-service training?
7. What are the inherent limitations in measuring the effectiveness of training? What reasonable measures might a manager take to collect data to help assess a recently completed training program?

Endnotes

- ¹ McCrie, R.D., 2007. *Security Operations Management*, second ed. Butterworth-Heinemann, Boston, p. 96.
- ² Nalla, M.K., Crichlow, V.J., 2014. Have the standards for private security guards become more stringent in the post 9/11 era? An assessment of security guard regulations in the US from 1982 to 2010. *Secur. J.*
- ³ Hylton, J.B., 1998. Is security training getting short shrift in schools? *Secur. Manage.* 42, 102.
- ⁴ Fletcher, M., 1995. Encouraging safety not always easy. *Business Insurance*, October, p. 3.
- ⁵ Maxwell, D.A., 1993. *Private Security Law: Case Studies*. Butterworth-Heinemann, Boston, MA, p. 15.
- ⁶ Thornburg, L., 1988. Investment in training technology yields good results. *HR Magazine*, January, p. 37.
- ⁷ National Advisory Committee on Criminal Justice Standards and Goals, 1976. *Report of the Task Force on Private Security*. U.S. Department of Justice, Washington, DC, p. 87.
- ⁸ Thompson, G.J., Jenkins, J.B., 2013. *Verbal judo: the gentle art of persuasion*. William Morrow, New York, NY. Also: Morton, J., 2012. *Take a stance on use of force*. Buildings, December, p. 20.
- ⁹ Rae, L., 1986. *How to Measure Training Effectiveness*. Nichols Publishing Company, New York, NY, p. 4.

Additional References

- Adams, M., 1999. Training employees as partners. *HR Magazine*, February, pp. 65–70.
- Brown, S.M., Seidner, C.J. (Eds.), 1988. *Evaluating Corporate Training: Models and Issues*. Kluwer Academic Publishers, Boston, MA.
- Calder, J.D., Sipes, D.D., 1992. Crime, security, and premises liability: toward precision in security expert testimony. *Secur. J.* 3 (2), 66–82.
- Facteau, J.D., 1995. The influence of general perceptions of the training environment on pretraining motivation and perceived training transfer. *J. Manage.* 21 (1), 1–25.
- Goldstein, I.L., 1989. *Training and Development in Organizations*. Jossey-Bass Publishers, San Francisco, CA.
- International Foundation for Protection Officers, 1998. *Protection Officer Training Manual*, sixth ed Butterworth-Heinemann, Boston, MA, (an Instructor's Guide for the sixth edition is also available).
- Leeds, J.P., 1994. Legal concerns in the use of psychological screening tests. *Secur. J.* 5 (4), 212–216.
- McLamb, J., 2014. Ready to respond. *Secur. Manage.* 58, 29.
- Nicholson, L.G., 1997. *Instructor Development Training: A Guide for Security and Law Enforcement*. Butterworth-Heinemann, Boston, MA.
- Phannenstill, R.J., Horvath, E.S., 1991. A comparison of computerized interviewing of job applicants with a personal security interview. *Secur. J.* 2 (3), 172–179.
- Quiñones, M.A., 1995. Pretraining context effects: training assignment as feedback. *J. Appl. Psychol.* 80 (2), 226–238.

Rojas, J., 2011. It's a day-to-day existence. February 22.

Taylor, W.C., 2006. To hire sharp employees, recruit in sharp ways. New York Times, April 23, sec. BU, p. 3.

Further Reading

Bodyguard training programs. <<http://www.bodyguardschool.com/TrainingPrograms.html>>.

Educational DVDs and on-demand media. <<http://www.insight-media.com/IMShop.aspx>>.

Emergency management training. <<https://fema.gov/training-1/emergency-management-training>>.

Managing disruptive behavior. <<http://www.crisisprevention.com/About-CPI>>.

Non-confrontational interviewing. <<http://www.w-z.com>>.

Supporting and Motivating Supervisors and Staff

There are few jobs more difficult but at the same time more interesting than that of supervising people.

—William R. Van Dersal

Executives and managers work through other people. No matter how talented the chief executive officer (CEO), chief operating officer (COO), chief security officer (CSO), and other “C-level” senior and middle management may be, results are achieved through the combined efforts of the larger organization working together. Since work is achieved by subordinates, managers higher in the hierarchy need a familiarity with the successful process for using supervision to achieve results. This chapter will consider aspects of supervision that brings results. Attention will be focused initially on first-line management.

Supervisors provide the key component to operational success of the organization. They are regarded as first-line managers – the lowest level of the managerial hierarchy, but management nonetheless. Supervisors differ from middle and senior managers in having larger directing and controlling responsibilities and less to do with planning, organizing, and staffing.

The titles of those subordinate to supervisors differ according to the nature of the employer. Operational-level security staffers may receive titles specific to their position, such as security guard or officer, agent, investigator, store detective, alarm console operator, fire console operator, or documents classifier. A few organizations use titles variants, such as assistant, associate, junior or senior, or team member. Generically, these individuals may be termed “staff” (not to be confused with headquarters senior staff at the C-level) or simply “workers.” Senior management often seeks to find a dignified, innovative, and enhancing term to refer to such personnel. For this chapter, first-level managers will be referred to as supervisors and the individuals they oversee will be referred to as staff. The term *worker* is not pejorative, of course, and is used interchangeably in various contexts by many management writers and educators.

Supporting Supervisors and Staff

For the work to be achieved and the desired results attained, management must not only provide ample workers capable of achieving, or surpassing, goals but also provide different types of support so that these staff members can thrive. The best planning and crack team of coworkers will come to naught if those persons do not have what they need. In a sense,

the failure of the staff in such circumstances is a failure of management. The requirement of routine supplies, vehicles, and other resources is clear enough. Less obvious are the procedural support commitments that are found in higher-performing organizations. The first section of this chapter, therefore, considers these specific needs for this cadre of workers. Nobody, for example, would blame an autoworker on an assembly line for not doing his or her fair share if that person didn't possess critical parts or tools needed to do the job. The same analogy holds with security employees, although in most cases what these individuals require are not nuts, bolts, and side panels, but mostly intangibles that are central to getting the job done. Providing the staff with various support items and resources is not merely a desirable action for first-line and middle management, it is a duty: their duty.

To achieve desired results, management plans conscientiously so that resources are ready before they are likely to be needed by supervisors or staff. This is a reflection of just-in-time (JIT) planning. But before that occurs, it is necessary to find the right person for the right slot. That is the role of placement.

Who Counts as a Supervisor?

The legal definition of a workplace supervisor has emerged as an important issue. If an employee who is a supervisor under federal employment discrimination law discriminates against or harasses a subordinate, the employer could be found liable. If one employee discriminates against or harasses a co-employee, the violation is not so serious.

The Equal Employment Opportunity Commission has held that people can be considered supervisors even if they do not have the power to affect the terms of employment of those they oversee. A report finds: "The EEOC's guidelines also state that employers can be held vicariously liable for damages for discrimination in situations where the alleged harasser does not have any real supervisory authority but is believed by the accuser to possess such authority because the chain of command is unclear."¹ According to a brief filed with the Supreme Court in *Vance v. Ball State University, No. 11-55*, people who recommend that a supervisor take some action can themselves be thought of as holding supervisory roles if their recommendation is given substantial enough weight.

Placement

Fitting people and their jobs together is the first step in successfully bringing newly trained workers into the job stream. Management has determined that openings are available for particular shifts, days, and levels of experience. The human resources and training officers plan the assignment so that newly trained workers can be placed in positions to work without delay. Prior to the assignments, the supervisor is consulted on facts involving new staff workers assigned to his or her unit. At this point, the supervisor may review the training files and pertinent information about each new worker coming onto the unit. He or she may conduct a brief interview to ascertain that the nature of the job and the characteristics of the worker are compatible. This is no time for uncertainty. For example, if the new employee begins by working the night shift, is he or she truly prepared to accept that

assignment for a minimum period of time? Has this prospective worker experience previously on the night shift? This is when the supervisor determines whether any reasons exist as to why the placement would not be successful. In addition to scheduling issues, the supervisor will review the particular nature of the position to assure that the fit for the worker to the position is appropriate. This includes an analysis of:

- The specific nature of the tasks to be performed
- The knowledge required for the site and the particular duties
- Past exceptions at the site to which the new worker must be capable of responding
- The equipment, supplies, and systems the security worker will require
- Any particular physical requirements, such as lengthy standing or walking, or the possibility of having to endure substantial temperature changes during a tour
- Any unusual requirements relative to the site and the position

Supervisors are likely to take for granted the physical circumstances of the job and the particularities of the personalities involved. This attitude could be counterproductive to staffers' success. Therefore, the supervisor needs to consider carefully any means by which the new worker might not succeed in this placement and ascertain how further information or additional support might help mitigate any possible assignment difficulties early on.

Providing new employees with a personal welcome is practiced at some workplaces. At Southwest Airlines, the new-hire orientation program includes the following signage: "New Hire Celebration: You, Southwest, and Success." Thus, Southwest Airlines provides an opportunity for new workers to be welcomed by their peers in a relaxed, friendly atmosphere, focused on success. In many organizations new supervisors are taken to lunch or offered some other welcoming gesture by the supervisor's manager.²

Within the context of supervision, several principles guide the relationship between supervisor and the supervised. The principles need to be learned when a staffer is promoted to supervisor or when an outside person is hired into a primary or secondary management position:

1. *Staffers must understand exactly what is expected of them.* Much of the information shared between the supervisor and the new worker will have been covered during training. However, such training is not generally site specific. The supervisor provides her or his own second orientation as a specific introduction to the job.³ This process is highly meaningful as the staffer is now about to start working and knows that pleasing his or her supervisor now will become a priority at the new assignment.

During this second orientation, the supervisor likely reviews topics of utmost importance at the time the worker begins the assignment. A number of issues are routinely covered at such times:

- a. *A few words about ethics and fair working conditions.* Security people work with the trust of others. The trade and professional organizations have codes of ethics, binding the members who belong to such groups. But ethical issues

do not stop there. At the job site, the nature of the ethical commitment of the organization itself and the nature of the tasks to be performed by the worker need to be reviewed. This is the time for the supervisor to make sure instructions are understood. This is also an occasion to make clear the extent to which the supervisor will be available for assistance, the ability to contact other coworkers on the job sites for any assistance, and steps to take in an emergency situation.

The supervisor may communicate informally a message: “You are fortunate to be joining the leading manufacture of smart widgets in the industry [or whatever the organization does]. Since the day this company was founded, all of us here have been committed to serving our customers with excellent products and services. Our commitment to fair, honest, and honorable dealings equally involves vendors and employees. Security is important in our success and growth. That’s why your role here is key to our success.” The new staffer may be referred to the organization’s ethical statement and information on the workplace ethics and ethos. This statement may be printed in the employee handbook or be posted at different locations in the workplace. By taking a moment to call the worker’s attention to these statements, the supervisor is bound to enhance their importance in the new staffer’s estimation.

The supervisor may point to the statement of principles involving the dignity and fair play for all employees. If an employee has a complaint and it cannot be or is not handled adequately by the supervisor, the new staffer should learn that higher management will be available to hear the dispute or issue. If the general manager has an open-door policy, this fact should be mentioned as well. These comments are relevant for proprietary organizations. When employees for the outside contractors have unresolved workplace complaints, mechanisms for dealing with them should be structured and communicated to those involved.

- b. *What the organization does.* After a period of orientation and training, it might be assumed that the new worker has a clear idea of what the organization actually does. This is not usually a safe assumption. The supervisor should therefore discuss with the new employee the work output of the organization: what it does, what the strategy appears to be, what the organization is particularly proud of, and what current challenges and difficulties the organization faces. Having established the ethical nature of the workplace, the supervisor should make it clear what the organization stands for in terms of its economic objectives and what impediments are in the way of the goal from being achieved.

The new staffer may think that he or she knows what the organization’s reason for being is, and probably does to some extent. But relating what takes place at the job site and putting it into a larger framework of the organization’s total goals and strategy is useful and valuable in the early interactions between the supervisor and new staff members. For example, a financial organization may seem like it is focused on retail services. In actuality, loans and domestic and foreign trading may be far more important to the enterprise for its profit objectives. Security personnel

might need to know which business segments are most critical to the enterprise at the current hour.

- c. *What the job involves.* The training received by the new worker is valuable, providing general, legal, operational, and emergency information to the new security worker. But on the job site itself, the nature of the tasks to be performed by the worker needs to be reviewed. This is the time for the supervisor to make sure instructions are understood. This is also the period to make clear the extent to which the supervisor will be available for assistance, the ability to contact other coworkers on the job sites for any assistance, and steps to take in an emergency situation.

Initially, the new worker is likely to assist or shadow the efforts of an experienced person who acts as an on-the-job trainer and facilitator for the new staffer. The supervisor usually introduces the two parties to each other and observes the nature of the interaction. If the on-the-job trainer previously has not trained a new worker, the supervisor will stay in touch with both on a more frequent basis than would otherwise be the case. Before leaving the new worker with the experienced security staffer, the supervisor may again review important aspects of the job. The supervisor also will emphasize possible pitfalls and ask whether the new worker understands what has been said and whether he or she has any other questions. It is usually not enough for the new employee to acknowledge that he or she understands. The supervisor may wish to pose a simple question to see how the new worker has integrated understanding the work expectations. For example: “You may need to make a decision between two possibilities both of which deserve attention. What would you do if your supervisor called on the way-radio for you to come to the control room right-away and at the same time someone slipped and fell within your vision?”

- d. *Review of post orders.* Critical details on what is to be done at a particular work station (post) usually are prepared carefully in advance. Post orders are not comprehensive but are based on the needs at a particular location. Orders are written based on previous experience at the post. Many organizations regard post order as critical guidance documents for workers. They are also regarded as business proprietary. Post orders usually should not be removed from the workplace and copies of them should not be made without higher authorization. The post orders are not narratives, but are usually work issues that are fundamental for the particular location.
- e. *Where to get what’s needed for the job.* The new staffer will need access to a supervisor and coworkers in order to obtain general information. Specialized information and supplies and services may be needed for the position as well. The worker is on post and may need instant help, replacement parts for equipment that fails, or routine supplies that are unexpectedly exhausted.
- f. *How the quality of work is to be measured.* Workers in production and service positions are interested in learning what the *quality* of work is to be expected. This is particularly the case when trainers have stressed how the organization places

emphasis on superior results. Security officers may have the quality of their work assessed primarily by direct observation and frequent interaction with supervisors. However, other methods are also available, including measurements and electronic recordings of data collected by the officer, observations and informal and formal reports by other workers, observations and reports by senior managers interacting with security personnel, and questionnaires and comments from customers or the public.

Alarm monitoring operators may have quality of their work measured by the speed, manner, and accuracy with which an alarm condition is responded to. Central monitoring operations often have quality control standards that will be subject to supervisory or management review.

Investigators usually are evaluated on the accuracy, completeness, and insightful evaluation of the investigative reports they complete. Such reports may be required for use in legal actions. Investigators often are separately judged by how well they use databases to speed their fact finding. Further, the ability to interview others well, including obtaining of signed significant statements, is attendant to evaluation of early stage performance by investigators.

Armored car personnel may be measured by the care and accuracy by which they note the deliveries and pickups from the various locations on their routes. Attention to security procedures will be another factor in determining quality of job performance. For example, does the guard vary routine as much as possible? Are firearms maintained in a safe and responsible manner? Does someone remain locked within the armored vehicle at all times, if company policy requires this measure?

Cash handling back-office personnel are similarly assessed by the accuracy and speed of their work. The ability to handle exceptions smoothly is a measure of performance.

Security technicians are judged by their ability to complete a task fully, without the need for subsequent service calls. For example, a particular alarm system installer might take a few minutes longer than a peer to install a system. But that technician may complete the job with higher quality and instruct users on applications well so that further service calls will be less frequent.

The staffer may be informed that quality is a constant issue to be discussed with the supervisor. However, near the end of the probationary period and during formal reviews, the results of such findings will be discussed specifically.

- g. *How the quantity of work is to be measured.* Quality matters; however, *quantity* does as well. In security work, the nature of tasks performed by security personnel is increasingly measurable by security systems that track completed tasks. Quantity of tasks completed by personnel is an important and usual basis of evaluating workplace performance.

Security officers may be measured by the frequency of security rounds to posts they must cover. Also, the number of specific recorded services may be a basis

of evaluation. For example, the actions of security officers who conduct escorts, key runs, or vehicle checks may be recorded by data entry systems. Over time, these will serve as a basis for comparison between security guards working during similar time shifts. Such reports may also be aggregated to document total services performed by the security unit over a period of time to the entire organization.

Alarm monitors may be evaluated by the number of customer interactions during a work period. To be sure, a slow number of alarm conditions may not reflect badly on a monitoring operative if that is the reality. In such cases, however, management will wish to evaluate the circumstance to determine whether an alternative way of managing alarms could be arranged to achieve optimal use of personnel, if an alarm monitor is not busy enough. In handling telephone communications with system customers, management may set a desired goal of maximum average customer contact time, for example, 2 min. Signals to the operator and supervisor can indicate when that point has been reached.

Armored car personnel may be monitored by time required for the number of runs assigned to the group for the course of a shift.

Security technicians may be judged by the number of installations and service calls completed during a period of work. Depending on the nature of the tasks, the assessment may be on a daily, weekly, or monthly basis. Adjustments can be made for time off or other circumstances that otherwise would make comparison meaningless.

In many cases, the quantity of work completed by security service workers is not comparable to that of other employees where measurable units of production or sales can be counted. That does not imply, however, that supervisors and their managers are not concerned about measuring the quality and quantity of individual personal efforts. Supervisors and their managers constantly search for fair, logical means by which work can be measured and assessed.

- h. *Relevant resources.* The supervisor will make the new staffer feel more prepared to deal with the tasks at hand by providing resources directly related to the organization and to tasks at the specific job site. The following are some important examples:
 - *New employee manual.* In most assignments for new employees, a new employee manual will be distributed, usually during the orientation phase. This may produce numerous questions for the new worker that have not previously been addressed. The supervisor should encourage the new worker to read the manual privately and raise any questions that may not be clear.
 - *Job description.* The new worker has been selected because he or she is capable of performing the required task and has been trained to do it. The job performance criteria should remain accessible for the worker. However, it should be made clear that job descriptions are not immutable documents, but rather change with the times as the nature of the job is modified to fit evolving circumstances. As part of the second orientation, the supervisor may wish to

review the job description and ascertain what tasks the new employee might have some concerns with.

- *Rules and regulations.* Requirements of the workplace need to be reviewed early in the relationship between the new staff member and the supervisor, even if the training provided covers many or all of these points. If the facility does not permit smoking even at entrances, that should be mentioned. The policy for personal use of telephones, facsimile machines, and Internet resources should be discussed. In some organizations, employees will be asked to sign a form indicating that they have read and understood the rules and regulations of the organizations.

Visitors usually are not permitted on the job site except for exceptional circumstances. How should such accommodations be arranged? Many operational security staff are expected to arrive a few minutes before the beginning of their shift or scheduled responsibilities. No work is to be performed. If it is, the time is compensable. Employees also may remain for a few minutes after their work is over without compensation. However, presence at the workplace for nonmanagerial workers when they are not scheduled to be at the job is not permitted in many security operations.

If the workplace requires security personnel to possess and carry firearms or weapons of any types, specific regulations will pertain to them. Security programs that require employees to be armed, for example, armored car firms, generally issue weapons at the beginning of a shift and recover them at the end. The state or county may require a designated firearms registrar to manage the program. Otherwise, any employee who brings weapons to the job without authorization is subject to sanctions, including instant dismissal.

- *Property.* The worker needs to know what property she or he will be assigned and how that property should be cared for. Property may include various types of keys, two-way radios, cellular phones, laptop computers, data collection devices, manuals, vehicles, uniforms, and weapons. Patrol cars, bicycles, and mobile conveyances also are important for surveillance. Conceivably, drones used for surveillance of a large area may be used as part of the program. The employee's role in protecting electronic assets, including programs, hardware, and output, should be made clear. Password protection issues should be covered.
- *Discretion about the workplace.* Employers expect that new workers at all levels will be positive about their new places of employment. It is natural for workers to want to share new experiences and observations with friends and others outside of working time. However, for many reasons that need not be articulated, workers should be encouraged to be discrete about personnel, procedures, and plans they learn of concerning their new organization. They surely are welcome to speak with others of their pride in being associated with their present employer.

The best rule of thumb concerning discussing something private with an individual not part of the workplace is need to know. If someone outside of the organization asks a question involving the proprietary organization, the need to know of such information needs to be assessed. If the outsider or insider asks about a proprietary matter, the worker should defer answering the question in a nonprovocative way.

- *Hazardous materials.* The worker needs to know what his or her rights are concerning any chemicals or material safety issues that could affect them on the job. Specific training on the observations of and response to any hazards must be provided before staffers are responsible for such materials. If a hazardous condition exists within the vicinity of the workplace, the worker needs to be informed of it.
- *Organization chart.* This helps the worker understand the personnel structure and reporting relationships at the place of employment.
- *History and CEO's welcome.* A leaflet, booklet, or video of the organization's history may help make the workplace more alive and relevant to the new staffer. It may also make the new staffer feel more connected with the breadth of operations of the employer. Sometimes, in large organizations, a video message from the CEO welcoming new workers is presented.
- *Career tracks.* Most new employees have cloudy visions about how they can grow in the job and where their initial positions can lead them. The supervisor or manager should make clear what the realistic career growth opportunities are and how individuals will have an opportunity to take advantage of them when opportunities arise. Examples may be provided of workers who advanced within the organization.
- *Compensation.* Human resources will have established the pay level for the new employee. Therefore, this topic is not one the supervisor usually needs to dwell upon. However, frequency of pay reviews and their significance over the first 2 or 3 years of employment may be discussed with the employee. This discussion should not indicate that pay increases will be automatic, unless this matter is a workplace policy. The supervisor is cautioned to speak of pay and performance reviews only in general terms and not to make statements more appropriate for a human resources manager. Generally, supervisors do have significant impacts on changes in compensation for workers in the unit.

How compensation is delivered physically or electronically to workers should also be explained. The location of the compensation office or its telephone number should appear in the literature provided to the new staffer. However, the organization may prefer that routine questions concerning compensation be transmitted via e-mail. Employees who work at dispersed posts are likely to have compensation and related issues handled by supervisors.

- *Benefits.* Technical questions on benefits are best referred to the human resources department. However, supervisors may provide some general advice,

if asked, on the different types of benefits when a choice is required. Supervisors should never put themselves in a position of forcefully arguing for one type of benefit option over another, but rather answer questions so that new staffers are fully apprised of the opportunities management has made available. A new worker may be grateful years later if a supervisor encourages her or him to participate in the employer's 401(k) self-contributory retirement or other similar program.

- *Creature comforts.* New workers need to know where the restrooms are on each floor, and where the cafeteria or canteen is located and the policies related to its use. Many workplaces provide subsidized meal facilities on-site for employees. Guest diners may not be possible under ordinary circumstances. The new employee needs to be apprised of such rules.
- 2. *Staffers need general guidance to do their jobs properly.* Despite superior efforts of employment selection, training, and orientation, circumstances may occur within the scope of employment in which the worker will need further assistance. This is the task of the supervisor.⁴ Several types of such guidance may be needed:
 - a. *Routine job support.* The supervisor's presence supports and guides security personnel in dealing with circumstances where the vision of a more experienced person could be of benefit. Frequently, these situations involve public contacts by security personnel in which the supervisor later may critique the performance of the worker. Often, the supervisor may be present to take responsibility for managing the situation on the spot. Supervisors also provide guidance to the worker on organizing tasks, writing reports, and dealing with unexpected events.
 - b. *Public relations skills.* Much of the activity of security workers concerns the public. Therefore, the enhancement of interpersonal skills is a concern of the supervisor and middle managers. The successful supervisor provides support to enable the staffer to understand his or her emotional predisposition in dealing with the public, particularly when members of the public are confused, stressed, or angry.
 - c. *Information support.* The job environment evolves constantly. Risks change. Procedures are altered. Personnel come and go. Workers expect to be informed by supervisors of the routine but significant news and information pertinent to the jobs. During contacts with staffers, supervisors are expected to share factual information that can help the worker understand the current circumstances at the job site.
 - d. *Specialty information.* When a new procedure, tool, device, database, or system is introduced to the workplace, the staff person may require assistance beyond training. At such times the worker turns to the supervisor for specialized assistance in mastering the new resource. In this sense, the supervisor continues the training by providing field support for workers.
- 3. *Staffers deserve to be recognized for good work.* Kenneth Blanchard and Spencer Johnson have provided a simple but compelling method of emphasizing the positive. Supervisors and managers are expected to recognize good performance

they observe among staffers to help their behavior become better still.⁵ Supervisors know that prompt recognition of good work reinforces it, increasing the likelihood that the desired behavior will become learned and be expressed as natural behavior. Supervisors are logical authority figures to observe and comment on superior and commendable behavior that they observe. Moreover, it is an expectation that they will do so. Normally, the supervisor will provide the direct positive feedback to sustain desirable performance. However, on some occasions, the supervisor may arrange for her or his manager to deliver the praise.

Supervisors have a number of means available of delivering the positive feedback that most workers crave. For example:

- a. *Verbal feedback.* The simplest and most direct means of recognizing good work is by a verbal message. Behavioral research over the past half-century has established the powerful implication of reinforcing desired behavior. The message should be direct and simple. The Blanchard–Johnson thesis suggests that people should know up front that the supervisor is going to inform them how they are progressing on the job. People are praised immediately on good work (Box 5.1). The praise is specific. The manager says how good he or she feels about what the worker did and how these actions help the organization. The manager stops for a moment of silence to let the person being praised “feel” how good the manager or supervisor feels. Further encouragement is offered. Finally, the manager shakes

BOX 5.1 THE ONE MINUTE MANAGER ON PRAISING GOOD WORK

Two wise and popular authors, Kenneth Blanchard and Spencer Johnson, have provided valuable guidance on how people who manage others may achieve goals productively and humanely. In *The One Minute Manager*, the authors describe a mythical extraordinary manager who achieves success with such brilliance that he leads an efficient and humane high-achievement orchestration of his subordinates’ performances. Much of the book describes the simple premises that lead to this achievement. At the center of the strategy the mythical marvelous manager believes in catching an employee “doing something right,” reinforcing this desirable behavior:

1. Tell people up front that you are going to let them know how they are doing.
2. Praise people immediately.
3. Tell people what they did right; be specific.
4. Tell people how good you feel about what they did right, and how it helps the organization and the people who work there.
5. Stop for a moment of silence to let them “feel” how good you feel.
6. Encourage them to do more of the same.
7. Shake hands or touch people in a way that makes it clear that you support their success in the organization.

Source: Blanchard, K., Johnson, S., 1983. *The One Minute Manager*. Berkley Books, New York, NY, p. 44.

hands or touches people in a way to make it clear that the manager supports the staffer's endeavors in the organization. For example, the manager might say: "That last visitor was irate when he arrived. You listened sympathetically to what was bothering him. Then you provided a helpful suggestion. In the end, he left in a better frame of mind. That's an ideal way to handle such a circumstance." Speaking directly, specifically, and objectively to workers about their exemplary behavior stimulates the acknowledged behavior to be remembered, and possibly further improved upon.

- b. *Formal written praise.* A letter or memorandum that summarizes superior behavior also can reinforce desired behavior. The difference is that such communication represents a tangible document and requires more effort: the tribute requires discernment and concern. The written praise also can become a permanent part of the worker's record.

Some supervisors pause about bestowing workers with written praise because they fear that the laudatory remarks could return in the future to haunt the writer. For example, an employee whose work was once praiseworthy might use letters in defense when that employee later is disciplined for cause. However, managers who are consistent can use written communications to complement workers as well as to correct behavior (see Chapter 7). The practice of formalizing approval of superior behavior in written form often produces a sense of pride and a commitment to further good efforts that extend beyond verbal honorable mention.

Formal written approbation is also appropriate when a director or manager at headquarters wishes to applaud superior behavior of those working at distant sites. The process of formal approval from an executive at headquarters has a powerful impact on individual performance, sustaining it in ways words alone could not achieve (Box 5.2). Writing costs little and means much. Employees understand this.

The physical letter is less frequently part of daily communications in a world operated by e-commerce. Subordinates respond well to e-mails from those higher in the hierarchy for work well done. The effect of sharing the praise can be achieved by copying significant others in the message.

- c. *Provide certificates.* A supervisor might provide a certificate of good service, signed by the supervisor and manager and presented thankfully to workers, as a tangible example of recognition. For example, if the organization is opening a new facility that will require an extensive period of intensive work, the awarding of certificates to the workers who participated in the process would be appropriate.
- d. *Promotion.* The supervisor may use good work as a basis of promoting the worker to a higher classification.
- e. *Better scheduling or conditions.* To reward the deserving, the supervisor may be able to find preferred hours, days off, locations, or improved conditions for the workers meriting positive feedback.

BOX 5.2 A LETTER FROM J. EDGAR HOOVER

For 47 years, John Edgar Hoover (1895–1972) not only led the Federal Bureau of Investigation but was also the FBI itself personified. Hoover was in his post too long and used his power to achieve control by attempting to destroy or silence those with whom he did not agree. In the years following his death, his reputation has been sullied by many critics and FBI personnel who later felt free to speak.

Nonetheless, Hoover should be regarded as a brilliant manager whose early efforts turned a poorly supervised group of politically appointed hack investigators into a highly efficient and ethically salutary organization. Hundreds of security directors in public and private organizations were trained during the Hoover years and were influenced from the controlling reaches of Hoover's Pennsylvania Avenue office suite.

Hoover trained special agents in charge of FBI field offices to observe and report to the central office details of superior field performance by individual special agents. Just days after a significant FBI operation, special agents might receive in their mail a letter personally addressed to them from FBI headquarters. With trepidation they would open it. Inside would be a brief recitation of the special agent's recent actions and would end with the observation that this behavior was in the "highest traditions of the Bureau," signed in ink by the director himself. Some special agents had received a number of such citations by the time their careers ended. The letters from Hoover were powerful motivators and served as lasting treasured mementos to the special agents who received them. (The opposite was also true. Hoover would criticize disappointing behavior of special agents with the same precise language used to praise. Attempting to defuse such a stinging message usually was futile.)

- f. *Award merchandise.* Numerous contract security guard companies provide merchandise awards for service above the normal standard. One major security guard company created a catalogue of merchandise available for achieving a certain number of points. Goods ranged from pens to jackets with corporate logo. Site supervisors as well as the client could provide points for superior performance.
- g. *Provide a night out.* In Great Britain, many service businesses, including security firms, provide recognition for superior performance by awarding the worker with an evening's entertainment and dinner for two on the town. These are popularly called "bennies." Scaled-down bennies may be concert or theater tickets without food.
- h. *Cash or bonus.* Almost all workers like to be told they have done a good job with cash.

This list is not complete, and is limited only by imagination. Some supervisors will find other unusual ways of recognizing their employees, which we will discuss later in this chapter. The tangible and intangible recognition that a supervisor might provide all carry with them degrees of desire and significance. Surely, excessive use of any reward system can cause it to become unproductive, leading eventually to its collapse. Regular compensation and the benefits of job security are, of course, the motivator

of greatest significance. The astute supervisor focuses on desired behavior to support it with a reward that is appropriate to the circumstance. Such tangible or intangible rewards should not disturb the web of workplace personal relationships by unfairly rewarding some persons and ignoring others.

Ideally, such awards and benefits are deserved and are seen by other workers who are not recipients, nonetheless, as a cause of general congratulations to the persons being recognized. Good work is recognized publicly so that the recognition and rewards can have a quantum effect on the immediate recipients and all other workers in the unit. Other programs such as Employee of the Month and Officer of the Month can reward superior achievements.

4. *Staffers deserve constructive criticism for poor performance.* Desired behavior is achieved more effectively by emphasizing positive traits rather than trying to suppress negative ones. Still, poor performance occurs in the workplace. Sometimes workers do less than their best to see if they can get away with such behavior. This is the top of a slippery slope that, when taken, leads to diminished quality performance. At such times, the supervisor must provide constructive criticism so that such behavior can change. In most cases, the worker is aware of the substandard performance and awaits reaction from the supervisor. If such a reprove is not forthcoming, the worker may lose respect for the supervisor and also feel permitted to engage in a continuance of such activities.

Unlike the public reward for good behavior, poor performance deserves prompt, constructive, private reproach. Again, the Blanchard–Johnson thesis has a strategy for responding to undesired workplace performance (Box 5.3). Positive feedback is easier for the supervisor to learn and use than the reverse. However, both are part of management techniques to support desirable behavior. The following steps ensue:

- a. The supervisor summarizes specific unsatisfactory behavior and asks if the facts are essentially correct. If the worker starts to explain or otherwise not answer the question immediately, the supervisor cuts off the digression until the worker agrees that the facts are essentially right.
- b. Next, the supervisor briefly states that the behavior was unsatisfactory. The supervisor avoids criticizing the worker personally, but rather makes it clear that the particular acts were unacceptable. The supervisor attempts to avoid circumstances in which the worker seeks to turn blame to others for the situation. The burden for the correct behavior is on the worker alone in most cases. (In some situations, additional training may be needed to correct the cause of the substandard performance; other measures also may be indicated.)
- c. The worker acknowledges the poor performance that has been described.
- d. The supervisor asserts that she or he has confidence in the worker's abilities, and a reference might be made briefly to positive aspects of the worker's performance. The supervisor indicates that the interaction has come to an end by lightly touching the worker on the shoulder or elbow. The worker returns to his or her duties. The process is over.

BOX 5.3 THE ONE MINUTE MANAGER ON CORRECTING POOR WORK

According to the Blanchard–Johnson thesis, successful managers leave subordinates alone to do their work undisturbed. However, sometimes work is not satisfactory and a reprimand is necessary. The *1-min praising* is conducted ideally in a presence of other people. By contrast, the *1-min reprimand* is *always* conducted outside of the view and hearing of other employees. The following presents the essence of the Blanchard–Johnson human relations strategy:

1. Tell people beforehand that you are going to let them know how they are doing and in no uncertain terms.
The first half of the reprimand:
2. Reprimand people immediately.
3. Tell people what they did wrong; be specific.
4. Tell people how you feel about what they did wrong, and in no uncertain terms.
5. Stop for a few seconds of uncomfortable silence to let them feel how you feel.
The second half of the reprimand:
6. Shake hands, or touch them in a way that lets them know you are honestly on their side.
7. Remind them how much you value them.
8. Reaffirm that you think well of them but not of their performance in this situation.
9. Realize that when the reprimand is over, it's over.

Source: Blanchard, K., Johnson, S., 1983. *The One Minute Manager*. Berkley Books, New York, NY, p. 59.

5. *Staffers should have opportunities to show that they can accept greater responsibilities.* Many high-performance workers are not happy with their *status quos*. They want to improve themselves. Astute supervisors realize that the needs of such self-improvement can be channeled productively when the employee feels that he or she has the supervisor's support in advancing in the workplace.

Promotion might be an eventual option for the worker seeking greater responsibilities. In the meantime, the worker may be given opportunities to demonstrate a competency in new circumstances. The worker may be assigned a special project or task, perhaps one that the supervisor does not have time for. Yet such an assignment requires burdens on the supervisor: the original worker may require some time realignment from his or her previous schedule; work normally done by the worker may be performed at less than its usual level; and other workers may sense that the special assignment reflects undue favoritism and creates new problems for the supervisor in the process. However, such assignments produce insights also, making the extra burdens on the supervisor worthwhile. The worker who is willing to accept increased or more challenging responsibilities deserves the chance to do so.

In many organizations, supervisors find ways of distributing special assignments and responsibilities among many staffers, indeed, among everyone who seeks additional opportunity. In all cases when such workers have demonstrated their abilities, such achievements should be recorded in their personnel file.

Safety at Work: The Responsibility of Supervisors

The American workplace is generally safe, or safer than it was in past generations. In the nineteenth and early twentieth centuries, for example, security guards were the knights of ownership, protecting private property from striking workers. In this type of assignment alone, scores of security workers were seriously injured in attempts to fulfill their duties. Similarly, numerous thieves, vandals, and strikers were killed or injured by zealous private security personnel.

Even now, security staffers have a higher risk than most employees of serious injury and death.⁶ However, while not minimizing any loss of life, private security personnel and public law enforcement are not among the occupations with the highest fatality rates when all sources of workplace death are considered. Yet, many security personnel have been victims of personal assaults at one or more points in their careers. In a few cases, injuries have reached the level of felonious assault. About 20–60 protective security workers lose their lives each year in the course of their employment (Table 5.1). In 2012, 49 homicides occurred involving non-law enforcement and other protective service workers. Most of these deaths occur during the commission of crimes; however, some are work-related, such as transportation accidents, or from other circumstances. From 2003 to 2013, 7 security officers died and 51 were injured during the commission of bank robberies, according to the FBI's *Bank Crime Statistics Reports*. Armored car deaths for the same period totaled 12 and an additional 75 injuries.

Industrial sectors have huge differences in terms of chances of fatal occupational injuries (Table 5.2). The difference in terms of occupational fatality between the safest (educational and health services) and the most dangerous (agriculture, forestry, fishing, and hunting) is 3 times per 100,000 full-time equivalent workers. In 2012, the total

Table 5.1 Homicides of Security Guards, 2003–2013

Year	Total Fatalities*	Circumstances of Homicide	
		Crime	Other
2013	57	26	–
2012	51	27	–
2011	64	32	–
2010	51	24	10
2009	63	30	7
2008	70	29	7
2007	84	35	8
2006	73	31	7
2005	60	25	6
2004	67	26	6
2003	71	28	9

*Includes fatalities from transportation, accidents, and other workplace incidents including crime.

Source: US Department of Labor, Bureau of Labor Statistics, 2013. National Census of Fatal Occupational Injuries, released September 11, 2014 (and earlier reports).

Table 5.2 Fatal Occupational Injuries by Industry Sector, 2012

Occupation	Fatality Rate Per 100,000 Employed	Number of Fatalities
Agriculture, forestry, fishing, and hunting	21.2	479
Mining, quarrying, and oil and gas extraction	15.6	177
Transportation and warehousing	13.3	677
Construction	9.5	775
Wholesale trade	5.0	191
Professional and business services	2.6	388
Other services (excluding public administration)	2.5	183
Utilities	2.5	22
Manufacturing	2.1	314
Leisure and hospitality	2.1	220
Government	2.0	438
Retail trade	1.9	262
Information	1.4	38
Financial activities	0.9	81
Educational and health services	0.7	139
Total	3.2	4383

Source: US Department of Labor, Bureau of Labor Statistics, 2013. National Census of Fatal Occupational Injuries in 2012 (Preliminary Results), August 22.

fatal work injuries reached 4383 with an all-worker fatal injury rate of 3.2 per 100,000 workers.

Occupations with high fatal working injury rates do not include security personnel. According to the US Bureau of Labor Statistics, US Department of Labor, among the 10 most dangerous vocations, logging workers rank 1st with construction laborers in the 10th position (Table 5.3).

Among all vocations, the most serious chances of fatality are from transportation accidents (41%). Other major frequent causes of loss of life in the workplace are falls and

Table 5.3 Occupations with High Fatal Work Injury Rates, 2012

Occupation	Fatality Rate Per 100,000 Employed	Number of Fatalities
Logging workers	127.8	62
Fishers and related fishing workers	117.0	32
Aircraft pilots and flight engineers	53.4	71
Roofers	40.5	10
Structural iron and steel workers	37.0	22
Refuse and recyclable material collectors	27.1	26
Electrical power-line installers and repairers	23.0	26
Driver/sales workers and truck drivers	22.1	741
Farmers, ranchers, and other agricultural workers	21.3	216
Construction laborers	17.4	210

Source: US Department of Labor, Bureau of Labor Statistics, 2013. National Census of Fatal Occupational Injuries in 2012 (Preliminary Results), August 22.

coming in contact with objects and equipment (31%). Chances of fatality from exposure to harmful substances and environments are less (7%). Fatalities from fires and explosions represent the smallest category (3%). Among workers, homicide represents 11% (463) of the total fatal occupational injuries in a recent year. Other forms of violence and injury at the workplace also occur. For example, in 2012, 225 suicides occurred in the workplace.

Not all security positions are equally dangerous. The night watchman in a warehouse or museum needs to fear the risk of an accident more than the possibility of felonious physical injury. Similarly, most investigators and central alarm station operators are at greater risk from falling than from being criminally attacked.

Physical assaults to security personnel are much more numerous than fatalities. Here again, security personnel are disproportionately victimized relative to most other vocations. According to a study based on the National Crime Victimization Survey (1992–1996), security personnel ranked fourth in occupational victimization for nonfatal violent incidents, adjusted for the number of workers, as shown in [Table 5.4](#). (This data set is the latest available.)

Workplace violence is a matter of concern for security supervisors and managers in many industries. Those at greatest risk work in armored car courier services, banking, food service, healthcare (especially emergency rooms), retailing (when making apprehensions), and at places of public assembly, such as theaters and concerts. Any location that has on its premises substantial cash and other liquid assets – check cashing businesses, cashiers, and jewelry businesses – creates risks for security and nonsecurity employees alike.

Security of workers is a management responsibility. Efforts to mitigate this risk extend from planning to training and supervision. This principle does not absolve, certainly, an individual security worker who abandons common sense and flaunts rules and regulations to take a risk that results in harm. Nonetheless, in such circumstances the supervisor bears inordinate responsibility in dissuading workers from actions that result in unacceptable risk-taking behavior. Further, the supervisor has direct responsibility in deciding whether a particular situation is too dangerous for trained security personnel. In such cases, the

Table 5.4 Occupations of Victims from Nonfatal Workplace Violence (1992–1996)

Occupation	Average Number	Rate
Police	234,200	306.0
Corrections	58,300	217.0
Taxi drivers	16,100	183.8
Security	71,100	117.3
Bar workers	26,400	91.3
Mental health	50,300	79.5
Gas station attendants	15,500	79.1
Convenience/liquor stores	61,600	68.4
Junior high teachers	47,300	57.4
Bus drivers	70,200	45.0

Rate is per 1000 workers. Calculated from National Crime Victimization Surveys for 1992–1996.

Source: Warchol, G., 1998. Workplace Violence, 1992–96. Bureau of Justice Statistics, Washington, DC. Report No. 168634.

supervisor should opt instead to keep security personnel away from the danger until the risk can be reduced to an acceptable level.

Most fatalities in the workplace are single events, that is, one actor and one victim. Incidents involving multiple homicides (three or more victims) are better understood. The author and Seungmug (Zech) Lee studied incidents and victims caused by workers from 1996 to 2013.⁷ During these years 46 cases occurred resulting in 273 dead victims (23 offenders committed suicide). An analysis of offender characteristics showed that 71.7% had no criminal history and 63.0% had no military experience. Additionally, only 21.7% had previous psychiatric histories. Those most likely to be predisposed to workplace homicide risk and, therefore, of concern to supervisors showed the following characteristics.

- To have been terminated recently or at any time in the past
- To be underperforming and facing a reprimand, negative evaluation, or termination
- To be argumentative with supervisors and coworkers
- To be described as possessing an “angry or loner personality”
- To have talked about perceived or actual slights by a supervisor or manager and who may have expressed the desire for revenge on the day of the incident
- To have access to guns or previously served in the military
- To live alone

When security staffers are in an environment in which workplace safety is poor, the supervisor holds direct responsibility on behalf of management in deciding the extent to which risk may be reasonably assumed. Chemical plants, healthcare facilities, and nuclear process industries are a few of the workplaces in which hazardous materials exist. Such facilities can be well managed and pose little risk for security personnel, yet wherever hazardous materials or conditions exist, supervisors have an obligation to assure that their people are not exposed to undue risks. In addition to hazardous chemicals, such factors as lighting, workplace design, safety devices, structural features, and even ventilation, when harmful, can present an unacceptable risk for employees.⁸

All employees have a right to know about the hazardous materials located within their workplaces. They have the right to obtain safety data sheets, which should be provided within 5 days of any request by an employee. While security personnel normally will not personally handle hazardous materials at such facilities, should the possibility exist, they need to be properly trained in emergency response procedures relative to such substances.

Why Be a Supervisor, Anyway?

The previous section indicated that “security supervisors are the direct link between the management of a security organization and the security officers who carry out the duties associated with the security function.” The security supervisor has to be willing to accept responsibilities, and must have demonstrated competence in technical, human, and conceptual skills. Often, the inducements to become a supervisor do not appear to be great, and many competent and valuable security staffers decide not to accept the promotion to supervisor

when offered one. Yet some compelling reasons exist for why operations-level workers may accept the challenge of a promotion and even seek it out from early days of employment:

- Achievement is reflected in the new position, buttressing one's self-image.
- Authority and control come with the position.
- Creativity is encouraged: the supervisor is a resourceful problem solver.
- Opportunity to higher positions such as middle management may be made possible.
- Pay and other benefits usually, but not invariably, are better.

Why Some People are Not Cut Out to be Supervisors

An assumption is that most workers deserve the right for greater responsibility. But some are not interested in accepting higher job duties. Their penchant should be respected, particularly if they are performing well in their current positions. Why upset the apple cart with a promotion that is not really wanted? The following are valid reasons for not accepting a promotion:

- The increased pay is not worth it to the worker.
- A promotion would upset familiar and comfortable working relationships with coworkers.
- The promotion would require a deviance from the familiar work schedule that would interfere with a familiar lifestyle.
- Family duties could not be handled so well following a promotion.
- The worker feels fully challenged and interested in the job as it is.

Duties of Employees to Supervisors and the Workplace

Up to this point in this chapter, obligations of the supervisor to his or her staff have been discussed. However, security employees themselves have obligations to their supervisors, management, and, by extension, to the management of the employing organization. This extends to contract employees and consultants who provide services. Such duties are not unreasonable burdens, but rather reflect the nature of the particular employment and its requirements. These are bound to change according to the workplace and its characteristics. Many of them will be described in the employee manual. As an example, the following are 12 rules and regulations established by a major casino for its employees, including security personnel. Note that rules 9 and 10 are specific to a gaming environment. While created for a particular type of workplace, the list may stimulate the reader to consider appropriate adjustments for other occupational settings:

1. Employees will conduct themselves in a manner promoting good public relations and goodwill.
2. Use of profanity, rude behavior, and lack of consideration for customers or other staff may be considered grounds for disciplinary action or termination of employment.

3. The use of force by company employees is forbidden, except as a last resort to protect the life of a customer, fellow employee, or oneself. In such a situation, only the minimum force necessary is acceptable. Protection of property *is not* considered grounds for use of force. Persons violating this policy may be prosecuted criminally or civilly or both.
4. The use or possession of alcohol, narcotic drugs, or any type of weapon while on company property is strictly forbidden.
5. Family members will not be hired as coworkers.
6. Sexual harassment – or any act that may be considered as sexual harassment – is strictly forbidden. Any reports of such conduct will be fully investigated.
7. No one other than authorized employees or official visitors is to be given access to any office or storage areas at any time.
8. Cash collection policies and requirements for recording transactions must be followed exactly as written procedures indicate. Failure to do either may result in termination of employment.
9. Employees will not play games, be a partner in games with customers, or finish a game for a customer or one that a customer has abandoned.
10. All refunds or settlements of customer disputes will be conducted as prescribed and recorded on the proper form.
11. Employees will not store or hold packages or valuables for customers.
12. Employees will not discuss company business, policies, or practices with any person not authorized access to such information.

This example of one organization's general rules and regulations reflects concerns about general civility, the drug-free work environment policy, sexual harassment, and policies and procedures that, if not followed, can promote internal and external crime. In this case, employees were asked to sign a statement that they had read and understood these rules and regulations. Further, employment terms stated in the employee manual are also to be considered conditions of employment and violation could lead to termination. The new employee signs and dates such a statement. The signature is witnessed by a supervisor or human resources manager.

Rules and regulations of other security departments commonly stress punctuality, care of uniform, personal hygiene (showering before reporting to duty and changing one's underwear each day), and respect of the employer's property.

Motivating Supervisors and Staff

Supervisors and managers at all levels are responsible for achieving and maintaining high levels of workplace productivity. As part of this objective, management is expected to maximize use of time. Personal time management techniques can be useful for management at any level. But apart from using one's time well, a separate conceptual category – motivation – is addressed to help supervisors and managers understand this topic.

Time Management for Supervisors and Managers

The first chapter of this book discussed the seminal contributions of Frederick W. Taylor in establishing the time study method for improving workplace productivity. This concept is applicable in process work in which employees are responsible for measurable throughput. But the tasks of first- and second-level management require time for planning, organization, direction, and problem solving. The need for time devoted to planning is hard for many managers to find. Although nobody has more than 168 hours per week, some individuals are able to accomplish more than others. Certain time management techniques can help motivated and disciplined individuals to accomplish more.

Business school professor Henry Mintzberg wrote: “Free time is made, not found, in the manager’s job; it is forced into the schedule. Hoping to leave some time open for contemplation or general planning is tantamount to hoping that the pressures of the job will go away.”⁹ Many books have been written on time management, and numerous others are doubtlessly awaiting their day. They have influenced millions. Nonetheless, time management is a topic not readily adaptable for quantitative research; therefore, it is not always clear which methods work best for particular individuals. Close observation of successful managers identifies attributes that lead to achievement and greater productivity. Superior time management is part of that achievement path. Some widely used techniques to increase managerial productivity are given in the next subsections.

The ABC Technique

Not all tasks are equally important. A manager can face a seemingly endless series of demands on his or her time. Yet concentrating on what’s most important, making these tasks the priority, and working on them until they are completed will enable the most important work to be completed before less important items.

The ABC technique directs users to divide all work-related matters to be handled into three categories: A, vitally important; B, of nominal importance; and C, unimportant relative to A and B. The manager learns to identify what is A, B, or C quickly on being presented with a task or opportunity. Greatest effort is devoted to A, B is next, and what time is left goes to C.

The Pareto Principle

Popularly called the 80/20 rule or Pareto’s law, this is another control scheme like the one previously discussed that ranks workplace tasks in order of their importance. The principle is named for Vilfredo Pareto, an Italian economist whose insight into management priorities emerged in a roundabout way.¹⁰ In 1908, Pareto proposed that the distribution of wealth and income in a population was mathematically predictable and generally held constant over time. In time, the principle expanded to fit other circumstances.

While the ABC analysis denotes three categories of analysis, the Pareto technique focuses on the inverse relationship between the percentage of items in each of a set of subclasses and the importance of such subclasses. The principle is best illustrated by thinking about

customers or clients in an organization. Not all are equal. Through the use of conventional analysis, some customers or clients will be particularly important. The Pareto principle posits that 80% of an organization's sales are due to only 20% of the customers, and vice versa.

The 80/20 ratio is not meant to be taken literally, but the point holds across numerous applications that a small number of issues or customers – external or internal – are substantially more important than others to the operation. The principle has limitations and dangers. It encourages proponents to focus on the important 20% in the organization. That certainly seems wise, but at some point various components of the important 20% may disappear for reasons over which the service supplier has no control. And components of the less profitable or urgent 80% might then become more important. Supervisors and managers must consider that all customers, clients, and tasks are important, but that the important differential over time can be helpful in prioritizing what to do first, if competing demands for service are received at about the same time.

Slow Down to S.T.O.P. to Move Ahead

Yet another and more recent technique for organizing one's time has been proposed by Clinton O. Longenecker¹¹ (Figure 5.1). The technique serves a purpose to aid supervisors, managers, and executives to optimize their use of time by allocating a few minutes *each day* to center on what's most important to be achieved. Longenecker determined from a survey of 1500 supervisors and managers that 66.3% believed they were “too busy.” When this happens, leaders were committed to something previously planned so were unable to undertake additional activity. They were engaged in constant, challenging, and ongoing activity.



FIGURE 5.1 Clinton O. Longenecker, a management professor, proposes a slowdown to S.T.O.P. process to achieve better management results to create rapid change in organizations.

Using an analogy from football – the 2-min drill – Longenecker proposes achieving better results by slowing down. First, S = sit at the beginning of the day to think clearly about the priorities ahead. Next T = think; devote real and critical thought to important and key results that drive cumulative effectiveness. Next O = organize, that is, plan for the specific actions that must be implemented on an ongoing basis to achieve desired outcomes. And P = perform, or execute the plan of action that addresses the key issues that lead to the desired outcomes and results.

Longenecker advises spending 15 min at the start of each day to develop a “performance script” to put the daily S.T.O.P. into action. Then midday a 5-min midshift takes place to adjust according to circumstances. Finally, at the end of the workday, 5 min are allocated to learn, adjust, and plan for the next day. All told, working a 9-hour day, S.T.O.P. requires 25 min or 4.62% of the day, time well spent to increase effectiveness.

Time Analysis Management

Why is it that some people are more effective when they appear to work no harder or longer than others in the same position? Perhaps they have learned and practice the previous principles. To determine whether excessive emphasis is placed on matters that are not true priorities in a manager's agenda, time analysis may help.¹²

One key to time analysis is to obtain an accurate record of how one's time is used. Time logs may be used for that purpose. A manager who keeps track of a typical week and then analyzes how his or her time is used may discover that too much time is devoted to tasks of minor importance. This leaves important obligations on which the manager is judged with less time than desirable to complete or to develop fully. In the process of keeping a time log, the logger quantifies time used for various activities and determines whether this pattern is satisfactory and justifiable. Often, the diarist is surprised to learn that counter-productive habits have crowded out valuable hours that should be allocated to priority work. This could bring the needed awareness that changes time-use priorities.

Delegate Everything Delegable

Supervisors and other managers have subordinates to whom work may be delegated. Directing and controlling activities generally are not amenable to being delegated.¹³ However, numerous other activities that a manager might ordinarily assume can be delegated. Routine memos and drafts of letters, reminder calls, organization of forthcoming meetings, normal requests for supplies, and related matters may be delegated to subordinates. This provides the supervisor and manager with more time for planning and for routine communication with workers, customers, and others.

Using Technology for Greater Efficiency

The highly productive manager constantly searches for ways to use time more effectively. Technology dramatically helps meet that objective. Managers accomplish more today than their predecessors. Personal computers loaded with time-saving software and apps,

laptops, palm computers, cellular phones, beepers, facsimile machines, and miniature portable dictating systems have greatly enhanced managers' effectiveness. A device or system that saves a manager as little as 1 or 2 hours per week is highly valuable over an extended period and is well worth the capital investment required. Technology that saves workers frustration and boring repetition can pay for itself. For example, investigators or field supervisors who regularly must visit new locations find it cost-effective to use a global positioning satellite (GPS) system in their vehicles, reducing likelihood of getting lost and reaching new locations with greater speed and certainty. Moreover, the investigator is likely to use GPS technology to surveil persons in an active investigation.

Clean Desk or Messy?

The vision of the manager with the desk completely empty of papers – except for the matter being worked on at that moment – seems powerfully etched in the minds of many CEO watchers. Such clean-desk managers are considered to be on top of things, cool, and fully focused on the decision immediately facing them. But are these persons really more efficient or effective? No strong evidence supporting the clean desk or messy viewpoint exists, although many high management achievers seem to have little paper on their desks. Others, though an apparent minority, achieve much – with piles upon piles of papers, records, books, and communications messages scattered everywhere.

Authors Eric Abrahamson and David H. Freedman argue that untidiness, hoarding, procrastination, and improvisation are not bad habits. A bit of disorder is beneficial for the creative process. A reviewer notes: “America’s professional organizers, a thriving and lucrative cult of tidiness coaches, are merchants of guilt, not productivity boosters.”¹⁴ However, some environments – surgery, a report for management, an income tax return, and a dinner table – need tidiness.

Starting the Day Early

Whether desks are paper-free or littered, attributes of high-performance executives lead to identification of personality differences. Stephanie Winston, a time management consultant and writer, has observed the “organizing principles” that have helped some CEOs reach the top.¹⁵

Skills of CEOs are pertinent to managers at all levels. These include structured but ample availability to receive the rich source of information from subordinates that help form executive decisions. Also, CEOs start their work days “very, very early to use dawn hours to grab some quiet time.”

Motivation Matters

Managers seek to elicit peak performance from subordinates. According to entrepreneur and writer Andrew S. Grove, high output from subordinates can be achieved in two ways: from training and motivation.¹⁶ Both can improve performance, yet training an individual with a low degree of motivation will produce far fewer benefits than training those

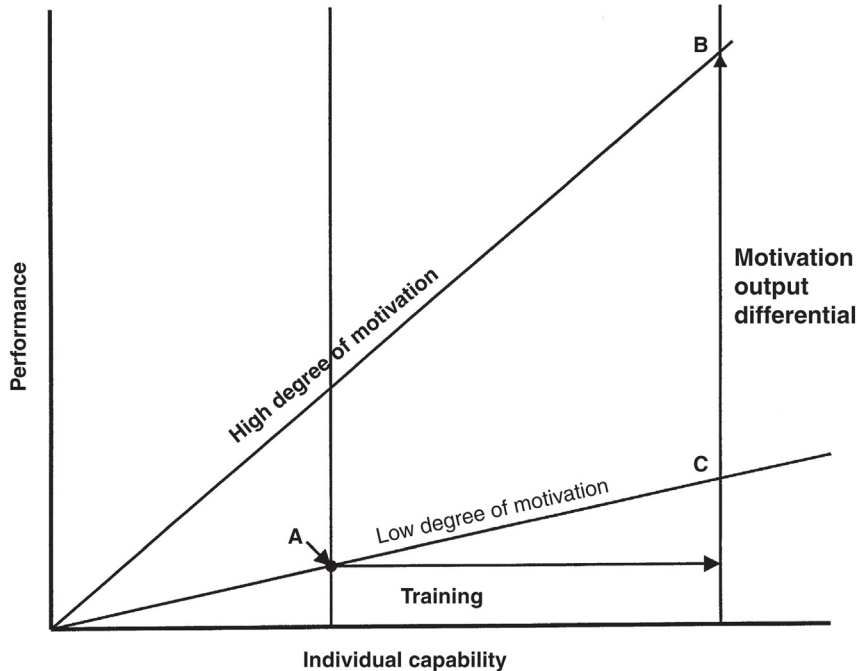


FIGURE 5.2 Linking performance to degrees of motivation and training. Managers have two ways to improve performance: training – or retraining – and motivation. Point A indicates the beginning of training, which serves to increase performance. Persons with high motivation increase capacity even further, eventually reaching point B instead of point C. (Source: Grove, A.S., 1985. *High Output Management*. Vintage Books, New York, NY).

who possess a high degree of motivation will. Figure 5.2 graphs the connection between motivation and training. Motivation research identifies the attitudes, habits, and motives that trigger desired behavior. A few theories have served to underpin the thinking of contemporary management and even have affected workplace performance.

Theory X and Theory Y

This famous management construct proposed by Douglas McGregor encompasses the complex and dynamic relationship between personality and motivation.¹⁷ A Theory X manager reflects authoritarian leadership favoring centralized decision making. Theory X is often thought of as the view of old-line management. Workers are to be supervised closely. Theory X managers tend to hold the following views:

1. Most people do not like to work and will avoid it whenever possible.
2. The average person prefers to avoid responsibility and would rather be told what to do than have to make a decision.
3. The most effective managers use punishment, or the threat thereof, to achieve their goals.

Theory Y, on the other hand, is sometimes considered to be “the unions’ view” of the ideal employer–worker relationship. The Theory Y view holds that:

1. Work is natural for most people and they do not avoid it.
2. If individuals are committed to the organization’s objectives, they will obtain satisfaction from helping to achieve those goals. Such exertion will be self-motivated.
3. Human potential is greater than what most managers realize. Most workers are capable of creative problem solving, but their employers are not conditioned to take advantage of this potential.

If placed on a continuum with X at one end and Y at the other, the X end would be harsh, punitive, and pessimistic. The Y end would be humanistic, optimistic, and laissez-faire. In reality, no known actual management practices constantly operate at either extreme. McGregor believed that most organizations possessed a culture that placed them on a changing but narrow band of the continuum. McGregor’s construct is useful for those who supervise behavior at all levels as it encourages supervisors to consider where they would place themselves – or be placed – on such a continuum. It also says something about the nature of workplace productivity and satisfaction. The popularity of McGregor’s research has engendered another concept, Theory Z.

Theory Z

Theory Z draws from observations of Japanese organizational management. The term was coined by William G. Ouchi, who identified practices that were unique expressions of Japanese culture and were difficult, if not impossible, to transfer to Western management practice.¹⁸ Ouchi posits that most Western-style firms embody McGregor’s principles in what Ouchi calls “Theory Z.” Ouchi uses Theory Z to refer to those American firms that copied or independently developed Japanese-style management concepts.

Theory Z allows the manager to move between the poles of Theory X and Theory Y depending on the circumstances. Theory Z focuses on stabilizing employment, greater employee workplace participation, and a slower system for evaluation and promotion. This scheme has been less admired by American organizational theorists since the Japanese economy faltered in the last decade of the twentieth century. It is likely, however, that Western managers will continue to look to Asia and elsewhere for ideas that might translate into greater productivity while improving worker satisfaction.

The Complexity of Motivation

What propels some workers to greater achievement fails with others. And what propels workers at one time may not be successful in the future. No single motivator is likely to work on its own. This is because motivation is complex and not amenable to sure-fire generalizations. Further, motivation is not equated with satisfaction. People are motivated (i.e., forced to perform) in order to achieve satisfaction (i.e., the pleasure of achieving a goal).

The Hawthorne Investigations

One of the earliest controlled research studies of production variables began at the Hawthorne, Illinois, telephone relay assembly plant of the Western Electric Company, a major telephone production facility of American Telephone and Telegraph (AT&T). In the 1920s, Elton T. Mayo, a professor at Harvard Business School, began research investigations into various environmental and situational factors that could alter production there.

In the early 1920s, Western Electric began a series of short experiments to ascertain the relationship between different intensities of workplace illumination and any changes in the resulting productive output. The studies were inconclusive and the researchers thought that relevant psychological variables were not adequately controlled. Advice was sought from Mayo, who began his research in 1927 and whose efforts continued through 1932. Mayo conceived the research in classic fashion: an experimental group of phone relay assembly testers worked adjacent to the general manufacturing area in a specially constructed environment that could be controlled for experimental purposes.¹⁹ The general manufacturing area would serve as the control group. The relay testers and other assembly workers – all women – were unaware of the objects of the experiments.

Over several years, experimenters sought to discover variables that could affect production, both positively and negatively. Initially, experimenters were amazed that productivity was enhanced even under adverse circumstances. Why? At length, the researchers found that workers in the relay assembly test room had developed positive personal relationships with each other. The socialization among the workers who had bonded with each other encouraged greater productivity compared with other workers in the general manufacturing area. Further, it was realized that the workers were operating in a social environment devoid of the supervisory controls operating elsewhere in the plant.

In all, about 20,000 employees were interviewed confidentially by members of the research team. The researchers concluded that attitudes within a social group affect productivity. The previous assumption was that the worker was an individual to be studied; post-Hawthorne conclusions were that the group needed attention. The human relations aspect of management research began.²⁰

In recent years, however, other observers have questioned the earlier sure assumptions of the research from Hawthorne. They noted that fear and uncertainty in the workplace may have had much to do with the successful efforts by the Western Electric workers to increase production despite disincentives. After all, by 1929, economic depression had arrived; jobs were not secure and the future seemed bleak. The workers apparently had no idea why they had been selected for the project and what the various experimental circumstances imposed on their working conditions meant for their personal futures. They were the subject of frequent visits by researchers and distinguished visitors who came to the Hawthorne plant to see what was going on. This made their workplace position seem special – they were the focus of special attention, yet the circumstances were ambiguous and unsettling at the same time.²¹ A once firm conclusion of the Hawthorne work – that paying attention to workers matters more than conditions – still seems reasonable, but is

not as firmly accepted anymore due to revised thinking about the economic times when the research itself was conducted.

The Hierarchy of Needs

In the early 1940s, an experimental psychologist, Abraham H. Maslow, propounded a theory that grasped the imaginations of many management thinkers because it recognizes that a variety of interwoven needs motivates human behavior.²² These needs reflect a variety of motivators and are believed by Maslow to be unchanged and instinctual. Maslow identified five interrelated need categories:

- *Physiological.* The fundamental needs of individuals relate to physiological concerns (the need for food, shelter, sex, air, and sleep).
- *Security.* Once basic physiological needs are satisfied, security necessities emerge. The dominant security needs are for reasonable order and stability and the freedom from being anxious and insecure.²³ Safety considerations also must be satisfied.
- *Belongingness (social).* With personal protection needs fulfilled, social needs occur. These reflect the need to affiliate with others and to be accepted by peers and supervisors in the organization.
- *Esteem.* Beyond the meeting of social needs, individuals require an opportunity to achieve self-esteem. This includes independence, freedom, recognition, prestige, status, and reputation.
- *Self-actualization.* Finally, Maslow coined the term self-actualization to point out that with esteem achieved, “what man can be, he must be.” That is, self-actualized individuals, not blocked by unfulfilled concerns of self-esteem, concentrate on assuming responsibility and involvement fully and at a creative level.

These needs are sometimes represented as a pyramid, a ladder, or a series of steps, as shown in [Figure 5.3](#).

What does this mean in relation to the management of general organizations as well as security work units? First, compensation has to be adequate to meet physiological needs. No matter how personally satisfying, a job may be abandoned eventually if basic living needs cannot be met by compensation (basic physiological needs). Next, security is an essential factor. A worker who is not safe on the way to or from work or who faces safety risks at work may leave regardless of the compensation offered (security and safety). Then again, if positive socialization is not part of the workplace, the environment seems unattractive for the worker and the job can lead to a low self-image (belonging and social needs). Next, self-esteem needs can be provided by management through various types of recognition in order to enhance feelings of worthiness and self-confidence (esteem and status). Finally, if all these needs are satisfied, the individual may become a fully creative and a wholly involved member of the workplace (self-actualization and fulfillment).

Maslow saw these needs as overlapping and believed that the average person was never fully satisfied in every category. Such completeness varies from 85% for physiological

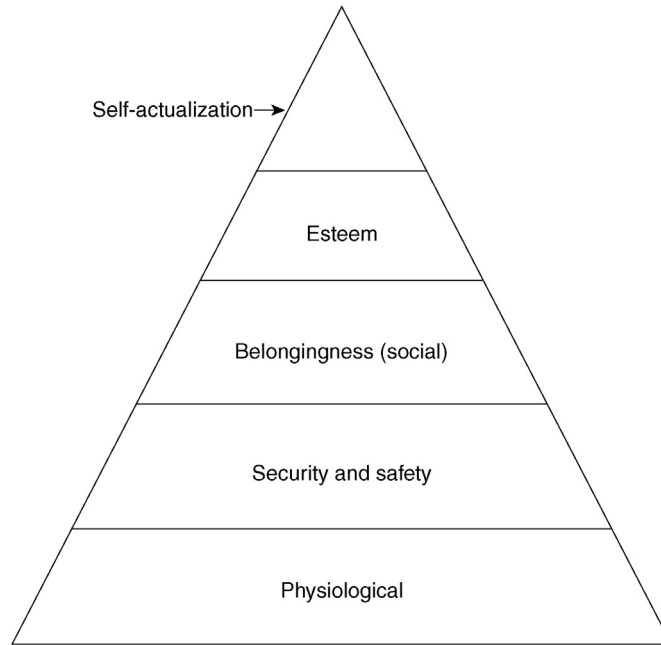


FIGURE 5.3 Maslow's hierarchy of needs. Maslow's hierarchy is sometimes referred to as need theory. The first-level needs involve basic survival. Normally, they are well satisfied in a typical work situation. Second-level needs do not dominate until first-level needs are reasonably satisfied. Then, third-level needs do not become significant until first- and second-level needs have been reasonably satisfied, and so on. (Source: Maslow, A.H., 1943. *A theory of human motivation. Psychol. Rev.* 50, 370.)

needs to 10% in self-actualization needs for the average person, he deduced. Yet Maslow's needs hierarchy encourages managers to think of the many levels of needs that exist within the workplace. Higher-order needs become motivators once lower-level needs are satisfied. Maslow arrived at this thesis by studying factory workers; however, the same points can be relevant to any management activity including protection program.

Motivational-Hygiene Factors

Another influential theory evaluated job satisfaction and the workplace. Frederick Herzberg and associates conducted semistructured interviews with 200 accountants and engineers concerning what they wanted from their employment.²⁴ The researchers also reviewed 155 studies that addressed the same question. Although they noted that results differ widely according to the research design, the Herzberg team found that motivational and growth factors determined job satisfaction. These factors included achievement, advancement, recognition, responsibility, and the work itself. The other aspects of the Herzberg study were found to be unrelated to the actual accomplishment of work. These aspects were referred to as "hygiene" factors because they were conceptually related to concepts of medical and mental hygiene. These factors included politics and administration, salary,

supervision, interpersonal relations, benefits, working conditions, and workplace policies and procedures.

Both motivators and hygiene factors affect employees, but motivators strongly influence job satisfaction. Herzberg provided statistical weights for job satisfiers (generally motivators) and *dissatisfiers* (generally hygiene factors), both of which exist concurrently. The dissatisfiers do not increase job satisfaction, but only affect the quantity of job dissatisfaction.

Money as a Motivator

The classical management strategist Frederick W. Taylor, referred to in Chapter 1, believed that people are highly motivated when their rewards are linked directly to performance. Later research showed limitation of this view. Obviously, money provides its possessor with a degree of control over life's circumstances. Beyond the fulfillment of human needs, money is a means of keeping track of one's status in a materialistic society. Yet since the early twentieth century, the power of money as the sole or paramount motivator has diminished in the assessment of workplace effort. Meanwhile, the power of other motivators has become more appreciated as drivers for human performance.

Workers surely need money to meet their physiological needs as identified by Maslow's terminology. But security managers know that even a small pay increment is appreciated for its psychological symbolism. Increases in compensation signify progress in the job at the same time as they help to meet material and social goals.

In an article in *Fortune* that dissected "the money society," a financial executive says: "It's not that people value money more, but they value everything else so much less – not that they are greedier, but that they have no other values to keep greed in check. They don't know what else to value."²⁵ It seems certain that monetary compensation remains so important because of its ability to help individuals track their progress personally and in relations to others. Managers constantly struggle to adjust motivators – including money – to achieve optimal staff satisfaction and program objectives.

Manipulated Self-Motivation: The Pygmalion Effect

In George Bernard Shaw's *Pygmalion*, a cockney flower girl named Eliza Doolittle comes under the persuasive admonitions of one Professor Henry Higgins, an apparently worldly wise elocutionist. Professor Higgins transforms the vulgar street girl into a poised, articulate, refined young woman with aristocratic pretensions. The much beloved play was made into a Broadway musical and later the motion picture, *My Fair Lady*. The concept of Pygmalion change derived from the sculptor in Greek mythology who carved a statue of a beautiful woman who then became real. Whether in mythology or in the movies, the concept of radical human change is a powerful one.

The Pygmalion effect is a kind of self-fulfilling prophecy, according to sociologist Robert K. Merton, who coined the term in 1948. Self-fulfilling prophecy is a three-stage process beginning with a person's belief – false at the time it is held – that a certain event will occur in the future.²⁶ Next, this expectation or "prophecy" leads to behavioral change that

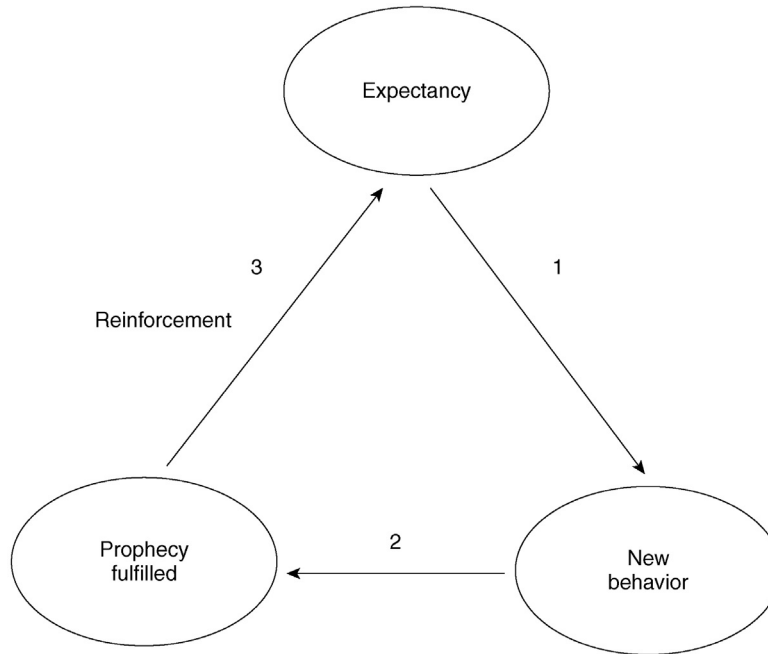


FIGURE 5.4 Pygmalion in management: the self-fulfilling prophecy. Robert K. Merton proposed the notion that expectations can produce results and coined this process. In the first step, a false belief is held. This is the “prophecy.” Arrow 1 shows the influence on new behavior. As a result, the prophecy results – Arrow 2 – in fulfillment. Finally, the prophecy is justified since the original expectation comes true. The original expectancy is further supported – Arrow 3 – after the prophecy is fulfilled, continuing the cycle. (Source: Eden, D., 1990. *Pygmalion in Management*. Lexington Books, Lexington, MA, p. 2.)

would not have occurred if it were not for this false expectation. Finally, the expected event occurs and the prophecy is fulfilled, as shown in [Figure 5.4](#).

The experimental consequences of the self-fulfilling prophecy were first explored by Robert Rosenthal in his doctoral research in clinical psychology at the University of California at Los Angeles in the mid-1950s.²⁷ Rosenthal divided 108 subjects into 3 experimental groups: “success,” “neutral,” and “failure.” The subjects selected for the experiment were randomly assigned to these categories, but were told the category to which they were assigned, and were made aware of its significance. Aware of their ranking, subjects participated in a cognitive exercise and then later were retested to discern any differences. The researcher predicted that the experiment would show that “failures” would do worse on posttests, “neutrals” about the same, and the “success” designees would do better than expected. In fact, this very prediction held true. The only difference among the subjects was the expectation implanted into their minds that they were expected to perform according to their (falsely) prejudged ability.

Rosenthal was approached by the principal of an elementary school, Lenore Jacobson, who invited him to conduct a teacher-expectation experiment in her school.²⁸ Near the

end of the school year, Flanagan's Tests of General Ability (ToGA) was administered to all pupils from kindergarten to fifth grade. ToGA, a nonverbal intelligence test, was described to the teachers as the "Harvard Test of Inflected Acquisition." It was meant to identify "later bloomers," those who have not fully used their native abilities up to that point, but who were about to bloom.

The next academic year, the experimenters identified 20% of each teacher's incoming students as "later bloomers." However, they actually were randomly selected. No further interventions occurred during the school year to influence teacher behavior. When ToGA was administered at the end of the school year, pupils who had been designated as late bloomers had gained four more points in IQ testing than had their controlled classmates. Presumably, the teachers had provided an exceptional level of attention to the "bloomers" and the results were positive and measurable.

In the workplace, the Pygmalion effect can have a powerful influence on job performance and career development.²⁹ If supervisors are told that newly completed trainees are "among the best" at the time they join their team, this belief will likely have a Pygmalion effect, and the supervisors will tend to believe that the workers perform better on the job than those for whom no special designation was given. Likewise, negative connotations about a class of workers are likely to affect the way in which employees are regarded by their supervisors. They may be appraised as not performing to standards if that is the expectation.

The Pygmalion effect is logical, once understood, and concludes that expectations alone can raise performance above – or plunge it below – established performance levels. This effect has been supported by many studies. However, the process seems calculating and manipulative and also prone to create circumstances that produce ambiguous results. Consider the individual who is designated as being exceptionally promising but who fails, despite his or her best efforts. Such a person is bound to feel rejected and bewildered by the process. Similarly, others are informed that not much is expected of them and become determined to show otherwise, and do.

The Limitations of Motivation Research

To many managers, motivation seems like a quick fix to overcome inherent obstacles to success. To other managers, motivation research presents a cynical view of rational behavior, promising more than it can produce. Thomas H. Fitzgerald, a personnel research director at General Motors, believes that motivation theory does not work: "When transported from the laboratory, the language of motivation may become subtly elitist by suggesting that the employee resembles a captive rodent in a training box equipped with levers, trick doors, food pellets, and electric grids."³⁰ Fitzgerald argues that many of the assumptions of motivation theory are untestable. Praise and approval can produce temporary improvement of individual effort, while inexpensive measures for employees "seem to have a positive effect on some of the people part of the time." Fitzgerald suggests managers put aside

some of the notions of motivation “and start to think seriously about how to go about becoming a society of persons.”

What’s Wrong with Praising Worker Performance?

This chapter emphasizes the power of enhanced worker achievement through praise. This is a conclusion from the work of numerous behaviorally oriented researchers. It’s a technique well used by high-performing managers.

But while *most* workers respond well to the oft-expressed phrase “Praise in public, criticize in private,” some do not. Perhaps they feel diminished that they are the praised and not the praiser, or possibly, the praiser delivers the well-intended remarks excessively that borders on insincerity, or possibly the worker feels he or she is doing the job the way it is supposed to be done and any praise received is not required. The sensitive manager understands what works best with individual subordinates and selects motivators that work best for individuals.

However, for many circumstances praising worker performance is “wrong” because it is not sufficiently thoughtful and, therefore, fails to achieve the desired behaviors. Example is as follows:

Worker: “How did you like the incident report I wrote about the incident?”

Supervisor: “It was great.”

What’s wrong: The worker isn’t really sure if the report was “great,” or what it contained that was so useful.

Better response: “Your report was clearly written and fully detailed. The interviews you conducted were timely and to the point. The language was factual and coherent. Because of that I was able to forward your report without change to Risk Management for use in claims adjustment.”

The worker now knows what was commendable about the report. The qualities in the superior incident report have been precisely articulated and are, therefore, likely to be remembered in future reports that must be written. However, such a response from a manager requires reflection and discernment. Such an effort is bound to be worth it in the long run for employee development.

Alternatively, suppose the report substantially falls short of the standards required by management: it was too short, was incomplete, lacked documentation, and had stylistic errors. Many managers would be upset, possibly exasperated, and would be inclined to issue an order. However, focusing on what *was* positive about the report might reach the desired objective in a more constructive fashion. Example is as follows:

Better response: “You started the report with all the critical facts laid out: who, why, what, and where. The one figure you included was helpful. But before this report moves on to senior management, you’ll want to expand details and provide other statistics to establish context and make your recommendations more convincing. Please use software tools to check syntax and spelling. I look forward to reading your revised report.”

A final issue about what can be wrong about praising worker performance is that the process stresses individual performance over that of the groups. Many tasks need teams of workers to accomplish them and managers to enlarge their positive re-enforcement, extending it to workers simultaneously.

Summary

Supervisors, or first-level managers, are critical in helping an organization achieve its goals. From routine service to new policy implementation, supervisors are often the main catalysts for action – or the main barriers to goal achievement. Supervisors are responsible for the reasonable safety and security of their employees. Motivational research over most of the past century has concluded that emphasizing the positive produces better results in terms of forming behavior than does negative enforcement.

Discussion and Review

1. What role might a supervisor have in connection with others in the placement of staffers into the organization?
2. On meeting new workers assigned to the unit, what topics would the supervisor discuss first? Why?
3. What special concerns would a supervisor have if the new worker was being assigned temporarily to someone with no previous experience as a mentor?
4. What significance does the job description have for both the supervisor and the persons being supervised? What are pitfalls in writing job descriptions?
5. What is the usual and preferred strategy for a supervisor to recognize good work in a subordinate?
6. What responsibility does a supervisor have for the workplace safety of subordinates? How do the risks of security employment compare with those in other vocations?
7. Compare and contrast the ABC technique, the Pareto principle, and the S.T.O.P. exercise. How does each theory aid management in managing time more effectively?
8. In your opinion, does Mayo's research at the Western Electric plant have any relevance to the management of a security program? Explain.
9. In your opinion, is the Pygmalion effect harmful or beneficial to management? Explain.

Endnotes

¹ Schmidt, P., 2012. Who counts as a supervisor? College groups weigh in on a Supreme Court case. *Chronicle of Higher Education*, December 7, p. A15.

² Tyler, K., 1999. Take new employee orientation off the back burner. *HR Magazine*, May, p. 49.

³ *Ibid.*

- ⁴ Van Dersal, W.R., 1985. *The Successful Supervisor in Government and Business*. Harper & Row, New York, NY, p. 13.
- ⁵ Blanchard, K., Johnson, S., 1983. *The One Minute Manager*. Berkley Books, New York, NY, p. 44.
- ⁶ New study confirms safety of office work. Workplace violence elsewhere can be lessened, 1996. *Security Letter*, vol. 26, part I, October 18, p. 1; Private security personnel 4th highest rank of violent workplace victimization, 1998. *Security Letter*, vol. 28, part III, September 1, p. 1.
- ⁷ Lee, S., McCrie, R., 2014. The violent vortex: appraising risk from workers who kill on-the-job. In: Gill, M. (Ed.), *Handbook of Security*, second ed. Palgrave Macmillan, New York, NY, p. 182.
- ⁸ Ahrens, S.A., 2011. The role of standards in workplace violence prevention and response. *Security Magazine* 55, 23–31; Loomis, D., 2008. Preventing gun violence in the workplace. CRISP Report. ASIS Foundation, Alexandria, VA.
- ⁹ Post leakage response: don't forget to remove ceiling tiles after water damage. *Security Letter*, part I, May 15, 1999, p. 2.
- ¹⁰ Brislin, R.F., 1994. *The Effective Security Supervision Manual*. Butterworth-Heinemann, Boston, MA, p. 8.
- ¹¹ Mintzberg, H., 1979. *Harvard Business Review* on Human Relations. Harper & Row, New York, NY, p. 121.
- ¹² Hillier, F.S., Lieberman, G.J., 1980. *Introduction to Operations Research*. Holden-Day, San Francisco, CA.
- ¹³ Longenecker, C.O., Papp, G.R., Stansfeld, T.C., 2007. *The Two-Minute Drill: Lessons for Rapid Organization Improvement from America's Greatest Game*. Jossey-Bass, San Francisco, CA.
- ¹⁴ The inefficiency of tidiness: in praise of mess, 2007. *The Economist*, January 6, p. 69.
- ¹⁵ Quoted in Fisher, A., 2005. Get organized at work – painlessly. *Fortune*, January 10, p. 30.
- ¹⁶ Grove, A.S., 1985. *High Output Management*. Vintage Books, New York, NY.
- ¹⁷ McGregor, D., 1960. *The Human Side of Enterprise*. McGraw-Hill, New York, NY.
- ¹⁸ Ouchi, W.G., 1981. *Theory Z*. Addison-Wesley, Reading, MA.
- ¹⁹ Roethlisberger, F.J., Dixon, W.J., 1939. *Management and the Worker*. Harvard University Press, Cambridge, MA.
- ²⁰ Landsberger, H.A., 1958. *Hawthorne Revisited*. Cornell University Press, Ithaca, NY.
- ²¹ Jones, S.R.G., 1990. Worker interdependence and output: the Hawthorne studies reevaluated. *Am. Sociol. Rev.* 55, 176–190.
- ²² Maslow, A.H., 1943. Theory of human motivation. *Psychol. Rev.* 50, 370–396; Bryant, A., 1998. Looking for purpose in a paycheck. *New York Times*, Sec. 4, June 21, p. 1. See also: Maslow, A.H., 1998. *Maslow on Management*. John Wiley & Sons, New York, NY.
- ²³ Globe, F.G., 1970. *The Third Force*. Pocket Books, New York, NY.
- ²⁴ Herzberg, F., Mausner, B., Snyderman, B., 1959. *Motivation to Work*. John Wiley & Sons, New York, NY.
- ²⁵ Magnet, M., 1987. The money society. *Fortune*, July 6, p. 31.
- ²⁶ Eden, D., 1990. *Pygmalion in Management: Productivity as a Self-Fulfilling Prophecy*. Lexington Books, Lexington, MA, p. 1.
- ²⁷ Rosenthal, R., 1985. From unconscious experimenter bias to teacher expectancy effects. In: Dusek, J.B. (Ed.), *Teacher Expectancies*. Lawrence Erlbaum Associates, Hillsdale, NJ.
- ²⁸ Rosenthal, R., Jacobson, L., 1968. *Pygmalion in the Classroom: Teacher Expectation and Pupils' Intellectual Development*. Holt, Rinehart & Winston, New York, NY.
- ²⁹ Livingston, J.S., 1988. Pygmalion and management. *Harvard Business Review*, vol. 66, issue 5, September–October, p. 122.
- ³⁰ Fitzgerald, T.H., 1979. Why motivation theory doesn't work. In: *Harvard Business Review* on Human Relations. Harper & Row, New York, NY, p. 277.

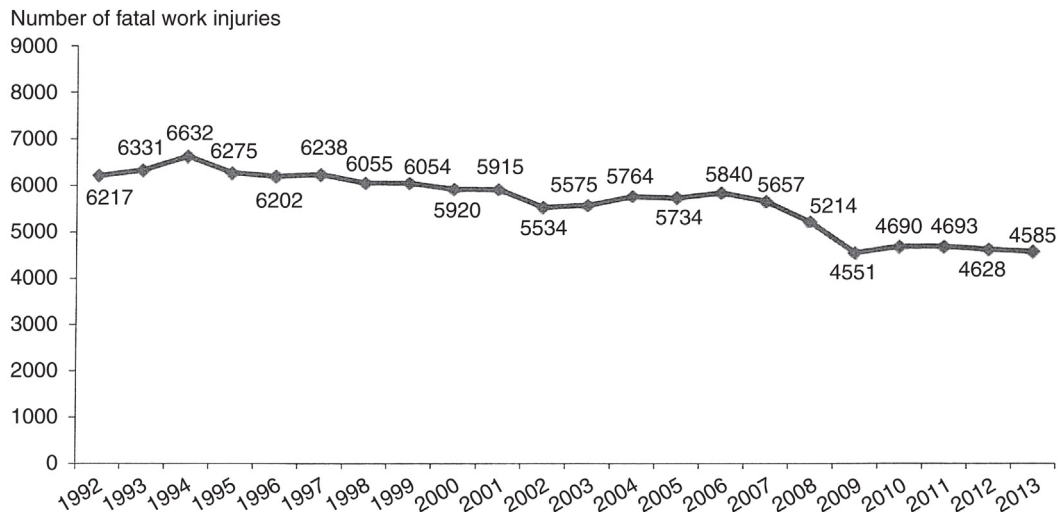
Additional References

- Abrahamson, E., Freedman, D.H., 2006. *A Perfect Mess: The Hidden Benefits of Disorder – How Crammed Closets, Cluttered Offices, and On-the-Fly Planning Make the World a Better Place*. Little, Brown and Company, New York.
- Bloom, M., 1999. Performance effects of pay dispersion on individuals and organizations. *Acad. Manage. J.* 42 (1), 25–40.
- Fisher, A., 1996. Stop whining. *Fortune*, September 30, pp. 206–208.
- Kotter, J.P., 1996. *Leading Change*. Harvard Business School Press, Boston, MA.
- McCaskey, M.B., 1979. The hidden messages managers send. *Harvard Business Review*, vol. 57, issue 6, November–December, pp. 135–148.
- Pozen, R.C., 2012. *Extreme Productivity: Boost Your Results, Reduce Your Hours*. Harper Business, New York.
- Rosenberg, M.B., 2003. *Non Violent Communications: A Language for Life*. Puddle Dancer Press, Encinitas, CA.
- Winston, S., 2004. *Organized for Success: Top Executives and CEOs Reveal the Organizing Principles that Helped Them Reach the Top*. Random House/Crown Business, New York, NY.

Further Reading

- Lee, S., McCrie, R., 2012. *Mass Homicides by Employees in the American Workplace*. ASIS Foundation, Alexandria, VA, (see below).

Number of fatal work injuries, 1992–2013



Fatal work injuries have trended downward in the past two decades. Averaging the first three and the last three of this time period, a decline of over 27% was recorded while the workforce increased over the same period of time. The salutary development was due to managerial and technical changes, making the workplace safer. **Note:** Data for all years are revised and final. Data from 2001 exclude fatal work injuries resulting from the September 11 terrorist attacks. (Source: US Bureau of Labor Statistics, US Department of Labor, 2015.)

Appraising and Promoting People in Security Programs

The secret of success in business of all kinds ... is a liberal division of profits among the men who make them, and the wider distribution the better.

—Andrew Carnegie

People are an organization's most important assets. Managing them successfully means providing opportunities for growth, including promotion to greater responsibilities. Promotions in formal organizations normally occur after work has been appraised over time as exceeding minimum expectations. Appraisal is the process of evaluating individual performance on the job and assessing it relative to goals and objectives. Appraisal not only is a measure of individual performance but also identifies potential for future performance and capability. When employees can be evaluated and compared with reliability and fairness, the workplace and workers gain from the process.

The Difficulties of Performance Appraisal

The organizational process of personal appraisal fits into the context of other aspects of management development: forecasting, recruiting, training, compensation and conditions of service, deployment, and management review or audit. Yet many security operations do not provide formal appraisal of workers. This may be because the process is time-consuming, demands judgment, and requires confronting individuals in what can be awkward situations involving workplace behavior. Some employers feel that statements made at such times can lead to litigation if the individual is terminated subsequent to an unfavorable evaluation. Litigation for wrongful termination is more likely if the employee is discharged shortly after a favorable appraisal has been issued.

Such reservations about formal appraisal processes are understandable. However, advantages of appraisals far outweigh their disadvantages. A well-conceived and conscientiously operated appraisal program can lead to motivation and growth of individuals, and produce higher performance. With such a process, justifiable criteria must be identified as the basis of promotions. No manager can be guaranteed that certain procedures will prevent the employer from being sued for workplace discrimination in failing to promote someone in a fair manner. However, the existence of a well-conceived employee appraisal system serves as a deflective shield against spurious civil litigation from employees passed over for promotion. Beyond the uncommon likelihood of such litigation is the larger issue that all employees will observe that management has sought to establish reasonable,

though imperfect, standards of promotion. Instead of encouraging litigation, such programs mitigate it.

Rapidly growing organizations sometimes feel they cannot spare time for appraisals. Yet this process helps identify individuals within the organization who are capable of assuming new responsibilities. In addition, appraisals are important in determining merit increases, special training, and layoffs.

Who Should Be Appraised and When?

In well-structured organizations, all employees deserve appraisal. Due to the time-consuming nature of the process, appraisals are generally conducted on an annual basis. However, some organizations will conduct appraisals on a semiannual or more frequent basis. Organizations should schedule appraisals at times that will interfere least with critical activity. In retail organizations, for example, it would not be logical to schedule appraisals in November and December, as workers are busy with the holiday season. However, late January and February are good months for retailers to schedule appraisals. Other workplaces will have different operating rhythms that will indicate when the most logical time for formal appraisal should be.

Many organizations schedule appraisals at least 1 year after the individual has begun a position and at each annual anniversary. However, as this chapter observes, employers frequently appraise workers during probationary periods, which are often particular to that organization or industry and should be mentioned specifically in the employee's manual. Probationary periods are usually 30, 60, 90, or 180 days after the commencement of employment. The annual review then might occur approximately 6 months to 1 year after the probationary appraisal has been successfully completed by the new hire, and on an annual basis subsequently. Positions in government frequently have a probationary period that lasts 1 year after the commencement of employment.

Appraisal for All Levels and by All Levels

How the appraisal will be designed and who may do the appraising differs from organization to organization and within an organization. The appraisal process should be flexible enough so that it produces the best returns for the time required. The following are a number of strategic methods of appraising workers:

- *Top-down.* Appraisals are traditionally considered top-down, that is, a supervisor appraises his or her subordinates. In a hierarchical organization, this will be the expected and usual method of evaluation, and perhaps the only one normally scheduled. The advantage of top-down appraisals is that the more experienced supervisor understands the needs of the workplace clearly and is the best judge of how subordinates have achieved workplace standards over her or his previous appraisal period. Also the appraiser knows how a worker's performance can be raised to higher level. The disadvantage of this process is that it is a reflection of an

autocratic style of management, especially when other forms of appraisal are not part of the process.

- *Bottom-up.* In this circumstance, subordinates evaluate their supervisors. The results of the appraisal document are received by a human resources manager, who analyzes the results and shares them with the supervisors involved. The advantage is that this process helps reveal strengths and weaknesses to the supervisor in a way that might otherwise not be discovered by upper management or the individual supervisor. Often, what the supervisor believes is a personal strength – for example, a penchant for delightful witticisms during the workday – may be regarded quite differently by those who are targeted for such remarks on a regular basis. The reverse may also be the case. A weakness that the supervisor believes he or she possesses may be interpreted differently by subordinates, enabling the supervisor to reassess his or her management traits. Many managers find it hard to accept criticisms from subordinates and may ignore their appraisals.¹
- *Peer review.* This is a situation in which peers evaluate each other. Typically, the results of the questionnaire used in such a process are seen only by a human resources manager, who then distills and shares the information with the persons involved. Peer reviews also help identify to management strengths and weaknesses of team members. The drawback is that such a process makes many participants uncomfortable. The process forces coworkers to raise unpleasant issues that possibly could be traced back to them and lead to disharmony.
- *Customer or client reviews.* Often, contract workers are part of the work environment for extended periods, sometimes for years. These individuals should be assessed annually by the contractor who assigns them to the work location. In the event the worker is a sole contractor on an extended assignment, that person may be reviewed much the same way proprietary employees are. Reviews by customers or clients of contract personnel provide the contractor with tangible evidence of worker qualities. They are the persons most in a position to evaluate performance under daily circumstances. In situations where contract workers are employed for extended service to the organization, the appraisal should involve collaboration between both the contractor and management of the contracted. Similarly, security service employees may be appraised by their “customers” within or outside of the organization. A security department within an organization serves the organization as a whole, and individuals who provide those services may be spot-checked periodically by a simplified evaluative document. Generally, senior managers do not opt for this type of evaluation unless criticisms have been raised and need to be substantiated or unless a new program requires evaluation.
- *Review of contracted employees.* Organizations that contract with security services such as guard companies, employment screening services, alarm monitoring services, or undercover investigative firms also may select a formal appraisal service. In actuality, such appraisal occurs day-by-day, or hour-by-hour. Still a structural process permits an organized means of reviews evolving issues that have or could change the delivery of services. For example, the contractor might ask what capital

investment the contracted workforce has made – or intends to make – that will affect business.

What Types of Evaluation Do Workers Prefer?

People being appraised are seldom questioned as to which types of performance appraisal they prefer. Some managers believe that such a preference is irrelevant, while other researchers of appraisal instruments conclude that such an inquiry may be “valuable.”^{*2} In 1 study, 52 full-time registered nurses were asked how they preferred to be rated, by whom, and for what reasons. The nurses displayed a marked preference for specific methods of appraisal. They also preferred performance appraisal that had certain objectives, such as determining promotion or an adjustment in compensation. By contrast, they were less positive about appraisals that compared themselves with others, that did not include scales, and that were completed by subordinates. (These techniques are discussed later in this chapter.)

What Needs to Be Evaluated and How?

If performance appraisal is important, what is evaluated must be of significance to the employer. This issue requires thought; not every trait of an employee should be subjected to the appraisal process. Relevancy to the organization’s goals is a basis for evaluative activity. The following are examples of goals and skills that may be subject to performance assessment at different levels of the workplace:

1. *Success performing functionally assigned tasks.* The employer may identify a series of activities routinely performed by the worker and specifically linked to performance standards. For this type of top-down appraisal, management would have identified the specific tasks required for the position and would have related them to standards the worker may be expected to fulfill regularly. These tasks flow from the job description, originally written for the individual, spelling out in greater detail the nature of the duties undertaken and their appropriate standards. (Examples of this process are found in the following section.)
2. *Trait analysis.* This determines how a worker performs in a specific activity, such as clarity in dealing with the public, efficiency, and reliability. Raters are asked to appraise workers on different scales. Certain scales use such words as “outstanding” (top 2%), “excellent” or “superior” (top 20%), “above average,” “average,” and “below average” or “needs improvement” to rate the worker. Trait analysis tends to be focused on narrow qualities considered important to management for specific positions. Supervisors who review specific traits of subordinates often have difficulties in providing unfavorable assessments. This characteristic limits, but does not negate, the use of such measurement.

* An annual or semiannual appraisal may not be sufficient for some employees. A study found that employees who received three or fewer performance evaluations annually wanted more (<http://www.nysscpa.org/printversion/cpaj/2008/208/p64.htm>).

3. *Critical incident methods.* Performance appraisers using the critical incident process note specific positive and negative actions taken by the worker during the evaluation period of complex actions vital to the job description. Such measurements have been identified previously by management as significant with regards to job function.³ An example is the technique by which a protective employee handled an untoward event that resulted in the completion and submission of an incident report.
4. *Behavioral measurement.* One type of behaviorally oriented evaluation is the Behaviorally Anchored Rating Scale (BARS). This scale identifies a number of possible actions by workers and then assesses performance based on a scale from very desirable to very undesirable.⁴ BARS graphically rates behavior with specific behavioral descriptions using a numerical scale. Since its introduction in 1963, BARS and its numerous variants have been widely used to evaluate the performance of law enforcement and, to a lesser degree, private security personnel.
5. *Mixed standard scale (MSS).* Another method of performance review, used in policing and security, is MSS. Such scales describe high, medium, and low performance and force raters to make a choice. The following are examples where a reviewer might have to critically differentiate performance on one of three standards concerning a particular behavior to be emphasized:
 - a. *High performance:* Takes numerous steps while on patrol both to prevent and to control crime and disorder, educates employees and others in prevention techniques, and has comprehensive knowledge of preventive measures and tools available to achieve objectives
 - b. *Average performance:* Makes some efforts to emphasize crime prevention or order maintenance on routine patrol and has an adequate knowledge of preventive equipment
 - c. *Low performance:* Has little or no contact with employees and visitors to inform them of methods of reducing their property from loss

What each standard represents to the rater is not always obvious. The rater indicates only that the worker's performance is "better than," "as good as," or "worse than" the behavior described.⁵ However, many appraisal-instrument developers believe that MSS evaluation decreases rater leniency. In assessing "crime prevention" qualities of patrol officers, for example, items were included that identified specific dimensions of performance.⁶ These included judgment, communication skills, job knowledge, demeanor, tolerance, cooperation, and human relations skills (Box 6.1). While this instrument evaluates law enforcement officers who patrol, it can be adjusted easily to private security or other worker groups.

Using a Formal Appraisal Document

A formal employee performance evaluation compares the employee's performance with a set of standards. A series of ratings used by one formal system allows reviewers the opportunity to provide specific assessments for each task, as shown in Figure 6.1. The form

BOX 6.1 A MIXED STANDARD SCALE (MSS) FOR PATROL PERFORMANCE

The following 13 items are used to assess performance in different facets of a patrol officer's job. The appraiser is asked whether an item is an accurate description of the patrol officer's typical performance in that area of work. If so, the appraiser places "0" in the space provided for the worker. If the patrol officer's typical performance is better than the item description, then a "+" is placed in the space. If the patrol officer's typical performance is worse than the item description, then a "-" is placed in the space. Appraisers rank officers on code sheets that can later be analyzed.

1. Behavior sometimes shows the effects of a stressful situation, but it does not tend to interfere with the performance of duties.
2. Looks neat most of the time, although uniform occasionally reflects a busy schedule.
3. Reports are good, but occasionally need elaboration or clarification. Sometimes has difficulty communicating.
4. Takes numerous steps in patrol area both to prevent and to control crime; educates citizens in prevention techniques and has comprehensive knowledge of preventive equipment.
5. Has little or no contact with citizens to inform them of methods of improving their property for crime prevention.
6. Performance reflects the proper judgment necessary to anticipate, select, and perform the appropriate behaviors in almost all circumstances.
7. Is quite emphatic about the types of people he or she can and cannot work with. Has difficulty getting along with many officers.
8. Shows maximum effort and enthusiasm almost all the time and in almost all circumstances.
9. Carries out assignments and responsibilities with satisfactory standards of performance. Rarely cuts corners or bends the rules.
10. Behavior with others is insightful and skillful, often preventing as well as ending conflicts.
11. Performance must be closely supervised, or it may slip to less-than-adequate standards. Behavior is often designed to find shortcuts in duties.
12. Appearance displays a careless attitude toward the job and the impression conveyed to the public.
13. Works adequately with most people, but has difficulty with some types of personalities. Although willing to break in new personnel, would prefer not to.

Source: Bernardin, H.J., Elliott, L., Carlyle, J.J., 1980. A critical assessment of mixed standard rating scales. In: *Proceedings of the Academy of Management*. Academy of Management, Athens, GA, pp. 308–312.

illustrated, used by a security program employing over 200 security officers, begins with the noting of directory-type information:

- Section I clearly indicates to the employee that a performance evaluation is part of the expectation and notifies the officer of the extent of the evaluation period.
- Section II identifies the tasks and standards deemed critical by management. During the training process, the new employee would have become aware of these tasks and the nature of the standards expected by management to be met. This would

SECTION I		EMPLOYEE INFORMATION	
Employee's Name		Soc. Sec. No.	
Title and Level		Functional Title	
Responsibility Center Name		Section/Unit	
Employee's Status: (Check one)		Evaluation Period: From To	
☐ Permanent ☐ Probationary ☐ Other ☐ Non-Competitive ☐ Provisional (Explain) _____			

SECTION II		ASSIGNMENT OF TASKS AND STANDARDS (Complete at beginning of evaluation period)	
Supervisor's Name (Please type or print)		Signature	
Reviewer's Name		Signature	
Date		Date	

"I have received a copy of the tasks and standards below." _____ Employee's Signature Date Master List Task No. <u>FUNCTIONALLY ASSIGNED TASKS</u> _____ STANDARDS		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: left; padding: 2px;">SECTION III</th> <th colspan="2" style="text-align: left; padding: 2px;">RATINGS (Check one)</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="padding: 2px;">EMPLOYEE'S PERFORMANCE COMPARED TO STANDARDS (Complete at end of evaluation period) Use comments and examples to justify ratings.</td> <td colspan="2" style="padding: 2px;"> Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate </td> </tr> </tbody> </table>		SECTION III		RATINGS (Check one)		EMPLOYEE'S PERFORMANCE COMPARED TO STANDARDS (Complete at end of evaluation period) Use comments and examples to justify ratings.		Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate	
SECTION III		RATINGS (Check one)									
EMPLOYEE'S PERFORMANCE COMPARED TO STANDARDS (Complete at end of evaluation period) Use comments and examples to justify ratings.		Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate									
1			Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate								
2			Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate								
3			Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate								
4			Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate								
5			Outstanding Superior Satisfactory Conditional Unsatisfactory Inadequate								

FIGURE 6.1 Nonmanagerial employee performance evaluation form.

serve as the guideline for the worker during the time allocated for the evaluation. The employee signs the list of functionally assigned tasks, often in the presence of the supervisor. In a sense, this is a contract between the employee and employer and it is an explicit understanding that the worker is to be judged predominantly on these functionally assigned tasks. Figure 6.1 provides space for only five functionally

Table 6.1 Examples of Master List Tasks and Standards for Security Officers

Master List Task Number	Standards
1. Patrols designated areas of public buildings, reports in uniform, makes rounds, checks that the public and staff are following rules and regulations to prevent crime, vandalism, disturbances, and are safeguarding life and property	Reports for patrol in uniform and at the designated time. Observation is acute and comprehensive. Makes complete rounds. Follows rules and regulations closely
2. Reprimands and ejects loiterers and disorderly persons by checking restrooms, stairways, halls, and other areas, and advising persons to leave. Uses persuasion to obtain results. Follows rules and regulations to remove unauthorized persons and quiet disturbances	Areas checked frequently. Persons asked to leave correctly, firmly, and courteously. Force used appropriately and only when necessary. Appropriate rules and regulations followed closely
3. Guards department's personnel and property. Restricts persons from entering unauthorized areas. Notifies supervisor of damaged and inoperative equipment. Patrols efficiently to prevent personal injury or property damage	Unauthorized persons barred from restricted areas. Supervisor notified promptly and clearly of damaged and inoperative equipment. Patrols effectively. Removes disorderly persons promptly and properly

assigned tasks and standards. These should be the critical broad workplace achievements that management expects from the employee at that particular title, level, and unit. These can be expanded according to the requirements of the position. Management then prepares a master list of tasks to be performed by the category of security personnel, as shown in [Table 6.1](#). Standards of satisfactory performance accompany the master list and are entered into the employee performance evaluation form.

- Section III is completed when the evaluation period has reached an end and the supervisor makes ratings appropriate to the worker's actual performance compared with the standards. The supervisor will use comments and examples to justify the ratings. Failure to include these can lead to the sense that the supervisor has made a decision without proper reference to actual performance on the part of the employee.
- Section IV provides an overall rating after individual tasks are considered. The overall rating takes into consideration the totality of the employee's work performance during the previous period of time. Again, comments and examples are needed to justify the overall rating.
- Section V is where the supervisor provides his or her recommendation of the employee to be retained, dismissed, demoted (for promotee only), and extension of probation.
- Section VI provides space for specific plans for improvement discussed in the evaluation interview. This section identifies an area or areas in which improvement of employee performance is required. Further, the specific means by which such improvement may be achieved is identified. Frequently, the behavior to be corrected can be altered by nothing more than additional personal effort following a discussion with the supervisor. In other cases, additional training may be needed to achieve the desired performance.

- Section VII provides the employee with an opportunity to add written comments to the evaluation. Such comments may be made on a separate sheet of paper and attached to the appraisal evaluation form if necessary. The date of the evaluation interview is also indicated.
- Section VIII concludes the evaluation process with the supervisor's signature. The employee generally signs the statement at this point indicating that he or she does not necessarily agree with the contents of the statement, but acknowledges that the document is complete. At a later date, a reviewer will add a signature indicating that the employee performance evaluation form has been reviewed by a higher level of management. Alternatively, the reviewer may be an independent human resources officer. Generally, reviewers are directly superior to the supervisor completing the evaluation form.

Job Performance Rating: Creating the Documentation

In some organizations, job performance evaluations are required during the probationary period. A monthly performance rating evaluating new security officers is presented in [Figure 6.2](#).

Following the conclusion of a successful probationary period, performance ratings and evaluations can be conducted at the same frequency as with all other employees in that job category. Use of the form acts as an incentive both for the supervisor to note performance on a daily basis and for the subordinate to be aware that the probationary period entails written performance verification on topics important to the work function.

Evaluation of contract employees may be aided by the use of a form designed for this purpose, as shown in [Figure 6.3](#). This document may be completed by the client on a monthly or semiannual basis and forwarded to the contract company as part of ongoing evaluation. The "Remarks" section provides an opportunity for management of the contract firm to take appropriate action. Of course, any substantive unsatisfactory job trait or behavioral quality should be transmitted to the security services contact supervisor quickly to result in corrective attention. A telephone call to the contractor as soon as such unacceptable conduct is observed may suffice.

Peer reviews may also be considered as part of the strategy to determine job performance, cooperation, and teamwork characteristics. A Colleague Confidential Evaluation form is used for coworkers to evaluate each other's performance, as shown in [Figure 6.4](#). The evaluation director distributes and later discretely collects completed forms from evaluators. The evaluation director looks for strengths, weaknesses, and cooperative patterns in workplace performance where close teamwork is required. These forms are then assessed and transmitted to the workers being evaluated. Organizations tend to use peer review when mutual cooperation is essential and cannot be evaluated fully by a supervisor due to the complex nature of the work performed by the teammates. The team members themselves are most likely aware of who is performing best and worst in the group and

NAME: _____ TEL. NO: _____

UNIT: _____ Page No.: _____

DATE HIRED: _____ ASSIGNMENT: _____

REVIEW DATE: _____ SOCIAL SECURITY: _____ SHIFT: _____

[illegible]

Officer Performance Evaluation Form

In order to assure the effectiveness of Security Service, the Security Department would appreciate your appraisal of officer performance

Officer's Name: _____ Unit: _____ Date: _____

Please complete the following and return to: _____.

Superior	Good	Needs Improvement	
_____	_____	_____	_____ Appearance
_____	_____	_____	_____ Courteousness
_____	_____	_____	_____ Co-operation
_____	_____	_____	_____ Effectiveness
_____	_____	_____	_____ Job Knowledge
_____	_____	_____	_____ Ability to communicate
_____	_____	_____	_____ Attitude

Please list recommendations that would improve our security service. Return this form to the undersigned.

Security Director

FIGURE 6.3 Officer performance evaluation form. (Source: Adapted from Guy, E.T., Merrigan Jr., J.J., Wanat, J.A., 1981. *Forms for Safety and Security Management*. Butterworth-Heinemann, Boston, MA.)

Colleague Confidential Evaluation

Evaluatee: _____

Department: _____

Evaluator: _____

Your comments will be reviewed by the Evaluation Director and will be anonymous to the Evaluatee in Evaluation and Development Summary.

Comments On Overall Performance

- Please describe the Evaluatee's strengths and development areas:
- Pay particular attention to the criteria listed below:

Work Production/Professional Skills: • Flexibility/Versatility • Communication Skills (i.e., relaying clear and accurate verbal and written work-related information) • Professional Demeanor	Teamwork/Cooperation: • Contribution to group • Providing assistance to all group members • Answering phones • Sharing firm knowledge/resources

Comment on greatest strengths (provide examples):

Comment on areas in need of further development. Indicate suggestions for developing these areas:

Evaluator Signature: _____ Date: _____

This form is prepared by managers and distributed to team for workers' mutual appraisals. The confidentially completed form is returned to management where it is assessed and used as the basis of appraisal of the evaluatee.

FIGURE 6.4 Colleague Confidential Evaluation form.

may be willing to share their insights via this means. Other barriers to group success may also be identified. The evaluation director must be discrete when sharing results so as not to reveal the identities of the evaluators who have prepared the evaluations, as this could cause friction in the workplace. These documents should be stored separately from other records in the worker's employment file.

The Need for Appraisal Documentation and its Protection

Employees sometimes sue their employers for failure to be promoted, for disciplinary action, or for termination. Similarly, unionized employees may turn to their representative to protest against a personnel decision not taken in their favor. In such actions, written performance appraisals are likely to become critical evidence. In appraising subordinates, supervisors have to find a balance between encouraging desirable behavior and identifying nonproductive behavior. A pattern of substandard performance could lead to termination that conceivably could be the basis of a civil action by an employee. Many supervisors emphasize the positive and ignore the negative in subordinates. However, such relevant negative features could become worse subsequent to their initial identification in the written performance appraisal. Therefore, the supervisor needs to document any negative behavior, potentially serious enough to be the basis of discipline or discharge, at the earliest opportunity.

Regrettably, many evaluators see only the positive in those whom they evaluate (Box 6.2). Failing to be observant of a worker's shortcomings is just as harmful as being excessively lenient or strict in judging workers as a group. Other evaluators who judge most or all of their subordinates as "average" may lack discernment and judgment expected of those with supervisory responsibilities. The appraiser needs to include specific, detailed observations, with the time and date noted, of notable workplace performance. This rigorous method of identifying both desirable and undesirable performance characteristics supports the overall objectives of operations management.

Appraisals for employees at all levels – indeed all human resources and investigative documentation – need to be securely protected. Most of these records are stored

BOX 6.2 RATING COLLEAGUES OBJECTIVELY IN APPRAISALS

The process of using written appraisals can be counterproductive if the rater is not objective about the person being judged. Raters can improve the accuracy of their ratings by recognizing the following factors that subvert effective evaluations:

1. *The halo effect.* This is the tendency of an evaluator to rate a person good on all characteristics based on an experience or knowledge involving only one dimension.
2. *Leniency tendency.* This is a tendency toward evaluating all persons as outstanding or above average and to provide inflated ratings rather than true assessments of performance.
3. *Strictness tendency.* The opposite of the leniency tendency, this is a bias toward rating all persons at the low end of the quality scale and a tendency to be overly demanding or critical.
4. *Average tendency.* This is the habit of evaluating every person as average regardless of major differences in performance.

Source: Neal Jr., J.E., 1994. *Effective Phrases for Performance Appraisals*. Neal Publications, Perrysburg, OH.

electronically. They should be protected in a way that only those with a need to know can access them. This protection also should render it impossible for an unauthorized party to make changes to any of the stored documents.

Other Written Appraisal Techniques

Performance evaluation usually involves creating documentation that is part of the employee's confidential personnel file. Prior to evaluation, the standards should have been made clear to everyone involved. They should be realistic, objective, and comprehensible to all security workers in the job category. However, more than one rating category can and should be used. The following are some options:

- *Ranking.* In this type of measurement, the supervisor is asked to simply rank all subordinate workers in the group on a numerical basis from best to worst. This may create a bias against the most recently hired and, therefore, less experienced worker.
- *Paired comparison.* In this circumstance, the supervisor compares subordinates with specific tasks ranking them in order from best to worst according to each criterion. In this situation, the overall highest ranking can be determined from an aggregate of different factors. A negative feature of this process is that those most recently hired – regardless of their level of training – are likely to perform less well than experienced work unit members.
- *Narrative form.* In this rating method, the supervisor writes a discursive passage on each worker to summarize individual strengths and weaknesses. This helps to provide a human dimension to the worker's performance during the evaluation period.
- *Forced-choice method.* In this measurement, the supervisor selects from a set of statements involving the subordinates in the work unit. The rater selects two items from a group of four descriptive items, one that emphasizes the most characteristic quality of the worker and another that emphasizes the least characteristic quality. Perhaps 10 or 12 sets of 4 characteristics are presented and then subsequently analyzed for each worker. The report is tedious to create and requires construction by a technical specialist, but it provides a portrait of the worker unattainable by other written appraisal techniques. One problem with this measurement is that the sets may be widely different in terms of their significance, and the appraiser may not understand which employee characteristics are deemed most significant.⁷ For example:
 1. a. Problems need not be stated in detail for him or her.
b. Double checks work others do for him or her.
 2. a. Does more than his or her share of the work
b. Works to improve his or her main weaknesses

The Appraisal Interview

The preceding section discussed written, documented appraisal forms. These generally are retained in electronic format and are prepared prior to sharing the results with the employee or have been used as part of the evaluation process. When transmitted to a subordinate worker, the results must be communicated with brevity, tact, and clarity. The supervisor who conducts the appraisal interview needs brief training or coaching on how to conduct such interviews. Initially, many supervisors are uncomfortable with the prospect of appearing to judge a subordinate, perhaps saying or doing something that will be counterproductive and could create an unpleasant environment within the workplace from that point on. This usually occurs subsequent to an unfavorable rating. However, even interactions where the workers' efforts are laudatory produce tension among the parties involved. The cooperative basis between the supervisor and subordinate could be tainted by the experience and a previously friendly environment may become soured.

These are fears many supervisors possess when they approach appraisal interviews for the first time. In the days and weeks prior to a formal appraisal interview, stress among those involved is common, and is not necessarily harmful. Some emotional tension concerned with appraisal is inevitable and causes interviews and interviewees to think about what's important for achievement in the organization. Yet for the vast majority of appraisal interviews, the process is positive and ultimately even enjoyable for both parties. High-performing workers leave the interview enthusiastic about doing better work. Substandard workers realize they have a sympathetic supervisor and another opportunity to do better; often, they too feel relieved by the process. The following are guidelines for letting workers know how they are doing:⁸

- Select a quiet, comfortable, and appropriate location for the interview, such as the supervisor's office, if private, or a conference room.
- Plan to avoid interruptions. The process has been on the minds of the interviewees for weeks. They deserve the supervisor's undivided attention during the interview. The supervisor also should allow extra time for the subordinate to discuss workplace-related matters. Such discussions, however, should not serve as a general sounding board for excessive gripes that are far afield of the main purpose of the meeting.
- Put the person at ease. Humor and informality can help reduce tension before substantive issues are considered.
- Conduct the interview in a positive manner. Even if the subordinate requires further training for a skill not fully mastered, the supervisor should emphasize initially positive job accomplishments, while not minimizing any failings that require correction.
- Review the ratings by category. The categories for security workers can include decision making, dependability, development, interpersonal skills, leadership, learning ability, management ability, motivation, personal qualities, professionalism, quality consciousness, and report writing (Box 6.3). Not all Insert qualities can or

BOX 6.3 USING SPECIFIC LANGUAGE IN PERFORMANCE APPRAISALS

Supervisors and managers are urged to use specific language in describing qualities among subordinates to be evaluated.

- Accuracy
- Achievement
- Administration
- Analytical skills
- Communicative skills
- Competency
- Computer skills
- Cost management skills
- Creativity
- Decision-making skills
- Dependability
- Development
- Evaluation skills
- Goals and objectives
- Improvement
- Initiative
- Interpersonal skills
- Judgment
- Knowledge
- Leadership
- Learning ability
- Loyalty and dedication
- Mental capacity and application
- Motivation
- Organization
- Performance qualities (general)
- Performance qualities (specific)
- Personal qualities
- Planning skills
- Potential
- Problem-solving skills
- Productivity
- Professionalism
- Quality
- Report writing skills
- Resourcefulness
- Responsibility
- Selling skills
- Stress

Supervisory skills
 Tact and diplomacy
 Team skills
 Time management skills
 Versatility

Source: Neal Jr., J.E., 2014. *Effective Phrases for Performance Appraisals*. Neal Publications, Perrysburg, OH.

should be covered in the time allocated for such interviews. The review should limit ratings to those considered most central to the tasks of the workplace.

- Keep the interview performance-oriented. The supervisor may wish to avoid the accusatory use of “you” in speaking with the worker and instead emphasize the way certain tasks were completed and their quality.
- Encourage the subordinate to talk. Often, supervisors and subordinates have little opportunity to discuss job performance in a quiet environment. At the interview, the subordinate has an opportunity to state whatever he or she thinks is pertinent to the review. Following or during the interview, the supervisor may wish to take notes of such statements. The supervisor may also wish to prepare an Employee Progress Report that is a simple but concrete direction for future growth (Box 6.4).
- Respond to objections, problems, and disagreements. The supervisor should calmly accept criticism from the subordinate. Appropriate objections, problems, and disagreements should be resolved by the supervisor within a reasonable period of time after the meeting. (Often simply relating a vexing incident to the supervisor relieves accumulated stress felt by the subordinate.)
- Concentrate on facts. The truth must guide the supervisor in such appraisal interviews at all times.
- Be a coach, not a judge. The objective is to improve performance, not to pass judgment that, although possibly accurate, will not lead to employee improvement.
- End the interview on a positive and supportive note.

The interview process might seem tedious from the above description. Yet the interview itself, properly planned and executed, takes only a few minutes, up to 0.5 hour. At its conclusion, the supervisor may note critical results from the interview and plan any follow-up actions indicated by the information provided by the subordinate. The observer is likely to use this occasion to identify plans to ensure employee growth. After a series of appraisal interviews, the supervisor may analyze teamwork performance and identify technical or behavioral issues requiring improvement.

With the conclusion of the appraisal interview process, the supervisor transmits reports to his or her supervisor for review. This process informs middle management about the advancements being made by operational employees and also by the supervisor responsible for success within a unit. Senior management uses this method, among others, to evaluate the capacities of work units and their managers.

BOX 6.4 EMPLOYEE PROGRESS REPORT FORM

Managers may need to evaluate particular qualities among security workers. Those qualities differ according to job title and level, and often overlap. The following are just a few categories by which workplace achievement or deficiency can be measured:

Employee Progress Report	
Name _____	Date _____
Position Classification _____ Department _____	
How long has the person been under your supervision? _____	
How well does the employee know the job? _____ _____	
How could job knowledge be improved? _____ _____	
How well is the employee performing in the position in terms of quantity and quality? _____	
How could job performance be improved? _____ _____	
What progress has taken place since the last appraisal? _____ _____	
What specific recommendations have you made for improvement and in what time period? _____ _____	
Signed _____ Date _____	

Source: Neal Jr., J.E., 2001. *The #1 Guide to Performance Appraisals*. Neal Publications, Perrysburg, OH.

The appraisal interview retains some characteristics of a confrontation between a superior person in the management hierarchy and a subordinate one. Like any confrontation, the process can be difficult; yet the possibility cannot be used as a rationalization for avoiding the course of action. The lack of such an encounter can leave superior performance unacknowledged. Equally, unsatisfactory performance may remain uncorrected. Unsatisfactory workplace performance that goes unevaluated and uncorrected is not likely to improve on its own. The appraisal process – from planning through written reports to oral interviews – is an obligation of high-performing management. The process has too many potential benefits relative to risks to be ignored.

Assessing Performance Among Different Employment Levels

Much of what has been discussed so far is written with the supervisor and subordinate at operations level in mind. These points also are applicable among members of middle and upper management throughout the organization. Assessment for these persons is directed at the different nature of work performed by employees with different levels of responsibilities.

The workplace demands activity that may be divided into three categories: conceptual (analyzing, directing, planning), human relations, and technical skills and operational services. While the proportion of these components differs according to the level of employment, all three are present for all employees, as shown in Figure 6.5.

All work within organizations contains a combination of three types of abilities shown in Figure 6.5. The proportions of each can vary widely according to the job position and employer. Performance evaluation can be directed to each of these categories weighted according to individual employment responsibilities.

A trained entry-level employee on the job for the first time, without a supervisor or coworker nearby, may be called on to make an on-the-spot decision of importance to

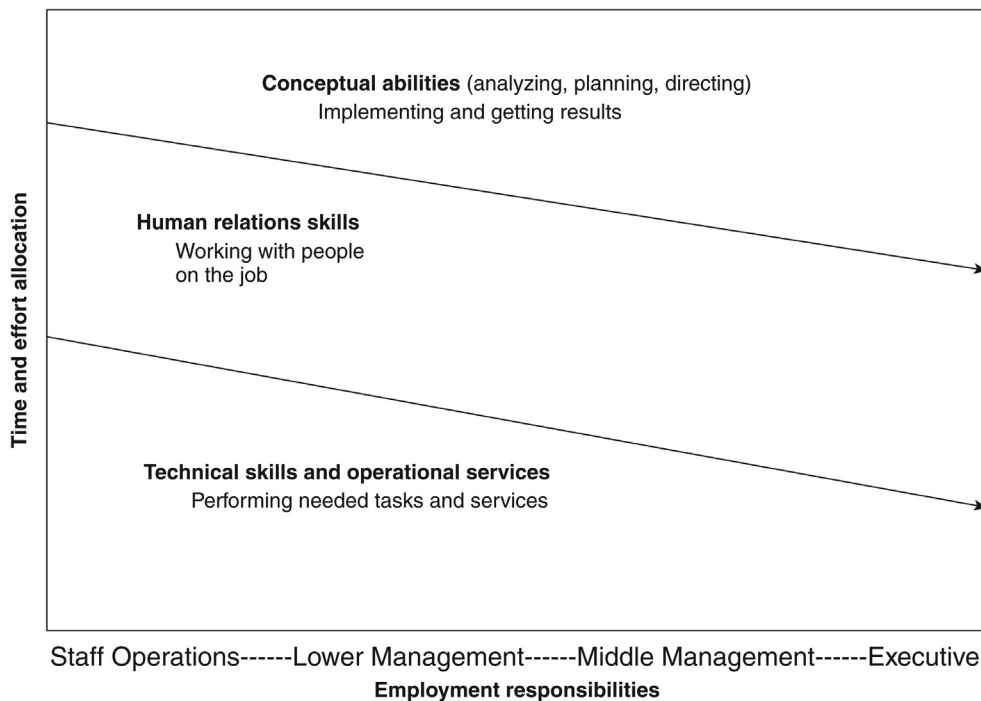


FIGURE 6.5 Performance evaluation related to different levels of workplace responsibilities. At all levels workers need technical and operating skills, the ability to work well with others, and conceptual strength to move the organization ahead with the times. This figure shows the changes in time allocations for each of these activities related to job function.

the organization. This certainly is conceivable for security employees who have extensive public contact. For this reason, even this operational neophyte must possess solid conceptual understanding and functional skills to respond to such a situation.

Nonetheless, the nature of management moves from being less operational to more conceptual depending on the worker's position within the workplace hierarchy. Therefore, middle and upper managers tend to be judged more on analytical, planning, and implementing skills than on technical and operational abilities. Note also that human relations skills remain a significant concern throughout the workplace, regardless of one's position.

Reviewing Management Strategy

Middle and upper managers deserve appraisal just as the operational staff and their supervisors do. This section concentrates on the nature of management plans and how they are created and evaluated. The nature of management review focuses more on programs and their success over the previous work period than on human relations or technical service skills. All components are significant. Any one of these skillsets cannot be significantly deficient for the manager to retain standing. A few strategies have had wide influence on organizations for getting work done and adjusting to changing circumstances. The next section discusses some of these techniques.

Management by Objectives

This concept was introduced by Peter Drucker and Douglas McGregor in the 1950s and was widely accepted in management circles about a decade later.⁹ The success of the management by objectives (MBO) model has been embraced by private industry, institutions, and the government. At the core are four principles:

1. The employee and her or his superior jointly set goals.
2. The employee endeavors to meet the goals.
3. Performance is evaluated against the goals.
4. The employee and superior jointly set new goals for the next measurement period.

MBO is a cooperative process, yet for it to succeed both the goal and the means of achieving that goal must be understood by all parties concerned (Figure 6.6). MBO was created with profit-making organizations in mind. It soon became apparent, however, that substantial applicability of MBO to nonprofit organizations and government existed. In order to use the model, the organization must affirmatively answer the following questions:¹⁰

- Does the organization have a mission to perform? Is there a valid reason for it to exist?
- Does management have assets (money, people, a plant, and equipment) entrusted to it?

The five-step MBO process

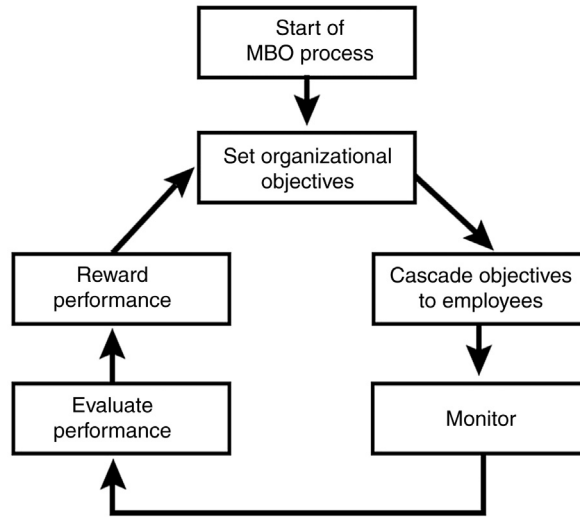


FIGURE 6.6 Management by objectives (MBO) is a process in which management objectives are agreed to and decided upon by management and employees. Therefore, both parties understand what is expected of them. The process is fluid and can lead to new challenges to be addressed. (Source: <http://communicationtheory.org/management-by-objectives-drucker/>.)

- Is management accountable to some persons or authority for a return on the assets?
- Can priorities be established for accomplishing the mission?
- Can the operation be planned?
- Does management believe it must manage effectively even when the organization is a nonprofit one?
- Can accountabilities of key personnel be pinpointed?
- Can the efforts of all key personnel be coordinated into a whole?
- Can necessary controls and feedback be established?
- Is it possible to evaluate the performance of key personnel?
- Is a system of positive and negative rewards possible?
- Are the main functions of a manager (planning, organizing, directing, evaluating) the same regardless of the type of organization?
- Is management receptive to improving methods of operations?

These questions are geared toward nonprofit organizations, although the same qualities can appear in any bureaucracy. Those who plan operations strategically often choose to design systems in which management has authority but not responsibility. Managers or entire work units normally have authority to conduct activities, and may take credit for any success. But in the event that the desired goals are not achieved, the same individuals or entities can argue that they are not responsible for the results. They

BOX 6.5 LINKING MANAGEMENT TO AUTHORITY AND RESPONSIBILITY

One of the circumstances in which management underperforms occurs when a manager or a group of managers have authority but not responsibility. This is the situation that MBO strategy seeks to make less possible. MBO links authority and the right to take credit for success directly to others, but holds the same manager responsible in case of failure. It might seem astonishing that organizations can have active units of authority without responsibility, yet this situation has occurred in organizations large and small with dismaying frequency. The following are just a few examples:

- *Organizational design.* The Port Authority of New York and New Jersey is a giant bureaucratic conglomerate that owns bridges, tunnels, airports, and commercial office space in the New York City area. The Port Authority employs thousands and has revenues in the billions. But who is responsible when things go wrong? Technically, the governors of New York and New Jersey have the responsibility. But it is hard to pin responsibility on two persons in different states who often have divergent and competing interests and priorities. In such situations, if results are unsatisfactory, no single authority answers for them. One might assume that such situations occur not through inadvertence, but by design.
- *Programmatic design.* Consider a security program in which the director has the authority to hire or fire personnel, to contract or terminate a contract of a security service provider, and to take other relevant actions. Yet in some circumstances, such a manager may claim to take little or no responsibility because results are not tied to other relevant factors. For example, such a manager could claim that insufficient resources and too little time were responsible for unsatisfactory results. This may be true, but managers need to document early on that resources, timing, and unforeseen circumstances could affect a carefully crafted plan.

may claim they did not have control over all circumstances and resources. Who does? Persons who work in such an environment are “never wrong” because they always take credit for success but shun responsibility for any failure (Box 6.5). Reversing this kind of mind-set is the target of MBO strategy. MBO makes individual managers or groups conceptually and factually responsible for defining objectives that can be independently verified and justified.

MBO brings managers, supervisors, and workers together to share authority for setting objectives and holds them responsible if those goals are not met. It can be structured for a particular work group or for a larger organization. The MBO team allocates and distributes personnel, identifies what resources are available, and determines what more is needed. This increases the opportunity for involvement by all personnel, provides specialized resources as needed, and uses varying management concepts as appropriate to achieve results. In the end, responsibility and authority, success and failure, rewards and penalties are all linked.

Examples of MBO in Security Applications

In the following sections, we will look at various examples of MBO in action.

Example 1

In this example, the organization is a regional distributor of brand-name gasoline and owns refining, storage, and transportation facilities as well as several filling stations, many with convenience stores attached. Additionally, the company has franchise relationships with many independent operators. The parent company has designed and installed an advanced proprietary central monitoring system and has connected its offices, processing, and retail facilities to it. Soon after installation, two needs emerge concerning the new system.

Objective: More efficient use of proprietary alarm monitoring resources.

Goal no. 1: Reduce the number of false alarms received by the department's proprietary alarm system by 20% over a 6-month period without losing quality of response.

Program:

1. Reeducate all internal users about the use of the alarm system, focusing on factors that frequently cause false alarms.
2. Designate an employee to review all false alarms within 1 day of occurrence and determine what actions could be taken to reduce such alarms.
3. Institute measures to verify alarms before calling police, for example, by using closed circuit television with interactive audio capacity to verify a possible alarm condition after receiving the initial alarm signal.
4. Provide management with written reports of alarm activity as they occur. The reports compare incidents on a year-to-date basis to document the trend.

Goal no. 2: Expand use of the alarm system to the organization's customers and franchisees.

Program:

1. Prepare literature on cooperative use of the proprietary system and distribute to all prospects emphasizing technological advancement. Mail a second time 2 months later to nonrespondents.
2. Schedule an open house so prospects can visit the alarm monitoring station and learn of its capacities. Demonstrate its surveillance and reporting capabilities and any two-way communication features.
3. Designate a program manager to call prospects subsequently to determine interest. The program manager should work from a carefully prepared script and should emphasize benefits to being protected within the company's alarm system, although the commitment is optional.
4. Train alarm installers to deal with the company's franchisee's special requirements and concerns.

5. Facilitate insurance savings for participants who contract for the service by providing details to the franchisee's insurance broker or carrier.
6. Design initial low-cost incentives for franchisees to adopt the system. These may include free installation and low monthly recurring charges.

Example 2

In the second example, a large urban medical center operates several of its own parking garages combined with nearby open parking lots. Due to the nature of the 24-hour service provided by the facility, a pattern of thefts from cars, vandalism, and occasional car theft has emerged over the previous year, and perception of the problem is increasing. Victimized employees and visitors have pressured the hospital administration and security director. Some threatened to quit if the problem was not resolved. Perimeter control and other measures are needed to reduce incidents.

Objective: Reduce theft from and of vehicles. Reduce vandalism.

Goal no. 1: Reduce chances of unauthorized access to parking areas.

Program:

1. Seal openings to all the parking garages so that users may not enter indirectly. (A redundant pedestrian back entrance to one multistory parking lot should be sealed permanently.)
2. Provide additional surveillance at the zone where cars enter and exit. (An office for the parking garage manager on duty should be relocated with windows open to the entrance.)
3. Improve lighting throughout. (Newer lights also cut energy costs.)
4. Install covert and overt closed circuit television, which collects images of all vehicles and drivers arriving and departing from the facility. The videotape recording of the traffic should be located in the office of the security department in the main hospital building. Signs should be posted stating "These Premises Under 24-Hour Video Surveillance."
5. Link the television image collection with a license plate lookup system so that use of the facility can create data points useful in managing the facility better, including managing loss issues.
6. During hours of little activity (10 p.m. to 7 a.m.) the garage door should be closed and opened only when traffic is present. Whenever the doors are open, a security person or garage attendant must be near and visible at the entrance in addition to the nearby visible parking garage cashier.

Goal no. 2: Reduce or eliminate chances of theft from automobiles and of automobiles themselves.

Program:

1. Provide a scooter or golf cart to patrol the lots frequently and on a random basis. It would remain visible and capable of responding to emergencies quickly.

2. Install signs to remind drivers not to leave valuables exposed in their vehicles. If customers make their cars tempting to thieves, provide extra surveillance and inform the customers when possible to be more careful.
3. Establish separate parking areas for regular medical center staff apart from spaces for visitors.

Goal no. 3: Reduce fear level of nighttime and early morning patrons of the garages and lots.

Program:

1. Offer an escort service from the building entrance to vehicles for those arriving or departing between 11 p.m. and 7 a.m.
2. Install an alarm and communications system at all levels of the parking garage and lot. If someone presses the emergency button, an audible alarm and a flashing strobe light should be illuminated. An attendant should have two-way communication with the person requiring assistance. Test this system on a regular (daily or weekly) basis so that monitoring personnel are used to signals coming in from this location.
3. Improve housekeeping in the parking garage and lot. Walls should be painted in bright colors and unused utility vehicles previously stored in the lot should be removed.
4. Conduct a brief preimplementation and postimplementation survey of users to determine success.

The MBO technique has many advantages. One criticism of MBO, however, is that it has not been subjected to rigorous analytical standards to critically establish success of the concept. This is true in loss reduction programs as well as other management applications using MBO. Yet this criticism could be raised with many other personnel tools currently in use as well. Further, one review estimates that MBO successes are about five times greater than its failures.¹¹ However, the benefits of MBO may decline over time, requiring a fresh analysis of situational circumstances that have changed months or years after the original objectives were achieved.

Failure to achieve the desired goals from MBO does not necessarily mean total failure. Planners and implementers in such situations have endeavored through numerous means to achieve success. Their lack of success may eliminate the value of some measures that have been tried and may suggest other measures that could take their place or augment them.

Critical Incident Review

Another way by which managers may be evaluated is through a case review of a significant incident or launched program that occurred over the previous 6 months or 1 year. The manager for this program might anticipate to have all aspects of the incident carefully reviewed, leading to an eventual statement or report of findings. In this sense, the critical incident review is like an internal audit of an incident or program.

The reviewers in such a process frequently are assigned from outside the immediate chain of command. They may or may not have any personal knowledge of the incident or program, but rather possess broad experience and analytical skills sufficient to enable a fair and comprehensive review of the facts. Critical incident reviews are often preferred by federal and state governments for program evaluation. The reviewers may be investigators, internal auditors, managers from other operations, or professional consultants. Indeed investigators are themselves normally judged, in part, by the quantity and quality of their case files. (Such redacted case files may one day be required for junior investigators to obtain their own licenses.)

Problem-Solving Ability

A majority of persons who work in security come in contact with the public as part of their assignments. Security exists partly to provide at strategic locations competent, trained individuals who can deal with exceptional circumstances on the spot. This prompt action prevents a simple issue from becoming a major problem. Management expects security personnel to be problem solvers, not deniers or problem shirkers. However, security workers should not be expected to receive and resolve untoward events for which they have not been trained. Security personnel, unlike human resources personnel who usually work from their offices, may be found throughout the organization's facilities, dealing with incidents that can be resolved quickly. They are placed strategically about the operations. They are generally the true first responders. This enables security practitioners to resolve low-priority incidents so that they will not escalate to significant issues.

Senior management assesses and rewards subordinate personnel who assume responsibility for a potential problem and find a solution. Management observers also seek to assess such behavior and use it as a basis for commendation or promotion. Other individuals may initially tend to ignore the problem, and then deny its consequence, and, learning otherwise, temporarily think that others should be blamed, as shown in [Figure 6.7](#). Instead, they should be conditioned to pass through these emotional checkpoints and maturely assume responsibility, which leads toward a solution of the problem presented. Other individuals accept responsibility and readily seek to resolve problematic issues.

Not all problems presented to security personnel should be solved by them. In many cases, the problem presenter should be encouraged to solve the problem himself or herself. Other issues are reasonably related to the concerns of security services and the burden for responding belongs to security. When this is the case, security personnel should push through any psychological barriers to resist acting, and assume responsibility for a solution.

Field Review

The term "field review" refers to programs located at distant facilities. It frequently represents a senior manager's critique of an operational manager's program elsewhere. At such times, the senior manager usually arrives at the distant location, conducts a

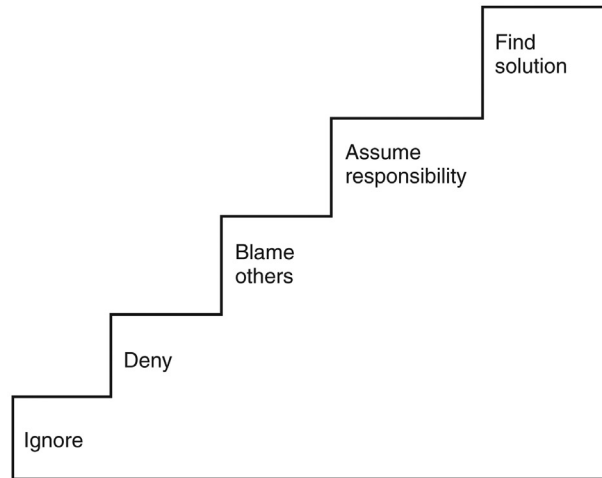


FIGURE 6.7 From ignoring to resolving problems: a process. Prevention outranks brilliant after-the-fact problem response and resolution. Some workers will ignore or deny ownership of an untoward circumstance. They may blame others. However, employees confident of themselves will assume responsibility for an incident and find the solution, despite the risks to them personally. (Source: Grove, A.S., 1985. *High Output Management*. Vintage Books, New York, NY, p. 194.)

broad survey of relevant factors, and later reports to local, regional, and senior management of the circumstances found during the scheduled field review (see [Box 6.6](#)). The field report evaluates local security management and programs for their strengths or weaknesses.

BOX 6.6 VISITS FOR A FIELD REVIEW

Field reviews of ongoing security programs give headquarters' management an opportunity to assess and respond to local problems and opportunities. A chief security officer or his or her deputy is likely to visit offices in a dispersed organization at least once a year. These are opportunities for the security policy to be emphasized with local general managers at these offices. Here are procedures for conducting a field review. The process is meant to enhance cooperation and good rapport between global headquarters and the local operating business. Generally, a routine field visit of an operating facility can be conducted in 1 or 2 days, depending on the complexity of the facility. The final analysis and report requires hours more to compile.

The following are guidelines used by senior managers on their periodic field visits:

1. *Plan ahead.* Schedule the visit weeks in advance so that the occasion will not be disruptive to local operations. (Obviously, if a pressing need exists, the review should be expedited.)
2. *Meet with the general manager at the beginning of the fact-finding visit.* Explain that the nature of the visit is largely consultative and supportive. But also state that if anything of a critical nature for action is discovered during the visit, such findings will be shared with the

general manager by the security evaluator before leaving. Another advantage of meeting with the general manager before beginning the inspection and evaluation is that the evaluator has the chance to learn about any recent concern that may affect the evaluation.

3. *Review quantitative data prior to the visit.* Other data set may be examined on-site and may be copied for later analysis.
4. *Allow time for local security managers to share concerns.* Endeavor to meet significant new employees who have joined the organization since the previous visit.
5. *Inspect any new security system that has been installed since the previous visit.* Purpose: to determine effectiveness and value of the system.
6. *Concentrate on the most important security problem concerning management at that location.* Additionally, review security matters of concern to headquarters and share what the plans are to respond to them.
7. *Meet with the general manager again before departing.* Share what has been observed and discuss possible problems. If they are of a minor nature, they may be resolved on the spot and not appear in the final written report. If they are major, begin dealing with a solution immediately, following up later until the issue is resolved.

Final reports contain an executive summary, findings, exhibits, and recommendations for actions. This plan details what work is needed to be done, who is responsible, and when the implementations are to be completed. Global headquarters follows up to make sure that both its tasks and those of the local operating business are completed in a timely fashion.

Performance Reviews for Senior Management

Appraisals need not be limited to operational staff personnel and lower and middle management. All employees in an organization committed to systematic evaluation of individual performance may be involved in the review process. This includes senior staff officers and the chief executive officer (CEO). In large complex organizations, the CEO may request that the senior officer for human resources conduct the evaluation of all senior staff officers, or the CEO might assume this responsibility. In addition, an outside consultant may be retained for the process.

Performance evaluations of the CEO and senior staff officers are less likely than appraisal further down the management hierarchy ladder. This is because senior staff officers are under scrutiny by a variety of outside sources. Principal among these is the board of directors, trustees, or an equivalent governing body. Since passage of the Sarbanes-Oxley Act of 2003, stricter financial reporting and accountability standards for public corporations also have been in effect. This requires more review between the CEO, the CFO, and others with the corporation's accounting firm. Review of performance of a different sort also takes place among officers of publicly held companies by stock analysts. Such analysts may follow the company and regularly ask penetrating questions about performance goals and results and then publish their findings and conclusions. Further, senior officials are subject to judgment by the media and shareholders, particularly when an incident has occurred that raises doubts about the capability of the team in the executive suite.

The Limitations of Appraisals

A case has been made that appraisals of individuals at all levels serve the needs of a dynamic organization. Because of the criticality of loss prevention in many organizations, performance appraisals may be more likely to be an integral part of the management strategy in the security department than in others.

Appraisals do have their limitations. Bias in judgment of one individual by another may be difficult to eliminate, particularly in the minds of a subordinate receiving a critical evaluation. A more searching dissatisfaction with the appraisal system has been raised by psychologist Harry Levinson, who argues that job descriptions must be behavior-oriented as well as results-oriented.¹² Levinson suggests employers create dynamic job descriptions in which behavior for different positions – particularly in management – is identified in advance. Examples of behavior-oriented questions to be answered in preparing the dynamic job description are as follows:

1. How does this job require the incumbent to handle his or her aggression and attacking capacity?
2. How does this job require the incumbent to manage affection, the need to love and be loved? Is the person required to be a socially friendly leader of a close-knit work group?
3. How does this job require the incumbent to manage dependency needs? Will the individual be able to lean on others who have skill and competencies, or will he or she have to operate alone?
4. What ego ideal demands does this job fulfill? If one does the job well, what is the gratification to be gained? Money? Recognition? Eligibility for promotion? The feelings of great personal achievement?

The Promotion Process

Promotions are substantial changes in a job, normally requiring additional responsibility and entailing greater authority for which increased income, perquisites, and status are provided. Persons considering the prospect of being promoted concentrate on these external benefits. Such benefits serve as important inducements that make promotions attractive for many. Employers also see promotions as a means to sustain vital programs. Promoting someone offers hope for improvement in the sector for which the newly elevated person will be responsible. Consequently, to the employer, the act of promoting someone involves the weighing of numerous factors before the decision is made. For this reason, organizations consider promotions carefully.

Advancement That Stops Short of Promotion

Frequently, management cannot promote someone at a particular time to a new position for various reasons. The new position may not be funded at the time and the supervisor or middle manager needs to await budget approval to cover the prospective promotion.

This may entail a delay of many months despite a desire by management of the segment to formalize the employee's advancement. Or management may require more time in order to make a decision because two or more candidates are in competition for the same position and a clear superior choice has not emerged. Additionally, the organization may be facing a change in senior management or in a policy direction that temporarily blocks promotions and other decisions down the chain of command. Still other reasons can delay an otherwise normal procedure.

Despite these conditions, the supervisor and middle manager have several options available to them so that they can provide greater recognition and challenge to their workers. Supportive managers endeavor to encourage subordinates, although the measures available fall short of a traditional promotion. The following are a number of ways in which supervisors can recognize and challenge their workers:

- *New responsibilities.* The supervisor or manager may provide new duties for persons who are exceeding requirements but for whom a promotion at the time is not possible. Sometimes, the assignment of duties to promising candidates can help identify the best performers in contention for the promotion.
- *Desirable perquisites.* If the individual cannot be promoted but deserves recognition, perquisites may be provided in ways available to management. These include better scheduling, preferred postings and vacation time, and special training.
- *Special recognition.* Ego-gratifying measures may be within the unit's capacity to fund easily and can satisfy the employee by recognizing his or her achievements. This can involve providing the security officer or investigator with a new title – for example, adding “senior” or “executive” to the title. Providing calling cards with the individual's name and position, and changing the person's uniform or office location also can serve as welcome perquisites that fall short of formal promotion.
- *New duties now; promotion later.* Pending the increased funding, the individual can effectively assume the new position without officially assuming the new job. When the budget line is approved, the position becomes available to the person to whom it was promised.

What's Wrong with Promotion?

Promotions work to advance the needs of the organization. However, several factors make promotions difficult decisions for management.

The Peter Principle

In 1969, Lawrence J. Peter and Raymond Hull introduced a facetious concept of occupational incompetence, named for the principal author. Their proposition stimulated debate almost immediately and has remained controversial since then. The Principle is also quite humorous as a serious basis of management theory. The Peter Principle

states that in a hierarchy, every employee tends to rise to his or her level of incompetence, or the cream rises until it sours.¹³ This notion is best considered as a jocular characterization of management ascension and postulates that workers eventually reach a level they should not occupy. It observes that persons in positions of authority eventually reach their level of incompetence and are not likely to be promoted further in the future.

The appeal of this notion is that it correctly reflects the experience of many managers who unflatteringly conclude that their supervisors have been promoted from a level of competence to one of incompetence. This is reflected in Peter's Corollary, which states that in time, every position tends to be occupied by an employee who is incompetent to carry out its duties. The assumption is that work is accomplished only because many persons have yet to attain their level of incompetence. The key to one's health and happiness on the job is not to accept the "final promotion." Peter suggests the key is the condition of "creative incompetence" in which the individual produces superior work while avoiding being promoted. But how can one ever be sure exactly what that level is?

The Peter Principle and its analogues have been resilient topics in management discussions because they reflect the fact that at least some promotions are failures.¹⁴ Most promotions require individuals to grow with their new positions and possibly make lifestyle changes, such as working different hours and physically relocating. These are stress-provoking circumstances and some people who are promoted later conclude that the promotion was not to their satisfaction. Despite the effort that management has expended to select and promote the right candidate, the process has failed. The best strategy is to permit the individual to resume his or her previous post as gracefully as possible. This is not an easy option. But if the individual and management can accommodate the shift, the future can make more sense. Surely, the individual has performed optimally in this role previously and can do so again in the future. Numerous security programs over the years have had such experiences and have made the necessary accommodations to people who sensitively chose self-demotion.

Why Promotions are Important

Apart from benefiting the individual who is promoted, promotions are good in reality for the work unit and the larger organization in several ways:

1. *The skills are needed to achieve goals.* This is the most obvious reason for promotion: the job has been budgeted for good reason and the work it represents needs to be done.
2. *The person promoted may take the program in a new, desirable direction.*

Organizations are constantly changing. Sometimes this is a result of internal forces, such as changes in management strategy; other times it is a result of external factors, such as modifications in the marketplace and advances in technology that affect how

the job needs to be done. A newly promoted person may add value in translating these forces to the workplace relative to the previous manager.

3. *Promotions permit individual growth.* Employees at all levels need to feel as if they are growing, although not all employees want challenges beyond those presented in their current positions.
4. *Promotions reward good work.* Unlike one-time bonuses or lesser recognition of competence and promise, promotions are enduring and set a platform to encourage further good work.
5. *Promotions inform all employees that career advancement is possible.* When one person is promoted, other workers are encouraged that greater opportunity awaits them also if they are qualified and motivated to assume greater responsibility.

Summary

Appraising workers' efforts at all levels is difficult. The resistance to appraisals takes many forms: dislike of judging others, fear of harming workplace comity, and concern that litigation or formal complaints from a union will be filed from dissatisfied workers at some point. Yet these fears are exaggerated and the returns from an appraisals program are worth the effort. Properly managed appraisal programs can document and correct unproductive behavior before it becomes unchangeable or causes harm. On the positive side, appraisals identify and encourage superior performance in the workplace and help develop talent. Numerous ways exist of assessing and ranking employees, all of which must be measured against the needs of the workplace. Promotions help the organization reward those best able to maintain the desired standards of productivity and to bring fresh ideas into the organization in order to move it forward.

Discussion and Review

1. Discuss specific reasons why personnel appraisals serve the interests of the organization.
2. How can top-down appraisals be designed to make judgments that are less likely to be biased by autocratic behavior?
3. How do appraisal guidelines differ for employees during the probationary period?
4. How can the halo effect be mitigated among managers who must assess subordinates?
5. Why should an evaluator look forward to an appraisal interview?
6. If work can be divided generally into three categories – technical/service, human relations, and conceptual – how do personnel appraisals change relative to these characteristics?
7. What accounts for the popularity and resiliency of MBO?
8. Why should organizations want to promote employees?

Endnotes

- ¹ Reibstein, L., 1998. Firms ask workers to rate their bosses. *Wall Street Journal*, June 13, p. 15.
- ² Jordan, J.L., Nasis, D.B., 1992. Preference for performance appraisal based on method used, type of rater, and purpose of evaluation. *Psychol. Rep.* 70, 963–969.
- ³ Carroll, S.J., Schneier, C.E., 1982. *Performance Appraisal and Review Systems*. Scott, Foresman and Company, Glenview, IL; Moulder, E.R., 1995. *Performance Appraisal and Compensation Programs in Local Government*. ICMA, Washington, DC.
- ⁴ Schwab, D.P., Heneman, H.P., DeCotiis, T.A., 1975. Behaviorally anchored rating scales: a review of the literature. *Personnel Psychol.* 28, 549–562.
- ⁵ Bernardin, H.J., Beatty, R.W., 1984. *Performance Appraisal, Assessing Human Behavior at Work*. Kent Human Resources Management Series. Kent Publishing Company, Boston, MA.
- ⁶ Bernardin, H.J., Elliott, L., Carlyle, J.J., 1980. A critical assessment of mixed standard rating scales. In: *Proceedings of the Academy of Management*, pp. 308–312.
- ⁷ Guion, R.M., 1986. Personnel evaluation. In: Berk, R.A. (Ed.), *Performance Assessment: Methods & Applications*. Johns Hopkins University Press, Baltimore, MD, p. 365.
- ⁸ Neal Jr., J.E., 1994. *Effective Phrases for Performance Appraisals*. Neal Publications, Perrysburg, OH.
- ⁹ Drucker, P., 1954. *The Practice Side of Management*. John Wiley & Sons, New York, NY; McGregor, D., 1960. *The Human Side of Management*. McGraw-Hill, New York, NY.
- ¹⁰ McConkey, D.D., 1973. Applying MBO to nonprofit organization. *S.A.M. Adv. Manage. J.* 38, (1), 10–20.
- ¹¹ Kondrasuk, J.M., 1981. Studies in MBO effectiveness. *Acad. Manage. Rev.* 6, 419–430.
- ¹² Levinson, H., 1970. Management by whose objectives? *Harvard Business Review*, July–August, vol. 48, issue 4, pp. 125–134.
- ¹³ Peter, L.J., Hull, R., 1969. *The Peter Principle*. William Morrow & Co., New York, NY.
- ¹⁴ Peter, L.J., Hull, R., 2011. *The Peter Principle: Why Things Always Go Wrong*, reprint ed. HarperBusiness, New York, NY.

Additional References

- Alain, P., 2013. *The Quick and Easy Performance Appraisal Phrase Book*. Career Press, Pompton Planes, NJ.
- Drucker, P., 2004. The rules of executive class. *Wall Street Journal*, June 1, p. B2.
- Fisher, C.D., Schoenfeldt, L.F., Shaw, J.B., 1993. *Human Resource Management*, second ed Houghton Mifflin, Boston, MA.
- Hoover, G., Campbell, A., Spain, P.J. (Eds.), 1994. *Hoover's Handbook of American Business 1995*. Reference Press, Austin, TX.
- King, P., 1988. *Performance Planning & Appraisal: A How-to-Book for Managers*, second ed McGraw-Hill, New York, NY.
- Krass, P. (Ed.), 1998. *The Book of Leadership Wisdom*. John Wiley & Sons, New York, NY, p. 375.

Discipline and Discharge

There is occasions and causes why and where-fore in all things.

—Shakespeare, *King Henry V*

The previous chapters discussed management's role in selecting, training, and supporting employees successfully. These processes provide the bases by which effective managerial programs thrive. However, some employees do not meet the expectations of management, despite earlier reasonable vetting and training and further appropriate interventions by their supervisors. At such times, supervisors and middle managers must resort to more strenuous measures in order to promote satisfactory work performance.

When the performance of employees does not meet minimum expectations, and a few words by the supervisor have not achieved their objective, a disciplinary procedure may be considered. The word discipline is derived from the Latin *discipere*, meaning to grasp or comprehend, and from *discipulus*, meaning pupil. The term “disciplined worker” may be used to refer to an employee who is reliable and completes required tasks. Yet the word in contemporary use often is equated with punish (from the Latin *punire*, denoting penalty and pain). However, in a workplace context, the two words should be regarded as distinct concepts. Supervisors use – or should use – discipline not to penalize subordinates, but rather to improve their behavior in order to meet agreed-to objectives of the workplace. As Henri Fayol observed in his seminal book *General and Industrial Management*, poor discipline is the result of poor leadership. Good discipline occurs when workers and managers know and respect the rules governing activities in the organization.¹

This chapter discusses why discipline is necessary, how operating programs use it, and what its pitfalls are. It also discusses the ultimate breakdown in the employee/employer relationship, namely discharge or removal from employment. These principles are applicable for security programs, but also apply to the entire organization where issues of sub-performance must be addressed.

Why Some Employees Fail to Achieve Desired Standards

In a well-planned and functioning workplace, most workers meet the minimally acceptable standards most of the time. But what of those who do not? It is useless for security managers to launch into a disciplinary mode before considering the reasons for poor performance. In fact, many reasons exist for why subordinates do not perform at a satisfactory level. These possibilities may be divided roughly into two categories according to their significance and credibility, as follows:

1. *Explanations that “may” satisfactorily explain poor performance:*

- a. A process critical to work malfunctioned. For example, utilities and support mechanisms for security operations sometimes fail. If a worker monitors alarm signals and the computer crashes, making it impossible for the worker to respond to the alarm in a timely fashion, the alarm console operator cannot be held responsible for substandard performance.
- b. Contradictory orders are given by another supervisor. The skills and job understanding of supervisors should be interchangeable. Yet if the primary supervisor sets the worker on a particular task, leaves the scene, and another supervisor preempts that original order, the worker should not be held accountable for not respecting the requests of the initial supervisor. This situation obviously would concern the supervisors’ managers who would likely regard the discordant communications as counterproductive to the objectives of the work unit.
- c. The task requested is illegal.
- d. The task required is immoral or unethical.
- e. The request is unsafe or dangerous. In such cases, the supervisor is responsible for the subordinate and should not have placed the worker in a position where safety is an issue.
- f. The worker has an acute health or personal problem. Supervisors tend to be lenient when an otherwise well-performing worker has an acute health problem or a personal emergency. But the nature of much security work requires regularity and reliability, and frequent performance exceptions are disruptive to its goals.
- g. The worker does not have the capacity to do the job. This suggests a failure in selection and training. While this is a possible explanation for poor performance or behavior, the situation is unlikely with any frequency to occur in carefully managed operations. If it does occur, discharge of the employee is an option. Another possibility is to assign the worker to a different type of position where he or she may have the capacity to perform satisfactorily in that position.

2. *Explanations usually “not” satisfactory to explain poor performance:*

- a. Insufficient supplies or materials are available for the worker. The absence of objects or substances routinely required at the worksite usually should not be an excuse for substandard worker performance. Workers generally ought to be able to recognize a situation in which needed materials are low and when reordering them is appropriate. For example, security officers may be expected to complete incident reports in a timely fashion on a prescribed form. The lack of availability of such forms should not be used by a security officer as a reason for not completing a report. Security officers are expected to be flexible in such situations. In this case, the details of the report could be written on plain paper, if necessary, and attached to the correct form when it becomes available. When something critical is required for worker performance but is not available due to an earlier failure by management, workers should not be penalized. (Increasingly, such reports

are prepared and transmitted electronically.) The same issue holds in terms of expecting workers to make best efforts if a system is down.

- b. The employee has been improperly trained. The corrective in such cases is to reassess the training process, if the objection seems reasonable, and retrain the individual. However, training that was carefully planned, adequately taught, and certifiably completed by testing to assure comprehension works against this as a credible explanation for poor performance.
- c. A coworker prevents the employee from completing a task. Employees are responsible for their specified duties. Saying that a coworker prevented the task from being completed is not a tenable excuse. Exceptions exist, for example, if one worker's behavior against another was harassing or flagrantly offensive. But could this worker have notified management of this circumstance and did not? In group or team assignments, management expects reasonable efforts by all members fully to contribute to combined success.
- d. Insufficient time exists to complete the task. This explanation would not be valid if work is assigned with an accurate understanding of how much time is required to complete it. The time required is generally measured against the average performance of established workers so that a reasonable work objective can be met.
- e. The worker does not like to do a particular task.
- f. The employee dislikes the supervisor or vice versa.

The Psychological Basis of Noncompliance

While some reasonable explanations for unsatisfactory workplace behavior are situational, others are psychological. That is, the worker has a conflict with the methods prescribed by the supervisor or the workplace itself. Unconsciously, the worker may resist authority seen in the embodiment of the supervisor. Failure to respond according to training and directions may be an act of rebellion that reflects deeper unresolved psychological conflicts on the worker's part. In extreme cases, the behavior may mask an adjustment disorder.^{*,2}

Consider the situation of a new uniformed security officer. The individual has been provided with a complete uniform, carefully selected by the employer. During training sessions, emphasis on the use and care of the uniform is stressed. Other uniformed security officers seen as role models by the novice during training are properly dressed. Nonetheless, on occasion, security officers may not be dressed according to regulations. This failure to be properly dressed in the prescribed uniform can be explained by the security officer as a situational exception, a lapse in judgment. This may be possible and excusable. However, a repeated pattern may be interpreted as a sign of resistance – even hostility – to managerial requirements.

*The psychiatric diagnosis for such a person may be adjustment disorder. The predominant manifestation is the inhibition in work or academic functioning, occurring in an individual whose previous work or academic performance has been adequate.

The supervisor's role at such times is not one of psychoanalyst for the errant subordinate. Workers who do not meet the standards of quality and behavior generally achieved by their coworkers require discipline. To fail to do so makes the employer a conspirator to poor performance.

Why Some Supervisors Do Not Discipline Well

A few tasks in the workplace are difficult for novice supervisors. The previous chapter mentioned appraisal interviews as a possible awkward task for supervisors. Providing adequate discipline for underperforming workers is another often onerous task for novice supervisors. But unlike appraisal interviews, which generally emphasize positive features of performance, disciplinary contact between the supervisor and subordinate is different.

The disciplinary process is awkward for both parties. Supervisors in particular may rationalize their inaction with regards to disciplining fellow workers (see [Box 7.1](#)). Yet like the appraisal interviews, if disciplinary measures are not taken, work performance could deteriorate. A lack of consistent disciplinary action by a supervisor in the workplace can be the basis of arbitrators' or civil court judgment against the employer. Poor performance without the presence of corrective action trains the worker that such behavior is permissible. The poor performance then is established as a fixed pattern.

BOX 7.1 WHY SUPERVISORS FAIL TO DISCIPLINE

A supervisor asks two workers to perform an unpleasant task, but one that is included in their job description. A few minutes later, the supervisor notes the workers taking a break for coffee. It is not their break time and the employees did not have permission to take an unscheduled break. The supervisor observes the situation and leaves the room without making a comment to them. The workers never perform the requested task and nothing is ever mentioned again by the supervisor.

Why do some supervisors fail to address employees' refusal to perform an assigned task? Edward L. Harrison, a professor of management at the University of South Alabama, surveyed supervisors from several industrial organizations participating in management development seminars. Based on their responses from his questionnaire, Harrison came up with 14 main reasons why managers fail to discipline workers:

Percentage	Reason for Failure to Discipline
42.9%	The supervisor had failed to document earlier actions so that no record existed on which to base disciplinary action
40.4%	The supervisor believed that he or she would receive little or no support from higher management for the disciplinary action
29.2%	The supervisor was uncertain of the facts underlying the situation requiring disciplinary action

20.9%	Failure by the supervisor to discipline employees in the past for a certain infraction caused the supervisor to forego current disciplinary action in order to appear consistent
20.5%	The supervisor wanted to be seen as a “good guy”
19.5%	The employee involved was a close friend of the supervisor
14.8%	Job demands and conditions made it inconvenient for the supervisor to discipline the employee
13.9%	The supervisor was uncertain of provisions in the labor agreement pertaining to the situation involved
13.5%	The supervisor provoked the employee infraction
13.3%	The employee problem was one that should be dealt with through the employee assistance program rather than through a disciplinary penalty
11.9%	The supervisor was concerned that a disciplinary penalty might result in a charge of racial or sexual discrimination
10.9%	The supervisor did not want to draw negative attention to his or her own operation
6.9%	The supervisor was reluctant to penalize the employee because the employee was a union officer
5.9%	The supervisor did not want to spend time on the grievance that might result from a disciplinary penalty

Source: Harrison, E.L., 1985. Why supervisors fail to discipline. *Supervisory Manage.* 30 (4), 18–22.

In effect, the supervisor who fails to appropriately correct the worker harms several parties. The deficient worker becomes complacent and may feel encouraged to flout more rules. Other workers observe the substandard coworker and wonder why he or she is permitted to deviate from the organizational policy. The quality of their work, too, may decline. The organization then becomes affected by an insidious decline in quality performance. Desired production goals or qualities of service are not met as planned. Finally, the supervisor realizes that by failing to correct subordinates, his or her job is not being performed as it should be. All of this is moot if the supervisor identifies errors in performance in a timely fashion, corrects them discretely and with dignity for the worker, and restores the employee to desired productive levels or behavior.

Human Relations–Oriented Managers

In the lore of the workplace, the bosses of yesteryear are remembered as Simon Legree or Ebenezer Scrooges. The characters are harsh, brutish, and cruel. Scrooge experiences a personal epiphany resulting in a happy ending for *A Christmas Carol*. Legree remains unrepentant until the end of *Uncle Tom's Cabin*. While the fictional portrait of past employers may have been stereotyped in literature, it is beyond debate that the contemporary

workplace is a kinder and gentler place for employees than in past generations, even concerning disciplinary matters.

Abusive bosses are no longer accepted or acceptable in the workplace. Yet not all managers have the sensitivity of trained counselors. Why should they? Managers have strengths and weaknesses like everyone else. Still, the reality is that contemporary managers are better attuned to and more tolerant of moods and feelings of workers than in the past. This is due to increased education, workplace training, changing workplace ethos, a growing understanding of psychological dynamics, changing employment laws, stronger union presence in parts of the security industry, and the risk of litigation or forced arbitration from complaints about supervisors from subordinates.

Progressive Discipline to Save Weak Workers

Management expends a great deal of effort on recruiting, selecting, training, and supporting employees. Considerable investment in the employee already has been made by the time he or she begins productive work. Further, the employer wants and needs workers to succeed. In such circumstances, the desirable goal is to turn any substandard behavior into acceptable or superior behavior with the least amount of stress and strain. Among some supervisors, the temptation to discharge an errant worker for solid reason often is strong and may be justifiable based on the circumstances. However, management has a financial incentive in endeavoring to improve substandard performance in lieu of dismissal if at all practicable. Therefore, initial or moderate deficiencies in behavior should not lead directly to a disproportionate response on the part of the supervisor. The response must be balanced, impartial, and appropriate to the circumstance.

Corrective or progressive discipline is an enduring and solidly based disciplinary strategy invoked by unionized and nonunionized employers alike. In unionized workplaces, such actions often are mandatory and included in collective bargaining agreements. These agreements usually state that discipline should be corrective in nature, rather than punitive, but the measures do not normally detail that discipline must start with a letter of warning and be increased after every subsequent behavior. Supervisors may initiate formal disciplinary action through the issuance of a letter of warning or suspension if an employee's actions do not improve after discussion. This process forces the manager who supervises the underperforming individual to make decisions and be held accountable. Resolution to problems is meant to be achieved expeditiously.

The stepwise or progressive disciplinary procedure, shown in [Figure 7.1](#), is used in many formal organizations and is meant to enhance levels of trust, communication, and dispute resolution. The sequence of events is as follows:

1. *Infractions at work or poor performance.* First, a potential disciplinary offense or behavior must come to the attention of a supervisor. Typically, these include chronic absenteeism, not being present at a post without leave, the performing of an unsafe act, poor work performance, and failure to follow instructions. When the infraction is

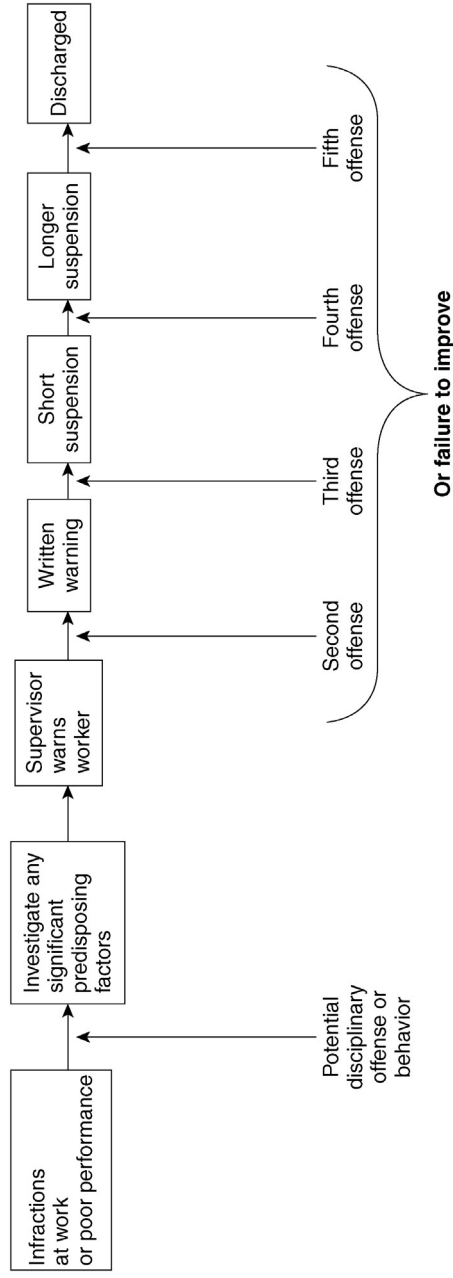


FIGURE 7.1 The stepwise disciplinary procedure. When an employee's performance does not meet expectations, a disciplinary procedure may be appropriate. The stepwise process seeks to correct errant behavior with the least force necessary. This procedure should not be regarded as a template for most workplaces, but rather as a reflection of a process that could improve behavior at one end or act as a reasonable defense against unlawful termination at the other end.

confirmed, the supervisor evaluates it further, confirming the facts in the situation, before confronting the errant employee.

2. *Supervisor investigates any significant predisposing factors.* The supervisor determines if any relevant predisposing factors might explain why the worker committed the infraction or performed poorly. Assuming the worker was tardy or absent from work (poor performance), was someone sick at home? Or were extenuating factors such as truly inclement weather responsible? Despite being tardy, did the worker call the supervisor to warn of his or her late arrival or absence so that scheduling adjustments could be made? Has the offense occurred previously? With what frequency? After gathering all related facts, the supervisor is now ready to discuss the performance deficiency with the worker.
3. *Supervisor warns the worker.* In a calm, nonconfrontational manner, the supervisor speaks briefly and quietly to the subordinate about the undesirable behavior. A supervisor may wish to employ a strategy such as the one for correcting behavior discussed in Chapter 5, that is, a gentle, 1-min reprimand. Subsequent to the encounter, many supervisors keep a workplace journal and note in it any significant worker disciplinary measures taken. This is by far the usual correction for an errant worker, and it usually suffices to improve worker behavior.
4. *The supervisor issues a written warning to the worker.* After an additional occurrence, the supervisor may “write up” the offense. The undesirable behavior and the response by the supervisor may be recorded in any one of several ways. The supervisor may send a brief, informal memorandum to the worker describing the offense. The supervisor also may write a longer, more detailed memorandum of the event, keeping one copy, forwarding a second to the worker, and providing the third for the employee’s personnel file. The supervisor may also use a Disciplinary Action Report in which the complaint, the method of reducing the undesirable behavior, and the corrective action are described, as shown in [Figure 7.2](#). If the workplace is unionized and disciplinary actions can be the source of a formal grievance, the form may be more detailed and composed of multiple parts: for the employee, the personnel department, the department head, and the union, as shown in [Figure 7.3](#).
5. *The worker is given a short suspension.* Verbal reprimand and written notice of substandard behavior usually result in improved performance. However, this is not always the case. In such instances, a more substantive measure is called for: suspension. The suspension may vary according to the workplace and the nature of the unacceptable behavior. One large security program sends the employee home for the day the offense occurred without docking pay. The goal is to dramatically inform the worker that the employer is dissatisfied with the worker’s behavior, but has faith that the employee’s behavior can and will improve.
6. *The worker is accorded a longer suspension.* Should an additional offense occur, or should a pattern of documented poor work behavior continue, the supervisor may

Disciplinary Action Report

Security Officer: _____ Date: _____

Post: _____ Time: _____

Violation:

Proper Procedure:

Corrective Action Taken:

Violation Reported By: _____ Date: _____

Mgmt. Review By: _____ Date: _____

FIGURE 7.2 Documenting substandard worker performance. Disciplinary actions need to be recorded to support a possible future charge of unlawful termination. The report also enables the workplace to make clear what the deficiencies are that require correction or improvement. Forms like this and that given in [Figure 7.3](#) are frequently part of electronic records. Source: Guy, E.T., Merrigan Jr., J.J., Wanat, J.A., 1981. *Forms for Safety and Security Management*. Butterworth-Heinemann, Boston, MA.

double the penalty of time suspended. The US Postal Service, for example, usually suspends workers for up to 7 days with loss of pay for the initial suspension. The duration of the penalty differs somewhat according to postal service zones and the severity of the offense.³ Seven- and 14-day suspensions usually are without pay.

Employee Misconduct Notice

To Personnel Department:
Date _____

Name of Employee _____ Time _____
 No. _____ Dept. _____

The above-named employee has displayed the following misconduct, and has been warned that this misconduct will be entered on his Personnel Record.

MISCONDUCT (Check where applicable and specify details in section indicated below)

Smoking in Restricted Areas ☐	General Inefficiency ☐
Leaving Work Without Permission ☐	a) Quality ☐
Violation of Safety Rules or Dept. Rules..... ☐	b) Quantity ☐
Refusal To Carry Out Supervisor's Instructions ☐	c) Accuracy ☐
Irregular Attendance ☐ (Specify No. of absences to date)	Discourtesy Toward Guest ☐
Frequent Tardiness ☐	Discourtesy Toward Fellow Employee..... ☐ (Mention other Employee)
Violation of Eating Regulations ☐	Attitude ☐
Breakage ☐	Carelessness ☐
Poor Service ☐	Other ☐

Specify Misconduct in Detail _____

Employee Comments _____

Disciplinary Action Taken _____

(Reprimand) (Layoff) (Other)

Signature of Supervisor

I acknowledge receipt of this notice

Original (White) to Employee
 Duplicate (Blue) to Personnel Dept.
 Triplicate (Pink) to Department Head
 Quadruplicate (Yellow) to Union

 Signature of Employee

FIGURE 7.3 Reporting minor worker misconduct. This form presents a simple way of indicating specific misbehaviors on the part of a worker. It is part of a "paper trail" employers retain to evaluate substandard workplace performances. Source: Guy, E.T., Merrigan Jr., J.J., Wanat, J.A., 1981. *Forms for Safety and Security Management*. Butterworth-Heinemann, Boston, MA.

7. *The worker is discharged.* With an additional offense, the next step in the disciplinary process is to dismiss the employee.

Preemptory discharge for cause. Stepwise disciplinary procedures are appropriate for unacceptable but correctable behavior. In the event the employee committed a more serious offense, such as theft or violating serious work rules, the supervisor may consider preemptory discharge. Not to discharge a worker who has committed a crime or a serious breach of regulations can place the workplace in a defensive position from later civil or regulatory action. This is discussed further in the pages ahead.

Why Employees Are Disciplined

Infractions at work and poor performance represent the two leading causes for discipline that can lead to discharge. These two categories include many specific types of offenses. No published data are available on how security programs discipline and discharge workers. However, the US Postal Service has identified unacceptable behavior into 26 categories of infractions, as shown in [Table 7.1](#).

Formal disciplinary actions include letters of warning, suspensions for varying lengths, and removals. Of 69,000 disciplinary actions (representing about 9% of all employees), close to 60% of the disciplinary actions resulted in letters of warning, 30% were suspensions, and 10% resulted in discharge.

It is impossible to say whether the disciplinary pattern of the US Postal Service parallels other programs. However, such infractions as absenteeism, absence from the post without leave, failure to follow instructions, the use of unsafe acts or work habits, and poor work performance are the five main reasons for disciplinary procedures in security programs. Many new supervisors and managers assume that dire actions such as theft and violence in the workplace are the top or near the top reasons for discipline or discharge. Not so. Simply the inability to show up on time and do the work one is trained and expected to do represents the main reason for discipline and discharge.

Legal Issues for Wrongful Discharge

The vast majority of employees who are discharged leave the workplace without taking further action against their employers. They understand at some level that they have not met their part of the worker/workplace understanding, accept that fact, and move on with their lives. A few, however, will not leave quietly. They will make vigorous attempts to retain their jobs despite extensively documented records that led to their discharge. It is important for the supervisor to understand what the rights and obligations are of the employer at such a time.

Table 7.1 US Postal Service Disciplinary Infractions

Infractions	Number of Infractions	Percent of Total
Absenteeism	22,829	33.01
AWOL	10,488	15.17
Failure to follow instructions	8,601	12.44
Unsafe act or work habits	6,217	8.99
Poor work performance	5,010	7.25
Unauthorized absence from assignment	2,443	3.53
Tardiness	1,765	2.55
Delay or failure to deliver mail	1,510	2.18
Failure to protect funds/mail/property	1,170	1.69
Other	1,086	1.57
Disrespect to supervisor/customer	1,073	1.55
Scheme failure*	973	1.41
Insubordinate	919	1.33
Altercation/assault threats	857	1.24
Expansion of office time or street time	791	1.14
Failure to account for funds or accountables	757	1.09
Use/possession of intoxicants/drugs	566	0.82
Machine qualification/proficiency failure	516	0.75
Falsification of record	363	0.52
Deviation from route	339	0.49
Pilfering/theft of mail or funds/property	294	0.43
Destruction/damage of mail or property	234	0.34
Crime (non-job-related off duty)	168	0.24
Crime (non-job-related on duty)	94	0.14
Falsification of application	56	0.08
Work slowdown/stoppage/strike	29	0.04
Total	69,148	100.00

This massive and interesting study shows that most workers, at least in the US Postal Service, were disciplined not for dramatic issues involving drugs or crime, but simply for not showing up on time or following directions. Likely as not, other employers see the same types of subperformance behaviors. AWOL, absent without leave.

*Failure of the employee to demonstrate knowledge expected of the position.

Source: U.S. Postal Service Discipline Tracking System, 1987. Summary Report.

At-Will Employment

In the United States, employees who do not have an employment contract cannot assume that their positions are secure. In 1877, Horace G. Wood wrote *A Treatise on the Legal Remedies of Mandamus and Prohibition, Habeas Corpus, Certiorari, and Quo Warranto: With Forms*. This publication observed that an employee could be discharged at any time for good cause, bad cause, or no cause at all. This viewpoint influenced decisions in American courts and the “at-will” concept of employment was broadly adopted. Less than 20% of the US workforce is covered by collective bargaining agreements. Under these conditions, an employer is often permitted to discharge a worker only for “good cause.” By contrast, under the at-will doctrine, employees may be discharged for whatever reason. (This policy

can be superceded by state or federal statutory restrictions requiring due process before termination of employment.)

Collective bargaining agreements began with the recognition of unions in the National Labor Relations Act of 1935 (USC Title 29, Chapter 7, subchapter II, §167). This law signaled that employees could bargain collectively with employers over a variety of issues, including discharge from work. The terms of such agreements were also binding for disciplinary procedures if specifically included in the agreement. Similarly, within government employment, Civil Service procedures came to govern how such workers could be subjected to disciplinary measures by supervisors.

Most private sector and institutional employers have few, if any, written employment contracts. Exceptions tend to be senior managers, research and development engineers, and technicians with the care and custody of important proprietary information. Executives, managers, and “the talent” in creative and entertainment fields ordinarily receive contracts for their scope of work. Additionally, organizations employing someone for a specific time-limited task are likely to provide contracts covering the work engagement. The presence of such contracts may or may not specify the basis for dismissal by the employer. Written contracts without a minimum employment term specified are regarded as terminable at will by either party.⁴

In the security industry, contracts for personnel are uncommon, but do exist. One national security services firm requires all new security officers to sign an employment agreement.⁵ Others have followed suit, usually for security workers who have had specialized recruiting and training at the contractor’s expense. The agreements protect the relationship between the contractors and their assigned employees. Nonetheless, they recognize the duration of employment is a variant of an at-will relationship subject to termination by the employer for defined reasons.

Currently, three major other “exceptions” to the at-will doctrine exist: (1) breach of an express or implied promise, including representations made orally and in employee handbooks; (2) breach of the implied covenant of good faith and fair dealing; and (3) wrongful discharge in violation of public policy.⁶ Supervisors concerned with possible legal problems related to discharge may wish to consider each of these issues in light of possible challenge to discharge. An in-depth explanation of each of these three exceptions is as follows:

1. *Breach of an express or implied promise, including representations made orally and in employee handbooks.* Express or implied oral representations made during prehire interviews and at the time job offers are being made and accepted can be considered oral contracts. Such contracts may be recognized by the court. Particular protection of the employment status occurs during times when the employer is contemplating furloughing or dismissing workers. However, discharges for violating the rules and regulations of the employer are not likely to be protected by such an agreement. The courts tend to recognize the language in employees’ manuals to reflect a unilateral offer that is accepted by the employee. Once the employment has begun, “the policies embodied in those pronouncements become legally binding.”⁷ The basis on which

employees may be subject to disciplinary actions, including dismissal, may be contained in a Personal Conduct Policy, as shown in [Box 7.2](#). Such a policy is likely to change with the times, as employers do not wish to be burdened with a fixed policy that cannot be flexible to unforeseen circumstances. Therefore, when new measures are added to the policy, they should be communicated to all employees and added to the handbook.

2. *Breach of the implied covenant of good faith and fair dealing.* Under certain circumstances, dismissal of an employee is rendered more difficult. As noted earlier,

BOX 7.2 SAMPLE PERSONAL CONDUCT POLICY

The employee's manual acts like a unilateral contract with the worker. Conditions for personal conduct can change over time and these may be reflected in a new edition of the manual. The following are the rules and regulations for employees, including protective staff, issued by a security-conscious hotel chain:

1. *Violations involving any of the following provide grounds for discipline up to and including termination:*
 - a. Supplying false or misleading information when applying for employment, or any time during employment.
 - b. Altering or falsifying hotel records, swiping the time clock for another employee, or having another employee swipe your time card, or other manipulation of attendance records.
 - c. Possessing, using, or being under the influence of illegal drugs or alcoholic beverages while on duty or in uniform.
 - d. Possessing weapons on hotel premises or while off hotel premises in the performance of hotel duties.
 - e. Abusing, defacing, or destroying hotel property or the property of guests or other employees.
 - f. Engaging in any act of violence or disorderly conduct, threatening or using abusive language or rudeness to a guest, supervisor, or coworker.
 - g. Failure or refusal to follow safety or health rules and regulations or failure to report an accident that results in injury to any person.
 - h. Gross negligence, carelessness, or misconduct.
 - i. The conducting of non-company business, such as canvassing, collection of funds, pledges, circulation of petitions, solicitation of memberships, or any other similar type of activity, during the working time of the employee doing the soliciting or being solicited.
 - j. Theft or unlawful possession of hotel property or the property of a guest, supervisor, or another employee, including lost and found items.
 - k. Immoral or indecent conduct or soliciting persons for immoral reasons.
 - l. Refusal or failure to perform assigned work, substandard guest relations, refusal or failure to follow a supervisor's instructions, or any act of insubordination.
 - m. Excessive absenteeism and/or tardiness. Failure to report to work on 3 consecutive workdays without proper notification will be interpreted as voluntary resignation and will result in immediate termination.
 - n. Unsatisfactory work performance.

- o. Gambling on hotel premises.
 - p. Sleeping while on duty.
 - q. Working overtime without prior approval from a supervisor.
 - r. Unauthorized use of hotel facilities, including telephones and computers.
2. *In addition, violations involving any of the following acts will be considered just cause for remedial action, which may involve oral or written reprimand, suspension from work without pay, or dismissal (especially in the event of repeated violations):*
- a. Failure to punch or sign in and out as instructed by your supervisor.
 - b. Consuming food or beverages in areas other than those designated for use during breaks. Gum chewing while on duty. Smoking by employees is prohibited in all areas of the hotel.
 - c. Failure to maintain a high degree of personal cleanliness at all times. Failure to wear prescribed clothing in good repair as well as appropriate company identification.
 - d. Failure to perform work assignments satisfactorily.
 - e. Failure to notify a supervisor prior to the start of the shift of tardiness or absence.
 - f. Being present on hotel property more than 15 min prior to the start of a shift or remaining more than 15 min after the end of the shift without express permission from a department head.

Employers with progressive disciplinary programs may wish to retain the right to terminate employees for particular conduct without the need for prior discipline. This policy should be stated expressly in the handbook. Due to concerns for workplace security, an increasing number of employers state that workers who act violently, threaten others, or without permission carry a firearm onto the employer's property are subject to immediate termination.

violation of terms in the employee's manual can result in termination for just cause.⁸ This is a circumstance in which the employer states that the employee will not be dismissed except on defined grounds. Just cause can be incorporated into the language of a written contract, oral agreement, and employee handbook or manual. In such a context, termination of employment for misconduct is possible only for substantial breaches.⁹ A minor neglect of duty, an excusable absence, and a minor misrepresentation or rudeness have been ruled by the courts as not meeting the standard for just cause.

3. *Wrongful discharge in violation of public policy.* A violation of public policy exists when the employee is threatened with dismissal while legally protected for such behavior. A dismissal at such a time could be construed by the courts to be a "mixed-motive termination" if the termination of the employee was motivated by lawful reasons (just causes) and also by unlawful reasons (violations of public policy). In such cases, the termination often is considered a violation of employee rights depending on the seriousness of these just causes. Regardless of such concerns, "an employer may discharge an employee if he has a separate, plausible, and legitimate reason for doing so."¹⁰ At such times, the employer may have to demonstrate that it was not acting discriminatorily in derogation of a statute. This is discussed in greater detail later in this chapter.

Special Defenses Against Discharge

This chapter has focused thus far on just causes for which employment may be terminated. Apart from these reasons, it is important to identify areas in which federal statutes protect workers' rights in the event of discharge. These issues often are significant in security programs, which investigate such charges and may be involved at the moment of separation from employment.

Generally, employees who are being dismissed from their jobs for refusing to perform unlawful acts, exercising their rights under state law (e.g., pursuing workers' compensation benefits), and performing a civic duty (e.g., jury duty) are protected.¹¹ Another public policy exception to separation is when an employee is terminated for reporting illegal activity on the part of the employer. So-called whistle-blower laws exist in about 40 states, but are not uniform. For example, in about half the states, only public employees are protected by these wrongful discharge acts. In some states employees working for contractors or subcontractors serving government are protected by whistle-blower protection. Public and private employees are protected in most of the remaining states. These acts protect employees from retaliation by the employer in cases of violations of laws or regulations, neglect of duty, and endangerment of public health and safety. Generally, such acts do not protect from discharge an employee who reports alleged violations of company policy, waste, or mismanagement.¹²

At the time of learning of an employee's allegedly justified complaint against the employer, security practitioners and human resources managers generally must respond to such assertions sympathetically and nonjudgmentally. Employees are less likely to call authorities to complain of suspected violations of public policy at their workplaces if they feel that management has the internal means for hearing their complaints and achieving positive change, assuming the complaint is valid.¹³ Employees who believe that the workplace is violating public policy not only may have the moral argument but could also pursue significant financial incentives if the organization subsequently were fined or paid damages for breaking the law (Box 7.3). At such times, representatives of management should express their organization's commitment to uphold existing

BOX 7.3 WHISTLE-BLOWER SUITS CAN COST AND PAY OFF

Numerous incentives exist for employees to expose dishonest practices committed by businesses against the US government. In some cases, the alleged offender can be a business that derives revenues from activities reimbursed by government. Security practitioners are concerned with whistle-blower cases from different aspects. First, they seek to maintain an ethical and legal order within the organization in which violations do not occur. Next, they investigate cases brought to their attention after the fact. And finally, they assist in investigations and trial preparation defense in circumstances where the organization is being sued in a whistle-blower action.

These cases are becoming more frequent. The whistle-blower provision of the Dodd–Frank Wall Street Reform and Consumer Protection Act offer workers bounties for reporting securities violations. The Securities and Exchange Commission’s Office of the Whistleblower lists dozens of cases where sanctions exceed \$1 million. The SEC estimates that it receives about 30,000 whistle-blower complaints each year.¹ The Attorney General in 2014 told a law school audience that he wanted to boost the potential payouts to whistle-blowers by changing the law that caps such rewards in cases that involve banks. The 1989 Financial Institution Reform, Recovery, and Enforcement Act (FIRREA) caps whistle-blower payment at \$1.6 million.²

GlaxoSmithKline, a pharmaceutical giant, agreed to \$750 million to settle claims that it made and sold certain adulterated drugs. The whistle-blower, the company’s global quality assurance manager, received the largest single settlement ever for a single whistle-blower: \$96 million.³ The whistle-blower found quality problems at a now-shut plant in Puerto Rico with at least four drugs made there from 2001 to 2005. She urged managers to correct the quality problems, even to close the plant. Instead, she was fired for raising the complaints. Later the company in a statement said that it regrets running the plant in a way that violated good manufacturing practices.

A small law firm, Quinn Emanuel Urquhart and Sullivan, organized a plaintiff suit against 16 of the best-known banks in the world. The firm proposed to a client, the Federal Housing Finance Agency (FHFA), that it should sue the banks for underwriting bad mortgage-backed securities that were part of the run-up to the crisis of 2008. After some hesitation FHFA agreed to the suit and one by one almost all of the banks settled before trial.⁴ The lawyers secured recoveries of over \$20 billion for the American taxpayers.

References

1. Greenwald, J., 2011. Whistle-blower risks get louder. *Business Insurance*, October 20, p. 1.
2. Barrett, D., 2014. Holder appeals to whistleblowers. *Wall Street Journal*, September 18, p. C2.
3. http://www.justice.gov/opa/pr/2007/september/07_civ_782.html.
4. Braithwaite, T., Scannell, K., 2014. The man who took Wall Street. *Financial Times*, August 30-31, p. 15.

laws and then investigate the complaint. Whistle-blowing actions are generally sustainable by employees and others who can demonstrate all the following elements in their action¹⁴:

- The employee has particular expertise regarding the alleged violation of the law.
- The employee’s charges relate to federal or state or regulations clearly applicable to the employer, or to the code of professional ethics that is recognized as equivalent to state law and clearly is applicable to the complainant.
- A nexus exists between the complainant and the violation.
- The employee is not a high-ranking executive or manager who otherwise owes a special degree of loyalty to the company.
- The employee has a valid complaint.

Legal Cases of Proper and Improper Discharges

Litigation helps mold the ways in which employers evaluate circumstances before discharging employees. Appellate level cases are instructive because they emerge from lower court issues and have been heard by the court of appeals or the Supreme Court within a state. They represent carefully considered arguments, though often on narrowly selected issues. Any decision by an appeals court becomes the law for similar situations within that state only. However, appellate decisions in one state often are broadly cited and affect policies in others. The following are a number of significant appellate decisions relating to the discharge process:

- *Discharge upheld after drug test dismissal was challenged.* A national hotel chain instituted a drug and alcohol testing program. All employees signed a consent and release form regarding their participation. Sometime later, an at-will employee was randomly selected to be tested. According to the analysis, she was positive for an illegal substance. The employee denied drug use and asked to be retested at a different laboratory of her choosing. The employer refused, but offered the employee an opportunity to be retested at the original laboratory used by the chain. The employee refused this offer and was discharged. She subsequently sued the hotel and her supervisor for wrongful discharge in violation of public policy and other charges. The state Supreme Court rejected the appeal, stating that the plaintiff could not show that her employer violated a clear mandate of public policy in the discharge by insisting on its own drug testing laboratory (*Stein v. Davidson Hotel Co.*, 945 S.W.2d714 [Tenn. 1997]¹⁵).
- *Employee mistakenly fired over theft can sue employer.* A housekeeper in a hotel was arrested for allegedly stealing items from a guest room. He spent 6 weeks in jail until his employer notified police that the missing items had been found. A Louisiana appellate court ruled that the exclusive remedy provisions of the state's workers compensation law did not prevent the house-keeper's suit for damages against his former employer (*McGowan v. Warwick Corp.*, 691 So.2nd 265 [LA. Ct. App. 1997]¹⁶).
- *Employee may be fired for violating the employee handbook.* A manager of May Department Stores Company, who had been employed there for 13 years, coordinated jewelry promotions. While visiting a store, she removed a large box of gold merchandise and took it across the store to lock it in a secured location. In the process, she left two other boxes unguarded. The store's jewelry manager was nearby at the time, but the promotion coordinator did not ask him to keep an eye on the exposed jewelry. When she returned after a delay, the two remaining boxes were missing. The next day she was called to the personnel office and was fired. Later, she sued for breach of an implied promise of "good faith and fair dealing." At trial, May provided a section from their employee handbook that stated:

Merchandise valued at \$60.00 or more must be housed in showcases with locked doors. All other merchandise, including all 14K jewelry, must be kept in locked

showcases or locked drawers. All jewelry showcases must remain locked at all times, unless a sales associate is attending a customer.

The employee handbook also stated that failure to follow operating procedures can result in “corrective action and possible termination depending on the seriousness of the violation.” The theft in this instance resulted in a loss of over \$50,000. At trial, the plaintiff provided no evidence to suggest that she was being fired for “capricious,” “unrelated to business needs or goals,” or “pre-textual” reasons. The court sided with May (*Moore v. May Department Stores Company*, No. B045481, Ct of Appeals of CA, end dist., Div. 2, decided July 31, 1990, 271 Cal. Rptr. 841¹⁷).

- *Fired guard has no claim when employee handbook gives employer discharge power.* At Peninsula Regional Medical Center, Maryland, three employees were attempting to secure a patient with leather straps. In the process, the patient bit a security guard on the wrist. The guard then struck the patient on top of his head. He was asked to leave the room and another security officer took over. In an investigation conducted by the security director and personnel director, written statements from eyewitnesses stated that the guard had struck the patient 15–30 s after he was bitten. The guard responded that his blow had been reflexive, in an attempt to prevent the patient from biting him again.

The guard was discharged for “committing an unnecessary act of putative retaliation.” The guard sued for breach of contract, wrongful discharge, intentional interference with prospective relations, and other claims. The trial court granted summary judgment to the defendant. The plaintiff appealed, and the Maryland Court of Special Appeals sustained the discharge stating that the termination did not violate public policy. The special appeals court said that the plaintiff also failed to show that he acted in self-defense.

The plaintiff also charged that two different police departments declined to employ him after learning why he had been fired from the medical center. The court of special appeals rejected this claim noting that the plaintiff had signed a consent form provided by those departments that also released from liability those employers, such as the hospital, that provided information to them (*Bagwell v. Peninsula Regional Medical*, 655 A.2d 297 [Md. Ct. Spec. App. 1995]¹⁸).

- *Supervisor's comments about fired employee not considered defamatory.* An employee was dismissed from a convenience store and gas station after her supervisor was not satisfied with the employee's explanation why scratch lottery tickets repeatedly were missing during her work shift. The employee denied any wrongdoing and sued her ex-employer for defamation when other employees, including her husband, who was a part-time worker there, learned of the reason for her dismissal. The state Department of Labor Unemployment Division later concluded that she did not steal the tickets. The issue about whether she may have mismanaged ticket security remained open.

The South Dakota Supreme Court found no evidence of malice on the supervisor's part in revealing to other employees that she thought that the former employee had

stolen the tickets. In a split decision, the court's majority held that the employer, through the supervisor, did not make defamatory comments about the worker in responding to other employees' queries about the departure of their former coworker (*Petersen v. Dacy*, 550 N.W. 2d 91 ([S.D. 1996]¹⁹).

- *Termination against striking health aides confirmed.* A homecare services business subcontracted with nursing and healthcare facilities to provide home care for homebound patients who are unable to perform daily living activities. They are required to call an automated attendance system at the start of their shifts. The union representing the aides notified the company that it intended to strike. About 75 aides anticipated being absent during the time of the strike, either to support it or for other reasons.

However, 48 aides who had not previously notified the company that they would be absent failed to report to work the day the strike began. Except for five positions, the absentees were covered by replacements. After the 4-day strike was over, the 75 aides who had advised the company of their planned absence were reinstated. However, the 48 employees who failed to report to work without notifying the company were not reinstated immediately. Though ultimately reinstated, they were not always given their prior patients or work schedules.

The union filed against the company with the National Labor Relations Board (NLRB). The NLRB found in favor of the union, since the company had general notice of the strike and the failure of the 48 workers to appear at work was protected by federal law. The US Court of Appeals for the Second Circuit ruled that home health aides who deceived their employer about their intention to strike are not entitled to reinstatement to their original shifts and patients. The court ruled that the aides' actions put their patients in imminent danger (*National Labor Relations Board v. Special Touch Home Care Services, Inc.*, US Court of Appeals for the Second Circuit, No. 11-3147-ag, 2013).

Insurance Against Wrongful Termination

In the event an employee institutes an action against his or her former employer for wrongful termination, the employer may expect its general liability insurance policy to help fund the defense. Such broadly written insurance coverage is likely to cover legal defense costs, related pretrial expenses, and judgment against the defendant, if any. However, insurers may seek to deny coverage of wrongful termination claims in a standard form by claiming that the event was a nonoccurrence.²⁰

Standard form general liability policies usually pay for occurrence-type losses. In commercial general liability coverage, an occurrence is called an "accident," and includes continuous or repeated exposure to the same general harmful conditions. For the wrongful termination claim to be denied because it was not such an accident, the insurer must prove that the policyholder had a subjective intent to harm or injure the fired employee.

Another related basis of noncoverage is that the policyholder “willfully” terminated the employee with a preconceived design to inflict injury. If the standard policy plainly and clearly excludes wrongful termination from coverage, the insured would have to look elsewhere for expenses related to the litigation. In conclusion, commercial general liability coverage is likely to support the insured’s defense in wrongful termination claims. This assumes the insurer does not have a basis for proving nonoccurrence.

Procedures at the Time of Dismissal

Organizations differ widely on how discharges should occur. The methods of terminating unsatisfactory employees also vary widely among nations and cultures (Box 7.4). Even in North American workplaces, strategies for dealing with employees who are being dismissed from their positions are diverse. The conditions can change according to the cause and seriousness of the dismissal, the rank of the employees involved, and the particular industry.

BOX 7.4 INVESTIGATING AN EMPLOYEE: JAPANESE-STYLE AND AMERICAN

Terminating a worker’s employment differs considerably depending on culture and laws. In Japan, for example, the concept of lifetime employment remains a goal of major employers, yet is presently crumbling as a workplace tradition. Generally, Japanese employers offer a severance package to individuals whom the company does not wish to retain. But what if the employee refuses? That’s what Toshiyuki Sakai decided to do when he rejected a severance package of 2.6 million yen (\$23,900) from his employer, the video-game maker Sega Enterprises Ltd. Sakai was told that his work was under par. He disagreed with that judgment. When he refused to resign and accept the severance package, he was transferred to the “Pasona Room.” This room, named for the English word “personnel,” was empty except for a desk, three chairs, a bare locker, and a telephone that received only incoming calls. Mr. Sakai was given no duties and had no personal possessions in the room. He was instructed in writing to report to the room from precisely 8:30 a.m. to 5:15 p.m. He was allotted 55 min for lunch.

After 2 months, the personnel department formally recommended that he resign, and offered him a severance package 9% lower than the original one. About 3 weeks later, he heard through the union that Sega was firing him and would offer him a severance package that was 28% more than the original package he was offered. However, he continued to report each day to the Pasona Room. A month later, he filed suit against Sega, seeking to have his old job and salary restored. Seven days later, on showing up for work, he was stopped by a security guard, who refused to allow him to enter. Sakai thus pursued his suit against his former employer from home. Meanwhile, Sega announced a plan to trim its workforce by one-fourth. Within a few weeks, most accepted Sega’s severance package. “Everyone’s afraid that they might be the next to be thrown into solitary confinement,” commented Sakai. The worker elected to remain in the Pasona Room to protect his job opportunities at Sega or elsewhere.¹

Most Japanese corporations are headed by Japanese nationals. However, Michael Woodford grew up through the ranks and became its first Westerner who spoke no Japanese to be

president of Olympus Corporation, a manufacturer of optics and reprographic products. Four months after he became president, Woodford received an e-mail from a subordinate. It contained a critical article from a Japanese business magazine charging that the company had spent hundreds of millions of dollars on questionable and money-losing acquisitions. Woodford asked his aides why they didn't tell him about the article sooner. They informed him that Olympus's chairman told them not to. When Woodford couldn't obtain internal details of the acquisitions, he hired a consulting firm to investigate for him. A few days later the board chair called a meeting and fired the CEO. He was escorted from the building. Woodford wrote about his experiences.² The chairman and two other former executives pleaded guilty to charges relating to an accounting cover-up.

In the New York City public school system, a teacher facing a professional, but noncriminal, sanction is removed from the classroom. He or she may be given clerical duties while the investigation occurs. In some cases, such teachers face transfer to what's called "a rubber room" in which teachers have no responsibilities except to report and leave on time. They are paid while the incident under investigation is resolved.

References

1. Landers, P., 1999. Refusing to move on. Wall Street Journal, September 14, p. A1.
2. Woodford, M., 2012. *Exposure – Inside the Olympus Scandal: How I Went from C.E.O. to Whistle-blower*. Portfolio/Penguin, New York, NY.

In most situations, dismissals are defined as permanent separations from the current employer. In many other occurrences, however, workers are placed on furlough – that is, temporary status without duty and pay. Furloughs occur when there is insufficient work or when other nondisciplinary reasons arise. Regardless of the basis for such action, security and human resources managers should anticipate the ways in which redundancy – temporary or permanent – might produce unwanted problems for management. The grounds for dismissal or furlough can be categorized as follows:

- *Economic downturn; retrenchment.* Organizations grow with actual success or the anticipation of it. Also, they can contract due to declining sales, decreased funding or support, recurrent financial losses, mergers that consolidate operations, uninsured or underinsured disasters, and other reasons. At such times, management often elects one of the most expedient means of reducing costs: cutting personnel. When economic factors cause staff reductions, management might respond to the situation in a variety of ways. Some employers allow workers – especially managers – to remain on the premises using their former offices and resources for a reasonable period of time as the basis of obtaining future employment. This lenient policy for the worker provides a humane way of helping the employee segue to his or her next opportunity.

At the time of redundancy, however, most employers would prefer that such workers leave the premises. This could mean after 1 week, 2 weeks, a longer time,

or immediately. In such cases, employees are expected to leave soon after being informed of their termination by human resources or their supervisors. (Workers who resign from significant positions in organizations with high-value intellectual assets may be expected to leave their place of work shortly after giving notice or immediately, according to corporate policy.)

Security-minded employers worry about the potential of sabotage from discharged workers who remain on the premises prior to or after official termination. Common sense dictates that such individuals be treated with respect and dignity as they move their job search activities off-premises. Fearful that such employees may harm company property, remove valuable assets, or create a confrontational situation, some employers expect security personnel to play coordinated and visible roles at the time of such dismissal. The use of security personnel to escort workers from their exit interview to their office to pick up personal effects and then, possibly, to the exit itself needs to be considered carefully before implementation. The practice can affect remaining employees negatively if no basis exists for treating the worker like a suspicious person. At such times, a worker being dismissed is likely to be angry and capable of irrational action. Security should be alert and responsive when dismissed workers are informed of the employer's decision, as attitude on the part of security matters.

For managers and executives it is increasingly common that outplacement services are provided. These services may include office space and secretarial resources, résumé services, and job counseling assistance.

- *Poor work and misconduct.* In cases of just cause for termination, it is normal for a security officer to escort the employee discretely to the exit. The security officer also obtains the employee's keys, identification, and any other materials belonging to the employer if they have not previously been collected. In the event that the materials are not obtained, the employee's final paycheck is usually held until the company's property is returned. The possibility of violent action from a discharged and disgruntled worker has emerged as a concern in recent years and is discussed later in this chapter.

The Exit Interview

The main purpose of an exit interview is to provide terminated employees with information on accrued wages and benefits, such as vacation pay. Related matters such as insurance coverage and pension options also need to be discussed. Terms of the employer's healthcare insurance coverage may be reviewed with options laid out for the employee. Such valuable information and assistance helps mitigate the shock and loss many newly unemployed persons feel.

The exit interviewer also uses this opportunity to obtain opinions of company operations and management. This can be a time to defuse possible hostility and correct employee misconceptions about the termination process.²¹ The possibility of a lawsuit and potential claims may be ascertained and noted by the interviewer. Any angry sentiments

or threats expressed by the employee should be received by the interviewer calmly. The contents of the unhappy worker's remarks should be recorded immediately following the interview. Threats should be discussed with a security manager immediately after the exit interview.

Some issues covered in an exit interview are relevant to security. The employee is asked to return all property of the employer at the time of the interview. Thus, the employer's representative in human relations or security should be aware of the assets the worker possesses or otherwise has available. If some assets cannot be collected by management at the exit meeting, arrangements should be made for their prompt return. Experience shows that if the employer does not obtain all property under the control of the departing worker before the last paycheck is delivered, recovery of such property becomes problematic. This generalization applies to all employees who possess assets of the employer. For example, if a technical developer was permitted to work at home with a computer owned by the organization, a security manager might send a tactful officer – with the employee's knowledge and permission – to pick it up.

Unionized employees may have the right to a union representative at the exit interview. However, if the interview concerns previously discussed disciplinary or discharge matters, union representation is not required.²²

Following the exit interview or while it is taking place, most organizations promptly delete the employee's access code for physical entrance to the workplace. The former worker also is blocked from the local area network (LAN) of the workplace, and telephone privileges cease. Security personnel at entrances and exits are informed promptly of workers who are discharged or have quit. Photographic images of all former employees may be available to security personnel at entrances with instructions on what to do in the event the former worker returns unexpectedly.

Dismissal and the Disgruntled Employee

An employee of Pacific Southwest Airlines, a unit of USAir, was fired for stealing \$69. His resentment mounted. In December 1987, he purchased a one-way ticket on a commuter trip from San Francisco to Los Angeles. He evaded preflight security controls in entering the plane. At 22,000 ft, he entered the cockpit and shot the pilot dead. The 4-engine plane crashed, killing 43 people aboard, including the gunman and his former employer, who was a passenger.²³ Although this type of incident is exceptional, incidents of violence by terminated and disgruntled employees deserve attention in protection management programs.

The issue of workplace violence cannot be ignored by high-performance security practitioners or human resources managers. Incidents involving disgruntled employees who act violently are far less common, but should be considered seriously by security and human resources managers. Data on the frequency of such incidents are unavailable. However, verified cases appear in the media with frequency, keeping the issue alive. [Box 7.5](#) discusses such incidents in greater detail.

BOX 7.5 THE VIOLENT DISGRUNTLED WORKER

About 2 million individuals are victims of violent crime each year in the workplace. About 75% of these incidents are simple assaults, while another 20% are aggravated assaults. Incidents of violence toward supervisors, managers, coworkers, and others from disgruntled employees are few and are therefore not included in some workplace victimization studies.¹ Nevertheless, highly publicized examples of disgruntled and revengeful employees killing or injuring former associates and innocent bystanders at the workplace have received national attention. These incidents remind security practitioners and human resources officials that complacency about the risks can be dangerous. The following are some examples of such violent workplace incidents:

- A 34-year-old warehouse driver for a beer distributor opened fire killing eight and wounding several more at his workplace. The shootings occurred right after a disciplinary hearing in connection with a theft. In the process of the hearing, he had signed a resignation letter. The worker used two handguns in the attack. He killed several company managers and ended the shooting by killing himself.²
- A 44-year-old biology professor at the University of Alabama at Huntsville opened fire during a faculty meeting, killing three faculty members and wounding several more. The shootings occurred just after her tenure application was denied by the department and the university. The chair of her department was among the victims. Later it was determined that she had shot and killed her own brother years earlier. At the time the poorly investigated incident was deemed to be “an accident.”²
- An accountant for the Connecticut lottery at the state headquarters in Newington, Connecticut, failed at his attempts to be promoted and subsequently filed a grievance. Returning 8 days early from a leave of absence for stress-related problems, he walked into the executive offices and stabbed one official, shot dead two others, and then chased the president into the parking lot and fatally injured him. The gunman then killed himself.³
- In Riverside, California, a former parks and recreation department worker was fired after working 5 years as a part-time chess coach. He instituted a wrongful termination suit for age discrimination and other causes. Four years later, before his claim had been heard, the ex-employee, now working for the postal service, invaded city hall and shot two city council members and two police officers there.⁴
- In Tampa, Florida, a worker for Fireman's Fund Insurance Company's local office returned 8 months after being fired. He roamed the office building shouting: “This is what you get for firing me!” He killed three managers with his former firm and injured two more before killing himself later in the day.⁵
- In Walpole, New Hampshire, the former police chief shot to death the selectman who had forced him to resign and then killed himself.⁶
- A kitchen worker in the Denver, Colorado, suburb of Aurora, returned a week after being dismissed from the Chuck E. Cheese® restaurant and killed four workers, including the night manager. A police investigator remarked that it appeared the gunman had “held a grudge over his firing.”⁷
- An ex-postal worker in Goleta, California, fatally shot six postal employees, before taking her own life. The shooter had a long history of bizarre behavior and at the time of the killing was

on medical disability for unspecified mental problems. (California and 41 other states have established commitment laws for people who show signs of being a danger to themselves or to others. This is known as Kendra's law for Kendra Webdale, killed when a schizophrenic, who had been in and out of treatment, pushed her in front of a New York City subway train in 1999.)⁸

References

1. For example: Violent crime strikes 2 million people in the American workplace each year, 1998. Workplace Violence Report, p. 1. Also: Lee, S., McCrie, R., 2014. The violent vortex: appraising risk from workers who kill on-the-job. In: Gill, M. (Ed.), *The Handbook of Security*, second ed. Palgrave Macmillan, New York, NY, p. 182.
2. Lee, S., McCrie, R., 2012. Mass homicides by employees in the American workplace. CRISP Report. ASIS Foundation, Alexandria, VA.
3. Rabinovitz, J., 1998. Connecticut lottery worker kills 4 bosses, then himself. *New York Times*, March 7, p. A1.
4. Terry, D., 1998. 6 at city hall are shot; ex-worker is accused. *New York Times*, October 15, p. A18.
5. Fired worker kills 3, self in Fla. bloodbath, 1993. *New York Post*, January 28.
6. Murder-suicide cited in town hall shooting, 1994. *New York Times*, February 14, p. A13.
7. Gunman kills 4 workers at Colorado restaurant, 1993. *New York Times*, December 16, p. A18.
8. Frosch, D., 2006. Woman in California shootings had history of bizarre behavior. *New York Times*, February 3, p. A19.

Michael D. Kelleher, author of *New Arenas for Violence: Homicide in the American Workplace*, states: "The act of terminating an employee can be a dangerous undertaking, even after the actual termination itself has taken place"²⁴ Predictions of future behavior can never be certain. The employee who seems calm at the time of dismissal may harbor resentments that build to a quiet fury over time and that may eventually trigger violent behavior. The following are guidelines for terminating an employee²⁵:

1. The employee must be treated with respect, sensitivity, and dignity throughout the termination process.
2. If the termination involves a performance issue, the organization must ensure that performance standards are applied to all employees, without exception.
3. The timing of the termination process is critical. Most employers endeavor to avoid terminating the employee when he or she is undergoing stressful life situations, such as a divorce, illness, or the recent death of a close friend or family member.
4. Two members of management should always be present at the termination meeting, one of whom should be a security or human resources professional. This is particularly important if the departing employee is known to have a history of aggressive or violent behavior.
5. Expect the terminated employee to react emotionally. Try to understand the shock and pain of the process from the employee's point of view. Regardless of

the emotional nature of the meeting, remain objective and calm. The employee in charge of the meeting should try to keep the meeting focused on the issue at hand, always using a dignified, sensitive approach.

6. Act professionally in the termination meeting. Confine conversation about the termination to the business reasons motivating the organization's decision. Ensure that the employee understands what is happening and why it is happening. Do not assess blame or react in a judgmental manner.
7. Be honest with the employee. Ensure him or her that the matter will be handled in a confidential manner. Provide straightforward answers to questions important to the employee.
8. If a reason exists to suspect a violent reaction from the employee, be sure to have security personnel present at the termination meeting and in the presence of the employee when he or she leaves the premises. Alternatively, security personnel may not be seen, but be nearby and alert to their possible need to intervene.
9. Be prepared for the meeting. Have all documents ready for presentation to the employee. Have all benefit information ready for review and immediate delivery to the employee. Ensure that arrangements have been made for the employee to gather personal belongings and return company property after the meeting. Prepare and rehearse the meeting in advance so that all points important to the employee are covered.
10. Take any follow-up action necessary to ensure the continued security of the workplace (involving keys, password, and so on) after the departure of the employee.
11. Ensure that an effective outplacement program is available to the employee. A strong outplacement program often makes a significant difference in the transition process.
12. Ensure that the physical departure of the employee from the workplace is handled with dignity and in a confidential manner. No possibility of embarrassment or undue stress should exist in the departure process.

Such situations are difficult for management and employees alike. Preparation prior to the meeting can be the critical factor in short- and long-term success in managing the interaction. Further aspects of the process that may be emphasized include the following:

- *Timing.* According to Sandra L. Heskett, termination should be conducted late in the business day.²⁶ Many employers choose to plan such meetings so that they end after most of the employees have left for the day. Fridays are often, but not invariably, the day of choice to break the bad news, since they give the worker the weekend to recover.
- *Surveillance and investigation.* In the event of threats from an employee, the use of covert and overt surveillance may be desirable. Richard B. Cole writes:

This process requires the striking of a fine balance in recognizing that this individual has previously exhibited irrational and endangering behavior directed against the corporation or its employee(s), the absence of formal authority to remove the

*individual from the opportunity to further endanger, and the obligation to protect the employee and the workplace.*²⁷

Most protective functions do not have the capability of conducting such surveillance; therefore, an outside competent service may be retained. An overt surveillance team approaches the offending individual, advising him or her that they are present, what they intend to do, and how they intend to do it. They make it clear that such surveillance is believed to be allowed within the spirit of the law.

Workplace Bullying and Disruptive Behavior Prevention

An issue in recent years within the workplace is the recognition that bullying and other disruptive behaviors can damage the workplace. Bullying is repeated, unreasonable actions of an individual or a group directed toward an employee or group of employees that are intended to intimidate, degrade, humiliate, or undermine the worker. Such behaviors can also cause risk to the health or safety of the workers. Bullying is not a rare phenomenon.

In a study of US workers, 41.4% of respondents stated they experienced psychological aggression at work in the past year. Extrapolated to the entire workforce, this represented 47 million US workers.²⁸ The research showed that 13% reported experiencing psychological aggression on a weekly basis. Bullying affects people by reducing self-esteem; causing musculoskeletal problems; work withdrawal and sickness absence; sleep and digestive disturbances; increased depression/self-blame, and family tension and stress; high stress, posttraumatic stress disorder (PTSD); and financial problems due to absence from the workplace.

Employers face a number of issues in creating an environment that can correct situations involving discipline and discharge for bullying. Some options are as follows:

- Create a zero-tolerance anti-bullying policy for the workplace.
- Address bullying behavior immediately when it is witnessed or reported.
- Hold awareness campaigns for everyone on what bullying is. Encourage reporting.
- Encourage open door policies.
- Establish an independent contact for employees such as security or human resources.

Disruptive behavior, once started, tends to have a progressive direction.²⁹ First, a single “unprofessional incident” occurs. This is responded to by informal intervention on the part of a supervisor. The next stage is an apparent pattern in which the supervisor meets with the bully or bullies to discuss the pattern. This usually results in amelioration. If the pattern persists, intervention occurs by human resources or security in which services that might be needed are identified and a timeline for change established. If this fails to achieve the desired results, disciplinary intervention, including reassigning the bully, may be considered.

Using Employee Assistance Programs for Aiding Workers

Part of the strategy to decrease violence in the workplace from employees is providing employee assistance programs (EAP). Problems seen by these programs include anxiety, depression, alcohol abuse, and drug abuse. Research shows that EAP are “woefully under-used by employees.”³⁰ A mere 3% of employees used their employer’s EAP services in 2012, according to EAP Technology Systems, Yreka, California, an EAP analytics company. New York-based Towers Watson & Co. found that only 5% of employees use these services while 85% of employers of all sizes offer stress management within the services.

The barrier to using EAP services, particularly among men, is the perception that people going to them have mental health problems of some sort. Employees distrust or are not aware of privacy policies. These are provided under the Health Insurance Portability and Accountability Act (HIPAA). For an EAP vendor to provide the workplace about specific conversations with the employee would violate a federal law.

Most large organizations offer EAP services as part of their corporate benefit programs. Availability depends on the number of employees. According to a survey by Mercer LLC National Survey of Employer-Sponsored Health Plans, over 90% of employers with 1000 or more employees offer an EAP. About the same percentage of employers offer face-to-face counseling within their EAP.³¹ Security programs are likely to turn to EAP immediately after a tragedy involving the workplace in some ways. Security departments are invariably part of EAP services because they are important after work trauma. But at any time security personnel should be informed about the availability of EAP and be willing to pass the information on discreetly to employees who might benefit from the services.

Bank tellers make more errors the day after a robbery than the day before. That’s because victimized tellers usually have trouble sleeping, have diminished appetite, and become hypervigilant to their surrounding than to the work at hand.³² According to the American Psychological Association, only about 8% of victims of workplace violence eventually are diagnosed with pathological PTSD. Employers can minimize incidence of PTSD by providing a supportive environment for workers following an untoward event.

T.I.M.E. is Not on Your Side

Consultant Gavin de Becker has described what he calls the T.I.M.E. syndrome, which occurs when management allows a growing situation to include *threats*, *intimidation*, *manipulations*, and *escalation*. de Becker comments: “When dealing with a difficult and violently inclined employee, T.I.M.E. is on his side, unless management acts quickly.”³³

Earlier in this chapter some facts were provided about a Pacific Southwest Airlines employee who was fired. Specifically, the reason was for taking \$69 of the airline’s bar cash. The employee’s history was more convoluted. The worker had been with the airlines for 12 years. During this time, he was a thief, a drug user, and a drug dealer. He had been warned by his supervisor previously to shape up or face the consequences. Could this person have been “screened out” at the time he was considered for hiring? The question is

impossible to answer for certain. But couldn't an employee of this sort have been disciplined and terminated much earlier?

Dismissing workers early is easier, with less emotional investment on the part of all involved, and with less perceived “unfairness” on the part of a supervisor or a manager. de Becker explains that workers often feel shocked and sense that they have been treated unfairly when facing dismissal. Simply put, managers who are reluctant to discipline or to terminate abusive employees are not astute. Joseph A. Kenney writes: “Employees who get away with rules violations often will push their luck in the future.”³⁴ The courage to fire some employees early may prevent the supervisor and organization from remorse later.

Writing in *Security Management*, Laura Spadanuta observes: “When an employee is terminated, regardless of the cause, the business must have protocols that minimize the potential for the departing employee to harm the company or steal corporate data. That process actually begins when a person is hired, at which time they should have been asked to sign appropriate documents, such as confidentiality, non-disclosure, or non-compete agreements.”³⁵

Summary

Fortunately, not all employees require formal discipline. However, some do, and the supervisor's task is to lead the worker into better behavior. To discipline effectively requires planning and awareness of the facts involved and options available. Logical but inexcusable reasons for unacceptable behavior should not allow an oral admonition to get off track.

Unfortunately, some supervisors do not discipline, or do so ineffectively. They hurt themselves, the worker involved, and the entire organization by such recalcitrance or ineptitude. Supervisors can, however, learn progressive disciplinary measures to increase their effectiveness. Dismissals rarely lead to violence, yet the possibility cannot be ruled out. Certain precautionary measures can decrease the possibility of such violence occurring. Thanks to security measures, the workplace has trended toward greater safety in recent decades. However, high-profile violent incidents in which numerous victims result reflect the importance of dealing with dangerous members of the public as well as disturbed current or past employees.

Discussion and Review

1. In your opinion, why do some workers not achieve the minimally acceptable standards most of the time? What role does management have in dealing with this? What are the limitations?
2. Why should a supervisor collect all available relevant facts before approaching a worker to reprimand him or her?
3. What are the main reasons why supervisors fail to discipline? To what extent is senior management responsible for supervisors' failure to discipline? To what extent are supervisors responsible for their own lack of action in appropriate disciplining?

4. Describe the steps in the progressive discipline procedures.
5. What test must a plaintiff meet in order to have standing in a whistle-blower case?
6. What role does insurance play against potential wrongful termination actions? How might an insurer seek to defend itself against such a suit?
7. When is an exit interview indicated? What are the gains for management? What are the risks?
8. What measures may mitigate the unlikely possibility of violent behavior from a disgruntled terminated employee?
9. Why are EAP services vital in the workplace? What is the role for security practitioners in supporting the work of EAP?

Endnotes

- ¹ Fayol, H., 1987. General and Industrial Management. David S. Lake Publishers, Belmont, CA (revised by I. Gray).
- ² Kaplan, H.I., Saddock, B.J., 1981. Modern Synopsis of Comprehensive Textbook of Psychiatry/III. Williams and Wilkins, Baltimore, MD (Chapter 23).
- ³ U.S. Postal Service, 1989. Discipline Practices Vary. U.S. General Accounting Office, Washington, DC.
- ⁴ Rothstein, M.A., Craver, C.B., Schroeder, E.P., Shoben, E.W., 1994. Human Resources and the Law. Bureau of National Affairs, Washington, DC (Chapter 8).
- ⁵ Guardsmark continues fight to have employees' restrictive work covenant respected, 1995. Security Letter, Part III, January 16, p. 1.
- ⁶ Rothstein, M.A., Craver, C.B., Schroeder, E.P., Shoben, E.W., 1994. Human Resources and the Law. Bureau of National Affairs, Washington, DC, p. 422.
- ⁷ *Ibid.*, p. 425.
- ⁸ *Ibid.*, p. 427.
- ⁹ *Ibid.*, p. 437.
- ¹⁰ Kauff, J.B., Rosenberg, A.P., Weintraub, H.H., 1981. Terminating the employment relationship – under increasing restraints. In: Employment Law: New Problems in the Workplace. Practicing Law Institute, New York, NY, p. 162.
- ¹¹ Rothstein, M.A., Craver, C.B., Schroeder, E.P., Shoben, E.W., 1994. Human Resources and the Law. Bureau of National Affairs, Washington, DC, pp. 438–447.
- ¹² *Ibid.*, p. 450.
- ¹³ Westman, D.P., 1991. Whistleblowing: The Law of Retaliatory Discharge. Bureau of National Affairs, Washington, DC.
- ¹⁴ Barbash, J., Feerick, J.D., 1981. Employment Law: New Problems in the Workplace. Litigation and Administrative Practice Series. Practicing Law Institute, New York, NY, p. 163.
- ¹⁵ Leavitt, P. (Ed.), 1998. Avoiding Liability in Hotel/Motel Security, second ed. Strafford Publications, Atlanta, GA, p. 294.
- ¹⁶ *Ibid.*
- ¹⁷ *Ibid.*, p. 231.
- ¹⁸ Private Security Case Law Reporter, March 1996, p. 8.
- ¹⁹ Leavitt, P. (Ed.), 1998. Avoiding Liability in Hotel/Motel Security, second ed. Strafford Publications, Atlanta, GA, p. 290.

- ²⁰ Miller, C.E., 1989. Wrongful termination. *Business Insurance*, March 20, p. 27.
- ²¹ Barbash, J., Feerick, J.D., 1981. *Employment Law: New Problems in the Workplace*. Litigation and Administrative Practice Series. Practising Law Institute, New York, NY, pp. 164–165.
- ²² *Ibid.*
- ²³ Security Letter, December 15, 1987, vol. xvii, p. 1.
- ²⁴ Kelleher, M.D., 1996. *New Arenas for Violence: Homicide in the American Workplace*. Praeger, Westport, CT, p. 131.
- ²⁵ Baron, S.A., 1993. *Violence in the Workplace*. Pathfinder, Ventura, CA, pp. 103–104.
- ²⁶ Heskett, S.L., 1996. *Workplace Violence: Before, During, and After*. Butterworth-Heinemann, Boston, MA, p. 85.
- ²⁷ Cole, R.B., 1997. *Corporate Personnel Protection*. Charles C. Thomas, Springfield, IL, p. 343.
- ²⁸ Schat, A.C.H., Frone, M.R., Kelloway, E.K., 2006. Prevalence of workplace aggression in the U.S. workforce: findings from a national study. In: Kelloway, E., Barling, J., Hurrell, J. (Eds.), *Handbook of Workplace Violence*. Sage, Thousand Oaks, CA, p. 47.
- ²⁹ Hickson, G.B., Pichert, J.W., Webb, L.E., Gabbe, S.G., 2007. A complementary approach to promoting professionalism: identifying, measuring, and addressing unprofessional behaviors. *Acad. Med.* 82, 1040.
- ³⁰ Dunning, M., 2014. EAP services woefully underused by employees. *Business Insurance*, January 6, p. 8.
- ³¹ Wojick, J., 2012. Taking good care of workers. *Business Insurance*, May 21, p. 6.
- ³² Wojick, J., 2012. Critical-incident response team helps workers cope. *Business Insurance*, May 21, p. 6.
- ³³ de Becker, G., 1995. The most powerful man in the company. In: Mattman, J.W., Kaufer, S. (Eds.), *The Complete Workplace Violence Protection Manual*, vol. 2. James Publishing, Costa Mesa, CA (Chapter 8), pp. 21–36.
- ³⁴ Kenney, J.A., 1995. *Violence at Work*. Prentice Hall, Englewood Cliffs, NJ, p. 183.
- ³⁵ Spadanuta, L., 2013. Confronting the insider threat. *Security Management*, October, p. 37.

Additional References

- Ahrens, S.A., 2011. The role of standards in workplace violence prevention and response. *Security Magazine*, October, pp. 23–31.
- Boyle, M., 2001. The not-so-fine art of the layoff. *Fortune*, March 19, p. 209.
- Burns, R., 2001. Constructing images of workplace homicide. *West. Criminol. Rev.* 3 (1), 1–25.
- Harell, E., 2011. *Workplace Violence, 1993–2009*. US Department of Justice, Bureau of Justice Statistics, Washington, DC.
- Loomis, D., 2008. Preventing gun violence in the workplace. CRISP Report. ASIS Foundation, Alexandria, VA.
- Nater, F., 2011. A risk mitigation strategy in preventing workplace violence. *Security Magazine*, October, pp. 22–28.
- Nemeth, C.P., 2005. *Private Security and the Law*, third ed Elsevier Butterworth-Heinemann, Burlington, MA.
- Teicher, S.A., 2004. Judged by the content of your credit report. *Christian Science Monitor*, March 1, p. 14.
- Wood, H.G., Bridge, C.F., 1997. *A Treatise on the Legal Remedies of Mandamus and Prohibition, Habeas Corpus, Certiorari, and Quo Warranto: With Forms*, third ed Fred B. Rothman & Company, Littleton, CO, (originally published 1877).

Accounting Controls and Budgeting

*Money for which no receipt has been taken is
not to be included in the accounts.*

—Hammurabi

Managers monitor and regulate their programs in several ways. This chapter is concerned with one of the most important controls: the use of financial policies. Controlling purse strings involves numbers. This discussion is meant for readers who are not particularly numeric and who may never have taken a course in accounting. The principles involved are simple, but also are fundamental to the success of any organization. Managers of security programs need to be comfortable with basic accounting processes in order to speak the language and understand the concepts raised by financial managers. The discussion thus takes into consideration simple but critical notions a manager will need to understand in dealing with financially oriented irregularities. Even more significant are formulas, ratios, and rules of thumb needed to understand and control the budget of a security department. To create a context in which controls needed for security operations can best be understood, some basic principles of corporate finance will be discussed first.

Financial Controls in the Organization

All organizations have financial aspects associated with their activities. Guidance is provided by people who are dedicated to the management of money. The principal senior manager in for-profit and not-for-profit (NFP) organizations is the chief financial officer (CFO) or vice president-finance. This individual may also have the title of controller in smaller organizations. The CFO's responsibilities include budget analysis and forecasting, monitoring of accounts payable and receivable, salary and compensation projections and recommendations, internal auditing, investment of excess funds, and compliance with tax and regulatory issues. The CFO is also in charge of financial management, which includes capital raising, determining the mixture of debt and ordinary capital, helping to decide on investment opportunities, valuing businesses that might be acquired or that might be sold, and recommending dividends or capital payouts to shareholders. The office of the CFO maintains accounting and financial records that are audited by an outside auditing firm of certified public accountants (CPAs). These accounting records, usually maintained electronically, are the basis for financial reports issued to various parties including management, stockholders, and creditors (banks and other lenders).

The finance department is concerned with past, present, and future monetary issues. In public corporations, certain financial reports are widely available documents. For

example, the finance department prepares an annual financial picture of operations of the previous 12 months. Quarterly reports are issued for publicly traded companies. Such reports are available on a more frequent basis as required by operations. These financial documents have similarities regardless of the type of organization involved, be they for-profit corporations, NFP organizations, or government units. Tax filings also are required for all nongovernmental units. Two fundamental documents central to organizational control functions are the consolidated balance sheets and the consolidated operating (income) statements. In addition to the two historical reports, the modern corporation may also produce a consolidated statement of cash flow. Complex organizations that include separate divisions and/or companies will issue these financial statements on a consolidated basis. The word consolidated simply means that a variety of operational entities are being combined into a single report.

The Evolution of Financial Controls

Accounting techniques have been important management tools for centuries, long before the modern corporation appeared. The Code of Hammurabi (about 1780 B.C.) recognizes the significance of accounts. Record keeping and accountability became developed during the wealthy classical Greek and Roman periods. The Parthenon or Elgin Marbles from the fifth century B.C. contain accounting records including the disbursements of the treasures of Athena, the ruling goddess of the city. A financial historian writes: “Accountability and freedom of financial information were considered essential for running the world’s first democracy.”¹

In the thirteenth century Leonardo da Pisa, better known as Fibonacci, grew up on the coast of Barbary (now Algeria) where his father worked at the Pisan customs house. Fibonacci was fascinated how the Arabs in bazaars used numerals to conduct their business, much more efficiently than Roman numerals. Fibonacci brought these Hindu–Arabic numerals to Italy where they over time became part of Western mathematics.²

Organizations grew in complexity during the Renaissance, and with that growth came an increase in the number of persons who managed the money. As a result, financial controls evolved to make sure that mistakes were not made or that assets were not misappropriated. By the fourteenth century, double-entry bookkeeping was used by the merchants of Tuscany in Italy. The first treatise on this topic was written by a friar, Luca Bartolomeo di Pacioli, and published in Venice in 1494.³ Pacioli wrote in the vernacular of the region rather than in the Latin of the church. Consequently, the treatise became broadly useful in local commerce. This “Venetian” or “Italian method” of reporting assets with liabilities soon was translated into English, Dutch, German, Bohemian, and Russian. Today, this method continues to be used throughout the industrialized world as the fundamental procedure for stating the financial position of an organization.

The notion of double-entry bookkeeping is that any resource of a business has two aspects: its monetary value expressed as assets and the corresponding monetary claims on those assets (expressed as liabilities or owner’s equity) according to who has a legal claim

arising from it either as a creditor or as an owner. In bookkeeping, the duality of the accounting method is expressed by recording assets in one page of a journal and liabilities and owners' equity in another. A monetary value is assigned to all assets and liabilities in the organization. The balance sheet may be created at any time and the two columns or sides will be equal. If the liabilities exceed the assets, the owners' equity will be a negative amount. This is generally an indication that the business is insolvent.

The following are formulas that describe the relationship between assets and liabilities in an organization:

$$\text{Assets} = \text{liabilities} + \text{owners' equity}$$

Therefore, we have

$$\text{Liabilities} = \text{assets} - \text{owners' equity}$$

or

$$\text{Owners' equity} = \text{assets} - \text{liabilities}$$

The modern bookkeeping techniques to record business transactions have evolved from the writings of Pacioli in the 1490s. These bookkeeping terms and procedures have evolved from handwritten documents to computer-prepared financial documents. The terminology of the accounting process discussed by Pacioli includes journal (the book of original entry or a diary of business transactions in chronological order), ledger (a book (or computer file) for each item on the financial statements), and debits and credits (technical terms related to the recording of transactions in the journal and ledger).

Consolidated Balance Sheets

All organizations use balance sheets to determine their periodic financial condition. (Table 8.1 is an example of a consolidated balance sheet.)

Assets and liability are constantly in flux; thus, periodic statements allow comparisons to be made with earlier times. The term “consolidated” here and elsewhere implied that financial reports from separate operating units have been merged into it, creating a master financial statement for the whole organization. If the corporation is small and is operating as a single unit, the word consolidated is superfluous. Balance sheets list assets at original historical cost and consequently do not necessarily establish the liquidated (in this sense meaning *settled* or *sold*) value of the organization. Assets held for long periods of time generally have increased in value, though not necessarily so. In any case, the balance will reflect the original cost. For example, land purchased in 1990 for \$10,000 would have a much higher current value, possibly \$100,000 or more. While balance sheets may vary in the items they include, generally the information will include the following components:

- **Current assets.** These assets represent cash or items that can be converted to cash, generally within 1 year. This is the strongest asset category because of its liquidity.

Table 8.1 Example of a Consolidated Balance Sheet

	Current Year	Previous Year
Current assets		
Cash and cash equivalent	_____	_____
Marketable securities	_____	_____
Accounts receivables	_____	_____
Inventories at cost	_____	_____
Other current assets	_____	_____
<i>Total current assets</i>		
Fixed assets		
Property, plant, and equipment	_____	_____
Land and building	_____	_____
Machinery and equipment	_____	_____
Less accumulated depreciation	(_____)	(_____)
<i>Net property, plant, and equipment</i>		
Other assets		
Payment and deferred charges	_____	_____
Intangibles	_____	_____
<i>Total fixed assets</i>	_____	_____
<i>Total assets</i>	_____	_____
<i>Liabilities and shareholders' equity</i>		
Current liabilities		
Accounts payable and accrued expenses	_____	_____
Notes payable	_____	_____
<i>Total current liabilities</i>		
Long-term liabilities		
Long-term debt	_____	_____
Other long-term liabilities	_____	_____
Total liabilities		
Shareholders' equity	_____	_____
Common stock	_____	_____
Nonvoting common stock	_____	_____
Reserves for dividends	_____	_____
Retained earnings	_____	_____
<i>Total shareholders' equity</i>	_____	_____
<i>Total liabilities and shareholders' equity</i>	_____	_____

The consolidated balance sheet is a means of determining whether the organization has a positive or negative net worth, reflected in shareholders' equity or its lack. Comparison with the previous reporting period permits the observer to determine the direction of the net worth. The discipline of creating a balance sheet helps to clarify the principal financial position of the workplace.

Cash is the first current asset listed. Next, marketable securities at cost, if any, are cited. (In most cases, the current market value will be different from the acquisition cost; this may be cited in the balance sheet or through a note.) Accounts receivable, less a deduction (allowance) for the estimated amount of uncollectible accounts are listed next. This category represents invoices owed by customers. Next stated inventories of merchandise available to sell to customers or to be used in the manufacturing process are listed. While the inventories are stated at original cost, the determination of this cost could be based on recent (current) purchases or older purchases, possibly years earlier. The notes to the financial statements will indicate the method of determining the cost employed. There could be a significant difference between current costs or older costs. Finally, prepaid expenses that represent items purchased for use in future periods (other than inventories accounted for separately) that were paid for in the current period are listed. For example, rent of the following year paid in the current year would be considered an asset until the use of the property.

- *Fixed assets.* Most organizations will have invested in capital expenditures to meet their needs. Once acquired, these assets will appear as fixed assets. Capital expenditures are used for the purchase of assets that increase the utility of operations when the benefit is likely to extend more than 1 year and more likely over a number of years. These include buildings, machinery, systems, vehicles, and land. Such expenditures will be subject to depreciation, which is an allocation of the cost of assets over its expected useful life. An estimated expected useful life of an asset is determined and then deductions from the original purchase price are made each year to allocate the original cost.* This allocation, called depreciation, reduces the values of the assets in the accounting records (book value). Both the value of the asset on the balance sheet and the profit recorded on the income statement are reduced by the amount of depreciation. Depreciable assets include buildings, fixtures, machinery, office equipment, furniture, and fixtures. Fixed assets specific to security programs include security systems, guardhouses, automobiles, golf carts, and sometimes security officer uniforms. Land is not subject to depreciation because it is not a “wasting asset.” Fixed assets are reported less accumulated depreciation. The schedule for depreciation relates to presumed lifetime use of the asset. A depreciation schedule usually is not fixed but has a range in years, allowing the accountant to make the decision on years for depreciation most advantageous for tax reporting purposes.
- *Payments and deferred charges, if any.* An example would be advanced payment of taxes and other credits earned. These are incurred charges that had been deferred to the future. Some examples include start-up costs, moving expenses, and certain income tax charges.

*Two types of calculating depreciation may be used: first, the straight-line method, by which the asset value (less estimated scrap value) is written off by equal installments over its estimated life; second, the reducing-balance method, by which depreciation for any year is a certain fixed percentage of the balance at the beginning of that year. Accounting policy maximizes the earning power of assets as much as possible by selecting the most advantageous financial policies for use.

- *Intangibles.* Assets like patents, trademarks, and goodwill are examples of these assets. These assets are listed at original cost. Consequently, if a company has goodwill or a valuable patent that it has developed itself, there may be no cost listed on the balance sheet. Some acquisitions are worth more than their asset value because they are believed to have more than average expected future earnings. Goodwill is the value of a business that has been acquired that is greater than its asset value. The allocation of the cost of intangibles against profit is called amortization, which is a similar concept of depreciation. The rule for determining the amount of intangible asset amortization and related expense (decreases profit) on the income statement each accounting period requires complex computations related to the impairment (reduction) to the value of the asset.
- *Total assets.* This figure represents the summation of current, fixed, and other assets.
- *Liabilities and owners' equity.* The other side of the balance sheet equation contains two parts: liabilities (which are economic claims on the organization) and equity (which reflects ownership interests). The owners' equity of a corporation is called shareholders' or stockholders' equity, while the equity of a firm owned by a group of partners or one individual is called partners' equity or proprietor's equity. The liabilities and equity are composed of several components.
- *Current liabilities.* These are liabilities owed by the organization either immediately or usually within 1 year from the balance sheet date. Most current liabilities are due within 30–60 days. They include accounts payable to trade vendors; notes payable to lenders; accrued expenses payable to employees, vendors, or others; and income taxes payable.
- *Long-term liabilities.* These include long-lived debts such as notes payable and mortgages (debts secured by property such as buildings or equipment) due more than 1 year in the future. All organizations use long-term debt as part of their management strategies.
- *Total liabilities.* This category summarizes current and long-term liabilities.
- *Owners' equity.* This section represents a claim by ownership to the net worth of the organization. This includes the value of claims from the capital contributed by the sole proprietor, partners, or stakeholders. Also in this category are accumulated profits available for payments as dividends to stockholders or withdrawals to partners or sole proprietors (an unincorporated business owned by one person).

The owners' equity of a corporation includes two categories: paid in capital and retained earnings. Paid in capital is the amount paid into the corporation by stockholders, both common and preferred. While there are many variations of preferred stock, these stockholders generally have a "preferred" guarantee on distribution of profits (dividends) and allocation of assets at the termination of the corporation. Common stock, the most "common" type of stock issued, represents the interests of owners of a corporation after the preferred stockholders have been satisfied. If a corporation has only one type of stockholder, the title common or capital stock is generally used. Normally, but not always, preferred stockholders do not have the right to vote on issues related to corporation management and financing. Therefore, common stock stakeholders have theoretically more control

over the future directions of the enterprise by voting on management and critical decisions. The “retained earnings” account is listed next in the owners’ equity section of the corporation balance sheet. This category includes accumulated profits (since inception of the business) less all payments (dividends) to stockholders.

The owners’ equity of a partnership or sole proprietorship includes one owner’s equity account for each owner, called a “capital” account. The capital account contains investments by the owner plus the owner’s share of business profits less withdrawals (usually cash) by the owner.

- *Statement of operations or income statement.* This important accounting report provides a picture of income and expenses over a previous stated period of time. An example of such a report is shown in Table 8.2. The statement of operations identifies the main types of expenses and charges against earnings that the enterprise experiences.
- *Net revenues.* This identifies the sales recorded over the reporting period for all the goods and services provided by the organization, for both cash and accounts receivable (credit sales), minus any discounts taken. A series of deductions from this gross revenue are made, leaving a final profit. The following categories are deducted from the net service and sales revenues:
 - *Cost of sales.* In retail business, it includes the wholesale cost of inventories sold to customers. For a manufacturing firm, the costs include factory operations for the period. This is adjusted for finished goods not sold (included in inventory

Table 8.2 Consolidated Statement of Operations

	Current Year	Previous Year
<i>Net revenues</i>	_____	_____
Costs of products and services	_____	_____
Gross profit	_____	_____
Selling, general, and administrative expenses	_____	_____
Depreciation of intangible assets	_____	_____
Other expenses, net	_____	_____
Interest expense and finance charge	_____	_____
Earnings before income taxes	_____	_____
Provision for income taxes	_____	_____
Earnings from continuing operations	_____	_____
Gain (loss) from discontinued operations	_____	_____
Earnings (loss) from continuing operations	_____	_____
Extraordinary item	_____	_____
<i>Net earnings (loss)</i>	_____	_____
Earnings (loss) per common share	_____	_____
Continuing operations	_____	_____
Discounted operations	_____	_____
Extraordinary item	_____	_____
<i>Net earnings (loss) per share</i>	_____	_____

The statement of operations is part of the financial reporting of all organizations. It allows for a quick comparison on major financial components for a period of time. Earnings or loss can be determined. Publicly traded stocks in the United States will include a minimum of 5 years’ comparative statements, and sometimes more.

on the balance sheet) at the beginning and end of the accounting period.

Manufacturing costs include the cost of raw materials, labor, equipment and systems (including depreciation), and other expenses of operating a factory as well as related expenses such as transportation and storage.

- *Gross profit.* This profit reflects the remainder after deduction of the fundamental costs of inventories or manufacturing (sales less cost of sales). It is called “gross” – or “gross margin” – yet numerous other expenses for operations are not deducted from it, such as finance, administration, possibly sales and marketing, and taxes. The gross profit, however, can be a useful comparative tool for one year’s performance with another’s. The gross margin ratio is the percentage of sales remaining after a firm has deducted the cost of sales. The ways a gross margin ratio can be increased are by increasing selling prices or reducing the cost of sales or both.
- *Selling, general, and administrative expenses.* Costs relating to sales and marketing personnel, advertising, and public relations, plus all the general and administrative expenses of operating the enterprise, are recorded here. They include senior operating staff costs (headquarters allocated expenses, sometimes called the C-suite, including depreciation of selling general and administrative assets), legal and accounting costs, subscriptions, fees, donations, and a host of expenses not previously recorded. Subcategories may also be reported.
- *Other expenses, net.* This category recognizes unconventional costs that the organization experienced for the reporting period. For example, if the organization had a minority ownership of a business that was not consolidated with other expenses, the amount could be indicated here.
- *Interest expense and finance charge.* Since interest expense relates to how a business is financed and not related to the operations of a business, it is generally shown in a separate category near the bottom of the income statement. Organizations normally have a line of credit, that is, funds available on a short-term loan basis from a bank. This category reflects the interest expense to continuing operations. Changes from one year to another could relate to different debt levels and the variable costs of debt. Sometimes, long-term and short-term debt are indicated separately. Short-term debt indicates debt that matures within 1 year of the date of the financial statement.
 - *Earnings before income taxes.* This amount represents the earnings before deductions for federal, state, and local taxes levied against the net earnings of a business. This may be significant if the organization has unusual tax consequences that could change from 1 year to the next.
- *Provision for income taxes.* For-profit corporations pay taxes. However, these can differ from year to year if the tax rate changes.
 - *Earnings from continuing operations.* Large organizations are dynamic, often selling or closing significant business units within a single financial reporting period. To aid comparison with ongoing operations, accountants distinguish

continuing from discontinued operations for which there may be a gain or loss reported.

- *Extraordinary item.* This assumes that an exceptional event that is both unusual and infrequent is being recorded, and presumably not likely to recur. For example, it could be due to the loss or gain from the early redemption of long-term liabilities, or natural disaster such as an earthquake in an area where earthquakes are unusual and infrequent. The extraordinary items, if any, are reflected less any tax benefits or cost related to the item.
- *Net earnings (loss).* This is the iconic “bottom line.” This reflects the income available to all shareholders after all expenses have been taken into account. This figure indicates the posttax earnings of operations for the year. However, the consequences for shareholders of a corporation are not apparent from this amount and must be determined from the earnings (loss) per share (EPS).
- *EPS.* As an example, a company that earned \$100 million after tax and had 100 million shares outstanding would realize earnings of \$1 per share. A note will indicate whether the number of shares has changed from one reporting period to another so that the consequences for the owner of a single share will be apparent. The calculation for computing EPS may be complicated by various issues including the existence of preferred stock or bonds payable that may be converted to common stock.
- *Impairment charges.* In recent years Securities and Exchange Commission (SEC) and general accounting policies have mandated the recording of impairment charges in some circumstances. These reflect the permanent decline in the value of a significant asset previously carried on the books of the enterprise. Therefore, recovery of the asset’s cost or book value is not realistic.

Notes to the Consolidated Balance Sheet and Statement of Operations

All consolidated statements include a number of explanations about the organization that are relevant in the opinion of the independent accountant.

To become aware of fundamental and structural financial changes in the organization, perusal of these notes is vital ([Box 8.1](#)). Such notes include a summary of significant accounting policies. This section also describes important procedures, including any changes made from the previous year. Other notes provide specific information on investment in affiliates, discontinued operations, valuation of types of financing held, leasing commitments, contingent liabilities (e.g., significant possible losses or gains), retirement benefits commitments, and stock options. The notes to the consolidated financial statements also provide business segment information (assuming the corporation has different lines of business), income tax information (both domestic and foreign), a review of quarterly financial information, notes on major acquisitions, and information concerning capital stock and EPS. Revenues also may be reported separately for international and domestic activities.

BOX 8.1 IN FINANCIAL STATEMENTS, NOTES TELL A STORY

The main financial information in a corporation's annual report often seems skewed to emphasize the positive. But in some cases, notes in the report reveal a serious problem that eventually will affect the ability of the organization to operate. Only by reading and understanding the consequences of these notes may an investor or employee be alerted to impending disaster.

An example of a company that was able to “hide” certain accounting practices in its annual report concerns Crime Control, Inc. This former Indianapolis-based business was incorporated in 1977, and was composed of small alarm companies owned by its two founders. In 1978, operating revenues were \$685,000, with a *pro forma* (estimated) profit of 14%. Two years later, operating revenues had grown to \$5,800,000, with a *pro forma* profit of 16%. Business grew steadily as the firm purchased accounts from other alarm businesses for both cash and stock. This growth, up to that point, was made possible mostly by bank financing based on the positive sales and profit trend. In 1982, Crime Control issued an initial public offering, selling about 27% of equity, while the founding shareholders retained the remainder. The public market for Crime Control's common stock grew, enabling the alarm business to continue aggressively on its acquisition path.

Crime Control's alarm monitoring business soared in sales and profits compared with their major competitors who were bewildered by how this newcomer was so much profitable than they were. Why? The answer relates to Crime Control's unorthodox accounting policies. Alarm businesses generate income in two ways: from leases or sales of alarm systems and from ongoing revenues derived from monitoring alarm signals, called monthly recurring revenues. Both forms of income usually are reported in the year in which they occur. However, if security system leases are accounted for as sales-type leases under the provisions of the Statement of Financial Accounting Standards (SFAS) No. 13, a more aggressive accounting method may be elected by the financial managers. This is what Crime Control elected to do. It accounted for future anticipated years of revenues the first year the alarm contract was signed with a customer.

The company offered incentives to renew the rental rate at the expiration of the original lease with a savings of 10%. The company assumed that the bargain lease term would keep the customer for 8 years. These sales-type leases were then accounted under SFAS since the 8-year lease term exceeded 75% of the estimated economic life of the equipment (10 years). Crime Control, with the approval of its accountants, Coopers & Lybrand (currently part of PricewaterhouseCoopers), was able to report exceptional revenues and profits relative to other peer companies that used conservative and conventional reporting methods.

Due to its accounting assumptions and policies and nothing else, the company grew quickly because it appeared to be so much more profitable than its peers. Rapidly increasing “revenues” were booked. But they were not received, since they would not actually be paid by customers for years into the future. To keep the accounting game going as long as possible, Crime Control vigorously sought more and more acquisitions, for which it was willing to pay unconventionally high purchase prices in stock or cash. The explanation how Crime Control was so much more “profitable” was clearly stated in the company's filings. Few people bothered to read them and understand the consequences until it was too late.

Despite strong apparent revenues and profits, the company kept running out of money because actual revenues were weak. When investors finally realized the scheme, it was too late for most. Crime Control was liquidated and the remnants were purchased at a considerably diminished value.

Another more recent and better known example concerns the former energy giant Enron. In 1999, total revenues were \$40 billion, up from \$31 billion the previous year. In 2000, Enron's revenues grew to almost \$101 billion. What's not to like? However, costs of gas, electricity, metals, and other products grew from \$35 billion (during 1999) to \$95 billion (during 2000). The percentage cash margin is defined as cash revenue less cash cost of goods (cost of goods plus increase in inventory) divided by cash revenue. For Enron, the cash margin sank from a positive number in 1999 to -7.8% in 2000. This abrupt change in fortune in what ostensibly looked like a brilliant enterprise was a clue that accounting was a signal that the company was inflating value. Enron's auditor was the venerable Arthur Andersen that was liquidated as was Enron.

Sources: Security Letter, February 1, April 1, August 1, September 4, November 15, 1984; July 1, 1985; July 1, 1986; April 15, 1987. Fischer, D., 2007. F is for fudging. *Forbes*, October 29, p. 72.

Statement from the Independent Auditor

All corporations are audited by independent auditors to assure stakeholders and the public that the financial statements and the process by which they have been created have been fairly stated. Attached to the annual financial statement and some other financial information issued by a firm, the auditors provide a statement that includes the statement: "In our opinion, such consolidated financial statements present fairly, in all material (large) respects, the financial position" of the corporation being audited. Recent changes in auditing techniques and reporting require that the auditor audit not only the numbers on the financial statement but also the systems and accounting controls used to develop the numbers. The independent auditor will insist that any critical issue relative to the corporation's activity be fully disclosed either on the financial statements or in the notes to the financial statements as well as in other publicly available documents. In extreme cases the auditor may include references to unusual accounting issues in their report.

In theory, the US economic system supports competition. That is supposedly a capitalistic principle. But for audit firms it is not that way. For most of the twentieth century, over 90% of the Fortune 500 companies were audited by just eight audit firms. They were called "the Big 8." As commerce became more global, the Big 8 acquired or merged with foreign-based audit firms. In 1989, Ernst & Whinney merged with Arthur Young to form Ernst & Young and the same year Deloitte, Haskins & Sells merged with Touche Ross to form Deloitte & Touche. It was now the Big 6. Then in 1998, Price Waterhouse merged with Coopers & Lybrand to form PricewaterhouseCoopers. Now it was the Big 5. Following the Enron scandal, Arthur Andersen was liquidated in 2002 for a conviction that was later overturned by the US Supreme Court.

This resulted in the Big 4, which continues to dominate – even monopolize – the auditing function of large enterprises based in the United States. The remaining Big 4 in order of revenues are Deloitte, PricewaterhouseCoopers, Ernst & Young, and KPMG.

The Significance of Change in Auditors

In publicly held corporations, auditors theoretically have a fiduciary responsibility, not to the corporate board who recommend them, but to the ownership of the organization, shareholders, and others with a potential legal claim on the company. The term fiduciary implies a trust relationship with legal implications for trust and due diligence in fulfilling duties. Failure of the independent auditors to identify to the shareholders and the public at large any substantial irregularity or fiduciary urgency, in the case of publicly held companies, can lead to civil action against the entire audit firm.[†] It is because of this fiduciary responsibility that the change in auditors for a publicly held corporation is normally a matter of public record. Shareholders vote annually on the appointment or reappointment of independent audit firms included as part of the annual proxy statement. The changing of one audit firm for another may be a normal and healthy development in which the corporation seeks fresh professionals to review their account. Indeed, the Sarbanes–Oxley Act (www.sarbanes-oxley.com) requires periodic changing of external auditors. The change can also be one that reflects unwillingness to pay the fees for the forthcoming year requested by the existing audit firm; such a change thus could represent significant cost savings.

However, the replacement of one audit firm for another, unrelated to periodic change or cost savings, may signal that the outgoing independent audit firm refused to report financial statements the way management wanted. The accountants may have wished to attach qualifications, or potential warnings, to their statements that would reflect unfavorably on the activities or prospects of their client. Or the independent auditors advise that certain impairment charges be taken. Should the audit firm refuse to back down from its proposed position, the client firm may opt to change its audit service in retaliation. However, changes in auditing firms based on disputes related to accounting policies are not usual. The auditor has a confidential relationship with the client and is not ethically permitted to release confidential information to the third parties without the client's permission. Yet, third parties such as creditors may insist on receiving information on disputes with the auditor as a requirement of continuation of granting credit including loans. Also the business will have difficulty appointing a new auditor if the previous auditor is not permitted to discuss accounting issues with the new auditor. Both the SEC (discussed below) and stock exchanges require disclosure of reasons for a change of auditor.

[†] Independent auditors are expected to identify accounting irregularities; most irregularities are discovered accidentally or are reported by whistle-blowers. Still, auditors are always subject to litigation for negligence if they reasonably fail to detect and report abuses that a diligent audit might be expected to uncover.

The Securities and Exchange Commission

In the 1920s and earlier, institutions and individuals who invested in stocks and bonds were frequently victimized by fraudsters who manipulated the market for their own benefit. Unfounded rumors – often fanned by scheming corporation officers themselves – might drive up the market price for stock long enough for insiders to liquidate their holdings before the market price crashed. To protect the public, the Securities Act of 1933 required issuers of securities, and their controlling persons making public offerings of securities in interstate commerce, to file with an agency created to receive such information. SEC was established under authority of the Securities Exchange Act of 1934 (15 USC 78a-78jj). It was created partially to receive registration statements concerning financial and other pertinent data about the issuers and the securities being offered. In the United States, it is unlawful to sell such securities unless a registration statement has been filed with the SEC and is in effect. Registration with the SEC does not suggest approval of the registration disclosure, nor is it taken to be factually accurate. Further, investors are not insured against loss of their investments in common stock by any federal or state agency. However, the securities legislation made it a criminal offense for anyone to cause the financial statements under the jurisdiction of the SEC to be false or misleading or both. Those affected by this legislation include, but are not limited to, management, auditors, and stock brokers. Consequently, anyone involved in the preparation and distribution of false or misleading financial statements could be subject to fines or prison.

Registration serves to provide information on which investors may make informed and realistic evaluations of the worth of such securities. However, about 10,000 public corporations are registered with the SEC, which provides a variety of timely information filed by the registered entities. [Table 8.3](#) presents a guide to the major filings of public corporations. To the general manager or security practitioner, this information represents readily available, substantially accurate, and valuable information about corporations.

Manipulation of Financial Statements

Businesses have some leeway regarding the means by which revenues and expenses may be reported. Corporate treasurers and independent outside auditors are bound by generally accepted accounting principles (GAAP), the industry's body of widely recognized concepts, standards, and rules followed in recording and summarizing transactions and in the preparation of financial statements.

Two separate accounting methodologies are possible. The accrual method of accounting records revenues and expenses when they are recognized, not when cash is actually transferred. Alternatively, cash-based accounting records sales and expenses when cash is actually received or used. Cash-based accounting is better at tracking cash flows. However, accrual-based accounting improves a firm's ability to match expenses with revenues. In most cases GAAP require accrual-based accounting.

Table 8.3 Guide to Financial Performance of Public Corporations

SEC Form No.	Descriptions
8-K	A "current report" that announces major events that shareholders should know about; a report of unscheduled material events
10-K	A detailed annual accounting including comparison with previous years. It may be included optionally in the annual report to shareholders; otherwise, it is available to shareholders on request and from the SEC as mentioned below. Amended filings are designated as 10-K/A
10-Q	A quarterly report that discusses the company's business and financial performance. Amended filings are designated as 10-Q/A. For companies that have a fiscal year end of December 31, 10-Qs must be filed by early May
10-SB12G/A	Amended small business issuer registration statement
6-K	Similar to an 8-K, but filed by foreign companies
20-F	Foreign companies file these annual reports. They discuss the company's business and annual financial performance. Amended filings are designated as 20-F/A
DEF 14A	The definitive proxy statement. This document contains material information about matters subject to a shareholder vote. Information on executive compensation and stock ownership is included
15-12B	Certification of no change in definitive materials
S-1	A general form of registration. This is commonly filed by companies planning to complete an initial public offering (IPO). The form can be amended several times. Those changes are filed under S-1/A
S-3	Prospectus filed for secondary offerings
S-4/A	Amended business combination transaction registration statement
SC-8	Employee benefit plan registration statement
SC 13D	Ownership statement. The amended ownership statement is 13D/A
SC 13G	A notice of change in beneficial ownership, meaning the acquisition of 5% or more of outstanding stock by passive investors and certain institutions. Amended stock ownership uses SC 13G/A
SC 14D1	Tender offer statement. Amended tender offer statement is SC 14D1/A
SC 14D9	Tender offer statement
13 F-HR	A quarterly report filed by institutional money managers that discloses their large holdings

The Securities and Exchange Commission requires issuers of securities and their controlling persons making public offerings of securities in interstate commerce to file registration and issue periodic activity statements. These provide the public with presumably accurate information on operations, including problems and opportunities. Filings may be examined at www.sec.gov/info/edgar/forms/edjform.pdf. Filings for individual companies can be found at www.sec.gov/edgar/searchedgar/webusers.htm.

In the goal of managing earnings or hiding problems, many organizations use methods that may not necessarily violate the GAAP norms but will result in misleading financial statements. Sometimes, these reports go unnoticed. The following are some financial actions corporations may take to manipulate their official financial records^{†4}:

- *Writing off exceptional expenses.* The company decides to write off one or more failed activities, restructuring expenses. Or other unusual costs are written off as worthless. By eliminating excess expenses, future profits look better. Yet some companies have

[†] H. Schilit, in *Financial Shenanigans*, provides another list of top 10 accounting tricks, which includes many of the abuses in Hector's article, but adds some new ones: recording revenues early, capitalizing costs, changing the way inventory is valued, and swapping debt for equity.

frequent restructuring write-off costs, suggesting an inability to produce a reliable stream of quality earnings, and reflecting negatively on management.

- *Smoothing quarterly profits.* Some companies experience a windfall, for example, from the sale of a major asset. But instead of reporting it in the quarter when the sale was achieved, the money is stored, typically in special reserves. Then when some bad news comes along, the company reports the special reserves as income to offset the loss. This is also referred to as managed earnings.
- *Deferring costs.* Consider a company investing in a major new product. The expenses may last for several years before income is generated. Should management recognize the development expenses as they are incurred, or defer some of them until revenues start rolling in? The difference can have a substantial effect on profits.
- *Reporting revenues variably.* The most common way of accounting for long-term contracts is a method called *percentage of completion*. Management determines how much of the contract work has been completed, and recognizes the income and expenses related to that portion, even though a major part of the payment might not be received until the contract is completed.
- *Hiding inventory.* Businesses can make a quarter look good by shipping inventory to some customers even if they do not order it. (On a smaller scale, this same irregularity is committed by sales persons seeking to obtain a higher bonus during a particular time period.) True, they may have to take some merchandise back later and issue credits for it, but in the meantime, the report for the quarter will be better than it otherwise would have been. Such a manipulation of reality is most common in the month prior to the end of the financial year.
- *Dabbling with depreciation.* The useful life of assets can be depreciated over a different time period. For example, capital costs entailed for a new alarm monitoring account customer are expensed by some companies the year they occur. Other alarm companies, however, assume that the account has a lifetime of 2–13 years. The longer the write-off, the higher the reported profits may be in a given year. Corporations may correctly use one type of depreciation for their tax filings and another for the firm's income statement.
- *Combining one-time gains.* A company that buys and sells assets, separate from its major business, normally reports one-time gains or losses carefully segregated from normal operating income. But some companies argue that such regular gains should be included with normal income. This can distort the perception of whether the corporation is actually prospering.

Not-for-Profit Organizations

The preceding discussion concerned private sector corporations that are established with the intention of making a profit. However, an important portion of the economy is composed of NFP organizations. These include charities, educational institutions, many healthcare and medical research facilities, religious organizations, and trade and

research groups. Over 1 million such organizations are incorporated in the United States alone. These organizations have enjoyed federal tax exemptions since the passage of the first income tax law in 1894. Prior to that, such organizations were exempted from state property tax laws.

Despite such NFP status, most of the accounting and audit concerns of such organizations are identical to those of for-profit corporations. Similarly, the security risks to such organizations are largely equivalent.

Budgeting for a Security Department

Up to this point in this chapter, a macroview of financial activities in an organization has been presented. The next part of this discussion concerns programmatic details incorporated in the cost of doing business. The total cost of operations includes numerous departmental and programmatic activities that are intended to achieve the overall goals of the organization. One of these is security. Therefore, security activities require budgets in order to operate. Indeed, the importance of this topic is reflected in the fact that many chief security officers find that they spend about one-fourth to one-half of their time on budget-related activities.

A budget is a statement of estimated revenues and expenses for a specified period of time. It is usually an annual plan of action, but it can also be set at monthly, quarterly, or semiannual periods. Budgets also can extend for several years in the case of multiyear projects. A budget may refer to a sum of money allocated to a particular purpose or project for a specific period of time. Budgeting is inextricably involved with good planning and operations, as it seeks to coordinate resources and expenditures.

The purposes of budgets are to:

1. Support planned operational activities with necessary financial resources
2. Commit money to complete planned programs and projects
3. Control allocated money
4. Evaluate management effectiveness by noting how well resources are managed within previously set guidelines

Annual budgeting is a process that extends over many months in large organizations. Throughout the process, planning and collaboration are vital between the chief of security (who is preparing the budget) and subordinates (who manage budget subsets). A security director with budget responsibility also will interact with senior managers, who will provide guidelines, raise questions about plans and proposals, and perhaps present obstacles in the annual budget approval process that must be resolved. A budget manual prepared by the CFO's office includes the budget planning calendar and distribution instructions for all schedules. For organizations operating on a calendar-year basis, the following is an example of the budget approval process:

Spring or summer: The finance department issues budget request guidelines to various operating units within the organization.

Two weeks later: Chief or director consults with subordinates on next year's plans.

Two months later: Security chief of director submits budget to finance department.

One month later: Budget is reviewed. Changes or explanations are requested.

One month later: Revised budget is approved. Consolidated budgets of all departments are presented to the board of directors for approval, or may be vetted by a board committee.

One month later: Budget is approved, subject to minor revisions.

One month later: Final revised budget is approved.

The budget process requires looking into the future to identify a variety of financial needs that conceivably could be growing while others are contracting and still others are being reorganized. Budgets must have details to show how money is to be allocated and spent. They also must be flexible enough to adapt to the dynamic contingencies that could arise in security programs. Some common types of budgets include the following:

1. *Revenue budgets.* These indicate the revenues that a department might generate, if any. Security departments generally do not bring in revenues, but some do become profit centers. If security operations generate income (see discussion later in this chapter), the estimate for such income appears.
2. *Expense budget.* These are the projected operating expenses for the budget period. Each item on the expense portion of the budget reflects a particular monetary outlay calculated in advance. This type of budgeting, commonly called incremental budgeting, takes the expenses of the previous year as a baseline and uses them as the basis of proposed increments to represent programmatic changes, inflation, and merit pay increases.
3. *Capital expenditure budgets.* In this category, the department identifies capital costs for systems, equipment, vehicles, furniture, and fixtures. These capital costs are amortized (depreciated) over time. In contrast, supplies – and often security guard uniforms – are “expensed,” that is, written off the year they are purchased as expense items.
4. *Variable budgets.* Expenses of an organization may be classified as either “fixed” or “variable.” A fixed expense is one that is fixed or remains the same at different levels of production or sales. For example, depreciation of equipment and rent are generally fixed expenses. They will be the same during the current period no matter what the level of output or sales. A variable expense varies or changes with sales or production. Inventory costs and sales salaries are variable since they change as sales change. Variable budgets include formulas that change certain expenses with different levels of sales or output budget must be submitted.
5. *Zero-based budgets (ZBB).* This concept was developed by Texas Instruments in the 1970s, and was proposed as an alternative to the incremental budget process. ZBB questions all costs by setting the new year's budget at zero and forcing all operating managers to justify their expense requests.⁵ It forces managers to scrutinize all costs, rather than assuming that a little bit more each year – incremental budgeting – will satisfy the needs of the organization under constantly changing circumstances. ZBB

requires that the security program “sell” its security services each year to the budget approval committee, as it assumes initially that no commitment exists to spend money on any activity unless adequate reasons justify it.

The Process of Budget Creation

Budget preparation and modification have changed drastically since the availability of software spreadsheets such as Excel™, Lotus 1-2-3, and Ability Office. Gone are the days when budgets were created on accountant-type paper and items would be written across broad columns reflecting various payments or disbursements over a year's periods. These would then be totaled for each payment or disbursement category and then for the year as a whole. If the allocated budget equaled the total on the bottom right-hand corner, the process was considered a success. If not, the manager and staff had to review and revise projections to see where alterations could be made.

The same process still occurs, although procedures are greatly eased by software programs that produce running totals of the budget, instantly adjusting with each change. This has vastly improved management control. Each significant expenditure constitutes a line in the personnel and expense portion of the budget, as shown in [Table 8.4](#). The manager reflects the budget changes that occur during the process. For example, if employees are granted pay increases at specific times, these are taken into account in the year's total plan by inserting the increase at the projected time.

Security program line item budgets usually are completed on electronic spreadsheets, which allows for specific indication of fund allocations. Personnel budgets frequently are expressed as line item expenses in that each position is considered permanent, and funds are allocated for an entire period. The spreadsheet allows numerous adjustments to occur over time. When a user changes an entry, the program immediately updates the data in all columns. The following are factors that affect change in a line item budget:

- *Personnel costs.* [Table 8.4](#) divides security program costs for illustrative purposes into four quarters. However, most programs allocate personnel expenditures according to pay periods, that is, weekly, biweekly, semimonthly, or monthly. In a line item budget, each employee will have a line for the entire year.
- *Expenses.* These predictable costs can be planned over an extensive period of time based on previous experience. They also represent variable expenditures. For example, plans for employees to attend conventions can be curtailed if projected costs get out of hand. In previous years, the “miscellaneous” category allowed managers a safety valve for adjusting their budget according to contingencies. Today, the category is small or is eliminated entirely in many reports. Contractual security guard services may be in this category and constitute the largest item in the entire budget.
- *Capital budget.* This represents spending for purchases that have a lifetime of 2 or more years.
- *Budget emergencies and contingencies.* As one budget is being planned, a budget for the current year is operating. Further, the implementation of unexpected plans

Table 8.4 Illustrative Security Budget Line Items Over Yearly Quarters

Budget Line Item	Quarters			
	First	Second	Third	Fourth
Personnel costs including benefits				
Director	_____	_____	_____	_____
Assistant Directors	_____	_____	_____	_____
Managers	_____	_____	_____	_____
Supervisors	_____	_____	_____	_____
Support staff	_____	_____	_____	_____
Expenses				
Other employees (contractual)	_____	_____	_____	_____
Travel	_____	_____	_____	_____
Office supplies	_____	_____	_____	_____
Uniforms and laundry	_____	_____	_____	_____
Telephone	_____	_____	_____	_____
Training expenses	_____	_____	_____	_____
Educational costs	_____	_____	_____	_____
Insurance	_____	_____	_____	_____
Automobile leasing	_____	_____	_____	_____
Automobile repair and maintenance	_____	_____	_____	_____
Consultant services	_____	_____	_____	_____
Memberships	_____	_____	_____	_____
Miscellaneous	_____	_____	_____	_____
<i>Total expenses</i>	_____	_____	_____	_____
Capital budget				
Security systems	_____	_____	_____	_____
Automobile purchases	_____	_____	_____	_____
Guard structures	_____	_____	_____	_____
Two-way radios	_____	_____	_____	_____
Office furniture	_____	_____	_____	_____
Other	_____	_____	_____	_____
<i>Total capital budget</i>	_____	_____	_____	_____
Corporate overhead charge	_____	_____	_____	_____
<i>Total budget request</i>	_____	_____	_____	_____

Budget planners allocate expenses for people, supplies, and major purchases over the length of the budget period. Numerous variations are possible to suit the recording and operating policies of particular organizations. The overhead charge, used in some organizations, is a charge management may impose on different departments reflecting a portion of the shared services provided by the organization to the department. A line item budget of this sort is best loaded onto a computer program so that cost items may be changed at any time, with budgetary consequences being instantly reflected. Security services may also be included in the organizational overhead, which is charged to other departments. The allocation for "other employees" under "expenses" can be a major one as it includes contracted security guard services planned for the entire year.

will cause budget changes that will have to be taken into consideration. Senior management expects operating managers to stay within their budgets without substantial deviation. Senior managers also may ask departmental managers to reduce their budgets on short notice. A reason for this could be to respond to an unexpected earnings shortfall or other reversal.

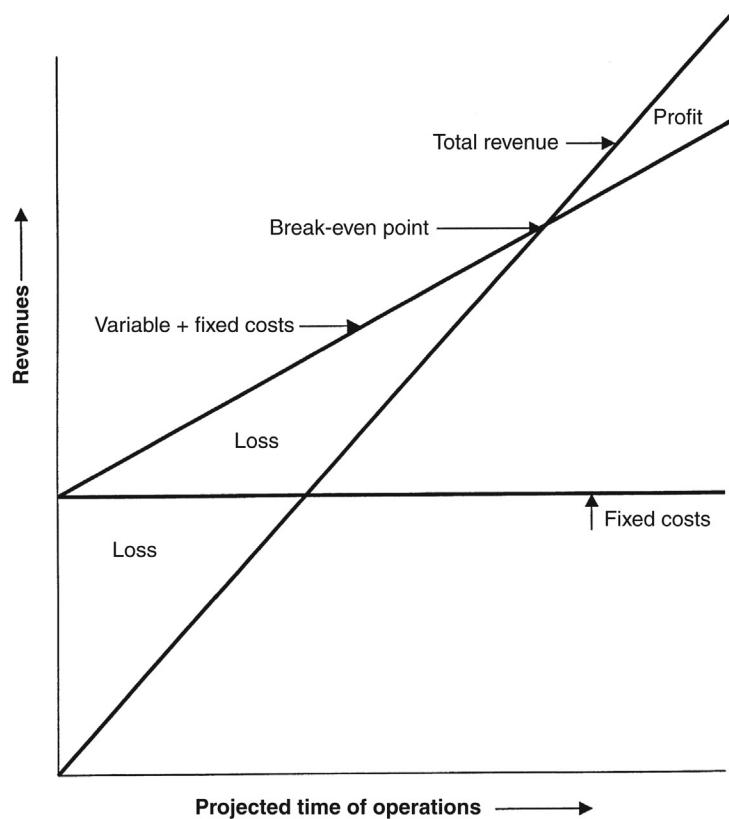
Managing the budget can be a challenge to security practitioners, who sometimes must deal with emergencies that create budget overruns. At such times, the manager is nonetheless expected to “find the money” within the current budget. This signifies that managers need to have the capacity to meet a contingency by cutting previously planned and allocated expenditures. Managers with budget responsibilities constantly analyze what cuts in programs or purchases could be made if they had to be made. Similarly, they consider how they would expand programs if additional resources not presently contemplated were made available. At all times, it is vital for the protection manager to understand what the program’s benefits are and communicate to senior management how the security function is contributing to the ultimate goals of the operations.

The Goals of the Corporation: Profits

For-profit organizations exist in order to make a profit. If a corporation does not achieve consistent profits, it will eventually face liquidation. If a corporation does not achieve sustained and adequate profitability, the providers of capital (shareholders, bond holders, lenders) will remove their money from the enterprise and use it where the return appears to be better and the prospects are safer. To achieve profit, the organization first must monitor fixed costs. These include overhead, such as space, utilities, and other normal operational costs. Such overhead costs exist whether the organization is just beginning, operating at a loss, or operating at a profitable level. In reality, overhead costs increase slightly as sales rise, but other factors – such as incremental production and service expenses – grow faster and in relation to increased production or service provided. Thus, considerable business must be generated before a break-even point is achieved; only beyond that a profit is possible. [Figure 8.1](#) illustrates the ways in which fixed costs and variable costs relate to profit.

Achievement of a profit within an organization surely cannot be taken for granted. Considerable effort is required to earn a profit. Once achieving a profitable level of operations, the concept of the enterprise becomes attractive to others. Competition and changing market conditions invariably threaten a profitable operation. To sustain growth, corporations use money from profitable operations to fund new products or services. These might one day become profitable and offset earlier products or services that might decline in their financial return. However, some new products or ventures will not succeed, resulting in a loss of capital and operating expenses allocated for this venture. The corporation must be managed so that such failures will not put the whole enterprise at risk.

New corporations and new ventures within a larger entity are not expected to make a profit initially. Developmental expenses are projected, followed by costs to produce the goods or



Profit is the objective of for-profit corporations, but it cannot be achieved until fixed and variable costs are met. These are not permanent, but vary constantly. As a corporation becomes more profitable, other organizations are attracted to compete to win a share of the profitable endeavor.

FIGURE 8.1 Fixed and variable costs related to profit.

offer the services. For example, in the pharmaceutical industry, a new patented proprietary drug may take 10–12 years to receive approval to enter the market. Then, only 5–7 years remain in the life of a patent, during which the extensive investments in research and development can be recovered. After patent expiration, other firms can market and sell exactly the same product under their own name, likely cutting the process in order to obtain market share.

Security programs must operate with the same level of objectivity as any program in an organization. Every department considers itself to be critical to operations. It is helpful to envision each operating unit interlinking independence with the others. Any weak link threatens the entire structure. Chiefs and directors of security programs need to understand the biases of financial directors toward the use of money for different segments of the operation. Programs are funded because they are critical, or at least desirable, to the goals of the operation. The security director needs to communicate how loss reduction programs contribute positively to the profit interests of an organization.

This is possible when the manager understands the nature of the business and how an intelligently conceived program is justifiable and necessary to the organization's success. The following sections discuss concepts that are important in explaining or justifying the necessity for security spending.⁶

Return on Equity

Return on equity (ROE) measures the return on shareholders' equity and gives a measure of the company's return relative to equity, that is, shareholders' paid-in capital and retained earnings. This can be represented as follows:

$$\text{ROE} = \frac{\text{net income}}{\text{equity}}$$

Return on Investment

Financially oriented managers often analyze the use of capital to determine what its value represents to the organization. This is done using the return on investment (ROI) measurement, which can be represented as follows:

$$\text{ROI} = \frac{\text{net income}}{\text{equity} + \text{debt}}$$

This performance measure is widely used by management because it accounts not only for earnings but also for the assets to achieve such earnings.

ROI is similar to ROE except that ROI includes debt. Both of these concepts are used to estimate the performance of the organization as a whole, and both are used to indicate the payback of a capital expense, such as the purchase of a security system. Assume that a security director wishes to purchase a security system. Will the cost of the capital commitment pay back the investment required to obtain it, including debt costs, in a satisfactory period? Or is the investment unlikely to be a good use of capital?

Consider a facility with a \$1 million per year budget for security, fire watch, and maintenance operations administration. Assume further that a new comprehensive security system costing \$1 million can reduce personnel cost by 25% of its purchase price. Therefore, the facility could save \$250,000 per year. Would the introduction of an electronic security-safety-fire communications system pay off sufficiently to pay for the cost of the system? An approximation of the value of such system could be calculated as follows:

$$\text{ROI} = \frac{\text{savings in personnel costs}}{\text{cost of system and finance charges}}$$

This would be calculated as follows:

$$\text{ROI} = \frac{250,000 \text{ (savings)}}{1,000,000 \text{ (total cost)}} = 0.25 \text{ (payoff in 4 years)}$$

Therefore, in this crude assessment, the investment would pay for itself in 4 years, with 25% being returned for each of the 4 years. Since the system would continue to be useful for several years longer, the loss prevention manager likely would have a fair to strong argument that the ROI is attractive to the company, and the purchase should be supported by senior management.⁷ Other factors, such as the necessity of bringing the facility into code or linking the system installation with a wider capital improvement project, might tip the balance to a favorable vote to provide the financing. For this illustration, no finance charges are taken into consideration. In many cases, a more detailed evaluation of the use of money for capital expenditure will be indicated.

A more detailed ROI scenario is provided by Walter E. Palmer, who proposes that the value of a security system – such as an electronic article surveillance (EAS) system for a retail store – be determined by first estimating the incremental cash flow.⁸

In this example, let's say that sales are at \$10 million and are growing at an annual rate of 2%. The baseline shrinkage rate is set at 3%. The assumption is that the shrinkage reduction from the new system that would cost \$75,000 and have a 5-year depreciable life would be 25% of the baseline shrinkage rate, resulting in a savings of \$75,000 the first year, as shown in Table 8.5. Because shrinkage is considered a cost, savings at retail must be calculated by the cost/retail ratio. In this example, the average cost of merchandise is considered to be 57% of the selling price, 0.57, and producing a savings at cost of \$42,750. It is

Table 8.5 Cash Flow Statement to Assess a Capital Investment*

	First Year	Second Year	Third Year	Fourth Year	Fifth Year
Sales (+2% each year)	10,000,000	10,200,000	10,404,000	10,612,080	10,824,322
Baseline shrinkage (%)	3	3	3	3	3
Baseline shrinkage (\$)	300,000	306,000	312,120	316,362	324,730
Shrink reduction (%)	25	25	25	25	25
New shrinkage (\$)	225,000	229,500	234,090	238,772	243,547
Savings (at retail)	75,000	76,500	78,030	79,591	81,182
Cost/retail ratio	0.57	0.57	0.57	0.57	0.57
Savings (at cost)	42,750	43,605	44,477	45,367	46,274
Less: expenses	10,000	10,200	10,404	10,612	10,824
Less: depreciation	15,000	15,000	15,000	15,000	15,000
Savings before taxes (SBT)	17,750	18,405	19,073	19,755	20,450
Tax (34%)	6,035	6,258	6,485	6,717	6,953
Net savings	11,715	12,147	12,588	13,038	13,497
Plus: depreciation	15,000	15,000	15,000	15,000	15,000
Cash flow investment	26,715	27,147	27,588	28,038	28,497
Cost of investment	75,000				
Cumulative cash flow	48,285	21,138	6,450	34,488	62,985

This illustration shows the payback on an electronic article surveillance (EAS) system that reduces shrinkage from 3 to 2.25%.

Adjusting for sales growth of 2% per year and accounting for wholesale costs, expenses, and other factors, the payback cost of the system can be evaluated.

*Cost of asset = \$75,000.

(Source: Palmer, W.E., 1998. Return in investment: beyond the conceptual. Pinkerton Solutions, January.)

assumed that the management of the system will require expenses of \$10,000, which are growing at an annual rate of 2%, which are now deducted.

Depreciation of the value of the cost of the asset is determined as a straight-line write-off over 5 years, or \$15,000. Expenses and depreciation are subtracted from the net savings.

The next step is to determine savings before taxes. Assuming that the tax rate is 34%, the net savings would be \$11,715. But depreciation is added back in since it is an accounting device and does not generate an actual cash amount and the \$75,000 first-year expenditure is deducted from cash flow.

Finally, the addition of net savings and depreciation produces cash flow. This now allows the advisability of the project to be assessed from three types of analysis: payback period, net present value (NPV), and internal rate of return (IRR).

- *Payback period.* The formula for calculating the number of years it will take to generate enough cash to pay for the project is as follows:

$$\frac{\text{Cost of project}}{\text{Annual cash flow}} = \text{payback}$$

If the system costs \$75,000 and was expected to return \$20,000 annually, the payback period would be $\$75,000 / \$20,000 = 3.75$ years. Using the cash flow example, the project cost would be completely paid for in about 2 years and 9 months, because \$75,000 is equal to the first 3 years' revenues, plus \$15,000. That remainder is equal to about 0.75 of the third year's revenues. The payback method of analysis may rank projects with shorter payback periods higher than those with longer paybacks. The disadvantage is that the straight payback method ignores the time value of money, which is discussed in the next example.

- *NPV.* This method considers future cash flows of a project. Assume the company desires a 12% return on its investments. [Table 8.6](#) illustrates this calculation using the assumptions discussed in [Table 8.5](#). The columns in [Table 8.6](#) are year, cash flow, discount factor (DF), and present value (PV). The year column (total 5 years)

Table 8.6 Discount Factor (DF) for Calculating Present Value (PV)

Year	Cash Flow	DF (12%)	PV
1	26,715	0.8929	23,854
2	27,147	0.7972	21,642
3	27,588	0.7118	19,637
4	28,038	0.6355	17,818
5	28,497	0.5675	16,169
Total	137,985		99,120

This is another way to determine whether the system is a good buy. This calculation takes into account the "present value of money." Cash flow is adjusted by a discount factor reflecting the cost of money. The present value of the money would decline each year. The EAS system is still an attractive project, but less attractive than it was under the payback period calculation. (Source: Palmer, W.E., 1998. Return on investment: beyond the conceptual. Pinkerton Solutions, January.)

represents the number of years the project is expected to generate cash. Cash flow represents the amount of cash the project is expected to generate each year after taking into account expenses including taxes (Table 8.5). DF is the value today of \$1.00 received in the future at a certain rate of return (12% in this case). For example, having \$0.8929 today is equal to receiving \$1.00 in 1 year at a 12% return ($0.8929 + 12\%$ of $0.8929 = 1.00$). Likewise, having 0.5975 today is equal to receiving 1.00 in 5 years ($0.5675 + 12\%$ five times compounded = 1.00). Financial calculators and computer spreadsheets programs (Excel, e.g.) are available for making these calculations. The fourth column, PV, represents the value today (PV) of cash expected sometime in the future. Looking at years 1–5 Table 8.5 indicates the project will generate \$26,715 in the first year through \$28,497 in the fifth year. Consequently, if \$1.00 received within 1 year is worth 0.8929 at an expected rate of return of 12%, then \$26,715 has a PV of \$23,854. In the fifth year the expected cash generated by the project is \$28,497 (Table 8.5). However, the value today of receiving \$1.00 in 5 years is only 0.5675. Therefore, the value today (PV) of receiving \$28,497 in 5 years is \$16,169 ($28,497 \times 0.5675$). The total column of Table 8.6 indicates the project that has an original cost of \$75,000 will generate total cash of \$137,985. However, the value of that cash today (PV) that will be received in the future is \$99,120. The project appears to have a positive cash flow since spending \$75,000 today will generate cash in the future with a value today of \$99,120.

- **IRR.** The IRR is the cost of capital that would make the NPV for the project equal to zero. (The calculation of the IRR is complex and will not be discussed here.) If the IRR exceeds the cost of capital, the project is attractive. If the IRR is less than the cost of capital, the project is likely to be rejected.

Each of the three methods has its advantages. The payback method is easiest to compute. NPV and IRR require financial calculators, but these methods are more accurate in identifying the time value of money. In times when inflation rates increase, management is more apt to focus on variable costs of funds over time for different projects. Typically, managers will consider different methods in making a decision. These issues are discussed in greater detail later in this chapter.

Capital Budgeting for Security Programs

Assume that a security program determines that it requires computerized control systems for a new facility. The security director would begin by preparing a written summary detailing the benefits and costs over the life of the system. The manager also will prepare a capital budget that will allow the parties involved to evaluate the proposal. They can then decide whether this capital proposal is attractive relative to others in the internal departmental competition for use of funds. Various ways of considering the value of the budget exist.

An important factor at the time such a decision is being made is the cost of capital. How it is determined can differ, and no single accounting method is used uniformly. In

addition, the security chief or director may likely face competition from other managers with their own capital requests. The attractiveness of capital expenditures for new systems, therefore, in part is that such systems may reduce ongoing costs over what is currently being paid. These benefits are calculated in order to identify factors related to savings through efficiencies. The following sections discuss widely used capital budgeting methods.

PAYBACK METHOD

The payback method is the simplest and most widely used technique to evaluate a project to determine the time it will take to recover the initial investment. The process determines the earnings required by an investment in order to pay back the initial capital outlay. As seen in the previous example, this method is popular because it usually demonstrates a rapid repayment of capital, allowing management to reinvest the savings. However, this method does not consider the time value of money. In times of high or rising interest rates, this issue gains in importance.

Money invested earns interest, while money borrowed costs interest. Therefore, the money to be used for the capital budget has to be considered in terms of compounding and discounting. These terms are the opposite of each other. Compounding asks, "If money is invested at the current interest rate, what will it be worth in a certain number of years?" Discounting asks, "How much money should be invested at a given interest rate in order to achieve a particular amount at a defined period in the future?"

The payback method fails to consider the significance of compounding or discounting required for purchase of the capital asset. The longer the time required for a capital investment to be paid back, the less the interest senior management is likely to have in authorizing it. If the payback is less than the goal set by management, then the project has a good opportunity of being approved.

INITIAL-INVESTMENT RATE OF RETURN METHOD

This method also overlooks the time value of money, creating a bias in favor of investments that yield a return quickly. The initial-investment rate of return (IIRR) method considers the effects that taxes and depreciation have on the investment, a consideration overlooked in most payback method computations. However, the method does not identify operating cash flows that can be significant considerations. Senior management is more likely to approve a project if the IIRR is greater than the cost of capital to the organization.

TIME-ADJUSTED RATE OF RETURN METHOD

This method considers discounted cash flow. Time-adjusted rate of return (TARR) provides the interest yield predicted by the investment over its projected useful life. It is also called the IRR method. TARR is calculated using a personal computer with a spreadsheet program. If future cash flows are the same for each period, the calculations are performed easily. If the cash flows are uneven, then a trial-and-error process is necessary to arrive at the NPV. If the TARR is greater than the organization's cost of capital, senior management is more likely to approve the project.

OTHER MANAGERIAL OPTIONS IF A PROPOSAL IS REJECTED BY SENIOR MANAGEMENT

What if the savings projected from the capital expenditure are not sufficiently attractive to senior management to approve a capital purchase? In this situation, other measures may be available to the security planner. Assume that the security chief of director advocates a new system but that a capital commitment is not available. One possibility would be to lease the system from the supplier or an independent leasing facility provided by the supplier. In this case, the system obviously would not belong to the user but this factor might not be consequential. One advantage of this arrangement is that service of the system might remain the responsibility of the lessor. Another benefit is that the cost of the lease would be expensed each year, which could produce a tax advantage to the organization. However, if the lease is approximately the same life as the system, accounting interpretations might require the entire cost of the lease at PV be put on the balance sheet as an asset.

If the leasing option is not available, the vendor may also offer flexible payment options to make the purchase attractive to the customer.

Another possibility, though one less frequently available, is that the vendor will provide the system free under certain conditions. The system must produce identifiable and certain savings. If the vendor can share in the savings, the vendor may be willing to “split the savings” with the customer, in effect, providing the system without cost but actually paying for it through cost reductions. For example, an organization may desire a system to automatically turn off lighting, heat, and air conditioning if no individuals are in the area. The cost for such an energy management system including installation could be paid by the systems company. The customer then splits the energy savings with the systems company above the previous base level costs of power.

When Senior Management Seeks to Cut Security Spending

Budgets are often management’s main way to gauge performance by matching actual results with budgeted results, but they can also block managers from shifting resources to take advantage of opportunities and can distort long-term planning.⁹ Budgets also concentrate on spending; however, the critical issue facing management at all levels is how to use limited resources for the betterment of the enterprise.

What if management proposes a cut in security program funding not out of exigency, but because a change in management doubts the value of security?

Security services, like research and development, accounting, and human resources, are sometimes referred to as expense centers, not profit centers, by persons who fail to grasp the interrelatedness of organizational units. This mentality puts security at a disadvantage if measures are not found to communicate value for the whole organization. Well-designed, relevant security metrics can be translated into value-added services that are critical to the entire operation. This can be achieved, for example, by demonstrating the utility of the security program compared with others in similar circumstances. Can

savings be gained by the lack of costly problems that beset other organizations with inferior security programs? Is turnover lower, are costly litigations fewer or nonexistent, is employee and customer satisfaction measured, and are insurance premiums reduced by the presence of a well-managed protection program? Answers to questions like these can serve to guide organizations seeking to educate managers who question or challenge funding for a security program. Ultimately, the program needs to demonstrate value and to communicate this to a wide managerial audience.

Security as a Profit Center

If organizations seek to create profits, how can proprietary security services be crafted into a profit center? In many cases, security programs have no options to create profits in the same way the principal business of the organization does. Further, it would be unwise for some organizations to attempt to develop new sources of income from security programs. However, in other situations, such possibilities exist. The following are a number of such services:

- *Alarm services.* A technology firm was required by federal contracts to maintain an advanced proprietary security system with backup guard response. The program was staffed round-the-clock 365 days per year. The firm was able to provide services to nearby noncompetitive corporations that were attracted by the advanced standards of the system and the certainty of nearly experienced security officer. These corporations preferred to contract with a well-regarded neighbor than with a distant security alarm service business or to provide the service for themselves.
- *Investigative services.* A diversified clothing manufacturing concern and retail chain developed a team of highly proficient investigators to solve a series of complex internal loss problems. When the initial issues they were hired to resolve gradually were brought under control, they had less work to do. With the encouragement of senior management, the chief security officer then made these services available at professional fees to vendors and customers. The investigative team had industry-specific knowledge and expertise that put them at an advantage over other investigators. A profit center was created.
- *Parking revenues.* The security department of a healthcare facility took responsibility for the management of parking garages and lots. The program was able to keep a portion of revenues for discretionary purposes. This led to improving and expanding parking use, which produced further revenues.
- *Consulting.* Security directors and their staffs develop deep expertise in their own spheres of work. Generally, sufficient demands keep the team busy on internal matters. However, in some circumstances, time will be available for internal personnel to work on projects for agreed-to terms and conditions. This may be termed creating a profit center for a service business unit.

Forensic Safeguards to Internal Fraud

The cost of fraud and abuse in the workplace is undoubtedly high. In fact, the *Report to the Nations on Occupational Fraud and Abuse* estimates this loss level at 5% of the monetary value of all goods and services.¹⁰ If applied to the 2013 estimated gross world product, this translates to a potential projected global fraud loss at nearly \$3.7 trillion. An analysis occurred of 1483 cases of occupational fraud in more than 100 countries. The United States represented 48% (646) of these cases with a median loss of \$100,000.

Richard C. Hollinger and John P. Clark conducted seminal research on workplace deviance that was reported in 1983.¹¹ It included surveys of 47 corporations in 3 communities: 9431 employees, 247 top executives, 30 labor unions and employee organizations, and a variety of other organizations interested in business-related crime. One-third of all employees self-reported that they had taken property from the workplace. The deviance was not limited to entry-level personnel. All worker segments – including physicians in hospitals – admitted in substantial numbers to stealing at work. It should be emphasized, however, that the majority of workers in all categories did not self-report for theft. White-collar crime is a far greater financial burden on companies than robbery, larcenies, and auto theft combined. Crime that occurs by manipulating financial assets in publicly held corporations as well as NFP institutions is a major issue throughout the world. Security management should regard such risks as an uppermost priority and establish controls that seek to mitigate it.

Generally Accepted Accounting Principles

All corporations have financial records audited by independent auditors. The purpose of this practice is to ascertain that the financial practices and records of the organization follow conventionally established accounting concepts and principles. The outside independent auditor (normally, a CPA) works with the CFO and designated personnel, such as controllers and internal auditors, to review financial procedures. Independent accountants maintain that the audit process is not intended to detect fraud and embezzlement, although auditors frequently do uncover serious defalcation from their efforts. Yet the failure of regularly conducted audits to identify a pattern of financial deviance or irregularity can lead to legal action against the accounting firm in the event an undetected or unreported embezzlement takes place despite regular audits (Box 8.2).

The financial information presented in the periodic statements issued to the public is prepared according to widely respected principles of accounting to assure that individuals external to the enterprise – such as shareholders, creditors, government agencies, and the general public – have accurate, relevant information. The same information is useful to management in directing the organization. In planning any future activity, management evaluates past financial statements for relevant past activities.

BOX 8.2 MAJOR CORPORATE COLLAPSES IN RECENT YEARS

Most examples of fraud and embezzlement in operations are not encountered by independent auditors. They are discovered by accident or are brought to the attention of management by insiders with specific knowledge of deviant financial practices. Such insider tipsters provide the most frequent information on occupational fraud and abuse.

Audit firms maintain that it is the responsibility of management to establish financial controls. Supreme Court decisions have supported this view and the number of lawsuits that auditors have been forced to defend decreased in recent years. Nonetheless, numerous celebrated cases of accounting improprieties attest to the fact that auditors can be negligent.

Incident	Year	Business	What Happened
Texaco	1987	Oil	In a legal battle with Pennzoil, Texaco was found to owe a debt of \$10.5 billion. The company went into bankruptcy and was taken over by Chevron
Bank of Credit and Commerce International	1991	Banking	Operating from the United Kingdom, BCCI broke US law and was charged with fraud, money laundering, and larceny
Long-Term Capital Management	1998	Hedge fund	LTCM lost \$4.6 billion in the space of a few months with a faulty program that traded derivatives
Pacific Gas and Electric Co.	2001	Energy	The company went into bankruptcy after a change in California regulations. Customers lost service
WorldCom	2001	Telecomm	Directors approved fraudulent accounting methods to prop up the stock price. Assets were bought by Verizon in 2004
Enron	2001	Energy	Executives and directors fraudulently concealed large losses in projects
Adelphia Communications	2002	Cable TV	Internal corruption
Arthur Andersen	2002	Accounting	US court convicted Andersen of obstruction of justice by shredding documents related to the Enron scandal. The Supreme Court reversed the finding, but it was too late
Refco	2005	Brokerage	After its successful IPO, it was revealed that the CEO had concealed \$430 million of bad debts
Bear Stearns	2008	Banking	Collapsed from investments in subprime mortgage market. Assets bought by JP Morgan/Chase with an Federal Reserve Bank (FRB) guarantee
Lehman Brothers	2008	Banking	Collapsed from investment in mortgage debt

Incident	Year	Business	What Happened
AIG	2008	Insurance	Held \$57.8 billion in subprime mortgages
Washington Mutual	2008	Banking	Also a subprime mortgage crisis investor
Dynergy	2012	Energy	Fraud in a subsidiary's purchase of another subsidiary. Emerged from bankruptcy later

The causes for these accounting improprieties are numerous: pressure for performance, industry competition, quality and integrity of management, and the goal-setting process. In most cases, the quality of auditing and the ethics of those involved allowed the improprieties to continue longer than what otherwise could have been the case.

Fraud, Embezzlement, and Security

Within an organization, internal auditors are charged with monitoring the controls and checking systems. They attempt to assure that fraud (the conversion or obtaining of money or other assets by false pretenses) and embezzlement (misappropriation of entrusted assets with the intention to defraud the legal owner) are detected early. The responsibilities and function of the internal auditors are different from the external auditors. While external auditors are concerned with the overall fairness of the financial statements, internal auditors are concerned with specific projects selected by top management. However, internal auditors also have some level of independence as they may report directly to the Board of Directors, not the management units they are auditing. Accountants and financial investigators are involved in the specialized process of investigating potential or actual monetary dishonesty. This type of activity is carried out by forensic accountants, a growing field of accounting, or investigators who often have specialized training in conducting such investigations, collecting relevant facts, and preparing an action for criminal or civil prosecution.

Security directors are frequently involved with the financial functions of the organization. This can include creating or consulting on the establishment of checks and controls within the operations, testing such controls, and investigating any monetary crime. Should a crime occur, the security director with forensic expertise will interface with financial management on aspects of the investigation. In some cases, the security director will retain and supervise forensic investigators in their fact-finding. The internal financial officer most often concerned with possible fraud or embezzlement is the chief internal auditor. By contrast, the controller is the chief accounting officer of an organization involved with financial reporting, taxation, and possibly auditing.

Separating Tasks: A Powerful Tool Against Fraud

One of the most fundamental controls created by security practitioners and internal auditors is to separate functions within the organization, as shown in [Table 8.7](#). Collusion, an agreement between two or more persons to defraud someone or obtain an object forbidden by law, is a difficult crime to prevent. Often working from different

Table 8.7 Separating Functions to Improve Security

Function A is separated from ...	Function B
Financial examples	
Accounts payable	Accounts receivable
Payroll preparation	Payroll reconciliation
Records custody	Use of records
General	
Authorizing	Transaction processing
Receiving	Sending
Purchasing	Approval of purchases
Ordering	Verification of order
Custody	Accounting
Vendor proposal	Vendor approval
New offer of employment	Independent review before final offer
Computer system controls	
Computer programming	Testing of computer programs
Computer operations	Directing computer operations
Library management	Use of library materials

Separation of duties is a powerful security safeguard against internal theft and fraud and embezzlement. To prevent collusion further, management institutes a third activity: verification of the process by an independent third party.

departments with separate understandings of vulnerabilities, the colluders have great advantages. By separating functions, an organization makes collusion difficult to commit. Such crimes may still occur, but abettors face lower chances of success. Collusion is much more difficult to control than a single rogue acting alone. To be sure, even a single individual acting alone can cause huge losses to the organization over extended periods of time. It is for this reason that security-conscious managers seek to minimize the possibilities of such crimes occurring by separating routine functions. While this principle is particularly relevant for financial controls, it has significance in other managerial venues as well.

The more persons are involved in collusion, the greater the loss to the organization is likely to be. According to a research report: “Collusion helps employees evade independent checks and other anti-fraud controls, enabling them to steal larger amounts. The median loss in a fraud committed by a single person was \$80,000, but as the number of perpetrators increased, losses rose dramatically. In cases with two perpetrators the median loss was \$200,000, for three perpetrators it was \$355,000, and when four or more perpetrators were involved, the median loss exceeded \$500,000.”¹²

A typical financial control separates check preparation from check authorization. But a third step – independent verification of the process – makes the likelihood of financial fraud less possible. Security practitioners are involved in the creation of controls that make financial deviance more difficult and that review and modify such measures regularly to reduce risks from changing vulnerabilities.

Disastrous or near-catastrophic fraud can befall any organization without a reasonable security program. Such programs fail to have compliance measures at a high standard. The financial services industry seems particularly vulnerable to such depredations. Presumably successful traders thwart the efforts of compliance officers who fail to ask the right questions. Randolph D. Brock III has cited three cases within recent years in which a single person has concealed trading losses of over \$1 billion, and many more with losses in the millions.¹³ He argues that security practitioners have roles to play in deterring, detecting, and investigating internal theft. There are three prevention principles: aggressively question success (it may be illusory), the most likely suspect probably did it, and suspect everyone all the time.

Summary

Accounting controls and budgeting are among the most potent measures used to direct the operations of entire organizations as well as individual programs. Often, the accounting mentality focuses on “making the numbers” rather than achieving long-term goals of the organization. Understanding the nature of such controls, nonetheless, is vital to interpreting successfully the value of security operations for the entire organization. Measures should be identified so that security can be judged according to important organizational goals and values. In some situations, security programs can create fresh revenues for an organization. However, such measures should not divert security management from its principal tasks for its own organization. Security practitioners should always search for ways in which critical job functions can be separated and then monitored by a third party. This practice is a powerful antidote to fraud and collusion.

Discussion and Review

1. How have accounting techniques changed in recent years? How do they resemble practices in Italy during the Renaissance?
2. Discuss the importance of notes to consolidated balance sheets and statements of operations.
3. How has the SEC improved reporting measures for publicly held companies? What are the weaknesses in SEC procedures?
4. What are the merits of ZBB compared with incremental methods?
5. Why is a series of break-even reports unsatisfactory for a corporation in the long run?
6. Compare and contrast three ways of determining the value of a capital investment that produces reduced losses or costs for operations.
7. Cite examples of separation of controls in addition to those discussed in the text.

Endnotes

¹ Gleeson-White, J., 2013. Accounting – our first communications technology. *Financial History*, Winter, p. 20. Also see Gleeson-White, J., 2013. *Double entry: how the merchants of Venice created modern finance*. W.W. Norton & Company, New York, NY.

² *Ibid.*

- ³ Lee, G.A., 1984. The development of Italian bookkeeping 1211–1300. In: Nobes, C. (Ed.), *The Development of Double Entry: Selected Essays*. Garland Publishing, New York, London, p. 25; Pacioli, F.L., 1996. *Double-Entry Book-Keeping* (P. Crivelli, Trans.). Institute of Bookkeepers, London, p. 8.
- ⁴ Hector, G., 1989. Cute tricks on the bottom line. *Fortune*, April 24, p. 193. Also: Schilit, H., 1994. *Financial Shenanigans*. McGraw-Hill, New York, NY.
- ⁵ Conrad, A.H., 1997. *Zero-Based Budgeting*. Council of Planning Librarians, Monticello, IL.
- ⁶ Hargrave Jr., L.E., 1999. *Plan for Profitability! How to Write a Strategic Business Plan*. Four Seasons Publishers, Titusville, FL.
- ⁷ DiLonardo, R.L., 1997. Financial analysis of retail crime prevention. In: Felson, M., Clarke, R.V. (Eds.), *Business and Crime Prevention*. Criminal Justice Press, Monsey, NY.
- ⁸ Palmer, W.E., 1998. Return on investment: beyond the conceptual. *Pinkerton Solutions*, January, p. 17.
- ⁹ Stewart, T.A., 1990. Why budgets are bad for business. *Fortune*, June 4, p. 179.
- ¹⁰ Association of Certified Fraud Examiners, 2014. *Report to the Nations on Occupational Fraud and Abuse – 2014 Global Fraud Study*. Association of Certified Fraud Examiners, Austin, TX.
- ¹¹ Hollinger, R.C., Clark, J.C., 1983. *Theft by Employees*. Lexington Books, Lexington, MA.
- ¹² Association of Certified Fraud Examiners, *op. cit.*, p. 4.
- ¹³ McCrie, R.D., 2001. Clues to catastrophic fraud in the financial services industry. *Security Letter*, Part II, October 2.

Additional References

- Brealey, R.A., Meyers, S.C., Franklin, A., 2006. *Principles of Corporate Finance*. McGraw-Hill, New York, NY.
- Ferraro, E.F., Spain, N.N., 2006. *Investigations in the Workplace*. Auerbach Publications, Boca Raton, FL.
- Friedrichs, D.O., 2004. *Trusted Criminals: White Collar Crime in Contemporary Society*. Wadsworth, Belmont, CA.
- Kane, J., Wall, A.D., 2006. *The 2005 National Public Survey on White Collar Crime*. National White Collar Crime Center, Fairmont, WV.
- Kovacich, G.L., 2008. *Fighting Fraud: How to Establish and Manage an Anti-Fraud Program*. Elsevier Academic Press, Burlington, MA.
- Salinger, L.M. (Ed.), 2005. *Encyclopedia of White-Collar and Corporate Crime*. Sage Publications, Thousand Oaks, CA.
- Tully, S., 1999. The earnings illusion. *Fortune*, April 26, pp. 206–210.
- Wells, J.T., 1997. *Occupational Fraud and Abuse*. Obsidian Publishing Company, Austin, TX.

Operating Personnel-Intensive Programs

Quis custodiet ipsos custodes (Who will guard the guards themselves?)

—Juvenal, *Satires*

Security programs concern themselves with people, technology, and procedures. Earlier chapters considered theories of workplace productivity and particular strategies of selecting, training, motivating, and generally managing employees in security functions. This chapter considers the macrolevel of managing people in functioning programs. It looks at two significant categories of security employment – security officers and investigators – and the programs that make them productive and efficient.

Like all aspects of protective management, personnel applications have experienced considerable change in the past years, and continue to experience change today. Contemporary security officers are more likely to be contract workers than permanent proprietary employees relative to past decades. Similarly, investigative resources in industry and government have increased, and both contract and proprietary investigative services have expanded to fit these new workplace needs. Moreover, the scope of investigative tasks has broadened considerably.

The Proprietary/Contract Employee Debate

For most of the twentieth century, security workers were permanent proprietary employees with the same expectations and corporate relationships as any other employee. Beginning early in the century, and most notably since the early 1950s, security guard positions have increasingly been provided by contract services. In fact, by the year 2000, about 60% of all security officers were provided by contract services, and this trend continues to grow. Although both proprietary and contract personnel have their own distinct advantages, it is important that all factors be weighed in making this decision, as shown in [Table 9.1](#).

The main reasons cited for contracting out security employees are as follows:

- *Less total cost.* Employers generally believe that it costs less to contract out for services than it does to employ a staff of security personnel as regular employees. In determining the level of savings, management must be certain to include in-house costs for acquiring, monitoring, and administering such services. Savings for liability insurance may also be factored in since the contract firm will provide its own coverage. (This does not mean, however, that all liability for negligent guard services passes to the contract service.) Nevertheless, taking such monetary factors

Table 9.1 Contract or Proprietary Security Personnel: Weighing Factors

Factors Favoring Contract Security	Factors Favoring Proprietary Security
Less total cost normally	Personnel retention high
Administrative ease	Perception of greater quality of employee
Criminal records screening	Greater site knowledge
Recruiting and vetting transferred	More flexible controls
Training transferred	Greater loyalty to the employer
Supervision transferred	Reliability of service
Specialized liability insurance	Cost savings in some circumstances
Specialized protective experience	A union agreement includes security personnel
Personnel scheduling flexibility	
Less likelihood of collusion with proprietary employees	
The workplace requires a guard union provided by the contractor	
Extra staff may be available on short notice	

Most security guard personnel are currently outsourced to contract security guard services. This is part of a trend for organizations to retain workers from specialty contract organizations rather than in-house status. Organizations depending on contract security personnel may or may not have proprietary officers acting as supervisors or managers. If so, the arrangement is termed site supervisor, or something similar.

into consideration, management typically expects a net savings of 5–20% from the previous cost level. That takes into consideration the administrative costs and profit objectives of the contract provider.

Rather than focus solely on economic benefits, however, employers considering converting from proprietary to contract services should perform a comprehensive cost/benefit analysis to determine whether the advantages are significant. In doing so, it is important to remember that fringe benefits are the responsibility of the service provider, as are benefits to attract and retain staff.

In some cases, management will have other compelling reasons for deciding to contract out or not to contract out that are more significant than cost savings. Dennis Dalton, a consultant experienced in security services conversions from proprietary to contract, says: “All too often executives make the decision to convert based solely on the economic gain. What they fail to consider are the dynamics involved in displacing long-term, loyal employees.”¹

- *Administrative ease.* The contract firm is responsible for recruiting and vetting its security employees. It should be highly proficient at this task. The security services firm handles routine details for contract security employees, similar to those for proprietary workers. Nonetheless, the security services firm’s client generally maintains a residual duty to review personnel files and may conduct interviews of workers who will be assigned positions of responsibility within the workplace. Taxes and benefits are the responsibility of the service provider.
- *Criminal records screening.* In some states and geographic areas, the law dictates that security personnel be screened through criminal justice databases for the presence of convictions that would bar them from working in the field. Such

databases are not always available to private sector employers. Many services providers are thus able to assure employers that security workers have no evidence of significant criminal records in the jurisdictions where such information is checked.

- *Recruiting and vetting transferred.* The process of recruiting and vetting new security personnel is the responsibility of the services provider. This process can be tedious and costly from which the client is absolved. Further, businesses that concentrate on providing security guard services may be better at it than their client bases that are likely to attract and screen job candidates from a smaller pool.
- *Training transferred.* The security vendor is expected to have the commitment and expertise to train security personnel to the level required for the contractor's needs. The quality of training is consequential. Some security guard companies have a training department and are committed to job development beyond entry-level training. Additionally, the contractor may provide specific additional training to meet the needs of the assignment.
- *Supervision transferred.* Security officers usually are supervised by the services provider. As discussed in Chapter 5, supervision and site management are crucial to a well-organized program. Many large contracts also include a full-time site manager who handles routine administration. The client may elect to provide its own site supervision by proprietary workers.
- *Specialized liability insurance.* Security services providers normally should possess comprehensive liability insurance as a safeguard against potential lawsuits. Even in the event that the contractor has some liability in a judgment, the amount is likely to be divided between two parties, lessening the burden on each.
- *Specialized protective experience.* The security services provider should serve as a general resource, as needed, in security matters. Security services firms may share their practices and resources, acting as informal consultants on procedures and policies on a limited basis.
- *Personnel scheduling flexibility.* When the contractor requires additional personnel for special purposes, such as a conference, annual meeting, or an untoward event, the services contractor can add employees on short notice. Similarly, if an employee fails to meet the needs of the contractor, the employee often may be replaced rapidly. That can mean on the spot, at the end of the shift, or at a later time. By contrast, the termination of a proprietary employee usually requires a more drawn-out process.
- *Less likelihood of collusion and fraternization.* Contract security personnel are hired and managed by a separate organization from the clients they serve. This managerial separation makes collusion less likely than if security workers were proprietary staff members. Similarly, the likelihood of fraternization – extensive socialization between security and nonsecurity personnel – is reduced. This principle is codified in Section 9(b)(3) of the National Labor Relations Act, which gives employers the right to terminate voluntary recognition of a nonguard union. That is, the employer

of a unionized workforce may require that security officers be members of a different union than the primary union.

- *Emergency and short-term staff available.* If the client requires additional security personnel for brief assignments, security services may provide extra officers as needed. This could be less burdensome than hiring additional personnel on a temporary basis. Examples of the need for such personnel include extra security at a site following an emergency, labor unrest, ceremonies, and outside meetings that will draw a large crowd.

Now that we have discussed the main reasons why organizations contract out for security services, let's look at the factors cited by organizations that have instead elected to retain a proprietary security service primarily or exclusively:

- *Personnel retention.* Security directors generally prefer to have low employee turnover. Proprietary employees are more likely to remain on the job longer. This is due to many reasons, including the time and cost of recruiting, training, and guiding workers. However, this is not guaranteed, and some security services providers also can point to extensive longevity with some of their employees. The most important reason why retention is desirable is because employees know operations better. If an exception or an emergency occurs, they are usually better at responding because of experience.
- *Perception of greater quality of employee.* Many employers believe that proprietary workers, in general, are superior workers because they are attracted to the normally better compensation and career opportunities within a proprietary organization. However, some employers ascertain that the quality argument is relative to the circumstances and that, given attractive inducements by a security services provider, the quality of service is not likely to be substantially different over time.
- *Greater site knowledge.* An aspect of greater worker retention is that such employees are likely to know people, procedures, and principles better than those with a shorter tenure do. Logically, this produces more reliable service.
- *More flexible controls.* In proprietary programs, personnel usually may be transferred from one location to another as a condition of employment. Contract employees also may be shifted with ease from one site to another. However, some security directors believe that this process is easier for employees who are permanent workers.
- *Greater loyalty to the employer.* Many directors of proprietary programs believe that staff workers are more loyal than contract workers are. This view, which they support with anecdotal evidence, cannot be quantified, although the argument is appealing on its surface. It implies that proprietary employees make extra efforts to provide quality service. However, it can be argued that contract workers have reason to be loyal to the place where they are assigned as well.
- *Reliability of service.* A few contract security firms prove to be disappointing after an initial period of meeting standards. According to Randolph D. Brock, a former security director and principal of a security services firm, "Contractors tell clients what clients want to hear and believe, and say they do. But they really don't, opting instead to maintain control of the relationship and dictate terms and conditions."²

- *Cost savings.* Normally, managers expect to achieve significant savings from contracting out for security guard and patrol services relative to their in-house equivalents. However, in some cases – particularly with smaller programs – savings will not be achieved, and the organization would save money by staffing its own program internally.

As indicated in this discussion, there tend to be more reasons for contracting out security services than for retaining them as proprietary services. Indeed, the direction has favored growth of the contract sector for several decades. Yet many organizations have retained proprietary security because they conclude that it is the best policy for their organization. The decision to convert from proprietary to contract or vice versa should be made only after careful consideration of all the factors involved.

Combined Proprietary and Contract Staffs

Many security directors conclude that proprietary and contract services have complementary benefits. Therefore, they include both types of services in their operations strategy. Similarly, some analytical directors will contract with more than one outside service. This permits qualities to be compared with different service vendors. It also serves as a means of an ongoing assessment of performance of each type of service unit.

The search for enduring, cost-effective, reliable security services challenges managers. Consultant Dennis Dalton notes that 7 out of 10 security directors for the largest companies in America identified “finding and retaining a really quality-driven contract security agency” as 1 of the 3 critical factors in their programs.³ There are, therefore, many reasons why organizations seek to obtain the perceived quality of a proprietary staff with the flexibility and depth provided by the contract sector.

Core Expectations of Security Officers

Security officers have numerous obligations to their employers, each of which is of critical importance. The following are the security officer’s main obligations:

- *Deter.* The primary goal of security personnel is to deter or prevent harm to people; protecting property is secondary. Adequately trained security personnel deter crime and disorder. The vast majority of potential offenders restrain themselves from disorderly or criminal conduct in the presence of security personnel. This is because the opportunities for identification, arrest, conviction, and possible civil recovery are too high a price for the crime to be attractive to a potential offender. In deterring illegal and disruptive behavior, security personnel provide visible security that makes the public feel safer and more confident about being where they are. This function may be the most important quality provided by security personnel in most circumstances.

- *Delay.* In the event that offenders commit a crime, security personnel may delay their successful flight, leading to apprehension.
- *Detect.* When an incident occurs or when procedures are not followed properly, security officers can ascertain the violation quickly, mitigating or reducing the chances of loss.
- *Respond.* Security personnel are trained to respond to detected incidents, alarms received, or calls for service while on duty. They are expected to take action at such times to protect people and property and to make the public feel safer.
- *Report.* In the event of an incident, a report from an independent observer, such as a security officer, provides important information for management. The report serves as a possible factor in changing internal procedures, a basis for an insurance claim, or possible evidence in an arrest or civil lawsuit. Reporting normally is completed as soon as possible following a response. Supplementary reports may be prepared as additional pertinent details concerning the incident are discovered following an investigation.

Events (untoward exceptions) and some incidents may not be reported as a policy of the workplace. And some incidents can be reported directly to the insurance carrier. Regardless, security officers are logical report writers when most security and safety incidents occur because they are usually first on the scene as responders.

Other Important Expectations

The security officer is expected to maintain a suitable appearance at all times, as this reflects positively on his or her employer. Also, personnel who make good impressions are likely to have more positive experiences with the public, thus improving their own self-esteem at work. Security workers often are the first individuals whom the public meets in the workplace. They often serve as providers of general information to the public and are in a position to enhance the public's impression and regard for the organization in the process.

Protective personnel, who have contact with the public, need to be sensitive to individuals who may be impatient, angry, confused, incoherent, and possibly mentally ill. Encounters with such people are exceptional. Yet they do occur and security personnel are the first or among the first workers to encounter such distraught individuals. Dealing with an unpredictable public must be anticipated in training. For the most part, security personnel best serve themselves and the public by being friendly and sincere, remaining calm whatever the mental state of a member of the public, and having relevant knowledge about their workplace. All security employees – proprietary and contract alike – need to make an ongoing commitment to advance the interests of the employer while protecting people, property, information, and other assets.

Finally, the honesty and integrity of security personnel are of utmost importance. Juvenal's query "Who will guard the guards themselves?" appears facetiously in his *Satires*. But a serious implication is clear: protection personnel should be above ethical reproach.

Nonexpectations of Security Officers

Regardless of proprietary or contract status, security officers should not be expected to perform tasks that are not part of their job descriptions. Unless required by an emergency or specifically requested by a supervisor, or both, the security person is not expected to undertake duties normally performed by other employees. This is in part because such diversionary activity prevents the security officer from performing his or her intended functions – that is, deterring, delaying, detecting, responding, and reporting security-related incidents.

Additionally, security personnel are not expected to take unreasonable risks in their tasks or to assume potentially hazardous tasks. Further, security personnel must never usurp the duties of sworn public law enforcement officers. (The exception is a security worker who is also an off-duty sworn law enforcement officer who takes such action in the context of official requirements. Also, some personnel may be trained as special police officers with limited duties of a sworn police officer.) However, in all case, if a simple, brief action by a security officer can correct, improve, or facilitate a situation, such action should be taken as a natural matter of course. This is preferred even if the task would normally be performed by another worker or at times even if the action appears to be against written policies and procedures ([Box 9.1](#)).

Peace Officer Use and Training Standards

In addition to trained security officers, some workplaces will use the services of peace officers, sometimes called special police officers. Peace officers are not sworn police officers who have completed a formal, lengthy training period. They have completed considerably more training than a security officer and may be trained to carry a firearm.

Peace officers contribute to security procedures by performing certain activities not expected by a security guard but maintain part of the same legal powers of police officers. These include the power to use force to make arrests, make warrantless arrests, conduct warrantless searches, and issue appearance tickets. Workplaces use the services of peace officers – generally as proprietary employees – to perform functions that link to police services. For example, if a place of public assembly or a retail complex were likely to arrest persons for illegal behavior, a peace officer can process the arrest according to state law that will aid local law enforcement in completing the arrest.

Because of their far-reaching powers, state legislatures grant statutory authority that permit peace officers to exist and to identify the longer training required. States set their own standards, if any. For example, in New York State, the Municipal Police Training Council determines minimally acceptable training and employment standards for law enforcement officers. This includes peace officers, private security officers, and others. Some characteristics are as follows:

- Instructors must be certified by having completed an instructor development course and having met acceptable instructional skills and educational attainment.

BOX 9.1 FIRE AND SMOKE AND AN EMERGENCY RESPONSE

The emergency: A contract security officer was performing a nighttime patrol of a new high-rise luxury office building, soon to be ready for use. On one floor, the security officer smelled what he thought was smoke coming from under locked doors. The floor was not occupied at the time as the space was being prepared for tenants. The security officer quickly returned to the base and obtained the key for the floor, which had been left with the security officer by decorating contractors who were preparing the new space.

When the officer returned, he entered the floor and found the source of the smoke. Decorators had been staining the new wood panel walls of a conference room. Inexplicably, they had left a heaping pile of used rags soaked with volatile chemicals, on the floor. The rags were smoking and would have combusted. The security officer seized a portable fire extinguisher and began to apply the stream of the extinguisher to the smoldering pile. At a certain point he stopped and called the fire department, which arrived 8 min later. Firefighters further spread and doused the rags and ventilated the area.

The next day, the agent for the building's owner called the contract guard firm to commend the firm for the officer's action. However, the security company manager initially was less than enthusiastic. Written policy directs security personnel to call the fire department first when discovering a fire condition. Then the security officer may return to the location and see what prudent measures could be taken. (Of course, if an actual fire was encountered, the security officer is expected to send an alarm, retreat safely, and then stay available to direct firefighters to the source of the problem.) The contract security manager felt conflicted: Should the security officer be rewarded, or disciplined, or both?

The resolution: The contract security manager discussed the situation with the building owner's agent and a fire inspector. All agreed that the stated written policy was correct: that is, security personnel should call the fire department first when a fire condition is encountered. However, they also agreed that exceptions do exist. In this case, a trained security officer with good common sense determined that a low level of personal risk was acceptable in attacking the potentially dangerous situation immediately. The few additional minutes saved by not contacting the fire department immediately were better used in attacking the fire risk immediately. However, praise and reward for the guard were subdued by the conflict between a sensible written policy and the equally reasonable action taken by an alert security officer. In retrospect, a preferred action might have been for the security officer to call the fire department and wait at the entrance to direct them to the suspicious condition.

- Training facilities must be sufficient for the purposes. Firearms range training (if conducted) must be delivered at appropriate training facilities. Driver training and physical fitness training (if provided) must meet established standards.
- Students who hold a valid Pre-Employment Police Basic Training Course record from an accredited college in the state are not required to complete the entire course. However, within 1 year of appointment as a police officer they must successfully complete 43 hours of firearms (if armed) and impact weapons training.
- Students must attend all sessions of a course and achieve a minimum passing score of 70% on the examination or series of examinations.

- Peace officers may or may not be authorized by their employer to carry or use a firearm. If they are not required to do so, they are not required to complete annual weapons training.
- The basic course for peace officers (not including weapons or driving training) does include 40 hours of interpersonal skills:

Introduction to law enforcement	6 hr
Laws of New York State	44 hr
Law enforcement skills	47 hr
Investigations	2 hr
Total hours required for peace officers	99

Hiring Current Police Officers on an Off-Duty Basis

Proprietary organizations and contract security guard companies may have a strong desire to hire off-duty police officers for part-time duty. They bring with them extensive training, experience and knowledge of the community, and the authority of law enforcement. For decades, off-duty police officers have worked as traffic wardens, and at public events for crowd control. In the last three decades local and state law enforcement agencies have facilitated off-duty assignments for armed personnel in an increasing variety of assignments. But what if a conflict in roles occurs?

Police departments have had conflicts for generations about allowing sworn police officers to work private security details during their off-hours. The issue is murky. For example, can the police department be sued if the officer uses excessive or deadly force while working in a private sector position? The answer is that a police officer does not lose his authority to arrest with probable cause and to use force if necessary. If a police officer working in a private sector capacity uses excessive or deadly force, the police department is a likely defendant in any subsequent civil action.

Searching for Investigators to Find Facts

While investigations may be contracted out, they may also be conducted internally if the capacity to do so exists. Searching for competent outside investigators is similar to the process of selecting a contract security service. Finding investigators with experience in the problem to be resolved is the first step. One's network will lead to referrals. The proprietary security executive meets with a principal of the outside investigative group, discusses the case generally, asks for references and later checks them out, asks about fee structure, and makes a decision.

Also called detectives and fact-finders, investigators are persons who systematically and thoroughly examine and make inquiries into an event. According to J.J. Fay, an investigative survey is "an in-depth probe or test check of a specific operation or activity, usually conducted on a programmed basis, to detect the existence of crime or significant administrative irregularities."⁴ Investigators or fact-finders undertake a wide variety of inquiries. Most organizational investigations deal with business or civil issues, but the private sector

Table 9.2 The Dichotomy Between Criminal and Civil Investigations

Factor	Criminal	Civil
Plaintiff	The state (public sector)	Private and nonprofit interests
Prosecutor	The people	The victim
Main purpose	Punishment of the guilty	Redress of injury
Investigations	By or on behalf of the state	By the victim
Sanctions	Jail, prison	Damages to victims
	Fines	Corrective action or behavior
	Specific corrective activity	
Conviction at trial	Beyond a reasonable doubt	Preponderance of evidence
Appeals	Possible by defendant	Possible by either party

Fundamental differences exist between criminal and civil litigation. A defendant may be sued criminally, civilly, or both, in which case different plaintiffs will bring charges. Private sector investigations normally serve the interests of plaintiffs and defendants in civil litigation. However, private investigators may be hired by the government, when indicated, to collect evidence on behalf of the public sector in criminal cases and administrative issues.

may conduct criminal investigations on behalf of itself or at the request of the public sector. A clear understanding between the two is imperative, and is explained in [Table 9.2](#).

Most private sector investigations concern specific incidents. A loss of assets, contract dispute, or crime may have occurred and facts need to be collected to stop the loss, resolve the contract issue, and, conceivably, conduct a portion of the criminal investigation. Most investigations for security operations, however, involve civil and contractual issues and are not criminal in nature. Retailing is an exception. Such investigations cover a huge range of possible topics, which grow as the nature of commerce evolves. An example is investigation for diversion fraud. This type of loss is a major activity, but scarcely existed a generation ago ([Box 9.2](#)).

Investigations can extend into personal concerns as well as civil and contractual issues.⁵ The following are types of investigations undertaken in the private sector:

- Accidents (aircraft, vehicular, industrial, construction, personal)
- Acquisition due diligence
- Adjustments (in the case of claims for liability)
- Antitrust activity
- Asset location
- Breach of contract (to determine facts and possible damages)
- Competitive information
- Computer crime
- Computer policy violations
- Consulting
- Conversion (controlling another's property)
- Copyright and trademark violations
- Cybercrime
- Electronic countermeasures
- Employee background (also called vetting)

BOX 9.2 INVESTIGATING FOR DIVERSIONARY FRAUD: A PHARMACEUTICAL CASE HISTORY

Often, manufacturers have price agreements that differ for various members of the distribution chain. As part of the agreement to distribute a product, an organization agrees to specific terms with the manufacturer or distributor that usually limit the area into which certain products can be marketed and sold. When such an agreement is broken, the manufacturer is deprived of rightful profits. Similarly, distributors in the areas undersold by rogue distributors lose profits and goodwill. Investigations often identify the source of such illegal practices and stop them.

The pharmaceutical industry frequently is victimized by diversionary fraud. (Similar examples could be cited from numerous other types of manufacturers including software vendors.) Here is how it works: a pharmaceutical company may charge distributors in the United States a particular price for its products. The price of the identical drug may be considerably less for distribution, say, in Central or South America or Africa. This is due to competitive, governmental, and humanitarian reasons. A foreign distributor may order the product from the manufacturer in the United States at the favorable foreign price and then scheme to divert the product back into distribution channels within the United States. This undercuts profits to both the manufacturer and American distributors of pharmaceutical products.

When the US pharmaceutical manufacturer discovers price undercutting in its normal distribution channels, an investigation is in order. Fact-finding is needed to ascertain the losses and identify the likely source of the product diversion. Investigators must become familiar with manufacturing codes and packaging variations in order to identify diverted products. They must gain access to pharmaceutical buyers for hospitals, drug chains, and other distributors in order to develop leads. Often, they must seize the back-channeled merchandise. At other times, they purchase products that do not belong on the premises of the organization they are visiting and hold such materials as evidence against the offender.

By collecting all the facts possible in a case, the investigators, in cooperation with management, are able to quantify the extent of the diversionary fraud. This may be the basis for a civil action against the offenders. When the facts are indisputable, the chances for a resolution favorable to the victimized manufacturer are good to excellent. Yet no recovery would be possible without the creative and persistent efforts of investigators – proprietary or contract – evaluating the problem and collecting facts.

(Source: Security Letter, Part I, July 16, 1984, pp. 2–3.)

- Espionage
- Fire incidents
- Fraud
- Injunctions
- Insurance claims or counterclaims
- Inventory shortages and shrinkage
- Locating lost individuals
- Marine investigations
- Mergers and acquisitions
- Negligence

- Personal injury
- Patent infringements
- Polygraph examinations
- Product liability
- Property and equity claims
- Public records searches (vital statistics, assets, credit, crime, debit, education)
- Return fraud (in retail environments)
- Security surveys
- Sexual harassment
- Social media checking
- Surveillance
- Trial preparation
- Undercover operations
- Workers' compensation
- Workplace violence

Investigations can occur for any reason that seems to make economic or strategic sense for an organization. The Association of Certified Fraud Examiners divides occupational fraud into the three broad categories (Figure 9.1). Investigative work depends on the experience, training, and abilities of persons available. In many cases, a business or institution anticipates its needs and is staffed with a large cadre of competent investigators. This is the case, for example, in the financial and insurance industries, which face many repetitive and serious types of investigative activities. Most organizations will not possess such depth of available investigators or need to. In addition, the varied nature of the types of business, contract, and institutional problems makes keeping a staff of suitable investigators more difficult. Therefore, organizations frequently turn to independent investigators who specialize in particular types of investigations.

Private Investigations to Enhance Law Enforcement

Investigations conducted in the private sector sometimes are an important part of criminal prosecution. Indeed, if the private sector does not help “make the case,” law enforcement and prosecutors may have no interest in pursuing an incident even if a serious crime has occurred within the workplace. Law enforcement might be loaded with more pressing cases to investigate. However, if the private or not-for-profit (NFP) sector has pulled the facts together on the case, law enforcement might look at the issue as “an easy collar.” Moreover, law enforcement executives understand that cooperation with the private and NFP sectors is essential for good communications.

While it is the duty of the state to prosecute alleged offenders, it is frequently in the interest of private or NFP organizations to conduct at least part of the criminal investigation. Often, a public prosecutor will not accept a case on behalf of the state unless the evidence is sufficiently compelling. Specifically, the state wishes to ensure that an offense has in fact occurred, that the offender has been identified, and that evidence collected for use at court is strong. Otherwise, a private investigator normally does not act as an agent of the

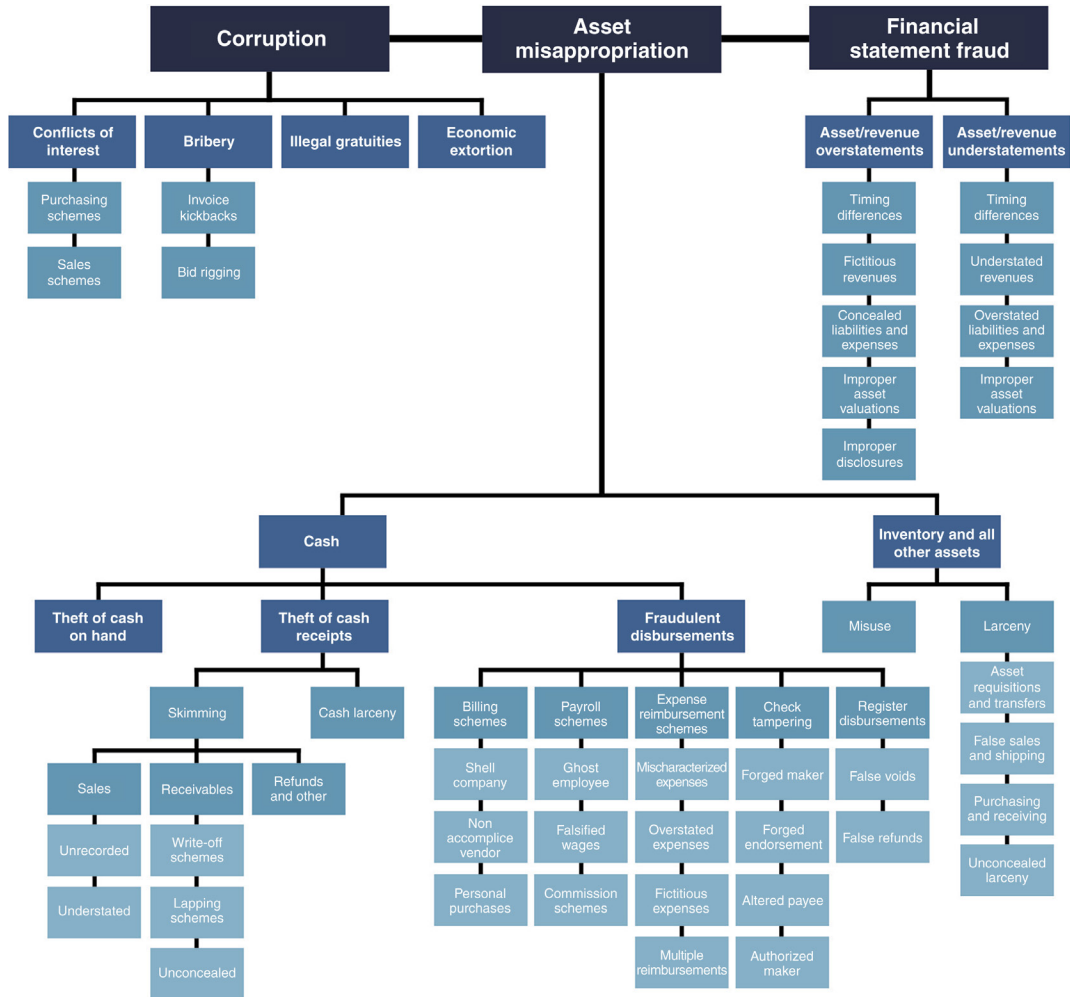


FIGURE 9.1 Investigating occupation fraud and abuse: a classification. Investigations for occupational fraud and abuse in the private and public sectors can involve corruption, asset misappropriation, and financial statement fraud as this fraud tree demonstrates. (Source: Association of Certified Fraud Examiners.)

state and must not imply this. However, he or she may develop the case substantially and turn it over to the police and public prosecutors to facilitate their efforts.

The following are criminal cases in which the private sector plays an active role in the investigation prior to arrest, arraignment, and trial:

- Arson
- Bomb threats
- Burglary
- Cargo thefts

- Computer crimes
- Conspiracy to commit crime
- Criminal defense
- Cybercrime
- Embezzlement
- Employee dishonesty
- Extortion
- Fencing
- Forgery
- Fraud
- Insurance fraud
- Kidnap and ransom cases
- Motor vehicle thefts
- Narcotics/drugs violations
- Organized crime
- Product diversion (transshipment)
- Shoplifting
- Substance abuse
- Terrorism
- Theft (personal, commercial, institutional)
- White-collar crimes
- Workplace violence

The Importance of Investigations in IT Crimes

Protection-related issues constantly evolve. In the twenty-first century, risks associated with information technology (IT), including communications, have taken on great significance. Chapman and Zwicky note: “The Internet is a marvelous technological advance that provides access to information, and the ability to publish information, in revolutionary ways. But it’s also a major danger that provides the ability to pollute and destroy information in revolutionary ways.”⁶

The IT revolution has produced a new category of deviance called “cybercrime.”⁷ Such crimes include extortion, boiler room investment and gambling fraud, credit card fraud, pyramid schemes, fraudulent transfer of funds, telephone fraud, and sex crimes. Additionally, denial-of-service attacks, privacy invasions, attacks by high-energy radio-frequency guns, commercial software piracy, and attacks by computer viruses all require systematic investigation to identify offenders and reduce chances of future recurrence. The alleged inadequacy of IT security can result in civil litigation. In one case, *Schalk v. Texas*, the defense argued successfully that the plaintiff had not taken sufficient due care to protect information that was stolen from a computer system.⁸

As with other types of offenses, IT crimes and attacks require postincident and pre-trial investigations. Generally, computer crime investigators and auditors specialize in this

area. In short: “Information created and used in organizations reflects all the intellectual property, competitive intelligence, business transaction records, and other strategic, tactical, and operating data for business and people. Regardless of industry, managers in organizations today need some understanding of how to protect these information resources, as well as their personnel.”⁹ Investigations frequently are part of postincident fact-finding necessary to build stronger systems.

Nonexpectations of Investigators

While exceptions exist, the investigator generally is not expected to arrive at a final conclusion relative to the point of the investigation. Rather, the supervisor of the investigation, or another person for whom the investigation is being performed, should review the facts and all other pertinent information and then make a conclusion about the central question. For example, an investigator may collect extensive information, both positive and negative, relative to an applicant in a background investigation. But the final decision on extending or not extending an employment offer is best left to others. The opinion of a seasoned investigator generally is welcome. But the hiring decision is ultimately the responsibility of a person who considers more factors than those unearthed by the investigation alone and assesses those facts within the general context of all that is known about the applicant.

An investigator also has ethical and legal obligations in providing services to the employer, which also extends to individuals who may be subject to the investigation. For example, federal rules of entrapment apply to private security agents.¹⁰ In particular, it is unethical and illegal for an undercover security agent to originate the idea of committing a crime. Such felonious notions should originate solely with suspects. An undercover agent can appear to be a willing participant in a criminal or improper act, but he or she must not step over the line and actually initiate a crime.

Trends in Proprietary and Contract Security

The necessity for security in the workplace has grown for several reasons, as discussed earlier in this book. In the year 2014, the aggregate employment of security personnel in the United States reached an estimated 2.1 million persons. This compares with about 750,000 sworn employees in law enforcement at the local, state, and federal levels. This trend represents a long period of growth in private security in absolute terms and also relative to law enforcement. Meanwhile, the structure by which those security services are being delivered to the workplace has also changed.

Proprietary Security Strategy

Private guards employed to protect individuals and private property have been used at least since the time of the Egyptians, when guards protected tombs and tomb sites.¹¹ In Psalm 127, Solomon observes the importance of security in urban life, though holding the security guard

as being inferior to divine presence: “Unless the Lord builds the house, those who build it labor in vain. Unless the Lord watches over the city, the watchman stays awake in vain.”

With the arrival of the Industrial Revolution, the scope of private protection grew enormously.¹² Protective personnel served employers in piecemeal, temporary assignments as the need for protection existed. Security personnel came to be required on a permanent basis because industrial operations had increased beyond small, discrete businesses into those involving hundreds of workers, sometimes working round-the-clock shifts. Further, as industrial production increased in scope, work became more specialized. Whereas the protective function initially was fit for anyone who could threaten possible malefactors away, it later became the task of individuals assigned to that particular process. Agents were hired to protect people and assets when risks were greatest.

Proprietary security began in the early nineteenth century in the United States as a means of general deterrence against crime, vandalism, and fire. In the second half of the nineteenth century, security agents protected industrial facilities against threats such as external and internal theft, vandalism, and sabotage, especially during times of labor unrest. During World War I and II, private security was responsible for heightened proprietary and vital information control, both as anti-espionage measures and as means of protecting industrial know-how. In the last 30 years of the twentieth century, physical protection remained an important facet of the security industry. In the twenty-first century, protection on people and physical assets continues, although the importance of IT-oriented risks and threats to intellectual assets have enormously shaped the way in which proprietary security is now structured in the workplace.

Several aspects of monitoring a proprietary security program have been covered in previous chapters. The following section will consider further operational management aspects of security personnel activity.

Scheduling Requirements

In the process of analyzing security tasks to be performed, security managers must determine the number of personnel required and the hours for which they will be deployed. The complexity of this issue is based on the size of the program, its geography, and the level of training required. In earlier years, security directors faced the tedious task of preparing scheduling plans on paper forms or chalkboards. The scheduling information was constantly being changed; therefore, the information had to be erasable to accommodate the new changes. Security directors frequently delegated the scheduling details to clerks who kept master records and distributed them to supervisors and area managers on a periodic basis. Derivative reports dealing with shift rotations, work locations, and event scheduling were made from the master schedule.

Software programs and services now are written specifically to help schedule security personnel.* Scheduling time has been cut, saving considerable clerical costs in the

* Examples include CCS Security Guard Management System from Complete Computer Service Ltd., Farmington Hills, MI; InTime Officer Scheduling from InTime Solutions, Inc., Burnaby, BC; and Security Management Systems (SMS) from Valiant Communications, Inc., Woodbury, NY.



FIGURE 9.2 Using biometrics to coordinate with time and attendance. Workplaces are able to obtain time and attendance data remotely. This system uses facial recognition technology along with precise location services using GPS, IP addresses, and cellular triangulation to provide assurance that the security officer is reporting in where he or she is expected to be. Information collected from the worker's biometric input is the basis for time and labor management and payroll. (Source: Valiant Solutions.)

process; schedules can be displayed graphically and changed with ease; and relevant information on security personnel can be instantly available. These software programs can help control overtime costs. They can also link to most software systems operated by human resources services. Billing errors are reduced. Management may review assignment plans over the Internet, while information can be linked to other management and financial controls software packages, further reducing time and costs. Security personnel may be able to access their schedules through their own smartphones or Internet-based mode. [Figure 9.2](#) shows an example of such a software package. These software packages can be learned in a short time. Managers and supervisors can create useful supportive reports such as those indicating guard availability and unavailability, scheduling conflicts, and assignment or customer work history data. They can also create “barred-from-customer” conflict lists and seniority lists. Exceptional circumstances such as holidays or client issues can be flagged within the program. Automated officer check-in systems allow managers the opportunity to be assured that security personnel are at their posts.

Management's support for such software packages is enhanced by their additional features. Costs are saved because the schedules are prepared much faster than the previous manual process. However, further cost savings result from the reduction of overtime by better monitoring of hours and separate links to payroll, invoice creation, accounts payable, accounts receivable, and general ledger software programs.¹³

Determining Personnel Needs for Posts

As a rule of thumb, managers require the equivalent of 4.2–4.5 persons to be available to staff each post on a 24-hour 365-day basis, assuming a 40-hour workweek. Complications in

planning occur because of vacations and other schedule changes, such as illness or personal time off. Consequently, an adequate pool of full- and part-time security personnel needs to be available to fill the requirements of large security programs with 24-hour posts.

Salary and Compensation

Money is not the only motivator for workers. It is, however, the most important one. Managers have to keep within their allocated budget guidelines, constantly improve services, and control payroll costs. The average (median) hourly pay for security guards varies widely based on geography alone. In some programs, average pay for security personnel will be consistently below average. In others, it will be within the midrange, and in still others, average compensation will be above average.

Managers can determine the average hourly pay for security officer services from data collected by the Bureau of Labor Statistics of the US Department of Labor.¹⁴ These reports are prepared by the Office of Compensation and Working Conditions in cooperation with the Office of Field Operations and the Office of Technology and Survey Processing. The data may be months old when a manager accesses the latest report for a particular region and therefore the rates need to be adjusted for any circumstances that may have changed. The information is national in scope and covers private and public positions. Scores of employers provide reasonably accurate base salary data to the survey, thus revealing the normal hourly compensation for 150,000–250,000 security officers. Managers can turn to this source to judge their own compensation programs relative to other employers in varying regions.

Compensation ranges for security supervisors, investigators, specialists, managers, and executives are equally important in determining the costs of operating a department. Such information can be obtained from compensation studies specializing in the security, protective services, and law enforcement categories.¹⁵ Compensation services are available that provide guidelines that can be used for setting compensation ranges.[†]

Managers can reduce operational costs for salary and benefits processing by using software dedicated to the tasks. Alternatively, the activity can be turned over to an outside service bureau that handles the requisite administration.

Contract Security Services

As previously discussed, the trend in recent decades has been for operating entities to contract out numerous types of services. The scope of such services is broad and includes diverse temporary help, technical services, entertainers, drivers, hospitality industry workers, janitorial workers, home healthcare workers, agricultural workers, and property managers. However, one of the largest contract services is security personnel. In fact, it may also be the earliest organized service industry. The Pinkerton Agency contracted out armed security guards to packing plants and commercial houses beginning in 1858.¹⁶

[†] Examples are as follows: www.acsbenefits.com, www.payscale.com, and www.iconixx.com.

By the end of the nineteenth century, scores of security services businesses could be found in urban America.

The concept of “employee leasing” has many attractive features in that the leasing firm must assume numerous accounting and administrative duties on behalf of the workers.¹⁷ Requirements for the administration of records and benefits are regarded as particularly burdensome to small businesses or those with temporary operations. The employer might have to:

- Maintain tax deduction records
- Compute tax liabilities and make timely bank deposits
- Respond to garnishment from the court or other taxing bodies
- Conduct audits for workers’ compensation benefits
- Conduct audits for unemployment claims
- Provide healthcare benefits
- Comply with Consolidated Omnibus Budget Reconciliation Act (COBRA) legislation (1986) requiring employers with more than 20 employees to offer continuation of healthcare coverage in the event that an employee is terminated or experiences another qualifying life event
- Manage a 401(k) program
- Reconcile employee paychecks
- Post records for state and federal taxing agencies
- Prepare workers’ year-end W-2 filings
- Maintain vacation and other authorized leave benefits
- Maintain payroll and tax changes
- Answer questions from workers on regulatory, pay, and benefits issues

Employers usually must provide such services to proprietary workers as a matter of course, and this includes security personnel. However, when such duties are transferred to an outside organization, the primary organization is relieved of these duties and related costs. Yet contract security programs are differentiated from proprietary ones on more substantive issues than who will be responsible for routine administrative issues. These issues were discussed earlier in this chapter.

Insurance for Security Services

Proprietary organizations include insurance coverage for all activities, including those within the security department. However, the use of contract protective services requires the workplace to understand some of the factors of insurance.

The actions of security officers, armored car services, investigators, alarm monitoring businesses, and other protective personnel are insured under the organization’s liability insurance coverage. Most of these organizations will turn to their commercial insurance broker for coverage. The broker in turn will seek quotations from a managing general agent (MGA) who has created a program with an insurance company. Technically, the MGA engages in a *treaty* with the insurance company to screen businesses before placing the

insurance. The insurance company will retain some of the risk, share part of it with other insurance companies, and perhaps place some of the risk with a reinsurance company.

The principal factors in liability coverage are coverage (what the liability policy will actually pay for in the event of a claim), limits (how much per occurrence and aggregate limits), deductible (the extent of self-insurance), and the premium (what the insured will pay per year for the coverage). Liability insurance is usually rolled over on an annual basis, but occasionally on a semiannual schedule. Some features for security guard, investigator and security consultant professional liability, alarm/security system installation and monitoring, closed-circuit television (CCTV) installation and monitoring firms, armored car services, and other protection-related businesses are as follows:

- General liability – assault and battery, false arrests, invasion of privacy, malicious prosecution, personal injury, and other potential reasons that could bring a civil action against employees or a security services business. Most clients will demand a minimum of \$500,000 per occurrence and \$1,000,000 aggregate. However, \$1,000,000 per occurrence and \$3,000,000 aggregate can be available as the initial limit of security.
- Errors and omissions (E&O) – including professional liability and possibly financial loss.
- Vicarious liability – intentional or criminal acts by an employee.
- CCC broad form property damage – damage to property in the care, custody, or control of the insured.
- Limited theft coverage.
- Incidental medical malpractice.
- Lost key coverage – in the event a master or sub-master key is lost and a system must be rekeyed, coverage is available in some policies.
- Electronic data liability.
- Umbrella coverage – excess and commercial umbrella liability coverage in addition to the primary level of coverage. This coverage can have a limit up to \$5,000,000; however, far greater limits can be written if the client requires it.
- Business auto – including security vehicles.
- Third-party employee dishonesty – if the general liability policy or standard fidelity bond does not cover dishonesty from a third-party employee, this coverage can be purchased separately.
- Commercial property.

Typically, the security services business will seek to obtain two or more quotations. The result is rarely apples for apples. Such factors in the case of a security guard operation as crowd control, working where alcohol is served, and the quality of personnel are among the factors that could impact the insurance premiums. Each quotation will have its own characteristics. The decision maker will consider the service reputation of the insurance provider. Equally important is the quality of the insurance company backing the policy. A client of a security company normally will expect a company rated A (excellent) class XV

(\$2 billion or greater in strength) in Best's *Key Rating Guide*. When the customer selects a security vendor, depending on the type of business, it could be important to have the business specifically listed on the certificate of insurance that will be delivered before security services commence.

Selecting Contract Security Services

The process of selecting a contract security service may be uncomplicated for small and simple organizations. However, it can be a formal and extensive process for large, complex organizations. This topic is being discussed because one of the biggest budget items in many security departments is contract personnel. The following sections discuss these two scenarios.

Small, Simple Programs

Employers requiring one or more security officer for an assignment that involves visible patrol begin the process by preparing a report or memorandum in which the specific tasks of the required security personnel are outlined. This need be only two or three pages long, but it should provide the basic vital information required by a contract security firm to make an informed proposal. This report should include the number of security personnel required, the type of vetting to be performed, the training to be completed prior to assignment, the duties to be performed, the nature of experience desired, the hours to be worked (including any exceptional circumstances), the type of uniform desired (traditional guard, military style, or blazer and slacks), the extent of the insurance to be provided, and the field supervision to be offered.

Additionally, the prospective employer should consider the level of pay desired for the security personnel, including projected increases over the length of the contract. This information will be sufficient for the prospective bidders for the contract to prepare a proposal. Many other nuances to the selection process may come up later, but the basic material just described will start the process for the contract proposal for a protective program requiring contract security officers.

The next step is to interview three to five security guard firms. Typically, a client wanting security officer services will seek to meet with one to three national security services firms and one to three local, independent security services providers. In some areas, the number of choices will be limited. In addition, many established security firms may not choose to pursue the business of an operation that offers little opportunity for growth and that does not provide the contract firm with its gross profit target.

The proposed service providers may be selected by references from colleagues who manage existing locally respected programs and from local membership lists of professional organizations such as ASIS International, the National Association of Security Companies (NASCO), and the National Council of Investigation and Security Services (NCISS). Additionally, many state associations for security guard and investigative services have

been formed that provide access to responsible potential service providers. It is also advisable to peruse relevant business directories or source books for names of service providers. An initial letter to the identified companies can provide details on the security services required and invite an expression of interest by a particular date. In some cases, security services firms will learn of the search on their own and ask management for the opportunity to be considered. Their enterprise should be recognized. A brief review of the company's capacities should settle if it also can be included among the prospects.

The next step will be to meet with the prospective bidders and provide them with full details on the assignment. For a new security services requirement, it is probably best to meet individually with the prospective bidders. The security firms – individually or as a group – should be able to see the exact area where the security personnel will work as part of a site visit. The prospective security services firms should have time to complete their surveys and have equal access to all relevant details. A date for the completed proposals must be set.

When all the proposals have been received, the client compares and contrasts the various submissions. Sometimes, a modified comparative scale is used to judge the security firm by various objective and subjective criteria. The client may briefly visit the office and training facility of the prospective services provider, and will wish to check references provided. Often, considerable negotiations occur on finer points of the agreement before both parties agree to the terms. When the winner is selected, a contract is signed. The contract is usually drafted by the client. But it may be provided by the security services firm and then must be carefully reviewed by the client, possibly with a lawyer or industry consultant.

Large, Complex Security Programs

Large organizations with formal structures require a much more detailed process to identify and award a contract for security services than the one just described. This is particularly true for institutions and the government, which often issue a request for proposal (RFP) when making selections for security services providers. (Large and medium-sized corporations also use RFPs, or modifications of them, when selecting security vendors.) Larger government or institutional contracts usually attract numerous hopeful bidders. However, sometimes excellent and well-experienced security services providers have to be encouraged to respond to RFP. Thus, RFPs are used both to ensure fairness and to defend against claims of unfair awards. The process is invariably structured with firm dates and specific demands for replying to the RFP. An outline for a formal RFP follows. It provides insight into the types of issues that have occurred in the past when organizations have contracted for protective officer services, experienced difficulties, and wrote specific demands into a formal agreement.

RFPs require effort and expense to prepare. The questions and concerns of bidders should be anticipated in advance, thereby facilitating the selection process. Often, the document begins with a Solicitation Summary, which provides proposed instructions, submission requirements, and conditions. These include such factors as follows:

1. *Statement of purpose.* This states what the task would be for the required security personnel.

2. *Client contact person.* Usually, a single individual is identified for all written or telephone inquiries or contacts. If a potential vendor requests interpretation of the RFP, this request should be placed in writing. The client reserves the right to respond to any and all such requests. Answers to substantive questions are shared with all responders, usually via fax or e-mail.
3. *Submission.* The final proposal usually is sent to a different office and contract officer than the client contact person identified to handle inquiries.
4. *Proposer's conference.* A proposer's conference is set for a particular date, usually in a conference room where all representatives can be accommodated. Proposers may be requested to notify the agency at least 5 days in advance if they plan to attend. Proposed vendors are under no obligation to attend such a conference, but normally they do. Attendance is usually taken at such times. If appropriate, the client will provide a tour of the facility or other detailed information so the vendors are able to understand what posts need to be covered.
5. *Letters of intent.* Proposed vendors interested in submitting a proposal are requested to submit a letter of intent to the agency.
6. *Submission requirements.* This section summarizes what the prospective vendors must prepare and submit in order to be considered. The number of copies of the proposal and the date and hour on which the sealed proposal package must be received by the client are stated.
7. *Modification or withdrawal of proposals.* The costs provided by the bidder to the proposal are deemed to be irrevocable until the contract award, unless the proposal is withdrawn or modified prior to the time or date set as the due date for the proposal and in accordance with the RFP.
8. *Postopening withdrawals.* The client may allow a potential vendor to withdraw its bid only after the expiration of a stated number of days after the opening of the proposals. Such a withdrawal must be in writing and in advance of the actual award.
9. *Late proposals, withdrawals, or modifications.* To prevent charges of unfairness, clients generally do not make exceptions for late proposals, withdrawals, or modifications. An exception is when any modification of a successful proposal makes the terms more favorable to the client than those initially presented. Occasionally, a client may allow a vendor to join the process after it has begun. Such a vendor would be expected to meet all stated submission deadlines and requirements pertaining to other vendors.
10. *Proposers' right of appeal.* The process whereby proposers may protest and appeal decisions regarding the solicitation and award of a contract is identified.
11. *Payment policy.* The customer for security services states when it expects to pay proper invoices, which set forth the description, price, and quantity of services rendered with the appropriate documentation appended. (A generation ago, some security services providers billed clients monthly, in effect giving the client improved cash flow. In recent years, weekly or biweekly billing has become the norm.)
12. *Amendments to the RFP.* If amendments to the RFP occur, all proposers will receive such notifications and must verify that they have received all addenda issued.

13. *Discussion with proposers.* The client may wish to conduct discussions with proposers who have provided the most responsive proposals. However, this discussion is not necessarily required prior to a contract award.
14. *Procurement policy rules.* The RFP may be subject to the rules of procurement by the government agency involved in the bid. In the case of a private organization, it may be stated that the decision to award is left solely to the discretion of the client.
15. *Fairness and ethics.* If any potential vendor feels that unfairness, favoritism, or ethical improprieties have occurred in the proposal process, the vendor may contact the client's attorney designated by name to receive such information.

Elements of a Comprehensive RFP

Following the Solicitation Summary, the proposal then provides considerable depth on the nature of the work to be accomplished by the proposed contracted services. A table of contents may begin the section, listing detailed aspects of the proposal covered in the document. The following is the outline of an expanded RFP, indicating considerations that could be important in completing a mutually beneficial contracting-out process:

1.0 *Introduction.*

- 1.1 *Purpose.* The name of the proposed client and the nature of the security services required are explained. For example, "the client is requesting proposals from fully licensed firms in the business of providing trained, uniformed, unarmed male and female security officers who have had at least five consecutive years of experience in furnishing such services to large institutions, corporations, or government units." The specific nature of the experience expected to be demonstrated by the security services firm is also mentioned.

The length of the contract is indicated (e.g., 3–5 years). The cost proposal must state a rate for each year of the contract. However, the client may wish to retain continuance of the contract for one to three 12-month extensions beyond the initial period at the client's discretion. The date at which the contract is to begin is indicated.

- 1.2 *Background.* This section describes the nature of the client's organization and states the importance of security in the view of management. Further details on the type of work generally provided by the organization may also appear in this section or be made part of the RFP packet provided to interested proposers.
- 1.3 *Specific facilities.* Next, the RFP will list all the facilities to be covered in the contract. It will include address, type of activities, number of employees working at the location, and any special features of concern from a security standpoint. If any physical changes in the nature of these facilities are anticipated within the life of the contract, they should be identified.
- 1.4 *Security issues.* A statement or section about the nature of the most significant security issues requiring management may be included here. For example, such issues as fire watch, employee theft, outsider theft, meeting and greeting the public, and emergency response capabilities are quite distinct activities and require that

the security firm consider them thoughtfully in arriving at a bid proposal that would provide security officers who had the required skills.

- 1.5 *Services needed at the facilities.* Following from the previous section, this section identifies the serious problems that have occurred in the facilities in the past. A potential risk occurs if the RFP fails to identify serious crimes and incidents that have happened, say, in the past 3–5 years that would affect the nature of the staffing required. Specific details do not need to be presented in the RFP; however, the document needs to identify the major issues that have been the focus of security in the past. If the facility is new, the RFP will identify the nature of the problems management expects the security services firm to be able to handle. How the client has dealt with these incidents elsewhere in the past may also be explained.
- 2.0 *Scope of services.* In RFPs for large and complex operations, it is possible for the organization to organize the work for one contract firm, several firms, or a combination of contract and proprietary services. The way management expects to divide such services may be identified here.
- 2.1 *Minimal specific tasks and requirements.* The writers of the RFP are not in the position to instruct the security services firm on how to do their job. Rather, the RFP writers can describe what the job involves and ask how the security supplier plans to meet the client's security objectives. For example, the RFP may identify specifically the salient issues of greatest concern to it:
 - Protecting staff, customers/clients, vendors, and visitors against malicious injury
 - Protecting the premises against theft, pilferage, vandalism, damage, or destruction
 - Permitting only authorized persons to enter protected areas
 - Responding to an alarm with a protocol set by customer
 - Reporting to the client all violations of regulations that are the nature of written reports
 - Operating and monitoring a comprehensive CCTV and communications monitoring center
 - Operating and using X-ray, walk-through, and handheld metal detectors at entrances to the facilities
 - Patrolling areas of the facilities including perimeter walls and fences, building exteriors, parking lots, roofs, main floors, corridors, stairwells, restrooms, and basements
 - Observing and reporting at assigned locations activities that can lead to improved security performance
- 2.2 *Guidelines for guards.* In this section, the client indicates the minimum expected guidelines of the services. The following are examples that may be cited:
 - Contract security personnel must view the safety of all site employees, visitors, vendors, and others on or near the premises as their main duty.
 - Security officers shall challenge all persons entering protected premises for proper authorization and identification prior to entry.

- In facilities deemed part of the nation's critical infrastructure, security officers should be alert to exceptional circumstances that may pose a threat and be prepared to respond reasonably.
- X-ray, walk-through, and handheld metal detectors and other physical security devices, where provided, may be used to process individuals who enter the facility.
- Doors, windows, and other portals must be secured when required.
- All incidents must be reported to the local director or site supervisor.
- A security logbook must be maintained.
- Contract security personnel must adhere to any site policies as prescribed by the local manager or other officials in charge.
- Contract security personnel should safeguard from damage all equipment, systems, and property on the premises.
- Contract security personnel must provide only general information to the public, such as directions and locations of various offices. At no time will contractors' employees be permitted to discuss with the public operating activities at any of the client's sites. Such a discussion may serve as a breach of security of the site and of the organization.

2.3 *Requirement for incident reports.* A policy on incident reports may be expressed:

- Unauthorized intrusion, trespassing, or other illegal entry onto the site.
- Any criminal or unlawful act that has been committed on the site.
- Any assault, altercation, or confrontation that results in any injury.
- Any emergency responses to the site by fire, police, emergency medical, or government agencies.
- Any safety or health hazards observed by the security officer.
- Any exceptional incident that could require a claim against management or that would require further investigation on the part of the client's management.
- No information contained in an incident report or brought to the attention of the security officer at the site shall be disclosed to third parties without expressed consent of site management.

2.4 *Vendor responsibility.* The following vendor responsibilities may be mentioned in this section:

- *Continuity of services.* It is vital that security services be provided without interruption to the client. Accordingly, the security services provider must propose how to assure coverage in the event of strikes, work stoppage or slowdowns, or in other situations in which services and operations may be disrupted. If the security firm is unionized, for example, the vendor might report that "a no-strike provision" is part of the agreement. Alternatively, a statement on labor/management working relationships – hopefully harmonious – may be included.
- *Provision for female security officers.* The security services provider may be expected to provide a certain minimum number of female officers depending on the locations and the nature of services to be provided.

- *Uniforms and equipment.* The following uniform and equipment guidelines may be mentioned in this section:
 - a. The contractor must furnish and ensure that each security officer wears a uniform in compliance with any state and local regulations. Security personnel should present a neat and orderly appearance at all times during the performance of their work. Proposers should identify details of their uniform options in the proposal. Alternatively, the client may prescribe special clothing to be worn by security personnel and may indicate whether the client will pay for the clothing or if it is to be included in the proposer's fee.
 - b. At no time shall firearms, knives, or other unauthorized instruments or tools that might be used as a dangerous instrument or weapon be carried by security personnel.
 - c. Supervisory personnel shall wear a uniform that distinguishes them from subordinate security personnel.
 - d. Security personnel shall exhibit identification credentials, as prescribed by the contract, in order to gain access to the facility for the performance of work.
 - e. Each security officer shall be furnished with a two-way radio, beeper, cellular phone, or laptop computer that is Wi-Fi ready. The purchaser may require a primary and a redundant communications system for each officer. Inoperable devices must be replaced immediately. The equipment shall be in working order at all times. The provision to safeguard and recharge the equipment remains the responsibility of the security services provider.
 - f. Security personnel responsible for the operation of security systems shall be held responsible for the systems' security and care. Any unreported or unexplained damages to such systems shall be deemed the service provider's responsibility.

3.0 *Guidelines for proposal preparation.*

3.1 *Proposal content.* The proposal specifically must explain how certain tasks will be handled. This content should include the following:

- The specific security tasks that will be performed by security officers
- The monitoring and supervisory control of the workforce
- A description of the training program to be provided to security officers and supervisors
- A security management assessment for the location – or part of the location – needed to adequately secure the facility
- The internal controls that will be exercised by the security services firm over the officers and their supervisors
- The security officer standard measures required to provide adequate security
- The measures to be taken to protect employees and visitors against malicious injury and to protect the premises and property against theft, pilferage, vandalism, damage, and destruction
- The means of securing and safeguarding documents and records

- Procedures for reporting, preparing, and maintaining logbooks, forms, and records
- Procedures and methods for excluding unauthorized persons
- Access control and security procedures for storage and equipment
- Details of uniforms to be furnished to and worn by security officers
- How the service provider monitors statutory requirements for annual training, if any
- Strategy for keeping security personnel updated on new technology, regulations, and procedures that could be pertinent to the assignment
- Any other security measures appropriate to the client and its sites

3.2 *General information.*

3.2.1 *Conflicts.* If the proposer feels that any part of the proposal appears to be in conflict with another part, or if an aspect of the work to be performed is unclear, the proposer should ask the potential client for clarification. If relevant, this elucidation will be shared with other proposers.

3.2.2 *Inspectors and tests.* The proposer should be aware that all personnel and equipment may be subject to inspection, examination, or test by the client at any time during the course of the contract. The client shall have the right to reject unqualified personnel who do not comply with the guidelines and requirements of the contract. Similarly, unsatisfactory equipment or materials may be rejected by the client.

3.2.3 *Supervision by contractor.* The proposal shall indicate in what manner a representative will supervise the work that his or her staff is performing to ensure the firm's complete and satisfactory performance in accordance with the terms of the contract. The representative shall be authorized to receive and put into effect promptly all orders, directions, and instructions from the client.

3.2.4 *Adequate and competent supervision.* The proposer shall provide, as part of its contract and at no additional cost to the client, a visiting site manager. The site manager should visit all facilities at least once during an 8-hour tour to assure that quality security services are being provided. The site supervisors shall have a minimum of 2 years' experience as supervisors in security-related or law enforcement positions prior to being assigned to the client.

3.3 *Additional requirements.*

3.3.1 *No arrest policy.* Security services personnel must not make any arrests without the expressed consent of the chief or director of security. Security services employees shall not sign a complaint on behalf of the client or sign any request to do so by governmental authorities.

3.3.2 *Tour limitation rule.* Security services employees should not be on duty in excess of 16 hours per 24-hour period or in excess of 60 hours per week. Each security officer shall have a minimum of 24 consecutive hours off each week. Any hours in excess of the above-stipulated maximum shall not be billed to the client.

3.3.3 Overtime pay policy. In the event of an emergency or other contingency requiring guard service for a period in excess of the stipulated shift, payment for such services shall be at the same rate as the standard contract rate. This provision will not apply if the contractor has not been notified at least 8 hours prior to the start of the shift, in which case the contractor shall receive the rate of one-and-one-half times the regular rate for that shift. If overtime is caused by the security services firm and is not attributable to the client, the service firm shall not be entitled to any overtime rate.

3.3.4 Training agreement. The proposer must provide a training program for its employees at no cost to the client. All employees must complete the training program prior to assignment. Such proposed training must consist of (a stated number) hours of training. The curriculum for the training and the resources used must be approved by the client prior to beginning such training. The client retains the right to provide part of the training prior to assignment.

3.3.5 Right to audit. The client reserves the right to audit relevant security services providers' financial records related to the contract to assure compliance.

3.4 Standards for workforce.

3.4.1 Education and background requirements. Proposers should offer security officers and supervisors who meet the following minimum requirements: at least 21 years of age; high school diploma or General Educational Development (GED) testing; at least 3 years, alone or in combination, of (1) satisfactory prior work experience in a security-related field or human care-related area; (2) military service; or (3) satisfactory completion of college-level study. Security officers with records of criminal convictions will not be satisfactory to the client. (However, minor traffic violations or misdemeanors not relevant to the assignment of some years earlier may not disqualify the officer for consideration.) In fulfilling the contractor's obligations under this requirement, the contractor shall comply fully with all laws of the state and disclose pertinent information to the client. Security officers shall be in good general health without abnormalities that would interfere with the performance of security duties, and must be capable of performing normal and emergency tasks requiring moderate to arduous physical exertion. Medical fitness is to be determined by a medical examination conducted and documented within 90 days prior to entry on assignment. Security officers must speak and write English intelligibly. They must be citizens of the United States or possess acceptable alien registration documentation. Documented proof in the form of true certified copies (i.e., birth records, diplomas, military discharges) and previous employment verification should be maintained in a permanent personnel folder for officers. The folder will include training records.

3.4.2 Hiring and replacing personnel. The contractor shall be required to provide the client with the names of all newly hired officers. The personnel dossier of each newly hired officer shall be provided to the client before the officer is assigned

to a post. The contractor shall provide a certification for each individual officer stating that he or she meets all contract requirements. The contractor shall provide the certification with the officers' folders for review prior to the beginning of their employment at the client's site for the first time.

- 3.5 *Information on the security services provider.*** The contractor shall provide the client with comprehensive information on the fitness of the contractor to perform the proposed contract. This information shall include historical information on the contractor; an organizational chart; résumés of the contractors' principals and managers in charge of the contract; a list of the board of directors; a list of current contracts including a contact name and address and the date on which service began; and letters of support/recommendation concerning the contractor.
- 4.0 *General guidelines for submitting proposals.***
- 4.1 *Letter of intent.*** Prospective vendors shall submit a letter indicating their intent to submit a proposal by the deadline stated in the Solicitation Summary at the beginning of the RFP. Letters of intent are not binding, and proposals received by the stated deadline from proposers who did not file a letter of intent will still be considered. The letter of intent should identify the name of the proposer, plus the name, location, and telephone number of an authorized representative and any proposed subcontractor.
- 4.2 *Application deadline.*** Proposals should be filed by the close of business on the date of the deadline stated in the Solicitation Summary. Proposers who mail their proposals should allow sufficient mail delivery time to ensure receipt of their proposals by the deadline. Delivery is the sole responsibility of the proposer. All appropriately filed proposals will be acknowledged in writing.
- 4.3 *Questions.*** Written questions are to be submitted to the client contact listed in the Solicitation Summary. Answers to all questions, as well as copies of the questions, will be provided to all proposers unless, in the opinion of the client, a question is of such a nature that it is proprietary to the asking proposer.
- 4.4 *Proposals or declinations.*** It is requested that the client receive responses, either proposals or declinations, from all parties receiving the RFP.
- 4.5 *Restriction on contact with the client's employees.*** From the issue date of the RFP, all contacts with the client's personnel must be cleared through the client contact.
- 4.6 *News release.*** The proposer shall make no news releases pertaining to this project without prior client approval.
- 4.7 *Proprietary information.*** All proprietary information submitted in the proposal that the proposer desires to remain confidential shall be indicated clearly by stamping the word "Confidential" on the top and bottom of pages on which such information appears. For those proposals that are unsuccessful, all copies of such confidential information shall be returned to the proposer.
- 4.8 *Contract award.*** The client reserves the sole rights to judgment and acceptance of the vendor's proposal. After the proposal(s) has/have been selected, the name(s) of the successful applicant(s) will be disclosed. On selection, the successful applicant(s) will be required to execute a contract with the client. In general, contracts will be

awarded to the qualified proposer whose proposal is most advantageous to the client in terms of quality, cost, and other factors. The contract to be entered into between the client and the successful proposer shall contain negotiated provisions based on the specific requirements set forth in the RFP, and on the successful proposer's treatment thereof, as contained in the proposal.

- 4.9 *Reservation.*** Notwithstanding anything to the contrary, the client reserves the right to reject any and all proposals received in response to this RFP; may select for contract or for negotiations a proposal other than that with the lowest net cost; can wave or modify any informalities, irregularities, or inconsistencies in proposals received; could negotiate on any aspect of the proposal with any proposer; may negotiate with more than one proposer at the same time; and shall terminate negotiations if a satisfactory agreement is not reached.
- 4.10 *Site visit.*** Proposers must inspect the client's named location(s) prior to the submission of their proposals.
- 4.11 *Oral presentation.*** Proposers may be required to give an oral presentation to accompany their written submission.
- 4.12 *Incurring costs.*** The client is not responsible for any precontract activity or costs incurred by applicants in the preparation of their proposals.

5.0 *Selection of vendor.*

- 5.1 *Method of selection.*** The client will evaluate all proposals and select the proposal(s) that it deems most beneficial. The quality and appropriateness of security operations will be evaluated first. Proposals meeting minimal acceptable standards will then be considered for overall costs. The final selection will be based on the combined merits of both the quality and pertinence of security services and the fee proposal. The evaluation will include the following criteria:
 - ***Organizational capability and quality (25 points).*** Prior experience of the proposer in similar undertakings and the quality of such work must be demonstrated. Proposers should submit evidence of managerial effectiveness in this field for the previous 5 years or more. Proposers also should provide documentation regarding their proposed team/organizational structure to oversee the scope of work required in the RFP.
 - ***Understanding the need of the client (10 points).*** This criterion is to be scored based on the proposer's ability to appropriately use required staffing, resources, and planning to address the nature of the client's unique needs.
 - ***Recruitment strategy and planning (10 points).*** Proposers should submit a complete plan for the recruitment of qualified security officers and supervisors for the duration of the contract.
 - ***Qualifications and experience of the proposer's personnel (10 points).***
 - ***Training plans, curriculum, and training capability (10 points).***
 - ***Supervisory control (10 points).*** Proposers should submit detailed job descriptions of the supervisory position, including span of control, and the method of disciplinary action for security personnel assigned to them.

5.2 Rating system. Proposals best meeting the minimal acceptable requirements on a 75-point scale will then be considered for their overall cost proposal.

6.0 Payment. The client agrees to pay the vendor on a timely basis from weekly invoices, which shall be submitted accompanied by attached original time sheets signed by the site director or designee. (Electronic verification of work performed certified by the contractor may be acceptable.)

7.0 Liquidated damages/adjustments of compensation.

7.1 General provisions. On the occurrence of any of the acts or omissions listed below, liquidated damages may be assessed daily against the contractor in the amounts indicated for each occurrence and for each day, starting from the day the occurrence commenced to the day the irregularity is corrected. The amount of assessment will be paid by the contractor or deducted from the contractor's invoices. (The dollar amount is not a standard and is included for reference purposes only.)

7.2 Liquidated damages: \$350 per day. Liquidated damages may be assessed against the contractor in the sum of \$350 per day per occurrence for each of the following acts or omissions:

- Failure to provide a security officer who meets the criteria specified in the contract.
- Failure to provide a site supervisor who meets the criteria specified in the contract.
- Failure to maintain complete personnel records folders for employees specified.
- The contractor's employees engage in a strike, work stoppage, or slowdown at the client's premises (a fee is assessed for each employee).

7.3 Liquidated damages: \$200 per day. Liquidated damages may be assessed against the contractor in the sum of \$200 per day per occurrence for each of the following acts or omissions:

- Failure to provide a visiting site manager who does not visit at least once during every tour as specified in the contract
- Failure to provide a site supervisor at each client location for each shift, covering 7 days per week
- Failure to provide security services in an emergency or other contingencies for a period in excess of the stipulated shift hours as specified in the contract
- Failure to notify the client of the names of security officers newly hired and assigned and to provide their personnel folders for review as specified in the contract
- Failure of the contractor's employees to obtain approval from the client prior to signing a complaint on behalf of the client

7.4 Liquidated damages: \$100 per day. Liquidated damages may be assessed against the contractor in the sum of \$100 per day per occurrence for each of the following acts or omissions:

- Failure to train guards required for a post or shift as required by the contract

- Failure to maintain complete records of all hours each security officer assigned to the client's premises is engaged in, for which work is computed on the basis of actual hours worked
 - Failure to assign a correctly dressed security officer
 - Failure to replace any security officer within 8 hours on request by the client
 - Failure to submit oral or written reports of incidents occurring on the client's premises to the client
 - Failure to provide each security officer with required and working equipment
 - Failure to report in a timely fashion missing fire extinguishers, smoke detectors, hazardous conditions, or exceptional occurrences as specified in the contract
 - Failure to properly maintain the security officer location logbook as specified
- 7.5 *Incomplete shift penalty.*** Failure to provide a security officer at a specified client location on time or the early departure of a security officer from a specified client location will result in an agreed-to hourly assessment.
- 7.6 *Improper assignment penalty.*** If the contractor assigns a security officer to the client's premises who, it is later determined, has a criminal record, the total paid to the contractor for the security officer's services shall be deducted from the contractor's invoices.
- 7.7 *Return of a previously terminated worker.*** If a security officer is dismissed from one client location and shows up for work at another without the client's permission, the total amount paid for the officer's services from the date of dismissal will be refunded to the client plus \$100 per day for each infraction.
- 7.8 *On-the-job negligence.*** If the client's security system or property is damaged or stolen as a result of misuse or negligence by the contractor's employees, the contractor will be held liable for replacement or repair costs of the items.
- 8.0 *Notification requirements.*** Vendors must notify the client and obtain advanced approval for any change, addition, or termination of major contract components and any change in the staffing by the vendor needed to serve the client effectively.
- 9.0 *General contract provisions.*** The contract entered into between the client and the successful proposer(s) shall contain negotiated provisions based on the specific requirements set forth in this RFP and the successful proposer's treatment thereof, as contained in its proposal.
- 10.0 *Submission of Federal Employer Identification Number (EIN).***
- 11.0 *Insurance.*** The contractor must have a minimum of \$10 million of general liability insurance at the time the contract is awarded. The contractor must provide a certificate of insurance listing the client as being insured under the vendor's policy. The contractor's insurance policy must be written with an insurance carrier with a rating of at least "A" from A.M. Best. In the event the insurer is reduced to a lower rating, the vendor must take timely action to replace the insurance coverage with an insurer rated as at least "A" as judged by A.M. Best. Additionally, the vendor shall maintain specific adequate coverage for any vehicles to be used in the function of the contract. (See further discussion later in this chapter.)

- 12.0 Reports.** The vendor shall maintain records and make reports as may be required by the client, including information needed for computerized data systems.
- 13.0 Prime contractor responsibilities.** The selected vendor(s) will be required to assume sole responsibility for the fulfillment of the resultant contract(s).
- 14.0 Subcontracting.** No part of the work covered by this RFP shall be subcontracted by the successful applicant(s) without prior approval from the client.
- 15.0 Reservations.** As the need requires, the client reserves the right to increase or decrease the number of personnel to be authorized at the protected locations subject to the contract without limit. In addition to furnishing security services at the client locations listed in this RFP, the contractor may be required to provide services at other client facilities not stated in the RFP.
- 16.0 Length of contract.** The contract is for a 36-month period to be extended for a second 12-month period at the same rate for the initial period (or for whatever rate and policy the proposer wishes to achieve).
- 17.0 Termination.** Either party to the agreement reserves the right to cancel any or all sites with 30 days' written notice.
- 18.0 Equal employment opportunity.** The contract is awarded subject to applicable provisions of federal, state, and local laws and executive orders requiring affirmative action and equal employment opportunity.

Determining Final Costs

The wise workplace is interested in both quality and price. Therefore, a point system is often used to determine the winning bidder. Normally, the winner is not the lowest-cost provider. Quality and competence of service make count for 75 points, and cost considerations 25 points. The workplace announces in advance how points will be allocated. Obviously, some factors are subjective, such as quality of service currently provided. But others can be objective – years in business, specific-industry experience, retention of employees, and so on.

The client determines the projected number of hours of coverage for security officer services. In the example of the above RFP, the client asks that the contractor anticipate a variety of expenses and incorporate them into the price to be charged for each hour scheduled by a security officer. In this instance, the vendor must consider a large number of ancillary costs – officer overhead, profit, selling and proposal preparation costs, uniform and equipment expenses, supervisory costs, potential liquidated damages, insurance, and other amounts – into the hourly proposed rate.

In other cases, proposed vendors and clients may identify other factors that could be expensed separately. For example, if vehicles are required to patrol the facilities, they may be provided by one party or the other, accounting for differences in payment.¹⁸

Other Considerations

The RFP discussed above leaves much to be negotiated between the prospective vendor and the client. To the vendor, successful agreement on numerous fine points may be the

difference between profit and loss on the actual contract performance. To the client, the difference can be between projected costs and costs that exceed budgeted targets. Clearly, a spirit of harmonious goodwill between both parties is needed throughout the life of the contract to resolve issues that normally occur. The RFP above provides for “liquidated damages,” or cash penalties, against the vendor for specified breaches of the contract. Wise clients do not desire a punitive environment in which such measures occur with any frequency. If the client has screened the vendors carefully, service will meet expectations without the necessity of frequent cash penalties.

The design of the security officer's job relates to quality of performance. A guard who sleeps on a post faces dismissal. Yet in candor some jobs are designed with such little stimulation that it is difficult for someone not to sleep, especially if the security officer is sitting during an evening shift. Meaningful tasks, built-in variation, and regular visits by supervisors can maintain the discharge of duties at an optimal operating level with high alertness.

Continuous Supervision

Whether the security contract is small or large, it is incumbent on the client to maintain an ongoing evaluation of security services. Observations on the quality of services – good and bad – should be constant. Feedback may be provided orally, in written form, or both to the contractor. It should be understood that a satisfactory level of service can lead to a continuing relationship between the parties.

General and Professional Liability Insurance

In the event a corporation contracts for the services of a security guard vendor, one consideration is insurance. Typically, when someone claims a security guard is negligent resulting in measurable damages, a civil suit is commenced against the security officer purportedly causing the harm, his or her contract company, and the employer or owner of the premises where the services were performed. Therefore, the organization retaining the services of a security services business needs to be assured that liability coverage is adequate and in place. (See proposed requirement for a large contract in Section 11.0 above.)

The list of security-specific coverage includes automobile liability, umbrella liability, and workers' compensation and employers' liability. Most significant is general and professional liability insurance. As part of completion of the agreement, the client should demand a Certificate of Liability Insurance to list the insurance companies and their identifications for each type of coverage. The coverage will have a policy limit for each occurrence and an aggregate in the case of multiple occurrences. The Certificate will indicate the extent of the self-insurance (retention) the service provider will assume in the case of an incident triggering a civil action for negligence.

The general (commercial) liability coverage may be written on a claims-made basis or occurrence basis. A *claims-made* policy provides coverage when both the alleged incident and the resulting claim happen during the time the policy is enforced. Coverage is triggered when the insured first becomes aware of the claim through timely notification. By

contrast, *occurrence coverage* protects the client against covered incidents that “occur” during the policy period even if the claim is filed years after the policy has been canceled. For this reason occurrence coverage is more expensive. It is the recommended form of coverage for security guard, investigator, or alarm monitoring businesses.

Retaining Services of Private Investigators and Consultants

Over 8000 private individual investigators and investigative firms are licensed in the United States. Countless others work under the supervision of experienced, licensed investigators. Many of these are solo practitioners who work only occasionally as assignments come along. A few are organized and deeply staffed, and have offices throughout North America and beyond. Some practitioners are generalists; others specialize in a particular field.

An employer requiring an investigator for a specific assignment must identify candidates who appear to have the experience, training, and ability to undertake the assignment. This is usually achieved by interviewing candidates for the assignment and describing in general terms the work needed to be undertaken. Competent investigators will outline how they would undertake the process, what resources they would need, the amount of time required, and the approximate cost for the service.

Compensation for investigators, consultants, or their agencies can be structured in different ways. The methods include a per-project basis in which the fee includes all personnel and out-of-pocket costs, a per-project basis with ancillary costs billed extra, and hourly rates plus extra expenses. The cost of an investigator or a consultant normally will be marked up 2.5–3 times the actual hourly rate paid to the investigator or consultant. This divergence pays for the overhead and benefits for the investigator or consultant and provides sufficient extra to subsidize the investigator during times when assignments are few. Generally, the fee is related to time, skill, and difficulty for personnel involved in the investigation or consultation.

Contracting for Alarm Monitoring Services

The alarm monitoring and installation business is an important part of the security industry. It is composed of almost 10,000 businesses with revenues of \$21 billion.[‡] Alarm monitoring is part of almost every security program of consequence. In the past generation the industry had grown in volume and services while the number of individual operators has shrunk. Generally speaking, alarm businesses seek to recover costs or make only a small profit on the hardware and installation portion of the contract. Their strategy is to earn profits over time from the recurring revenues from monitoring and responding to alarm inputs.

Alarm monitoring services may be in-house, that is, totally monitored and responded to by employees or contract officers of the workplace. However, the majority of security programs will turn to outside contract companies to install and monitor alarm signals.

[‡] <http://www.ibisworld.com/industry/default.aspx?indid=1491>.

Additionally, the security program may expect the alarm monitoring firm to design the alarm system, to verify the authenticity of the signal, and to respond to it. These are issues that are negotiated for the particular sites or programs. Typical aspects to an alarm monitoring contract (for the hardware aspects see the next chapter) are as follows:

Terms of agreement. Normally an alarm contract is signed on an annual basis. But the alarm provider is interested in customers for the long term. Indeed, contracts that are likely to last less than 5 years might not be economic to alarm businesses without extra fees or penalties provided. Often agreements are considered “evergreen” in that they are automatically renewed on an annual basis unless one party notifies the other of a plan to terminate or of a fundamental change in the agreement.

Notification for termination. Alarm companies may penalize the customer if the contract is terminated before the end of the annual period. The customer may be charged fees through the end of the annual period. In the event of a catastrophe or disaster, the agreement may permit either party to cancel before the termination of the contract. Alarm businesses also usually reserve the right to cancel service when payment dues are more than 30 days overdue and unpaid.

Ownership of the security system. Despite the fact that the subscriber has paid for the design and installation of the system, it may in actuality belong to the alarm company. This may not matter to the subscriber particularly because systems reach obsolescence in a few years’ time. But this could have a significant strategic impact on the subscriber who wishes to cancel the contract: the alarm company may threaten to remove the alarm equipment on short notice leaving the former customer unprotected. The loss of sensors and alarm panels in such circumstances is not as significant as the cost of the wiring of the system, should the alarm system provider argue that the wiring is theirs.

Maintenance of the security system. The customer may not own the system but is expected to maintain it. The alarm company is willing to service the system and to respond to problems, but maintains that it has no duty to maintain, operate, actuate, or nonactuate the installed system.

Suitability of the system. The alarm installation and monitoring company may state that it does not represent that the system is suitable for the subscriber.

Interruption of telephonic signals. The alarm business is not responsible if signals do not reach it due to a loss of utilities. (In such cases, the subscriber would plan for backup.)

Daily testing of the system. The subscriber is responsible for testing and setting the system each day. In some cases, a “walk test” if motion detection is provided must be conducted by the subscriber. Any operating defect must be reported to the alarm company.

Burden of customer to carry own insurance. Alarm company contracts normally notify customers that they are not insurance companies (see next point). Therefore, the payments made by the subscriber are for the value of the services and have no relationship to the value of the property or other assets to the subscriber. The alarm

company makes no warranty, normally, for the fitness of its own services and for the alarm system that it may have designed, configured, and installed.

Liability for negligence. In the event the alarm monitoring firm is negligent resulting in loss to the subscriber, the amount the subscriber will be reimbursed will be limited to the amount cited in the contract. That could be for \$100 or the equivalent of 1 year's monitoring services. Thus, negligence that resulted in substantial losses because of failure to respond, for example, would result in a *de minimis* payment to the aggrieved subscriber. (An exception would be if the alarm monitoring business were to be *grossly negligent* in its duty to subscribers.)

Obligations of the subscriber. Opening and closing times and holiday schedules are likely to change. It is the duty of the subscriber to notify the alarm company of any changes or corrections in the previously agreed-to schedule. The subscriber must determine at the beginning of an engagement how many minutes before or after a scheduled opening or closing time may pass before an alarm condition prevails. Such changes can be made easily when an authorized person contacts the service center and verifies that the change is authentic.

In contracting for alarm services, the subscriber should determine in advance what is needed for response. That is, in some areas an automatic response by police will take place when an alarm condition is signaled to law enforcement. However, in the effort to reduce false alarms, many communities expect alarm monitoring firms to verify the alarm before notifying the police. This verification may occur through telephoning the subscriber, checking on-site CCTV, sending private security to evaluate the alarm, or other measures. Before signing an agreement with an alarm business, the subscriber needs to determine where the alarms will be monitored and what backup has been provided in the event the primary monitoring location is out of service.

Purchasing Security Services Through Internet Proposals

Security services traditionally have been negotiated between people. The Internet has changed that, even for services as distinctive as guarding, investigations, consulting, and alarm monitoring. The process is so new that it has not been subject to rigorous scrutiny and criticism. For now the concept of inviting service providers to bid online is appealing if safeguards protect the interests of all the parties. In the end before a contract is awarded, the customer will want to meet face-to-face with bidders on the short list so that any uncertainties can be eliminated and so that the sites may be visited.

Summary

Personnel represent the largest cost in most security programs. Consequently, the optimally performing manager will seek to assure that security functions are achieved with the minimum number of people required. Both proprietary and contract security services

have advantages; therefore, managers sometimes plan to employ both in large operations. Software programs specifically written for security applications have improved accountability and decreased costs since their introduction. Investigations are currently playing an ever-widening role in both civil and criminal processes. A RFP is a bureaucratic, costly, and burdensome means of selecting a security services vendor. However, the process sets out a fair basis for identifying the best security company for the client and also helps to determine the most favorable arrangements for the client.

Discussion and Review

1. What factor is “all too often” not considered by management when the possibility of converting from proprietary to contract guard services is considered?
2. What is the significance of possible collusion between employees and security personnel? What do many security directors feel is a measure that combats collusion?
3. How important is making people feel safe in security programs?
4. Outline the critical differences between criminal law and civil or contract law as discussed in this chapter.
5. What new types of investigation have emerged in recent years?
6. Security officers who are on “barred-from-customer” lists can be monitored most easily by what type of management tool?
7. What are convenient means by which security directors can determine compensation ranges for security officers in various geographic areas?

Endnotes

¹ Dalton, D.R., 1991. *Managing Contract Security Services: A Business Approach*. Mill Creek Publishing, Fremont, CA, p. 5.

² Dalton, D., 1994. Looking for the quality-oriented contractor. *Secur. Technol. Des.* 4, 6.

³ *Ibid.*

⁴ Fay, J.J., 1987. *Butterworth's Security Dictionary*. Butterworth-Heinemann, Boston, MA, p. 102.

⁵ Buckwalter, A., 1984. *Investigative Methods*. Butterworth-Heinemann, Boston, MA.

⁶ Chapman, B., Zwicky, E., 1995. *Building Internet Firewalls*. O'Reilly & Associates, Cambridge, MA, p. 1.

⁷ Parker, D., 1998. *Fighting Computer Crime*. Wiley Computer Publishing, New York, NY.

⁸ *Ibid.*, p. 428.

⁹ Workman, M., Phelps, D.C., Gathegi, J.N., 2013. *Information Security for Managers*. Jones & Bartlett Learning, Burlington, MA, p. 3.

¹⁰ Barefoot, J.K., 1995. *Undercover Investigations*, third ed. Butterworth-Heinemann, Boston, MA, pp. 92–94.

¹¹ David, A.R., 1986. *The Pyramid Builders of Ancient Egypt*. Routledge & Kegan Paul, Boston, MA, pp. 68–69.

¹² Lipson, M., 1975. *On Guard: The Business of Private Security*. Quadrangle/The New York Times Co., New York, NY.

- ¹³ Winston, W.L., Albright, S.C., 1997. *Practical Management Science: Spreadsheet Modeling and Applications*. Duxbury Press, Belmont, CA; Krajewski, L.J., Ritzman, L.P., 1993. *Operations Management: Strategy and Analysis*. Addison-Wesley, Reading, MA. For example, see *Valiant SMS*.
- ¹⁴ Security Letter, vol. XXX, Part II, October 14, 2000.
- ¹⁵ Moran, M., 2012. Just compensation. *Security Management*, August, p. 54 (ASIS International conducts a periodic salary survey of US security practitioners, www.asisonline.org).
- ¹⁶ Morn, F., 1982. *The Eye That Never Sleeps*. Indiana University Press, Bloomington, IN, p. 98; also Horan, J.D., 1967. *The Pinkertons: The Detective Dynasty That Made History*. Bonanza Books, New York, NY, p. 50.
- ¹⁷ Willey, J., 1988. *The Business of Employee Leasing*. Employee Leasing Consulting Group, San Bernardino, CA.
- ¹⁸ Brownyard, T., 2015. The do's and don'ts of contract security. *Security*, January, p. 24.

Additional References

- ASIS, 1998. *ASIS International Presents Introduction to Security for Business Students*. ASIS International, Alexandria, VA.
- Ferraro, E.F., Spain, N.M., 2005. *Investigations in the Workplace*. Auerbach Publications, Boca Raton, FL.
- Heil, R.D., 2006. Guarding against poor performance. *Secur. Manage.* 50 (6), 57.
- Meadows, R.J., 1995. *Fundamentals of Protection and Safety for the Private Protection Officer*. Prentice Hall, Englewood Cliffs, NJ.
- Office of Federal Protection and Safety, 1984. *Contract Guard Information Manual*. U.S. General Services Administration, Washington, DC.
- Sennewald, C.A., Tsukayama, J.K., 2015. *The Process of Investigation: Concepts and Strategies for Investigators in the Private Sector*, fourth ed Butterworth-Heinemann, Waltham, MA.
- Sklansky, D.A., 1999. The private police. *UCLA Law Rev.* 46 (4), 1165–1287.
- Slywotzky, A.J., Drzik, J., 2005. Countering the biggest risk of all. *Harvard Business Review*, vol. 83, April, p. 78.
- Travers, T.G., 2005. *Introduction to Private Investigation*, second ed Charles C. Thomas, Springfield, IL.

Operating Physical Security- and Technology-Centered Programs

The ultimate purpose of any security system is to counter threats against assets and strengthen associated vulnerabilities.

—Joseph Barry and Patrick Finnegan

Most of the costs of security operations are personnel costs created by security services. But it is the nature of management to drive down costs, whenever possible, while maintaining or improving quality of services or product. Is this realistic? An important means by which security operating dollars can be made more effective is through the judicious use of physical- and technology-centered programs. These are concerned with physical security measures and electronic technology – often computer-based – used to safeguard people, to reduce chances of theft, to evaluate ongoing operations, and to safeguard assets against damage or loss. Well designed and executed, such operations may decrease the number of personnel required to implement and maintain a high-performance protection program. If conceived and implemented poorly, however, physical- and technology-centered programs can produce unsatisfactory results. Further, if badly conceived and implemented, such initiatives can produce a sense among workers that management is “putting systems above people.” Clearly, physical- and technology-based measures should enhance the use of protection personnel and other resources, not detract from them.

We begin this chapter by reviewing the theory of situational crime prevention concepts. Then we will consider technology trends to enhance security programs.

Situational Crime Prevention: A Strategy of Crime Reduction

Law enforcement and criminal justice practitioners are concerned with priorities that they have identified. These include community crime mitigation programs, juvenile deviance, coordination with prosecutors and the courts, as well as police staffing and environmental and technological strategies. By contrast, persons concerned with security operations management for a corporation or institution have little short-term control over many environmental and circumstantial factors. These include where the facility is located, policies and programs related to juvenile offenders, the responsiveness and leadership of local criminal justice programs, and how well local police do their job. These differences have influenced the ways in which law enforcement and private security firms tend to view the causes of crime and disorder. The differences historically have been substantial.

Over the years, legions of criminologists and social critics have written on supposed “root causes” of crime, and the social disorganization and individualism that perpetuates deviance.¹ These same writers largely fail to consider why a few individuals in a particular social, ethnic, political, economic, and even familial situation commit crimes while most do not. In the end, the manager concerned with reducing losses does not speculate on what is neither quantified nor provable, but rather concentrates on what can be accomplished in security programs based on the results of accepted research activities. In part, this means deterring or suppressing crime rather than focusing on apprehending and prosecuting violators.

For example, a facility can be designed to make it less amenable to loss. In many circumstances, however, the manager faces situations in which changing the facility design – using architecture and engineering methods to create spaces that are less amenable to crime, loss, or injury – is not an option. Instead, personnel, procedures, physical measures, and technology must be altered to prevent or mitigate losses. The clear trend in recent years is for security executives generally to become involved early in the design considerations of a new facility. This allows their insights into loss control to be implemented at the earliest stages. (This process is discussed near the end of this chapter.) Large architectural and engineering firms have staff members with loss prevention outlooks who stay abreast of protective and life safety measures so that such advances may be designed into new facilities. Other specialized consultants offer services that lower property risks to existing sites through better security planning and design.

In the 1970s, the architect Oscar Newman studied public housing in New York City and elsewhere and determined that crime rates vary according to territoriality, surveillance, image, and environment.² “Territoriality” refers to the sense of possession by residents or workers of an environment and the tendency of people to defend this territory against those who would commit criminal acts within or near the area. “Surveillance” relates to the ability of people within buildings to view people outside their immediate environment. It also discusses the ability of people in an environment to see others some distance away, minimizing hidden spots and being able to interconnect with others easily. “Image” refers to the general reputation of a place. And finally, “environment” refers to the nearby area that renders the zone safe or unsafe.

Defensible space, therefore, defines an area where surveillance is extensive, the image is positive, and the nearby environment is safe and protective of residents and visitors. Newman’s theory produced a design concept called crime prevention through environmental design (CPTED), discussed in [Table 10.1](#). Defensible space theory concludes that crime may be reduced by improving surveillance of public areas, demarcating private versus public space, and improving the image and environment of the area.

Research on defensible space concepts sometimes concludes that the methods are not always successful at reducing crime. That may be because they fail to take into consideration the cognitive processes individuals use to adapt to physical environments.³ Patricia Brantingham and Paul Brantingham analyzed crime rates by occupation and economic specialization and have determined that crimes such as murder and assault occur in areas

Table 10.1 Crime Prevention Through Environmental Design (CPTED)

Principle	Methods of Applications
<i>Territoriality</i>	Property looks cared for; broken windows are repaired; graffiti removed promptly Residents are seen making improvements or enhancements to their areas Access control discourages unauthorized visitors and deters their entry Controlled space is differentiated clearly from nearby transitional zones
<i>Surveillance</i>	Residents can observe outer areas from within their buildings with clear lines-of-sites to call for assistance in the event it is needed Hallways and public areas are designed to be open and nonconstraining Cul-de-sacs and hiding places in public areas are designed out Closed-circuit television (CCTV) and modern access and alarm systems are likely to be in use
<i>Image</i>	The property has a favorable image in the area and is looked at as being well maintained and cared for Events and activities are programmed to increase use of public spaces
<i>Environment</i>	The area immediately beyond the property – nearby buildings, streets, retail space, and parks – is equally well cared for Communications systems permit persons in both congested and isolated areas to call easily for assistance when needed Conflicting activities – such as a playground for toddlers and a basketball court – are separated Street furniture, sitting areas, and fountains are designed to serve locals while not attracting vagrants

CPTED argues that changing the environment through design can make certain types of crime less likely to occur. Antisocial and criminal behavior will not disappear, but the frequency will decline because the environment is less hospitable to potential offenders. This is because the area seems better protected by its owners and thus the would-be criminal is deterred from offending due to being more likely to be detected and arrested. The principle is based initially on research involving residential buildings, although the same concepts relate equally to commercial and institutional property. CPTED posits that private and semiprivate spaces are better cared for and, therefore, safer than those for whom responsibility is diffuse or public. CPTED is based on four principles as given in the table.

of economic decline and neglect, whereas white-collar crimes occur in areas in which a high number of potential victims exist.⁴ Research has also found that certain environmental changes increase public use and, therefore, generally decrease fear among members of the public.

More recently, CPTED has evolved to include the concept of situational crime prevention, which argues that crime may be reduced in a particular area when aspects of the environment are changed, often involving little cost or effort. For example, making it harder to commit a crime by modifying the environment – by installing better lighting, broader surveillance through visible patrols, closed-circuit television (CCTV), and alarms that will call police to the scene quickly – can decrease crime in an area.⁵ This concept was introduced in Chapter 1 (Box 1.3). The implementation of CPTED primarily helps by increasing appropriate controls that serve to demotivate a potential offender.

The Risk Versus Cost Ratio

The level of security in a particular area can depend on many factors. Therefore, a range of options should be evaluated for their pertinence to a given condition. A broad spectrum involving widely varying degrees of risks and controls exists. At one end, controls

are absent and risks for loss are high. At the other end, the reverse is true. The thesis of this book, indeed the view of many security practitioners, is that weakness is eventually exploited. Therefore, lack of adequate security increases the likelihood of losses. Further, as assets increase in value, the potential for their loss also grows, as shown in [Figure 10.1](#). Security conditions vary according to risk factors. A continuum of response to threat vulnerability is reflected in the following:

- *Protectionless places.* The author's grandparents lived in a small, safe community. Their front door was rarely locked. Once they left their house for a trip, they locked it, but left the key in the front door keyhole "in case someone needed to get in." This seemed to make sense to them. Security depended on the fact that residential burglary was rare at that time and place. Those who might be inclined to commit such a crime did not systematically survey the neighborhood to see what residences were unlocked and were easy targets. In time, the younger generations convinced their parents and grandparents that wisdom dictated that the key should be left elsewhere and it was henceforth placed under a nearby flowerpot.

Such seemingly protectionless behavior still exists in some residential areas. These circumstances are not thoroughly precarious as vigilant neighbors, visibility of the residence, and a culture of low residential property crime make the risks less than what would seem initially obvious. However, contemporary organizations realize that reasonable and adequate measures must be taken to protect their operations. The orderly and lawful behavior of others cannot be assumed. That means implementing appropriate security measures to protect the value of the assets located there.

- *Minimum security.* With little effort, this type of system impedes some unauthorized external activity, which is achieved by physical barriers and locks.⁶ Local or centralized alarms are not installed in such facilities. This level of protection may be adequate for some residences, but not for commercial or institutional activities.
- *Low-level security.* This system impedes and detects some unauthorized external activity requiring modest effort by the offender. Doors and windows may be reinforced and a local alarm system may be installed.
- *Medium security.* Here the system impedes, detects, and assesses most unauthorized external activity and some unauthorized internal activity. This is achieved by the use of a properly installed centrally monitored alarm system. Unarmed security officers may be on the premises for part of the day.
- *High-level security.* Relying on greater capital investment, adequate personnel, and well-considered procedures relative to the previous category, this system impedes, detects, and assesses most unauthorized external and internal activity. In addition to features found in lower levels, this level of security can include Internet Protocol (IP)/CCTV, access controls, advanced perimeter and interior (volumetric) security systems, highly trained and supported security officers, and management dedicated to constantly seeking programmatic improvements.

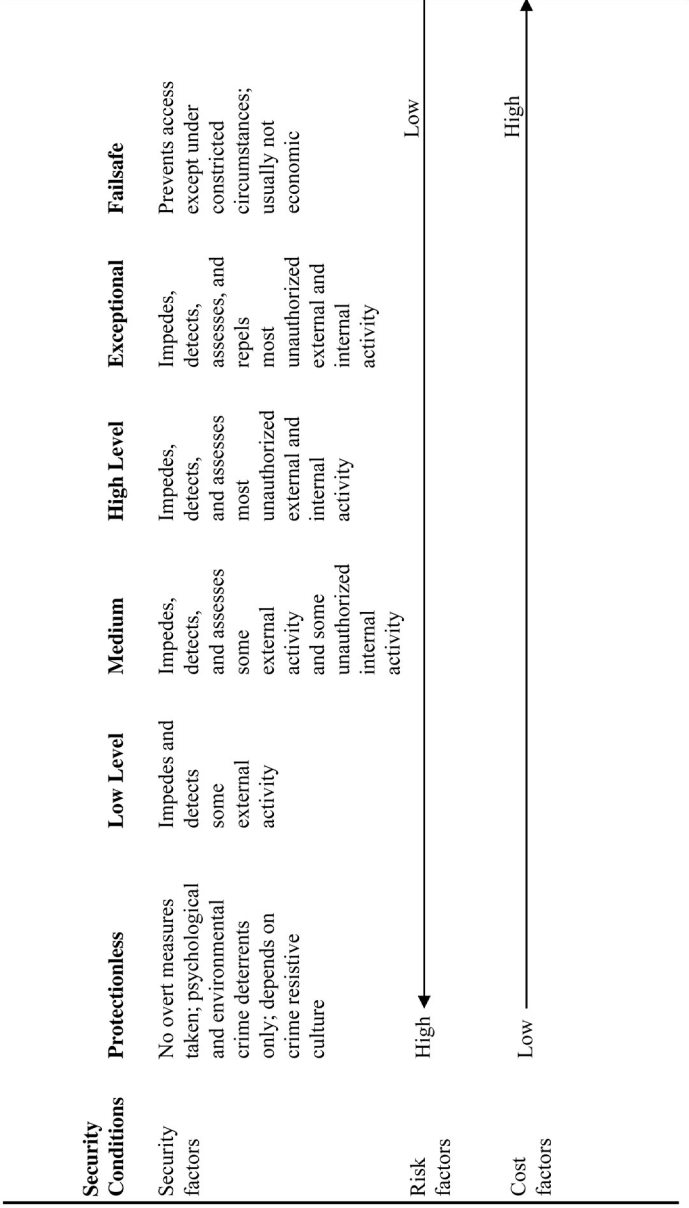


FIGURE 10.1 The risk versus cost continuum. Risk of losses and the cost of security measures have a reciprocal relationship. Low protection has low cost, but invites higher risk of loss. In response, the cost of security can increase.

- *Advanced security.* This protective status impedes, detects, assesses, and neutralizes most unauthorized external and internal activity. This is achieved by tamper-resistant, complex systems, and highly trained and vetted personnel capable of responding promptly to any alarm condition and most threats. If indicated following a security survey, 24-hour per day security personnel may be on duty. IP/CCTV will connect with megapixel cameras to produce high-resolution images that can identify physical features of intruders or other unknown persons. Security management is alert to any lapses in protection – for example, a camera system that is down or a security officer not on post – and takes steps to correct the vulnerability immediately.
- *Fail-safe security.* This is a conceptual level of security in which serious losses over an extended period of time are highly unlikely because of the exceptional defenses that prevent such occurrences. Such a level of security is costly and impractical in most situations because the controls are deliberately restrictive and time-consuming to overcome even for those with some authorization over control and custody of the assets to be protected. Fail-safe security is unlikely to permit losses, but its nature also suppresses normal economic activity.
- *Dealing with managers who oppose security programs.* Sales and marketing-oriented managers often battle against the recommendations for and installation of protective controls. They argue that such measures in retail settings discourage purchases by establishing barriers. That is, security to them turns off customers. Therefore, security directors face the task of justifying and obtaining the maximum level of protection reasonable for the situation required. Lack of any security is not an option; neither is fail-safe security. The strategy for security operations is to find the right level of security measures to satisfy constantly changing requirements.

Organizations work like teams. As a member of the team, the chief security director must use the language and thought processes of other managers in making the case for the security program. Not all battles can be won. But demonstrating how security provides value and makes other organizational departments do their jobs effectively is a persuasive approach.

Determining the reasonable protection level for an organization involves evaluating four types of issues. These include the types of risks faced by the organization, the likelihood of their occurrence, the impact they would have on operations, and the resources reasonably available to identify the risks. This is a topic of considerable importance in justifying security programs and their expenditures. Some managers prefer to create programs based on their and their associates' experienced judgment. Others use a matrix of risk types, likelihood, and impact, which can lead to an estimate of the resources needed. Other managers use software programs that guide them into identifying risks and considering various possibilities of occurrences.* These are converted into strategy during the planning period to meet management's objectives.

*Threat assessment and level determination aid is found at: <http://www.wbdg.org/ccb/AF/AFDG/ARCHIVES/afinstal.pdf>. Also: RAMCAP Plus, www.asme-iti.org/RAMCAP/RAMCAP_Plus_2.cfm. Software for specific industries is available. For example, DHS has approved a program for the food industry, CARVER + Shock, www.fda.gov/Food/FoodDefense/CARVER/default.htm.

Why Physical Security Is Important

Physical barriers have been used as a means of protection for centuries. Along with animals and human sentries, walls, fences, weapons, and locks have always been important means of protecting people. Early humans chose their housing with defensive features in mind, and communities were formed to take advantage of mutual protection. Safes and vaults became important ways of protecting assets in early market centers when their owners could not be present and in locations where hiding places were limited. The ancient Egyptians, meanwhile, developed the pin tumbler lock.⁷ Early and medieval communities protected themselves from foreign armies as well as organized brigands with walls, fortifications, and careful placement of the structure. Such physical security measures had many advantages: they represented one-time-only costs, they were usually reliable and worked well for long periods of time, and they achieved their objectives by deterring or reducing opportunity for unauthorized entry.

John J. Fay defines physical security as “that part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against damage and loss.”⁸ The term encompasses measures relating to the effective and economic use of a facility’s full resources to meet anticipated and actual security threats. Concerns of physical security planners include design, selection, purchase, installation, and use of physical barriers, locks, safes and vaults, lighting, alarms, CCTV, electronic surveillance, access control, and integrated electronic systems. The term physical security includes physical obstacles and mechanical devices. These are supplemented by technology-centered processes for communications, control, and directing mitigation efforts. They depend on electricity in order to operate. Typically, comprehensive security programs involve a combination of two or more distinct measures to protect people, physical assets, and intellectual property.

Security operations planners sometimes think first of physical security in their protection strategies. Several reasons support this tendency: physical security substantially requires a one-time cost only; physical measures are usually clearly visible and deter unlawful or unwanted acts; care and upkeep are limited; specific standards have been set in many cases to guide the security planner on decisions; and physical security measures are uncomplicated to purchase, install, and care for. Finally, security personnel provide a visible awareness of the protection program and suggest the capacity to respond to an incident as required.

Technology can be applied as a powerful tool in well-conceived security programs. All contemporary protections depend on electronics components and systems to achieve their objectives. Technology performs complex monitoring operations and possesses control features beyond the capacities of individual security personnel. As a result, contemporary high-tech implementations permit a higher level of confidence in protective programs than in the past. Just as changes in communications, sensing, and computing have affected society at large, these developments also have reshaped the means and quality by which security services are performed. Indeed, a security planner learning of a new

technological development is likely to wonder how it can be applied to enhance operating security programs in the future, if not immediately.

The following section on security countermeasures to loss is neither comprehensive in its scope nor detailed in its discussion. The discussion does, however, serve to provide an overview of physical security measures to consider when creating or assessing protective programs. A final section in this chapter offers guidelines for designing and constructing a complex integrated system with the aid of security engineers or consultants. In addition, the notes at the end of this chapter provide resources in which to further pursue individual topics.

Selecting Security Countermeasures to Reduce Loss

Security planners should consider drawing upon a variety of countermeasures to protect the organization from physical attack. This has been historically referred to as concentric circles of protection. The term “concentric circles of protection” reflects the concept that dedicated intruders will not be stopped by a single barrier. Therefore, numerous protective measures are designed to separate the outer environment from the innermost protected locations. In planning the measures to be taken, thought is always given to the appropriateness, utility, and cost of the procedures, equipment, and personnel required to meet the expected objectives.

Effective countermeasures may serve one or more of the following objectives: deterrence (i.e., preventing or discouraging unwanted action), delay or denial (i.e., impeding or stopping an unwanted action), and detecting (i.e., discovering or ascertaining the significance of a possible security breach; [Table 10.2](#)).

Table 10.2 Physical Security Countermeasures – Strengths and Relative Cost

Countermeasures	Strength			Relative Cost
	Deter	Delay	Detect	
Facility design	x	x	x	Low
Animals	x	x	x	Low
Barriers	x	x		Low
Signs	x			Low
Locks, keys, containers	x	x		Low
Lighting systems	x			Low
Internet Protocol/closed-circuit television	x		x	High
Intrusion detection systems	x		x	Moderate
Access control systems	x	x	x	High
Alarm systems	x	x	x	High
Robotic systems	x	x		High
Communications	x			Moderate
Information security systems	x		x	Low to high
Contraband detection		x	x	High
Fire detection and life safety			x	High

This list includes physical and electronic crime countermeasures.

Source: Introduction to Security for Business Students, 1998. ASIS, Alexandria, VA.

Facility Design: Location, Area, and Architecture

From earliest known times, humans have improved their safety and security by evaluating the advantages of location and using its protective environmental advantages to the fullest. Natural barriers that provide an intrinsic protective value include bodies of water, marshy areas, deserts, mountains, and hidden areas such as caves and tunnels. These naturally occurring physical characteristics were enhanced with walls, fences, bars, moats, ditches, cleared spaces, and other adaptations. From Neolithic times to the early Iron Age (4000–450 B.C.), lake dwellers created communities in the Alpine Arc from France, through Switzerland, to Slovenia, although similar settlements were found in other parts of Europe. Lake dwellers built abodes on stilts over marshy areas. Why these locations were selected is unsure, but security is believed to be one of the factors. Medieval cities, for example, were often built on hilltops in order to take advantage of the superior lookout provided there, as well as the natural superiority height provides in repelling attackers. (Examples of such hilltop villages include Carcassonne in France and Urbino in Italy.) Fortified dwellings expanded over time, eventually becoming castles. These were developed partially to protect residents from endemic warfare, as well as against organized bands of thieves in Europe that threatened the safety and security of small communities.[†]

Locations that had natural defense characteristics, often strengthened by structural barriers, serve many purposes. They were selected with discernment. The best locations defined property boundaries, controlled access to restricted or privileged areas, delayed and impeded unauthorized entry, channeled and restricted the flow of traffic, facilitated the identification of possible intruders or threats to the area, and provided for efficient use of security personnel or other guardians.

In the contemporary organization, location matters just as much as in earlier centuries. In crime prevention research, the study of location holds considerable importance. Areas with high personal and property crime and persistent urban problems will lose residents, commerce, industry, and institutions. Further, new organizations will be reluctant to locate to such crime areas without considerable inducements. Nonetheless, it is possible for an organization to locate in a distressed area and thrive with appropriate physical security measures. However, employees and services may be reluctant to come to it. Before committing capital investment in a new location, therefore, security-conscious managers carefully consider crime patterns in the immediate location and general area. This includes collecting crime data, studying law enforcement resources and culture, and determining how these factors relate to the security measures that must be put in place before the decision to establish a security program or expand it.

Animals

Some of the earliest protective sentries were animals, not the human kind. Livy describes how geese on one of the hills in ancient Rome sounded an alarm when the invaders from

[†] Castles were designed for security. Defenders operated from parapets atop the walls during an attack. The concept of concentric circles of protection is clear enough in construction of some castles, which have two or three walls, a moat, and protected places within the central structure.

Gaul (modern France) sought to surprise an army encampment at night from a steep and unprotected side of the hill.⁹ In current applications, geese have been used sometimes to protect NATO facilities.[‡]

For centuries, dogs have played an important role as guards, as well as for their ability to be trained to help investigations. Guard dogs usually patrol inside fenced areas and buildings without a handler, and are often used in facilities with no evening security personnel or workers, such as at retailers, car dealers, construction yards, and distribution facilities. In other circumstances, guard dogs work with handlers. Because of their superior sense of smell and acute hearing, dogs play a large role in searching for lost or hidden persons, contraband, and explosives.¹⁰

Breeds of dogs vary in their ability to be useful for security purposes. Canine breeds can be categorized as high or low in such diverse characteristics as reactivity, aggression, trainability, and capacity for investigation. Dogs used in security and police work for bomb or drug detection are trained by Pavlovian methods. The handler trains the dog every day to find hidden explosives or drugs and then feeds and praises the dog with each success. Security planners interested in using dogs for security tasks must select personnel who will be trained with the animals and will be committed to their welfare over the lifetime of the animal.

Barriers

Barriers may be constructed to further safeguard the protected area. For example, a body of water or deeply rooted shrubs may provide psychological and distance deterrents. Manufactured fences also provide an important barrier for physical security.[§] If a security planner determines that a fence is desirable, related issues may be raised: Will one fence be enough, or will two fences with a patrol space between them be better? Will the fence have clear areas around it so that a good line of sight is maintained? What impediments to climbing will be used? To digging under the fence?

While fences may be made of many materials, chain-link fence is commonly used due to its availability, flexibility, cost, established use, and ease of installation. In security applications, fences are typically no. 11 American wire gauge or heavier, with 2-in. mesh openings. They are at least 7 ft tall and are topped by three strands of barbed wire or razor ribbon evenly spaced 6 in. apart and angled outward 30–45° from the vertical. Mary Lynn Garcia writes: “Security fences are not usually less than 8-feet high and are braced, as necessary, at all corners, gate openings, or structurally weak points.”¹¹ Since attackers may pass under the fence, the bottom may be designed so that penetration there is difficult. Typically, the bottom of a wire gauged fence will be attached to a base, deterring someone from prying the bottom up.

To many security planners, a fence may seem like an attractive security option: chain-link fencing is a widely used visible deterrent requiring little maintenance. However, fences

[‡] Geese may be more alert than sleeping dogs at detecting nocturnal intruders.

[§] Note that the term “fence” also refers to a receiver of stolen goods. It is also a metal pin that extends from the bolt of a lever lock, preventing retraction of the bolt unless it is aligned with the gates of the lever tumblers.

do have shortcomings and should be regarded as being able to provide only temporary deterrence. As Gigliotti and Jason note:¹²

Regardless of how elaborate fences may be, they still offer only a modicum of security. Fences are necessary, but investments in this area should be kept to a minimum as the money can be better used on other components of the total system.

Consider that someone wanting to pass from one side of a fence to the other has three options: they can go under the fence, through it, or over it. It is possible to go under a fence by digging a hole beneath it, although the time and effort required to successfully accomplish this make this approach onerous. Going through the fence is possible, as wire cutters can cut out an area for someone to pass through in a few minutes' time. Finally, someone can go over the fence. Research at Sandia National Laboratories, Albuquerque, for the Department of Energy, determined that trained individuals with penetration aids such as ladders, sheets, carpet fragments, and wood planks can scale over a fence in 5–10 s depending on the penetration aid used and whether someone was assisting in the passage or not.¹³ The average untrained individual surely would not be able to cross a fence so quickly, and the presence of the fence would discourage casual attempts. However, the inherent weaknesses of fences indicate that the security planner must think beyond this structure to make a facility safe from penetration. In addition, most fences present an unwelcoming, rigid impression, which may be unacceptable to an organization fostering a friendly working environment. Some facilities with medium-to-high security vulnerabilities have decided not to use fences, but rather to rely on other means of protecting facilities.

An alternative to metallic fences is the use of plants such as hedges to serve as a natural fence. Such measures are limited to facilities in which the hedge will not be needed for a few years as it grows to the proper height, depth, and thickness so that it can serve its intended protective function. One of the most widely used protective hedges is *Trifoliate orange*, which grows in many types of soils, putting down deep roots in time so that even a jeep would have trouble driving through it.

Security Glazing

Glass is a transparent and brittle substance composed mainly of silicates and an alkali. The raw materials also are fused at high temperatures. Glass may be manufactured to suit a variety of purposes. For security needs, glass is often fused with layers of plastic, usually polyvinyl butyral (PVB), although laminates of polycarbonate have a robust protective value and are also transparent. Thousands of glazing configurations have been created, but only a few meet security standards. Some products can withstand bomb blasts; others can withstand burglary attempts. Transparent security glazing is best known for withstanding bullet discharges of various caliber weapons. Well-selected security glazing can provide performance, control, and cost savings.

Transparent film placed over ordinary glass (from 4 to 15 mil thick) can increase bomb blast resistance and is frequently installed at high-risk locations. Craighead notes: "Security

window film is inexpensive to install (as compared with installing tempered safety or laminated glass) but may require replacement. Some high-rise buildings in preparation for turbulent events, such as planned protests and demonstrations outside of their buildings, have installed security window film on windows near the ground level.”¹⁴

Signs

Warning signs have an important deterrent effect. Placed at the perimeter of a protected facility, they discourage would-be offenders from a variety of unwanted behaviors. The excavated ruins of Pompeii revealed that 2 millennia ago homeowners sought to deter possible housebreakers with prominent signs, some made of mosaics, warning *cave canem* (beware of dog). That same message – but in English – still appears on the fences of construction lots, on the doors of garages and distribution facilities where guard dogs are found, and in countless other types of locations.

Much more common are warning signs that indicate that trespassers will be arrested and prosecuted or that electronic security systems are in use. Such signs are an indication of guardianship; that is, the owners and operators of the facility are aware of risks and have taken measures to protect assets, or say they have. Such signs should be placed around the perimeter so that potential perpetrators from any direction will be warned of the protective measures being taken.

Signs usually represent a small one-time cost. Although they will not stop determined thieves, they will signal such individuals that they must move quickly due to the threatened risks of being detected and apprehended.

Locks, Keys, and Containers

Locks are one of the earliest manifestations of physical security. The art of the locksmith has been respected over the centuries for its beauty, practicality, and necessity. Locks remain an integral part of contemporary physical security planning. Locks, along with their keys and the containers of which they may be a part, have many benefits for security programs. Simple to use, they are complicated to make. Involving a one-time cost, they may be used repeatedly with reliability over years of service. Locks and keys may meet different levels of security according to requirements of the location. They are easy to employ and can be designed into containers, furniture, doors, clothing, and machines.

A disadvantage of mechanical locks is that they provide no evidence of who accessed the lock over its previous uses. This drawback is eliminated by electronic locking systems now available. These systems may be opened with cards or tokens that are inserted or brought near (proximity lock) a sensor, which in turn opens the door. The security planner should concentrate on a series of easy-to-understand principles in deciding what locks to use and why.

Key-Operated Locks

Most locks use “tumbler mechanisms” to operate. That is, the key enters the keyhole and moves the variable tumblers into a straight line so that they then can turn the lock cylinder.

Table 10.3 Pin Tumbler Lock Security

Factor	Consequence
Picking tools	Available for sale in locksmith publications and the Internet
Picking skills	Taught in legitimate locksmith schools, but the skills are available also in mail order instruction courses
Age of lock	With use over time, pins and keys get worn down making them easier to pick
Number of pins	A 3-pin tumbler has about 130 combinations; a 6-pin tumbler has about 65,000. However, for technical reasons, the number of possibilities is actually much lower. Yet the principle remains: more pins, higher security
Angle of pins	Pins that are vertically aligned to the cuts of the key are easiest to pick. Those which are aligned on different planes are extremely difficult or impossible to pick
Control of master key	Pin tumbler locks may be subdivided into master, submaster, and other divisions permitting key control. However, if a master key is lost, stolen, or inappropriately copied, all the locks in the protective systems may have to be changed at great cost and inconvenience

Pin tumbler locks are the most widely used mechanical lock type. Despite their popularity, this type of mechanism may have – depending on the lock type – inherent weaknesses of which the security planner should be aware.

If the correct key is not inserted into the keyhole, all of the tumblers will not be in a straight line (shear line) and the lock cylinder will not be able to rotate around the shell of the lock.

The most widely used key-operated mechanism is the pin tumbler, for which a wide variety of security levels is available. Mechanical pin tumbler locks were ingeniously cut so that a sequence of keys would operate a series of doors, such as on the floor of a hotel. Then a sub-master key would open all of these doors, but would not operate on another floor of the hotel where a different sub-master key was used. Finally, a master key would operate on all of the floors. The disadvantage of this system was that if a sub-master key were lost or stolen, all of the doors operable by it would have to be rekeyed. If a master key were lost or stolen, all of the keys operable by the system would have to be rekeyed.

As every observer of action programs on television or the movies is aware, pin tumbler locks – despite their ubiquity – may be picked; that is, they may be entered without a normal key by manipulating the tumblers to the shear line so that rotation can occur. Picking is one of several ways by which mechanical pin tumbler locks can be defeated ([Table 10.3](#)).

In addition to pin tumbler locks, other mechanisms are available, including magnetic or optical locks. The security planner may wish to evaluate and compare the strengths and weaknesses of these other mechanisms with pin tumbler locks. In hotels and motels most of the new construction use key-cards with magnetic stripes or a chip to open the door. This technology has the advantage of keeping track of all uses of the room by date and time. A hotel security agent is able to quickly download room activity in the course of making an investigation. Such locking systems could be used in other entry systems, and are, but market penetration has been far behind that of the hospitality industry. Management of physical keys that may be borrowed by numerous persons represents a huge challenge. A computer-based system, accessed with the card or token, can provide a management solution ([Figure 10.2](#)).



FIGURE 10.2 Linking key control with an electronic system. Management of physical keys, as seen here, or weapons or other physical assets can be controlled with an RFID-enabled access. Removal and return of keys, or other assets, are both recorded and linked to the person accessing the cabinet. (Source: Deister Electronics USA.)

Lock Hardware and Mountings

Locks are integral parts of the inner layers of the concentric circles of protection. The oldest piece of furniture owned by the Bank of England is a multipoint locking secured chest dated from about 1700, visible today in the bank's museum in London. The Lock Museum of America in Terryville, Connecticut, contains an Egyptian pin lock perhaps 4000 years old.¹⁵ Mechanical locks remain an important part of security today, although electronic computer-operated entries have management appeal for their ability to establish an audit trail and reliability (Figure 10.3).

For moderate- to high-security applications, locks are mortised; that is, they are installed within the core of the door or locking device rather than attached on its surface. Mortised locks can be changed by a locksmith when needed, thus maintaining the level of security after the previous lock setting has been damaged or compromised and must be replaced.

A high-security lock on a low-security door, inserted into a weak doorframe attached to a plasterboard or glass wall, offers paltry security. The intruder will bypass the lock and instead attack the door, frame, or adjacent wall. Thus, all of these parts must have comparable resistance to attack; otherwise, the security objective will not be achieved. Bolts and locks must be inserted so that they are temper-resistant and do not represent a temptation to the would-be intruder. Doors should be solid core wood doors or stave or solid wood flake doors with a minimum of 1.375 in. in thickness. Hollow doors, not filled with a second compositional material, are appropriate for security purposes.



FIGURE 10.3 Linking a resistive door with electronic monitoring. This secured door to a high-voltage signal room closet is protected by two kinds of locks. The lockset is an electrically released automatic deadbolt mortise lock, released by card reader or key from the exterior and ensuring free egress at all times from the interior. A card reader is to the left. (Source: Securitech Group.)

Vaults and Safes

Vaults are windowless enclosures with the walls, floor, roof, and one or more doors designed and constructed to delay penetration. Safes are containers, usually with one or more locks, and are smaller than vaults. Both vaults and safes are constructed with tool-resistant steel as well as brick, concrete, stone, tile, or similar masonry. The lock may be either electric or mechanical, with other locks placed on inside containers. But the essence of protection is provided by the combination lock, front, side, and back constructions.

Underwriters Laboratories (UL) provides standards for the burglary resistiveness of vault doors. For example, UL608 signifies protection against expert burglary attacks by cutting torches, fluxing rods, portable electric-powered and hydraulic tools, and common hand tools. UL also promulgates standards for safes. A typical standard (UL687) is for Class TL-30X6. This signifies a combination locked chest or safe designed to offer protection against entry by common mechanical tools for 30 min on all six sides. The safe weighs at

least 750 lb or, more likely, is equipped with suitable anchors to the floor substrate or on other surface. This last point is important. Safes that look and are heavy can be raised from the floor with an air pump; a tool can then be slid in the space created, and a hand truck can be slid under the safe moving it away with ease.

Burglar resistance and fire resistance are not the same things. Vaults and safes that are fire resistive demand a minimum thickness for walls on floors where they may be located. The National Fire Protection Association establishes minimum standards for the type of materials required to meet 2-, 4-, or 6-hour fire protection classifications.

Lighting Systems and the Need for Power Backup

Violent and property crime, disorder, and accidents occur disproportionately at nighttime and in poorly lighted areas. Good lightning therefore represents one of the greatest deterrents to crime, disorder, or unauthorized access after dark. Dark commercial areas that undergo improved lighting become accessible to more people and stimulate use. The technical quality, energy costs, and longevity of different lighting systems vary widely, although standards exist for minimum-security lighting (Box 10.1).

BOX 10.1 MINIMUM-SECURITY LIGHTING STANDARDS

Formal standards specify the minimum lighting required for different security applications. The topic can be complicated because of the irregular ways in which surfaces are illuminated at night. That is, a particular spot may meet minimum standards in one place, but a few feet away, the light may be inadequate. Security practitioners take readings with light meters over several spots to determine whether illumination is satisfactory, that is, meets the minimum standards. This device measures illumination in foot-candles, where a foot-candle is defined as the amount of light shining on a square foot of surface from a single candle 1 ft away. Generally, measurements are taken 3 ft off the surface – about waist high – or on the surface itself. Lighting specifications can also extend to the width of the lighted strip. For example, a vital structure with non-glare interference requires a lighted strip 50 ft total width from the structure; pedestrian entrances inside a fence require a 25 ft lighted strip.

Surface	Minimum-Security Illumination
Perimeter fences	0.5 foot-candle (ft-c) on either side of the fence
Building exterior	0.5–2 ft-c on the surface
Potential hazardous area	1–3 ft-c minimum
Parking lots (covered)	5 ft-c at about 3 ft above surface
Entrances	10 ft-c on ground level

Source: Illuminating Engineering Society of North America, 2011. Lighting Handbook, 10th ed. IES, New York, NY. Also note: Girard, C.M., 1989. Security lighting. In: Fennelly, L.J. (Ed.), Handbook of Loss Prevention and Crime Prevention, second ed. Butterworth, Boston, pp. 279–293.

Protective lighting should permit the public – including security officers on patrol – to easily see physical features in their immediate environment. Light should be evenly intense along the patrol route. Illumination may be directed toward the outer area where unauthorized people may seek to approach a facility. When buildings are to be protected, lighter or fluorescent colors and unobstructed areas for clear vision are advisable.

Security planners also are conscious of the need for standby and movable lighting to supplement normal lighting conditions. Emergency lighting may supplement standby and movable illumination and is used during times of power failure or other occasions when normal systems are inadequate. Normally, local public utilities are the primary sources for power, but all comprehensive security plans anticipate periodic, unpredictable outages. In such cases alternative power may be provided by standby batteries or diesel-driven generators.

Internet Protocol/Closed-Circuit Television

Television transmission that does not broadcast TV signals but rather transmits signals over a closed-circuit via an electric wire or fiber-optic cable is called a CCTV system.¹⁵ These systems are invariably part of integrated security systems, which combine CCTV surveillance with image storage and other devices.

The first generation of CCTV cameras used for security applications relied on cathode ray tubes (CRTs). These are vacuum tubes in which electrons emitted by a heated cathode are transmitted via a beam toward a phosphor-coated surface, which then becomes luminescent. CRTs have different performance qualities, requiring the systems designer to select different types of tubes according to the circumstances encountered. For example, some tube models are indicated for normal lighting conditions, others for nighttime or dusk, and still others where dark and bright light sources may appear in the same field of vision.

Beginning about 1990, security planners have shown a marked preference for a new generation of camera: the charge-coupled device (CCD). This is a camera that uses a chip – a solid state semiconductor imaging device – that transfers information by digital shift register techniques. Chip cameras have numerous advantages over CRT technology. As a result of their light weight, CCDs present less demand on their environmental housing and on motors that pan-tilt-zoom the mechanism. They are smaller in size, lending themselves to aesthetic demands of the environment as well as use in covert surveillance. Of greater significance still is that picture quality is superior with no loss of definition at the edges of a visual field. CCDs are also rugged. The smearing and blooming that plagued tube cameras and created burned spots do not occur with CCDs. Additionally, chip cameras offer good value with a lifetime use several times that of a CRT model. These systems require hardwiring. However, within a few years, wireless battery-operated camera installations will be available.

Till 2015, about half the installed base of television used for security purposes has remained analog. But decision makers prefer CCD technology for new installations. Still another advantage of this technology is that images can be transmitted via IPTV. This permits images to be accessed anywhere an Internet connection is possible. For example, the security director is at home on a weekend. The alarm monitoring system calls to say that a

burglar alarm has been tripped. Is it a burglar or a false alarm? The director is able to scroll through images at the point of the alarm to see if police need to be called, or if the alarm is of no great consequence.

This is just one of the examples by which IPTV has revolutionized security and, for that matter, public safety. The revolution continues. Many managers conceive of placing large areas of operations under camera surveillance. These have some deterrent value. Much more certain is that after an incident, clear identifiable images of suspects are immediately available to law enforcement for their investigation. With costs for systems declining as quality improves, IPTV represents a powerful resource to make the working environment safer.

Monitors of IP/CCTV Displays

IP/CCTV systems involve more than cameras. Monitors are devices for viewing a television picture from the output of a camera. The monitor may display the video signal directly – live from the camera, from videotape or other stored media, or from special effects generators. Often, but not invariably, monitors possess better performance characteristics than those made for consumers, and their price generally reflects this. Digital monitors are available in standard sizes of 5, 9, 12, 15, and 19 in., with the 9-in. screen being used most widely. Larger-size screens are used when the application divides the screen into multiple images or when a security officer wishes to move an image from a small screen to a larger one for better visibility.

Text information may be superimposed on the visual screen and made part of the visual storage record. The text may include time, date, camera number, and location. Additionally in some large monitor systems, text details can be superimposed on the field. This permits a console operator to make an informed decision by accessing records that bear upon the required action to be made (Figure 10.4).



FIGURE 10.4 Communications and command in a control center. Internet protocol television (IPTV) and closed-circuit television (CCTV) are integral parts of a comprehensive premises protection plan. Here a security monitor is able to view data and live action on displays. Action requiring greater attention can be switched to one of the large screens in the center. (Source: AT&T.)

Flat screen monitors, not long ago costly extravagances, have reduced in price while quality has improved. Flat screens possess numerous advantages over conventional CRT models. It is likely that CRTs will cease to be made within the next generation as the attractiveness of flat screen options grows steadily. Three types of flat screen display are available. Rear projection is not used extensively for security monitoring, although it is often selected for training purposes. The more desirable technologies are plasma and liquid crystal display (LCD). For security applications in big screen displays plasma has many advantages over LCD. Plasma permits a 160° viewing area from all sides compared with 120° for rear projection and 40° for LCD. It has a brighter picture, better color purity, and higher contrast ratio than LCD. An earlier complication of plasma display was image burn-in. An existing disadvantage of plasma is that the screen creates more heat than competitive technologies. For small screens (less than 37 in.) LCD is preferable. These flat panels are lighter and best for desktop placements. Both plasma and LCD have about the same life span rating (typically 60,000 hours to one-half brightness).

Images may be transferred from the camera to the monitor via coaxial cable (commonly RG59U or RG11U), fiber-optics, and, increasingly, wireless means such as radio frequency (RF) or microwave transmissions. Signals can also be transmitted via telephone lines, making it possible to monitor signals over the Internet.

Recording Devices and Media

IP/CCTV images collected for security purposes often are recorded and archived temporarily. Real-time videocassette recorders (VCRs) record the signal from a video camera onto magnetic tape. During playback, the video signal is reconstituted for viewing on a monitor or, if needed, printed copies of images may be downloaded. VCR videotape has a finite life depending on the speed with which the image was registered on the tape and the frequency on which the tape was re-recorded. Tapes that have been used beyond their normal lifetime may be useless for identification purposes. The advent of new digital storage media enhances the ability of an image to be retained for long periods of time, retrieved when needed, and to do so at low cost.

More recently digital video recorders (DVRs) have been replacing VCRs. DVRs record video signals from IP/CCTV with numerous advantages over earlier analog technology. Digital recordings provide many features unavailable from the previous generation of technology; for example, audio may be included with the imaging. DVRs may be PC-based or embedded. PC-based DVR is made possible with the installation of capture cards. Embedded-type DVRs record directly to storage systems. DVR software is available in three different operating systems: Linux®, Macintosh®, and Windows®.

VCRs, DVRs, and other storage technology have made immense improvements in the utility of security systems. These are further enhanced since contemporary systems often have built-in time/date/camera number generators. For prosecution purposes, the evidence collected by such images can be persuasive. Similarly, descriptive inserts on the screen can pinpoint where the images are being recorded.

A single IP/CCTV system can include hundreds or thousands of cameras, if needed, within a unitary configuration. A video multiplexer allows the same system to encode, decode, or view live multiple scenes at the same time.

Images may be retained in several places. Years ago VCRs and digital cassette recorders (DCRs) were the most expected place for image storage. However, images may be also stored in a hard disk within a host system. Another option is at the camera itself. A smart camera may be programmed to record only certain activities of interest. If nothing happens, no recordings are made and storage is not wasted. Yet another and highly important storage area is the cloud. Here images may be stored and accessed only if there is a need to. Such cloud-based storage system may have inherent security risks, although none have been demonstrated to date. What is clear is that even with cheap storage costs the fees add up. Management must set an image retention policy that will delete stored images without value. (Naturally, if an incident occurs, images prior to, during, and after it should be retained for several years.)

Video Surveillance Trends

The strategy of how to use IP/CCTV output has evolved over the past generation. In earlier years it was assumed that the best practice was for console monitors to be silent to any exception that might be seen on the screen and then react to it. This was a futile expectation. The next phase was to regard the system primarily as a deterrent but also as a recording medium to aid in the identification of a suspect in an incident or to confirm aspects of an event that was captured by the video system. Systems today have enormously more and better-quality surveillance capacities. Further, the information flow has been expanded enormously by wireless technology. Real-time off-site video storage that can be “water-marked” permits the use of video to be stored for future retrieval and forensic use, if necessary. Since visual images may be stored on large servers, the capacity to maintain extensive libraries for longer periods of time than were possible with VCR cassettes is now a reality. As mentioned above, the cloud is also a storage medium that can be used.

Seamless communications allow video information to be monitored conventionally at a console station or anywhere else. Security managers have the capacity to link a video or data feed to their personal digital assistants (PDAs), laptops, tablets, desktops, or smartphones. Decision making for critical events can occur anywhere as the information flow is transmitted fuller whenever wireless transmission can be accessed.

Technical Features

Selecting the right lenses for IP/CCTV systems is an integral part of a high-performance system. Most lenses used for security purposes are fixed focal length (FFL) and produce a single focal length (FL). A FL is the distance from the lens center to a location in space where the image of a distant scene or object is focused. FFL and FL are expressed in millimeters or inches. FFL lenses must be matched with the image sensor size or with the smaller sensor size. They cannot be used with a larger sensor size than that for which they are designed. For example, a 0.5-in. sensor formatted camera will require a 0.5-in. or larger

formatted lens. The image size of the picture is determined by the FL of the lens and has nothing to do with format size. Lenses for wide-angle and telephoto viewing also may be selected for applications. Zoom lenses are variable focal length (VFL) lenses that allow a smooth, continuous change in the angular field of view so that the view can be made narrower or wider depending on the setting. This is generally accomplished by a motorized adjustment that can be directed remotely. For covert surveillance or privacy purposes, pinhole lenses are widely available.

IP/CCTV is increasingly integrated with other technologically advanced resources. For example, video motion detection (VMD) is a software-based hardware device that detects intrusion and generates an alarm condition set by the parameters of the security system. CCTV images may also be used to confirm alarms from intruder detection systems, combining the CCTV with another intruder technology, and using the alarm of this technology to establish a video link to a remote monitoring center.¹⁶

Intrusion Detection Systems

Intrusion detection systems deter and detect potential entry to a protected area by unauthorized means. The security planner has an extensive choice of sensors that can identify such incursions to a protected location, each of which has advantages and disadvantages (Table 10.4).

Table 10.4 Intrusion Detection Systems

Type	Advantage	Disadvantage
Underground*	Hard to detect	Costly to install
Fence [†]	Increases deterrent value of fence	Does not detect tunneling
Photoelectric	Indoor, outdoor beams	Can be spotted and avoided
Microwave (exterior)	Cheap, easy to install	Requires line of sight
Microwave (interior)	Detects movement in area	Prone to some false alarms
Passive infrared	Reliable; inexpensive	Susceptible to defeat by covering lenses
Active infrared	Can protect oddly shaped	May require repeated adjustments
Ultrasonic	Covers large, diffuse area	False alarm from traffic, operating machines
Sound	Highest robbery detection	Privacy concerns
Capacitance	Triggered by weight	Avoidable, if known
Vibration	Identifies burglar tool use	False alarm from nearby operating motors
Door/window switches	Widely used, inexpensive	Magnets can defeat
Metallic foil	Detects window attacks	Cracks with age; unaesthetic
Glass breakage	Identifies breakage sounds	Can cause false alarm from street noise

Intrusion detection types are desirable for external perimeter and internal detection. No one system is ideal and many security planners employ two or more different kinds of sensors to protect the same area. Each type listed in the table has numerous advantages and disadvantages in addition to the principal ones noted.

*Such as buried microphones, underground sensor tubes, and buried seismic sensors.

[†]Such as taut wire, leaky cable, and microphone. Taut wires signal an alarm condition when someone places tension on the wire; leaky cable sends and receives an electric signal, which alarms when someone absorbs transmitted energy; and microphones collect audible signals of possible intrusion attempts. *Note:* Software for intrusion detection is a different topic and is related to protection of databases.

Sensors to detect possible intrusion may be used at outer or inner perimeters, within interior spaces (volumetric), and for particular objects or at spots requiring protection. The sensors discussed in this section are electronic. The principle of all of them is simple: a normal system is disturbed; it then goes into an alarm state. An audio alarm may be sounded at the site or at a distant monitoring station where security personnel evaluate the circumstances and respond as the situation warrants.

Numerous environmental and other factors need to be taken into consideration in order to determine which sensors are to be selected for desired security applications. More reliable sensors and systems are constantly being created.

The workhorse for interior (volumetric) motion detection is the passive infrared (PIR) sensor. This operates on the principle of heat detection. It is widely used in nonsecurity applications, such as to open doors in buildings. PIRs are sufficiently sensitive so that they do not cause false alarms from a wide ambient temperature range or from the heat of a small animal. However, PIRs may cause false alarms from hot spots caused by lights, bright reflections, and solar and mechanical heat sources. To overcome the possibility of false alarms, sensor manufacturers provide dual technology sensors, incorporating PIR with either microwave or ultrasonic technology. These sensors will not alarm unless both types of technology indicate an intrusion.

Access Control Systems

Access control systems control persons, vehicles, and materials through entrances and exits of a protected area. (The term is also used in computer security where it has a meaning in a different sense.) Access control systems use hardware and specialized procedures to control and monitor movements into, out of, or within a protected area. Access to protected areas may be a function of authorization time or level, or a combination of both.

In the concentric circles of protection concept, access control represents a particularly important protective measure. After all, if unwanted persons are kept out, losses will be minimized. Access control depends on the authorized person being correctly identified as part of the approval process. In a simple protective system, on-the-spot visual recognition of an unauthorized person, vehicle, or materials may suffice. However, large systems with numerous personnel and individuals with varying levels of authorization are best managed with systems that identify such persons automatically and with a high degree of certainty. Such systems typically involve use of three features:

- *Something that the person knows.* This can be an access code or password supposedly known only to the individual.
- *Something that the individual possesses.* For example, an approved identification (ID) card or a token that cannot be easily counterfeited.
- *Something physical and unique about the individual.* This could be a biometric feature such as a fingerprint, iris or retinal signature, writing dynamics, voice, or a person's facial features.

These characteristics can be designed into manual, semiautomatic, or fully automatic systems. Accept/reject levels can be set depending on the level of security desired.

Identification Numbers and Passwords

Individuals may select or be assigned an ID number for use in access control devices such as keypads. In higher-level security systems, individuals may gain access by using a keyboard in which letters and symbols can be combined with numbers. Systems that use numbers only may be compromised; hence, the ID number or a supposedly private password must be regarded as a minimum effort at system reliability. A password must be combined with other identifiable means to achieve a higher level of confidence.

Nonetheless, the dependence on passwords seems assured for the next generation or so. Passcodes for push-button entrances are adequate for law security, barriers, but should not be confused with passwords that must be unique to an individual. Computer passwords using Windows may be up to 135 characters in length. In practice for security applications a password should be at least eight characters long and be composed of upper and lower case letters, numbers, symbols, and punctuation. To periodically change the password – an important policy – the user needs alter only one character, for example, changing a lower case letter to upper case. With letters, numbers, symbols, and punctuation to choose from, the security-conscious user is able to create a password that is sufficiently robust that it will survive most directory-type attacks to discover it.

Consider *password example*: *Ineed\$s4mycars! Or cOmplic@t3d*. The first example makes a whimsical statement that the user remembers easily. The second one is more complicated. Upper and lower case letters, a number, a symbol, and punctuation mark are included. To change the password in the future the user could raise one lower case letter to an upper case; in this example the “n” becomes capitalized creating a new password.

The *revised password* becomes *INeed\$s4mycars! Or cOMplic@t3d*. In the event a person's original password is stolen or successfully spoofed, an entirely new password should be created. Of course, the examples above are for illustrative purposes and should not be used by readers. However, someone setting a new password can think of a technical word, unusual geographical location, bizarre nickname, or other word to use as the basis of a tough-to-crack choice.

ID Cards and Tokens

ID cards and tokens are available that vary regarding facility of use, degree of security, ease of automatic and personal identification, and cost. Badges may be permanent documents with a lifetime measured in years or they may be designed intentionally to expire within a defined period of time. Disposable self-expiring badges are available that self-void after being issued. Ink migrates from the back of the badge to the front, indicating that the time for its use has expired. These self-expiring ID cards are used in places where visitors are expected to remain a few hours but not more than a day.

Widely used cards and badges are likely to have more than one security feature, including visual images in color or black and white, logotypes, signature panels, key personal

information, encrypted data, magnetic stripes, computer chips, and redundant features to make counterfeiting difficult or impossible. Redundant features include holographs, microprinting, an isotope, and hard-to-obtain card stock. These ID cards may be visually identifiable, machine-readable, or both. Each factor affects use, image, and cost. Security operations planners often seek to commit to systems that may be used for extensive periods of time so that capital costs can be amortized.

Another feature for low- and medium-security applications is a distinctive lanyard. The ID card may have a photograph with a logo imbedded, bar codes, or machine-readable indicia such as QR (abbreviated from Quick Response code).

While the control of visitors and employees is emphasized, such systems have numerous capabilities that relate to other management operating concerns. For example, these systems may be linked to time and attendance procedures whereby individuals' payroll data can be created from normal badge use. Also, some systems indicate where in an organization the individual may be found at a particular time. Above all, however, such systems have remarkable flexibility in allowing or denying personal access to defined locations, much as an access control system for computer systems does. Records of such activities may be easily retained and consulted concerning access patterns. Lost cards may be replaced, while anyone who finds the lost ID and tries to use it could be shut out and called to the attention of security personnel. A single card could allow an individual into numerous facilities, including parking lots and at locations in other parts of the world if the organization is managed by a single integrated system.

Biometric Features

A password can be learned by or given to another person who could misuse it. An ID card, badge, or token may be lost or stolen and used by another until the card is no longer system-accessible. However, biometric features, such as fingerprints and iris or retinal information, rarely alter over a lifetime. Therefore, in theory, systems that use these features have a more reliable means of identification. Exceptions are as follows: identical twins may have substantially identical biometric features and certain progressive diseases may change a retinal pattern over time. Biometric systems have been made more user-friendly in recent years. They are no longer as expensive and now rely on simple hardware interfaces. In earlier years, some biometric systems used long data signatures that organizations had to store and then sort through for identification purposes. The cost of storing data signatures and searching among an extensive data file for a match is no longer a significant economic issue. New commercial biometric applications – such as facial recognition and wrist vein identification – have intriguing and important applications.

Like any system, biometric systems have limitations. Systems operate by first enrolling people into the system, often by taking several recordings of the physical feature crucial to the system. This analog information is transferred by an algorithm into a digital number according to a proprietary algorithm for the system. When a person seeking access presents a physical feature to be identified, the digital identifier will not be absolute, but will have some variability. Sensitivity can be adjusted by the systems operator. Hence, biometric

systems usually identify positively the person with the closest approximation to that found in the file. In using biometric systems, a trade-off may exist between ease of use with faster throughput from the system and a corresponding increase in false-positive rates.

False-positive (also called Type I or A) errors occur when an unauthorized person is able to access a restricted facility when he or she should have been denied entry. This is the more serious type of error. *False-negative* (Type II or B) errors deny admission to someone who rightfully should have been accepted but is not. This type of denial often occurs because the subject was hasty at entering his or her physical feature. A repeat attempt often confirms identification.

Radio-Frequency Identification

The functionality and application of radio-frequency identification (RFID) tags, badges, and readers has been a striking feature of security systems in the twenty-first century. Applications are constantly expanding and include access control, mustering, emergency rescue, automatic weigh scales, time and attendance contractor control, parking control, safety, and supply chain management.

RFID technology incorporates tags made of silicon chips and a miniature antenna.¹⁷ The chips store a unique ID code. Scanners authenticate the tag or product with the chip as it moves throughout a facility in the case of an ID card, or a product in the case of supply chain management.

The power of RFID systems is tremendous, some fear too much so. RFID cards can track movements of people much like a cellphone. Privacy concerns have been raised as a result. To aid supply chain logistics, Wal-Mart and other mass merchandisers have required major suppliers to embrace compatible RFID technology. To control high-risk, high-value medicines better, the US Food and Drug Administration has asked pharmaceutical companies to develop standards for RFID and implement them. Security is also improved with such applications.

Alarm Systems

Mechanical alarms were first used in the mid-nineteenth century.¹⁸ Today, alarm systems are predominantly electronic, although numerous types of alarms are available to meet a variety of needs. Alarm systems were created to deter, delay, and detect burglary, and they remain the main purposes of such systems. However, these alarm devices can detect and monitor other actions, including robbery (through a panic switch), smoke and heat signals, and requests for specific services. Such alarms may sound locally or be monitored by police, a proprietary system, or a commercial central station.

UL, a voluntary nonprofit organization, sets widely accepted and respected standards for alarm systems and vets the reliability of monitoring stations that receive the signals and act upon them. UL standards focus on burglary deterrence and detection capabilities. Types of UL burglar alarm certificates are shown in [Table 10.5](#). Customers with systems meeting UL standards often receive a certificate issued by UL at the request of the

Table 10.5 Types of UL Burglar Alarm Certificates

Type of Alarm	Coverage	Operation	Maintenance	Type of Equipment
Mercantile alarms	UL Std. 681 <i>Premises:</i> Extent: 2, 3, or 4 <i>Safe and vault:</i> Extent: complete or partial	Outside sounding device <i>Or</i> Sounding device <i>And</i> Remote connection to police or listed CS	Service within 18 hours One annual operational inspection	Mercantile burglar alarm units UL 365
Central station burglary	UL Std. 681 <i>Premises:</i> Extent: 1, 2, 3, or 4 <i>Safe and vault:</i> Extent: complete or partial	Supervision of openings and closings and guard investigation of alarms Response time and equipment used is shown on the certificate	1-hour response plus the designated investigator response time One annual operational inspection	Central station alarm units UL 1610
Bank alarms	UL Std. 681 Safe, vault, night deposit, and ATM Extent: complete or partial	Outside sounding device <i>Or</i> Sounding device <i>And</i> Remote connection to police or listed CS	Service within 24 hours One annual operational inspection	Mercantile burglar alarm units UL 365
Residential alarms	UL Std. 1641 Extent: basic or expanded	Sounding device required	Service with 24 hours One annual operational inspection	Household alarm systems UL 1023
Holdup alarms	Semiautomatic or manual	Manual or semiautomatic	Service within 24 hours One annual operational inspection	Holdup alarm units UL 636
Central station proprietary	UL Std. 681 <i>Premises:</i> Extent: 2, 3, or 4 <i>Safe or vault:</i> Extent: complete or partial	Supervision of openings, closings, and alarms by the subscriber UL 1076	Service within 18 hours One annual operational inspection	Proprietary alarm units UL 1076
National industrial security systems	UL Std. 2050 UL Std. 681 <i>Alarmed area:</i> Extent: 3 or 5 <i>Container:</i> Extent: complete	Supervision of alarms/ openings/closings (alarms only at police station) Remote connection to a listed central station, government contractor monitoring station, or police station	Service within 4 hours One annual operational inspection	Central station alarm units UL 1610 Proprietary alarm units UL 1076

Note: "Extent" of security device protection is described in the UL standards.

Source: Underwriters Laboratories, Inc.

UL-listed alarm service company that is maintaining the system. This certificate may be required for insurance purposes.

In addition to receiving and verifying alarm conditions, operators at the monitoring service may call and request that police be dispatched, call designated persons and inform them of the alarm condition, send security personnel to the premises, dispatch someone to reset the alarm, call the fire department or an ambulance, direct maintenance staff to check a machine or process stoppage or irregularity, and perform other desired actions.

Because of the perennial concern with false alarms, alarm installation and monitoring businesses endeavor to select systems with low likelihood of inaccurate signals. The customer may wish to have someone physically present as an antiburglary measure at the facility until the alarm service is restored. Training users how to avoid false alarms is essential to make good use of the service. Nonetheless, false alarms remain a problem. Therefore, many systems will verify the alarm before calling police or taking other action. This may be accomplished through a telephone call, real-time IP/CCTV, sending a runner or security officer to check the premises, or other means.

An inherent weakness of most alarm systems is that their signals travel over wires or cables that can be cut, intentionally or accidentally, leaving the alarmed premises without services. At the least, the monitoring center should confirm that a connection has been broken; it should inform customers promptly that service has been interrupted at their facility. The loss of a primary method of communication may be backed up with a RF system that does not depend on wires or cables.

Robotic Systems

Security officers frequently patrol office buildings, making observations and checking the safety and security of the premises as they do so. The same activity, theoretically, could be accomplished by robotics. A robotic device may be fitted with a variety of sensors and alarms. IP/CCTV on the mobile device can observe real-time activities; remote two-way communications can inject an immediate connection with the scene from a distant monitoring post. Robots can follow a fixed or random patrol and can climb or descend stairs, avoid unexpected obstacles, and either confront or retreat from a dangerous situation. Robotics has an intriguing potential to enhance the efforts of security personnel. However, the cost versus benefit ratio or using robotics to replace or supplement security officers has not been attractive to date, although costs are dropping. While a robotic system will work 24 hours a day, 7 days a week without complaining, frequent and costly service requirements have deterred wide use.^{¶,19} (In law enforcement, robotics has a secure place in confrontational circumstances such as bomb threat analysis. In some fire-fighting situations, robotic devices approach hot areas where even uniformed firefighters cannot approach safely.)

Security robotics in Japan is in advanced use to support activities of patrol officers. Robots are flexible in mounting on declining stairs and transmitting information back to

[¶] Robotics for security purposes should not be confused with applications for law enforcement, particularly in high-risk situations to evaluate bombs or contraband and to enter dangerous areas where lives are at risk.

a base. People can be detected by body heat, confirmed by IP/CCTV, queried by two-way communications, and, if necessary, scared by a loud noise or other warning. Robots can be selected for their likely need at the location. For example, a robot can detect bomb materials from sensors that approach a suspicious person or object, thus not placing the welfare of the security officer at risk.

Drones for Security Use

Drones are able to extend the reach of security services – quickly, remotely, and at little cost. The drones can take pictures and send them back to base, order someone to take a particular action, or perform other services for security. The Federal Aviation Administration (FAA) prohibits the use of an unmanned flying vehicle for commercial purposes. Exemptions are available when drones travel over one's own property for security purposes if no risks to aviation are posed.

Nonetheless, FAA regulations will be made public in 2016 that may provide exemptions more broadly. Quadcopters can shoot images of a distant alarm condition and can even provide two-way communication with persons at the site of the alarm. Currently, amateurs and hobbyists are driving interest in drones. Amateur drone pilots may not fly them higher than 400 ft off the ground and not lose sight of the vehicle.

Communications

Effective security operations must allow seamless communication among managers, supervisors, staff personnel, and others. This is a requirement during normal operations. During an emergency, this requirement is even more important. Because a single system might be compromised or incapacitated due to an emergency, security planners think in terms of multiple channels by which personnel can stay in touch during such times.

Typically, security planners rely on commercial telephone service as the basis for communications. However, some applications will merit the use of a dedicated system that serves only a single organization or network. Dedicated lines to local law enforcement authorities, fire, or ambulance services are common features at larger central monitoring stations. In the event that hard-line communications are down, contact with significant parties by two-way radio or cellular telephone is important.

Many security managers have different layers of personal communications. They will have available ordinary telephone service and, in high-security applications, a separate encrypted communications system. They may also carry with them a two-way radio, personal pagers, and smartphones. Wireless Fidelity (Wi-Fi®) and voice over Internet Protocol (VoIP) are transforming communications. Wi-Fi is a term promulgated by the Wi-Fi Alliance and refers to networks that are interoperable despite the manufacturer of the component or the specific transmission band used. Wi-Fi enables text, images, and voice to be sent without wires. It adds immeasurably to security control, but protection of such transmissions poses challenges for the administrator.²⁰ Also, such electromagnetic wave transmissions can be downgraded by solar flares and adverse weather conditions. Wi-Fi is limited by the

output power of the transceiver, the distance between the transceiver and the antenna, and the height of the above-ground antenna. VoIP uses the versatility of corporate Wi-Fi local area network (WLAN) to transmit information with high-quality production characteristics. WLAN permits security executives to stay in touch with inputs from the system with flexibility and low cost.²¹ Wi-Fi and VoIP applications are growing rapidly. With voice, audio, video, and text applications, quality of service may be a challenge to the bandwidth of some organizations. The network owner can set priority levels that correspond to different types of traffic. Individual data streams can be prioritized according to the individual requirements considered most significant to the user.

Information Security Systems

Protection of data systems is an important and complex topic. The nature of cyber-threats continues to grow as networks play a larger role in everyday operations and as new vulnerabilities from the Internet and e-commerce emerge. Information security is covered competently in other books;²² for the sake of this discussion, physical security and systems protection will be considered.

Physical Security and UPS for Information Systems

Data facilities are usually considered one of the most restricted and sensitive areas in an organization. Unauthorized visitors are not welcome. Extensive measures are taken to protect hardware and software of the central processor, as well as file storage areas, other processors, switchers, and communications lines. Many of the highest applications of access control are applied to the computer environment. In addition to access restriction, attention is given to fire risks within such a facility.

Protection against loss or disturbances in electrical power is generally a protective activity. An uninterruptible power supply (UPS) is one way in which normal operations can be maintained at least temporarily when power fails. UPS systems may be provided with batteries and supplemented with a solid state rectifier that continually charges a battery bank. Additionally, an emergency alternator, such as a diesel engine or gas turbine, may be available to drive the alternator. Such UPS systems may provide emergency power for a few minutes to a few hours when hopefully regular power may be returned.

A more common problem with computer systems relates to power irregularities that cause momentarily spikes, surges, and drops in voltage levels. In the event power loss exceeds the capacity of the UPS system, the system should be backed up and, if possible, activities transferred to another facility not likely to be affected by the power failure. Data must be backed up, preferably on a real-time basis, although batch or computer-run backups will be adequate for less than critical applications. Backup may be via teleports, physical records archival procedures, and other means.

Systems Security

Hardware and software used to protect local area networks (LANs) and wide area networks (WANs) are supplemented by numerous procedural factors to enhance file service

security. These measures concentrate on log-in, password, trustee, directory, and file attribute security. Other factors such as directory and user creation must be safeguarded from being easily compromised by those outside the system. Firewalls, encryption, and traffic management systems also play important roles in reducing the possibilities of successful attack from those outside the LAN.

A major issue in IP security has been protection of transmitted or stored data. Encryption of transmitted and stored information is a vital safeguard. The emergence of enterprise digital rights management (E-DRM) allows the possessor of data to control how others may access it.²³ E-DRM combines encryption with access control application software. Sensitive data can be protected on remote desktops in e-mail, or when copied to CDs or USB drives.

Other Considerations: Disposing of Media; Tempest

Preventing sabotage, vandalism, and theft are high priorities of data security. While a process center may be protected internally by robust physical security, other considerations must be included in planning. Printed records, diskettes, printer ribbons, and tapes may be destroyed by a shredder or turned over to a bonded destruction service. When disposing of printers, copiers, or any other computing medium with a memory, the memory must be purged. If necessary, it may be physically destroyed to prevent others from accessing the information.

Electronic collection of information is also possible. In high-security federal systems, “Tempest” programs prevent electronic emanations from leaving the immediate environment and being collected and analyzed presumably by an adversarial power. Tempest-enclosed components are much more expensive than devices without such protection and must be certified by the Department of Defense.

Contraband Detection

Articles or materials that are illegal for the public to possess and carry into one’s protected area might be screened by specialized processes. A physical pat-down may identify the presence of the weapon on an individual carrying one onto a commercially scheduled airline, for example. However, a pat-down process is slow, uncertain, objectionable to many, and costly. By contrast, automated systems that screen for such illegal objects are rapid, more reliable, nonintrusive, and cost-effective when large numbers of persons must be screened. Like other types of preventative technology, contraband detection systems are constantly evolving.

X-Ray

Packages, garments, and baggage may be inspected by X-ray technology for contraband, including explosives and illegal drugs. Computer-enhanced and analyzed images increase the accuracy of contraband identification. Agents must monitor the enhanced images to determine whether a physical search is indicated. The principle of X-ray technology is that pulsed energy that penetrates most objects (lead and some alloys are exceptions) is absorbed by a

plate, which then intensifies the image of materials programmed to be highlighted by intense, distinctive coloring. The images are projected for analysis on a color monitor.

X-rays have some disadvantages. Some explosives and bomb-making materials may mimic items normally found within packages or luggage. Similarly, some firearms have plastic parts and are not easily identifiable in enhanced X-ray imaging. Sometimes a weapon can be hidden along the edge of a suitcase that is difficult for a screener to detect. Much depends on the skills of the agent who interprets the images. Surely, the enhanced use of X-ray technology since 9/11, drawing upon advances in medical imaging, has reduced the carrying of weapons into scheduled airlines or into other facilities that employ this technology.

Explosive and Drug Detection

While X-rays may detect some explosives and illegal drugs, other technology may be specifically devoted to such detection. The physical principle is that explosive compounds and illegal drugs may be identified either by sniffing for telltale molecules of the contraband materials or by bombarding a container with energy that will “excite” materials such that they can be identified automatically. Walk-through detectors currently available are found in preboard screening programs of airlines and other high-risk locations (Figure 10.5). This technology permits screening packages or luggage

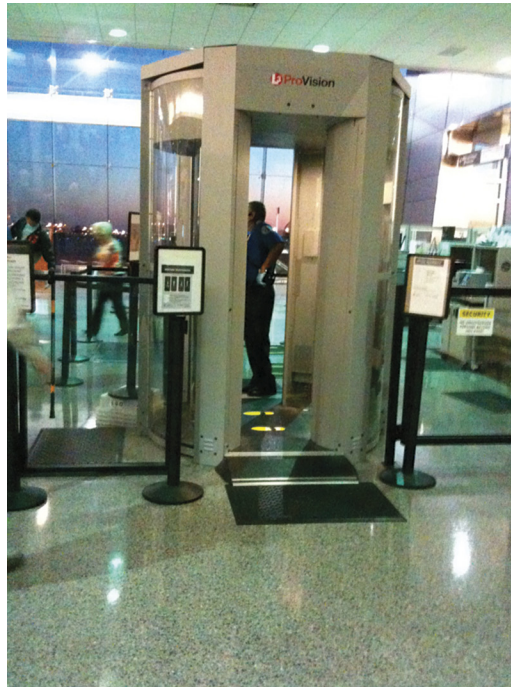


FIGURE 10.5 Walk-through detectors to identify contraband. Walk-through detectors may identify weapons or contraband materials as part of a preboard screening process at an airport, as seen here, or for protection in entering a high-security location. (Source: L-3 ProVision.)

without opening the contents. The accuracy and utility of such systems vary greatly. A bomb-detection system may be highly reliable, but it could also be stationary, costly to operate, subject to variable service problems, slow to process items, and expensive to purchase. Other devices are lighter, portable, and less expensive, but with an equivalent lower detection rate.

A drawback is that some materials may be prepared with such awareness of the detection technology and its limitations that their contraband contents are undetected. While thought of not so long ago as a technology with limited application, these detectors increasingly have broader applications as access control becomes more necessary in screening members of the public.

Metal Detectors

Most metal detectors operate by transmitting a time-varying magnetic field, which is monitored by a receiver (Figure 10.5). When a metallic object is introduced into the electromagnetic field, reception of the signal is disturbed; this is then reported by a light, an audio signal, or both. Walk-through metal detectors may also indicate where on the body metal has been identified. A security officer may then use a handheld metal detector to identify precisely where under the clothing the metal is hidden.

A disadvantage of metal detectors is that they can provide false alarms from metal within the body, such as from a prosthetic device or other types of surgical implants. Also, the sensitivity of metal detectors may be changed at the discretion of the operator. For example, sensitivity can be so acute that a single coin or a metal button weighing less than 0.5 oz can be detected. In such cases, however, the throughput is slow. Yet the same instrument can be set less sensitively so that small weapons will escape detection. Walk-through metal detectors can be configured to include explosive and drug detection during the same screening.

Fire Detection and Life Safety

About 488,000 fires occurred in the United States in 2013. Losses ranged from \$9 to \$21 billion in property loss in a recent decade.²⁴ The majority of structural fires (79.3%) are residential. However, about 18,000 fires in stores and offices and 6000 in institutions occurred in 2013. The trend for such events has been on a decline numerically, while the property losses have varied. Improved techniques for constructing fire-resistive structures and improved fire suppression procedures have produced beneficial results. Tragic multiple-death fires are less likely to occur, particularly in commercial, industrial, or institutional buildings. In the most recent year for which data are available, 3900 civilian fire deaths occurred. But of these only 80 took place in nonresidential structures. These include store and office buildings, educational, public assembly, industry, utility, storage, and special structure properties. Meanwhile, these advances have been offset partially by loss increases from the number and value of such structures.

Smoke and Heat Detectors

Two technologically different smoke detectors are widely available. The ionization type uses a small amount of two radioactive materials (usually americium-241 and radium-226) to make the air electrically conductive – or to ionize it. Smoke from flaming fires contains carbon particles that are electrically conductive. When they enter the ionization chamber of the smoke detector, an alarm is activated. Hence, flaming fires with darker combustion products tend to trigger this type of detector better than other types of fire.²⁵ This type of smoke detector is susceptible to low temperature, high humidity, and dirt or dust that may interrupt the current and cause a false alarm.

Photoelectric smoke detectors by contrast operate on a light principle. Smoke entering a chamber either obscures the beam's path to a photocell receptor or reflects light into a photocell, causing an alarm condition. Visible particles common in smoldering fires are apt to cause an alarm with such a detector faster than an ionization type.

Ionization and photoelectric detectors require some maintenance relative to heat detectors, but are more sensitive and provide an earlier warning of fire. Since the type of fire or fuel that may affect an area often is unknown, the best strategy may be to use both types of smoke detectors in the same system. While smoke detectors may be battery operated, such devices are usually found in residences. Industrial and commercial applications require that smoke and heat detection systems be hardwired and monitored by a system.

Another type of fire-detection technology measures heat. These detectors have the lowest false alarm record, but are slow to respond to incipient fire conditions. One type of sensor is a fixed-temperature detector, which uses a bimetallic strip thermostat possessing a different coefficient of expansion for two metals. When the detector is heated, the strip bends in one direction in a way that an electrical circuit is completed, causing an alarm.

A rate-of-rise detector goes into an alarm state when the temperature increase exceeds a stated rate, usually 12–15°F/min. These detectors may trigger a false alarm when temperatures increase rapidly but not because of a fire. They also may not respond when a fire propagates slowly with a gradual temperature rise.

In industrial applications, still other specialized smoke and heat detectors are available. Security planners often elect to use a combination of detector types to increase the possibility of early detection of fires.

Life safety considerations are embodied in design and construction methods. The National Fire Protection Association promulgates the *Life Safety Code* (NFPA #101), which is revised every 3 years. The code contains detailed provisions and requirements relating to structural occupancy, wall openings and door fire resistance, emergency lighting, smoke and fire detection, and other topics.

One life safety trend has been the increased use of automatic sprinkler systems. A national standard (NFPA #13) relates to the design and installation of such systems, which mandates that only qualified contractors should install these systems. Six main types of sprinkler systems exist, and numerous models of sprinkler heads are available for different applications. Systems currently available break water into a fine mist, thus extinguishing

the fire with greater efficiency and causing less property damage than past types in which large water droplets were discharged from more sprinkler heads than were needed to suppress the fire.

Designing Security Systems

Security operations managers tend to follow a formal process when a significant new security system is required or when an existing system faces an upgrade. Once management determines that the capital investment for such a system must be considered, the following steps generally are taken:

1. *Preliminary design.* The manager and the project team assume various tasks. Necessary physical information is collected, such as existing facility drawings and security documents. Often with the help of an architect, engineer, or consultant, project scheduling and initial cost estimates are produced relative to the design requirements. Special attention is given to assure that all components are compatible with each other. The system and its components should be scalable. That is, expansion or contraction should be possible without affecting performance.
2. *Design approach.* After approval of the initial design requirements, preliminary drawings, including site plans and system block diagrams, are produced. A cost analyzer will review the requirements and produce a cost estimate range. Each component in the system will be specified. Estimators may use worksheets – paper or electronic – to determine project costs, an example of which is shown in [Figure 10.6](#). The cost analyst will identify possible job cost and time-completion uncertainties at this time. The design will consider such issues as crime prevention strategy, human factors including ergonomics, and the rapid change of technology likely to affect the project. Such issues as operational factors, communications, lighting, power sources, terrain, emergency possibilities, and year-round weather variability will also be considered. A more detailed cost estimate will be created next, including design cost, hardware (including some extras), installation, construction supervision and testing, security during construction, and other costs such as contractors' taxes, profit, bonding, and a contingency fee to be held pending completion of the project.
3. *Bidding or negotiation.* The project will be placed up for bid for local and regional contractors. These will be evaluated by management and its consultant prior to awarding the contract. While management seeks to achieve the best price, total overall value is the primary objective, and frequently the lowest bidder is not awarded the contract. Point systems are often used to help select the winning contractor.
4. *Construction phase.* This is the period and process in which the materials and services are integrated and the work is undertaken to construct, assemble, and install the system.
5. *Testing and training phase.* Integrated security systems are complex. As portions of the system are completed, they need to be tested repeatedly to make sure they

Security alarm system planning estimate form					
Product		Brand, type	Cost	Quantity	Total
Control panel	Burglar alarm				
	Burglar-fire				
	Residential				
	Commercial				
	Digital communicator				
Remote stations	Digital keypad				
	Keyswitch				
	Electronic guard monitoring				
Perimeter detection	Magnetic contacts				
	Glass breakage				
	Fence sensors				
	Outdoor beams				
	Shock, vibration				
Interior detection	Ultrasonic				
	PIR (volumetric)				
	PIR (wide angle)				
	PIR (long range)				
	Microwave				
	Photoelectric beams				
	Passive audio				
	Switch mats				
	Verified sensors				
Fire	Smoke detectors – ionization				
	Smoke detectors – photoelectric				
	Pull stations				
	Heat sensors – rate-of-rise				
	Heat sensors – fixed temperature				
Audible visible	Alarm				
	Bells, horns				
	Strobe lights				
Reporting backup	Digital communicator				
	Communications backup				
	Power backup				
Other	Holdup/panic				
	Safe/vault sensor				
Total					

FIGURE 10.6 Using a form to plan security alarm costs. An electronic form is usually preferred due to the extensive changes required. Often general contractors will propose an estimate that will encompass actual cost of parts, labor charges, overhead, and profit.

perform as intended. Too many false-positive or awkward system integration needs to be minimal. Similarly, operations personnel may be trained by installers and manufacturers on using the new systems. Operating manuals, paper and electronic instructional materials, and possibly graphic user interfaces (GUIs) may be created for use by personnel who will remain to operate the system.

6. *Operational phase.* The system is fully installed and operational. Unexpected adjustments are made. The final payments to the engineers and contractors are authorized pending approval and acceptance of the work completed.

Summary

In this time of high-tech innovation, security systems constantly draw upon new advances, incorporating them into a cohesive, integrated system. Increasingly, management seeks technical resources to improve the quality of protection operations while decreasing operational costs. The Internet offers management an extraordinary tool for flexibly, reliably, and economically controlling operations from disparate locations and under different circumstances.

Discussion and Review

1. How does situational crime prevention differ philosophically and practically from the traditional objectives of policing?
2. Why must security planners be involved early in facility design? What is the expected payoff from such involvement?
3. What is the reasoning behind security signage? What are its drawbacks?
4. Explain the limitations of cylinder-type locks.
5. Why have cylinder-type locks been the mainstay for commerce and industry for almost a century? Why have electronic proximity locks become preferred for some installations?
6. Why is CCTV almost invariably an important part of an integrated security system?
7. Describe capacities and qualities of a central alarm monitoring station.
8. Provide examples of noninvasive technological methods to detect contraband.
9. What critical stages occur before a security contractor is selected to undertake a major contract?

Endnotes

¹ Young, J., 1994. Incessant chatter: recent paradigms in criminology. In: Maguire, M., Morgan, R., Reiner, R. (Eds.), *The Oxford Handbook of Criminology*. Clarendon Press, Oxford, p. 86.

² Newman, O., 1972. *Defensible Space: Crime Prevention Through Urban Design*. Macmillan, New York, NY.

³ Mayhew, P., 1979. Defensible space: the current status of a crime prevention theory. *Howard J. Penology Crime Prev.* 18, 150–159.

- ⁴ Brantingham, P.J., Brantingham, P.L., 1981. *Environmental Criminology*. Sage Publications, Beverly Hills, CA; Brantingham, P.J., Brantingham, P.L., 1984. Surveying campus crime: what can be done to reduce crime and fear? *Secur. J.* 5 (2), 160–171.
- ⁵ Examples from the literature include Clarke, R.V., 1992. *Situational Crime Prevention*. Harrow and Heston, Albany, NY; Clarke, R.V., 1997. *Situational Crime Prevention: Successful Case Studies*. Harrow and Heston, Albany, NY; U.S. Department of Housing and Urban Development, 1997. *Creating Defensible Space*. Criminal Justice Department, Office of Policy and Research, Washington, DC.
- ⁶ Gigliotti, R., Jason, R., 1984. *Security Design for Maximum Protection*. Butterworth-Heinemann, Boston, MA.
- ⁷ Hopkins, A.A., 1928. *Lure of the Lock*. General Society of Mechanics and Tradesmen, New York, NY, pp. 29–31.
- ⁸ Fay, J.J., 1987. *Butterworth's Security Dictionary*. Butterworth-Heinemann, Boston, MA, p. 142.
- ⁹ de Sélincourt, A. (Trans.), 1960. *Livy: The Early History of Rome*. Penguin Books, Baltimore, MD, pp. 376–377.
- ¹⁰ Eden, R.S., 1993. *K9 Officer's Manual*. Detselig Enterprises, Calgary, AB.
- ¹¹ Garcia, M.L., 2006. *Vulnerability Assessment of Physical Protection Systems*. Elsevier Butterworth-Heinemann, Burlington, MA, p. 207.
- ¹² Gigliotti, R., Jason, R., 1992. Physical barriers. In: Fennelly, L.J. (Ed.), *Effective Physical Security*. Butterworth-Heinemann, Boston, MA, p. 77.
- ¹³ *Barrier Technology Handbook*, 1980. Sandia Laboratories, Albuquerque, NM.
- ¹⁴ Craighead, G., 2008. *High-Rise Security and Fire Life Safety*, third ed. Butterworth-Heinemann, Burlington, MA, p. 256.
- ¹⁵ McCrie, R.D., 2006. A history of security. In: Gill, M. (Ed.), *The Handbook of Security*. Palgrave Macmillan, New York, p. 26.
- ¹⁶ Damjanovski, V., 2014. *CCTV: From Light to Pixels*. Butterworth-Heinemann, Waltham, MA.
- ¹⁷ National Research Council, 2004. *Radio Frequency Identification Technologies: A Workshop Summary*. National Academies Press, Washington, DC.
- ¹⁸ McCrie, R.D., 1988. Development of the U.S. security industry. *Ann. AAPSS* 498, 24–25.
- ¹⁹ Harrington, J.J., Jones, D.P., Klarer, P.R., Morrow, J.D., Woien, R.M., Wunderlin, E., 1989. Sandia National Laboratories proof-of-concept robotic security vehicle. In: *Proceedings of the 5th Annual Symposium and Technical Displays on Physical and Electronic Security*. Armed Forces Communications and Electronic Association, Philadelphia, PA, pp. B3–B16.
- ²⁰ Chan, H.-L., 2005. Overcoming the challenges of wireless transmission. *Secur. Technol. Des.* 15 (10), 46–48; Silverman, L., 2005. Wi-Fi here and now. *Secur. Technol. Des.* 15 (5), 36–41.
- ²¹ Anderson, R., 2005. IP access on the way. *Secur. Technol. Des.* 15 (1), 30–34.
- ²² For example, see: Biringer, B.E., Vugrin, E.D., Warren, D.E., 2013. *Critical Infrastructure System Security and Reliability*. CRC Press, Boca Raton, FL; Das, S.H., Kant, K., Zhang, N., 2012. *Handbook on Securing Cyber-Physical Critical Infrastructure*. Butterworth-Heinemann, Waltham, MA; Doherty, E.P., 2013. *Digital Forensic for Handheld Devices*. CRC Press, Boca Raton, FL; Freund, J., Jones, J., 2015. *Measuring and Managing Information Risk*. Butterworth-Heinemann, Waltham, MA; Gonzalez, D., 2015. *Managing Online Risk: Apps, Mobile, and Social Media Security*. Butterworth-Heinemann, Waltham, MA.
- ²³ Software: to protect email & precious documents, just seal them, 2006. *Secur. Lett.* 36 (8), 3.
- ²⁴ Insurance Information Institute, 2014. *The I.I.I. Insurance Fact Book 2015*. Insurance Information Institute, New York, NY.
- ²⁵ Ladwig, T.H., 1991. *Industrial Fire Prevention and Protection*. Van Nostrand Reinhold, New York, NY, pp. 148–154.

Additional References

- Barry, J., Finnegan, P., 1997. System integration. In: Konicek, J., Little, K. (Eds.), *Security, ID Systems and Locks*. Butterworth-Heinemann, Boston, MA.
- Black, I.S., Yeschke, C.L., 2003. *The Art of Investigative Interviewing*. Butterworth-Heinemann, Waltham, MA.
- Caputo, A.C., 2014. *Digital Video Surveillance and Security*, second ed Butterworth-Heinemann, Waltham, MA.
- Felson, M., 2006. *Crime and Nature*. Sage Publications, Thousand Oaks, CA.
- Gouin, B., 2007. *Security Design Consulting: The Business of Security System Design*. Butterworth-Heinemann, Burlington, MA.
- Kirchner, Jr., R., 2014. *Surveillance and Threat Detection: Prevention Versus Mitigation*. Butterworth-Heinemann, Waltham, MA.
- Lang, R., 2005. The new functions of RFID technology. *Secur. Technol. Des.* 15 (2), 28.
- Levine, D.E., 2005. Wide open Wi-Fi. *Secur. Technol. Des.* 15 (8), 54.
- Park, P., 2009. *Voice Over IP Security*. Cisco Press, Indianapolis, IN.
- Richey, D., 2015. The security enterprise and integrator game plan. *Security*, March, p. 20.
- Smith, S., Marchesini, J., 2008. *The Craft of System Security*. Pierson Education, Boston, MA.
- U.S. Department of Housing and Urban Development, 1997. *Creating Defensible Space*. Office of Policy and Research, Washington, DC.
- Zwirn, J.D., 2014. *The Alarm Science Manual™*. Zwirn Corporation, Tenafly, NJ.

Further Reading

- Biometric impact on privacy in the public sector. <www.bioprivacy.org>.
- Haas, D.J., 2010. Electronic security screening: its origin with aviation security 1968–1973. *J. Appl. Secur. Res.* 5, 460.
- McMunn, M., 2006. Machine readable travel documents with biometric enhancement: the ICAO standard. ICAO MRTD Rep. J. 1, 1.
- Quinn, G.W., Grother, P., 2012. *Iris Exchange (IREX) III*. NIST, Washington, DC.
- Woodward, K., 2006. EPassports await real-world tests. *Card Technology*, March 1.

Global Leadership for Optimal Security Operations

Leadership is a matter of intelligence, trustworthiness, humaneness, courage, and sternness.

—Sun Tzu, *The Art of War*

Organizations require leadership in order to commence, grow, survive adverse circumstances, and adjust to constant change. Leadership knows no geographical boundaries. It may be reflected locally, but its impact may be global as the precepts in this chapter demonstrate.

Leaders can be entry-level workers, contract employees, full- or part-time employees, managers, executives, or members of the board. That is, leadership can come from anyone with a position to understand and influence organizational outcomes. Arthur Jago defines leadership as “both a process and a property.” He further states:

The process of leadership is the use of non-coercive influence to direct and coordinate the activities of the members of an organized group toward the accomplishment of group objectives. As a property, leadership is the set of qualities or characters attributed to those who are perceived to successfully employ such influence.¹

This chapter will pursue the topic of leadership from four perspectives. First, we will look at the aspects of leadership that are supported by widespread experience, empirical research, or both. Next, we will look at distinctive characteristics of security functions and how they differ from other management disciplines. Third, we will look at the discrete tasks that a twenty-first-century leader of security programs may be most fully engaged in. And, finally, we will opine briefly on the future of security operations as based on current trends.

Learning About Leadership

Leadership studies as an intellectual discipline began in the 1970s under James MacGregor Burns at Williams College. Since then programs have grown to support and analyze research in the field.

Many writers on leadership generalize about styles that lead to high performance in which vision, trust, listening, and participatory skills are delineated.² Positive and effective leadership has always been understood as a critical component for organizations to

succeed. The search for such qualities – particularly at managerial and executive levels – is unyielding. Insight into the traits of good leaders may come from numerous disparate sources, including literature.³ Further, looking at past military strategies can provide insight into the behavior of current organizations.⁴ Meanwhile, the use of humor to lead organizations and improve management has received attention, especially for its ability to overcome personal inhibitions and to improve communications and marketing objectives.⁵

Books that interpret past high achievement behaviors and apply them to contemporary situations frequently are valuable. Equally or more significantly, research on the nature of leadership also has emerged as a valid topic. For example, researchers on leadership have studied the lives of elite MBA recipients to understand their personal qualities and how they relate to the functioning of organizations.⁶ Until recent years, most criteria for leadership selection and training have not been adequately validated by empirical methods. However, leadership has moved from being anecdotal, personal, and inspirational to being based more on principles that use scientific methods based on industrial and organizational psychology and sociology. Fred E. Fiedler, a psychologist, comments:

The most important lesson we have learned over the past 40 years is probably that the leadership of groups and organizations is a highly complex interaction between an individual and the social and task environment. Leadership is an ongoing transaction between a person in a position of authority and the social environment. How well the leader's particular style, abilities, and background contribute to performance is largely contingent on the control and influence the leadership situation provides.⁷

Leadership is changing because the nature of organizations and their requirements continue to evolve to create new needs. According to Peter R. Scholtes, a management consultant, the *old* competencies needed to survive and excel in the organization included the following⁸:

1. *Forcefulness.* Part of a manager's responsibility was to control the workforce, making people do what they may otherwise be inclined to ignore. Good managers could look their people square in the eye and get them to respond.
2. *Motivating.* The "softer" side of forcefulness was the ability to inspire people to do great work. The judicious combination of carrots and sticks, of inspiration and exhortation, was the manager's stock-in-trade.
3. *Decisiveness.* To make quick decisions in the absence of information was routinely expected of the old-style manager.
4. *Willfulness.* Good bosses knew what they wanted and were dogged in their pursuit of it.
5. *Assertiveness.* A good boss was outspoken. Old-style leaders could not show weakness or ignorance lest their people run all over them.
6. *Results- and bottom-line-oriented.* Bosses held people accountable for meeting quotas and standards and achieving measurable goals. Maximizing ever-increasing profits each quarter and minimizing ever-diminishing costs were the manager's goals.

7. *Task-oriented.* Managers kept everyone busy and occupied. There was no slacking off or socializing. Managers believed that people don't really want to work and, left to themselves, they will screw off. Therefore, it was their job to be the conscience and taskmaster for their subordinates.
8. *Integrity and diplomacy.* Good bosses covered toughness with tact and amiability. They were honest, fair, and respectful while letting their employees know that they knew what to do when things got out of hand.

These competencies are still the prevailing expectations of managers, Scholtes asserts. However, the changing nature of organizations has affected management style and structure. The needs and expectations of contemporary organizational leaders have changed. Newer competencies emphasize collaboration, education, global vision, and worker development so goals may be achieved with less hierarchical intervention than in the past. A newer competency addresses the importance of understanding systems and how to lead them, while another concept recognizes the nature in which the traditional relationships of hierarchy are counterproductive. Some of this thinking stems from the research and management practices advocated by the late W. Edwards Deming, who devised these practices over a career lasting several decades (Box 11.1).

BOX 11.1 W. EDWARDS DEMING AND THE QUEST FOR QUALITY IMPROVEMENT

In the twentieth century, quality control of manufactured products increasingly came under analysis in a structured way. One pioneer was W. Edward Deming (1900–1993), who determined that about 85% of manufacturing errors were related to work structure and manufacturing design, not to the performance of individual workers. Deming created statistical quality control concepts for Bell Telephone Laboratories in the 1920s. His precise way of creating a new philosophy of the workplace was adopted by Japanese manufacturers in the years following World War II and helped that nation transform itself into a quality leader in only a few years. He was honored in Japan in many ways, including the establishment of the Deming Prize in 1951.

Deming's philosophy called for teamwork in which small groups of workers would devote themselves to an assigned task, with all the teams working as part of a collective effort to achieve quality and productivity targets. Deming wrote: "Cease dependence on mass inspection to achieve quality. Eliminate the need for inspection on a mass basis by building quality into the product in the first place." The concepts of constant product improvement argued by Deming are mostly thought of in manufacturing terms and have been widely implemented in the industrial sector. However, the same emphasis on quality over quantity is important to security services as well. Deming's concept produced *quality circles*, which sought to improve quality, enhance productivity, and encourage employee involvement through group applications. Ideally functioning quality circles provide an enriched job experience, greater customer satisfaction, and bottom-up improvement.

Sources: Walton, M., 1986. *The Deming Management Method*. Peregee, Putnam, NY; Deming, W.E., 1993. *The New Economics for Industry, Government, Education*. MIT Center for Advanced Engineering Studies, Cambridge, MA.

Leadership and Power

The military or police command and control method does not work well, or for an extended time, in nonmilitary or policing organizations, even those concerned with security services. The screaming, tyrannical boss of past generations is gone (mostly). The new generation of leaders, however, has a different kind of power. According to John Kotter, who created a course on the topic at the Harvard Business School, five basic types of power exist⁹:

1. Power to reward by providing a promotion, raise, better working conditions, or direct approval.
2. Power to punish by invoking progressive disciplinary methods or coercing or terminating the individual's employment.
3. Power of authority to approve or reject the quality of work presented or plans for the future.
4. Power to assert expertise. The leader insists that she or he really does know best and makes a particular decision based on personal experience or knowledge.
5. "Referent power" is the quality of a leader that leads to admiration and compliance by others.

Kotter sees contemporary managerial leaders drawing more from this last category.

The workforce in the twenty-first century is highly mobile. Contemporary leaders endeavor to provide authority when delegating tasks to others. When leaders surrender power to provide subordinate workers more authority, it may seem as if they are transferring power away from themselves. Yet in effect, the leader gains by the efficiencies from decentralization and subordinate empowerment.

Leadership Traits

Personal qualities, including ethics and psychology, matter enormously in the success of persons who influence others to achieve a common goal. The image of a symphony conductor – managing diverse talents to produce a complete arrangement – is sometimes used to explain such leadership traits. In other circumstances, the military model of leadership provides guidance because of its broad relevance. Patrick L. Townsend and Joan E. Gebhardt have codified leadership traits in *Fundamentals of Marine Corps Leadership (MCI 033N)*, a correspondence course for noncommissioned officers.¹⁰ The following are personality traits that the Marine Corps uses to teach leadership. They are offered here with private security in mind. Although the Marine Corps states that possession of these traits does not guarantee success, it also says that these traits "are a good guide for determining the desired personality to be developed as a leader."

1. *Integrity.* The authors comment: "Attempts to practice integrity part-time are hypocritical and forfeit any chance of engendering trust in seniors or subordinates." Honesty must be practiced with oneself as well as with others. The manual urges:

“Don’t tell your superiors only what you think they want to hear. Tell it as it is – but tactfully.”

2. *Knowledge.* The leader may be a generalist, but in some aspects, for example, in investigations or technical security, he or she is likely to possess a high degree of information and understanding. This knowledge is retained at an advanced level through reading, attending conferences, obtaining new experiences, and consulting with experts in the topics.
3. *Courage.* The leader looks for and readily accepts new responsibilities. She or he never blames others for personal mistakes. In some circumstances, fear is natural and should be recognized, while one’s emotions meanwhile are to be controlled.
4. *Decisiveness.* Good ideas can come from anywhere in an organization. The leader should consider all points of view for every problem, take a stand, and then determine whether the decision is sound.
5. *Dependability.* This quality is similar to reliability, which in turn is akin to professionalism. Dependable leaders tend to be prompt and complete all tasks to the best of their ability. They are careful about making promises, but build a reputation for keeping them once they are made.
6. *Initiative.* A leader with initiative looks for tasks to be performed and then completes them without being asked by a superior.
7. *Tact.* In the air force leadership manual, General George C. Marshall is quoted as saying: “A decent regard for the rights and feelings of others is essential to leadership.” Tactful leaders are considerate of others. They are tolerant and patient. Similarly, the Corps manual urges: “Let no Marine, superior or subordinate, exceed you in courtesy and consideration for the feelings of others.”
8. *Justice.* A leader searches his or her mental attitudes to determine what prejudices may exist and then seeks to rid them from their thinking and behavior. A leader recognizes those subordinates worthy of praise, not just those who merit punishment.
9. *Enthusiasm.* This word is derived from the Greek *enthousiamos*, meaning “inspiration” or “to be inspired by a god within one.” Enthusiastic people believe in what they are doing and what they can accomplish. Their behavior is contagious.
10. *Bearing.* This means both looking good and conducting oneself in a positive manner. The Marine Corps manual advises: “Frequent irritation, loss of temper, and vulgar speech indicate a lack of self-control or self-discipline and should be avoided.”
11. *Endurance.* The Marine Corps manual advises readers to keep fit physically by exercise and proper diet and to avoid excesses that lower physical and mental stamina. Security practitioners demand much the same stamina. Often, the hours are long. Planned days off or vacations may be jettisoned because of changing circumstances or an emergency. To accomplish the goal, fatigue must be successfully fought.
12. *Unselfishness.* The Marine Corps manual states: “Put the comfort, pleasures, and recreation of subordinates before your own. In the field, your Marines eat before you do.” An unselfish leader focuses on subordinates. (The author visited the dispatch

office of a quality regional security services business that sought to make this emphatic. On the wall, a large sign was directed to the managers and dispatchers who worked there. It read: “What have you done to help security officers on their posts today?”) Leaders who care for subordinates retain them in their service even when tempting opportunities for them elsewhere beckon.

13. *Loyalty.* This trait pertains to an ideal or custom, or the feeling of faithfulness to a cause or activity. Loyalty today, like yesterday, goes two ways: employees have a loyalty to the structure of the organization and vice versa. Loyalty is interdependent. While the leader is loyal to the interests of subordinates, he or she expects loyalty in return.
14. *Judgment.* Leaders anticipate situations that require decisions. This helps them be ready when the need for action arises.

In today's workplace environment, objectives are achieved by team work. According to Jon Katzenbach, author of *The Wisdom of Teams*, “One of the best places to find real teams is in elite military units. If you look at teams in the US Marine Corps, every member is trained to lead, because every member may have to be a leader.”¹¹ The manager faces a long list of expectations. To this list is added another quality: the manager as a coach and as a teacher of coaches. Coaching includes instructing, training, or guiding others in a particular activity or endeavor. Coaches make their personnel perform better, which translates into superior productivity and profit (Box 11.2). The image of the leader as a coach

BOX 11.2 SHOULD YOU BE A COACH? DO YOU NEED A COACH?

Management strategies of the past sought to *control* others. Management practices of the present seek to *empower* others. Coaching is one technique by which managers can demonstrate a committed partnership to help the worker exceed previous levels of accomplishment.

A sports or dramatic coach is someone who aids players and performers. A coach also may be retained to help improve individual executive or managerial skills. Coaching is different from other supportive roles, such as educators or trainers, because of the high degree of mutual trust required between the coach and those being coached. Further, coaches can be more assertive with those they are coaching. Results occur more when there is an interrelated commitment than when a hierarchical authority forces such an arrangement.

Some managerial coaches may themselves benefit from a coach. Coaches help high-performance managers achieve even greater results. Some coaches are independent management consultants who have insight into an individual's strengths and weaknesses and guide them to see patterns of behavior differently and to improve upon their current performance.

Sources: Benton, D., 1999. *Secrets of a CEO Coach*. McGraw-Hill, New York, NY; Lenzner, R., 2005. Quelling your inner jerk. *Forbes*, September 5, p. 156; Brown, P.D., 2006. Coaching employees: a delicate balance. *New York Times*, sec. 3, May 7, p. 6; Middleberg, T.M., 2012. *Transformational Executive Coaching*. River Grove Books, Austin, TX.

has taken its place next to the image of the leader as a symphony conductor or military field commander to stimulate thought about behavior.

The Importance of Discretion in Management

The formidable list of personality traits of leaders catalogued by Townsend and Gebhardt may be supplemented by another trait: discretion. Discretion is similar to loyalty in that organizational and personal matters are not discussed with those who do not have a right to such information. While the leader is discrete, he or she also expects discretion from anyone who has a right to know proprietary information about the organization. This is especially the case among security practitioners and their associations.

For example, contract security officers in the leader's organization may draw their paychecks from the security services firm that has selected them for the position. Yet the leader correctly expects these persons not to reveal proprietary information to anyone without a bona fide need to know. Similarly, when an organization invites architects, engineers, consultants, and others to bid for a contract, the leader expects that all parties with access to formal data presented in the request for proposal (RFP) – and informal insights obtained during the process – to respect such information as proprietary, even if they do not receive a contract assignment.

Major breaches to organizations' Web sites have occurred from lower security standards of vendors who have access to the system. They have such access because they need it to serve their customer. But such access has allowed other parties to exploit weaker protective standards to access databases. New vendors who are expected to have a proprietary relationship to their customer need to be briefed on all relevant security expectations.

Security personnel generally learn how to be open and friendly with others while not revealing confidential information about the enterprise. Similarly, they are conscious that others in the workplace may not have such reticence about discussing confidential matters. Much information about the organization can and should be made public. But other plans, processes, and procedures are strictly for internal use. What constitutes confidential information constantly changes in character. For example, a generation ago many employers saw no problem with providing the exact addresses and contact details of executives and managers. That is no longer the case.

The Problems with Leadership

Leaders are critical for the establishment, growth, and adjustment of an organization to changing times. The term "leader" is equated with the term "innovator," while the term "manager" relates to the term "program operator." Clearly, any operation – large or small – requires persons in positions of responsibility to possess some qualities of leadership. Leaders often reach heroic or mythic status, while managers are considered subordinate functionaries. They supervise the creative contribution of the innovator-leader. Yet it is important to note that the visionary leader can also sink an organization.¹² Managers often must step in to save the enterprise from the leader's misdirection or errors.

Henry Mintzberg, a professor of management at McGill University, comments: “We’re overled and undermanaged.”¹³ He adds: “The truth is, many of the most successful strategies are not conceived in isolation at the ‘top.’ They grow throughout the organization via a kind of distributed leadership. Moreover, studies show that vital information is typically transmitted to a CEO informally – orally, often, rather in formal reports.”

According to Jay A. Conger, a professor at the University of Southern California, leaders who have helped their organizations achieve also may lead these same entities into free fall. Conger cites four reasons for this:

1. The leader’s vision reflects his or her internal needs rather than those of the market or constituents.
2. The resources needed to achieve such vision have been seriously underestimated.
3. An unrealistic assessment or distorted perception of the market and constituent needs may hold sway on the leader’s vision.
4. There has been a failure to recognize environmental changes that should redirect the vision.

Conger also notes that leaders may be so absorbed with the big picture that they fail to understand critical details of operations, except in terms of pet projects that involve them. Another problem with the true leader is that she or he often fails to develop an effective successor. Conger also notes: “(U)nder charismatic leadership, authority may be highly centralized around the leader – and this is an arrangement that, unfortunately, weakens the authority structures that are normally disbursed throughout an organization.”¹⁴

What Is Distinctive About Leadership for Security Operations?

The essence of security management traditionally relates to the appropriate creation, imposition, and implementation of controls over personal behavior. Other management disciplines market and sell, finance, make, move, and administrate products or services. While security management relates to all of these, the discipline is primarily oriented in manipulating behavior to reduce or eliminate loss. To accomplish this, the operations security manager considers appropriate controls that can achieve the desired objectives within the context of the organization’s total operations.

Security operations managers concentrate on internal and external controls because they are more amenable to change than are other factors. For example, genetic factors seem to play a role in crime causation: men disproportionately are more responsible than women for serious violent and property crime. Yet some women commit such crimes, and it is not reasonable or logical for a security manager, say, to urge that mostly women be hired because they are less likely to be involved in crime. Both men and women are needed in workplace. Similarly, employers do not select workers based on any narrow set of environmental preconditions. Most flourishing workplaces thrive when employees represent

diverse social, ethnic, and national backgrounds. This means that managers must direct loss prevention while working with all types of people.

Control theory emanates from the work of Emile Durkheim, a suicidologist who concluded that the control and discipline of one's desires and the subordination of inclinations to the expectations of others stem from group integration and its intensity of involvement over behavior.¹⁵ Those prone to suicide lose this control. Durkheim's work influenced Travis Hirschi's seminal work, *Causes of Delinquency*, which assumed that antisocial acts occur when an individual's bonds to society are weak or broken.¹⁶ Hirschi's work centered on violence and property crime. Another theorist has concentrated on crime not in the streets, but in the suites. Edwin H. Sutherland, a pioneering sociologist at the University of Chicago, first named and described "white-collar crime," which is crime of a substantially different nature than street crime.¹⁷

Often referred to as "crime in the suites" or "gray crime," nonviolent financial crimes often escape prosecution, but are an utmost concern to corporate security practitioners.

Yet although these prescient observers' theories added to the understanding of deviance in the workplace, they provided little in the way of guidance to managers who sought to reduce loss. Other researchers would later fashion practical measures to deal with situational incidents that could be anticipated and controlled or resolved.

The security operations manager plans to respond to actual or reasonably possible situations by establishing situationally appropriate control measures. Since such measures generally cannot guaranty certainty of success, the manager also must be prepared to respond with alacrity once normative violations occur in the workplace.

Critical Leadership Issues for Security Operations Managers

Many distinct leadership issues face and challenge protective program decision makers. The priority of such tasks is as dynamic as the changing nature of the organization. New significant issues constantly emerge. For example, the Ebola virus suddenly emerged as a public health issue in three West African countries. Transportation, possible spread of the virus, and supply chain issues became concerns for global security programs. Meanwhile, matters that at one time captured the full attention of a manager decline in importance as control measures are devised and implemented, reducing their urgency.

Critical issues will differ according to the type, size, geographical location, and financial resources of the industry. However, a survey of security executives responding to a *Fortune* 1000 list, cited earlier in this volume and sponsored by Securitas, identifies 26 issues of highest concern (Table 2.4). The survey includes responses from about one-quarter of the identified security directors among the largest manufacturers, business services, and retailers.

The security operations manager or chief security officer normally oversees a number of ongoing programs and services. These include facilities management, which requires the services of personnel and technology. Superimposed over the organizational routine

are issues that direct the security executive's time and concerns. These complex issues are covered in other books and by specialty organizations. The discussion below concerns the top 10 of the 23 greatest security threats in 2012.

Cyber/Communications Security

The French scholar Blaise Pascal invented the adding machine in 1642, the first example of a device in which tens were carried to the next column. This invention created the basis for finding a mechanical way to rapidly automatic computations. The first electronic computer was called the "ENIAC" (for Electronic Numerical Integrator and Computer), and was created in 1945 at the University of Pennsylvania's Moore School of Electrical Engineering. In the subsequent half-century, computers grew from being esoteric scientific tools to becoming commonplace, ubiquitous aides to most human endeavors.

In 1990, the "World," the first commercial Internet service provider (ISP), came online. Two years later, the number of computers connected to the internet exceeded 1 million. By 2013, according to the US Census Bureau, almost 84% of US households reported computer ownership, with 78.5% possessing a desktop or laptop computer, and 63.6% having a handheld computer. In 2013, 74.4% of all households reported Internet use with almost all of them having high-speed connection.¹⁸ The issue is a global one. With an estimated global population of almost 7.2 billion, Internet users constitute over 3.0 billion.¹⁹

The Internet has transformed every aspect of business, and the pace of change continues unabated. From its onset, the Net was an open system, designed so that users could enter and leave, read and write, and share and transmit data with the greatest of ease. For organizations, the Net permitted the speed of business to soar. The capacity for organizations to communicate with each other and with anyone else achieved runaway growth. Because it was designed as an open system, the Net has no real policing. Therefore, chances of a variety of abuses are high and may expose the organization to a variety of threats never anticipated during the early development of the Net. A principal vulnerability is that the Internet puts access (freedom of communications) ahead of authentication.

In some ways, the security of the Internet and intranets is similar to conventional physical security. For example, access control to electronic databases can be divided into different levels of permission. Individuals may have access to databases under circumstances that can change according to the desire of the host system's management. The same way a customer's check must be trusted by a retailer; those involved in e-commerce need to be assured that the personal identification of the customer can be trusted and that the credit authorization for a purchase is genuine. At the same time, such transactions need to be protected so that unauthorized individuals will not have access to pertinent details in a transaction. They must include audit trails so that, should an irregularity occur, an investigation can determine the culprit and minimize further economic loss. Automatic data encryption makes protection of electronically stored information stronger.

When the first Securitas/Pinkerton survey was conducted in 1997, cyber or information technology (IT) security ranked 10th. In the top security threat survey for 2010, it reached

first place and has remained there for the 2012 survey. Clearly, the threats to information security rank highly in concerns and risks for *all* organizations and, for that matter, all households. Millions of identities have been stolen from organizations that might have protected their electronic resources better but didn't. The stolen data sets include information that can be used to create new identities with which fraudulent funds and other assets may be obtained. The thieves who steal the data sets might not use them directly but fence them on international electronic markets.

Another issue is where the entire host system can be surreptitiously entered by an unauthorized party. Using time to become familiar with the system, the data interloper can act in harmful ways by overriding controls. Computer crime is so vast and global in nature that organizations must depend on assistance from the government to fight it and to protect themselves. In the event of any cyberattack, the workplace should notify the FBI and follow instructions. Government needs private sector feedback and is more inclined to aid the marketplace than ever before. The Cyber Threat Intelligence Integration Center (CTI-IC) was created in 2015 to help the federal government analyze foreign cyber threats and to make sure that government centers will have access to intelligence about the threats in order to counter them. A voluminous literature concerns the analysis and response to cybercrime.²⁰

As computers have grown larger in importance and smaller in physical size, they have become objects of theft. Further, the input, output, tapes, and peripheral hardware are also tempting to thieves. Meanwhile, software programs written for an organization at great cost – in terms of both money and time invested – and critical databases can be copied in a matter of minutes, often with the owner not being aware that its proprietary software or valuable records have been copied until harmful effects occur later and are discovered.

The strategy to protect hardware and software involves a combination of factors, mainly related to procedures, personnel, and hardware.²¹ Procedural issues involve identifying what physical and electronic assets are most valuable and creating means whereby they may be identified and protected. Personnel issues include policies and procedures for those individuals having contact with the central computer facility where computers, peripheral equipment, processing units, storage units, communications equipment, and power backup are located. Hardware issues encompass physical security measures to restrict access control throughout a facility containing a computer center, particularly in the computer room itself. The physical security involves automatic access control to restricted areas, enforced by the resources of trained personnel. Software theft can be mitigated by programs that make copying difficult. Just as IT assets – both physical and electronic – represent greater risks to an organization, security measures gain to better protect them. For example, access to databases may require a biometric feature (fingerprint usually). A token (SIMS card or smart card that attaches to a USB part of a laptop or desktop) may also be required as access. Sensitive documents can be auto-encrypted via Data Encryption Standard (DES) and stored in an encrypted folder. If a system user steps away from the screen or disconnects the fingerprint reader, the screen saver auto-encrypts. A system operator can give permission for the user to transmit encrypted documents to another

colleague enrolled in the system. Theft of sensitive data becomes more difficult as measures like these are adopted to protect hardware and electronically stored data.

While protection of the Internet itself is beyond the capacity of nongovernmental organizations, much can be done to enhance computer security. The American Bankers Association proposes four suggestions to reduce chances of cybercrime for individuals; the principles are also applicable to organizations:

1. *Create cOmplic@t3d passwords.* Most common types of identity theft or fraud come from someone the victim knows. That means don't share personal info – even with family members. Also, make those passwords *cOmplic@t3d*. Add capitals, symbols, and numbers with eight or more characters and the password is robust. “Think about a favorite college course: likely there were authors, formulas, or scientific names you remember. Use them.”
2. *Keep tabs on your accounts.* Advice: check more than once a month when the bank and credit/debit statements come in. Fraud, if any, then can be spotted sooner.
3. *Stay alert online.* That means use up-to-date antivirus and malware protection. Nobody should have your password. When submitting financial info on a Web site, look for the padlock or key icon on a browser and make sure the Internet address begins with “https.” This (somewhat) assures that your info is protected during transmission. (Organizations need to delegate someone to patch the system for software updates.)
4. *Think and act defensively.* Use the passcode lock on your smartphone and other handhelds. Before donating, selling, or trading a mobile device, use the manufacturer's recommended technique to wipe data. Some devices may be wiped remotely if lost or stolen. Remember that apps may contain malware. Therefore, use them only from trusted sources.

When the worst occurs, call credit/debit card issuers immediately to report the fraud. File a police report. Notify the fraud to the three credit-reporting companies. Place a victim statement in your credit report and a fraud alert on your account. (They are time-limited, but renewable.) Keep a log of all contacts you make. Report the incident to the Federal Trade Commission (FTC) at 1-877-ID THEFT (1-877-438-4338) or www.ftc.gov/idtheft. Organizations should report data breaches to the FBI. Due to the evolving specialty of computer security, separate certifications and career tracks have evolved. Often computer security personnel are headed by a chief computer security officer (CCSO) and may report differently in the organization's management structure.

However, computer security is different from physical security in the way assets largely are electronic in nature. Thus, IT security involves a systems approach that must be comprehensive, dynamic, and flexible and suitable to the circumstances. Electronic data can be encrypted by an algorithm that protects them within a communications network from the point of origin to the final destination. The initial algorithm to protect electronic transmissions made available by the federal government was the DES. With the growth of powerful, cheap computing, DES alone provides modest security. The National Institute of Standards and Technology (NIST) has selected a new cryptology, Rijndael, to replace DES

or multiples of DES. Many other broadly available algorithms exist that e-security managers may consider.²²

Other means have been created to assure trusted operating systems, database security, and protection of distributed systems. Attacks on computers by hackers, crackers, and cyberterrorists pose a challenge to operating security practitioners.²³ Entire systems – if unprotected by filters and warning systems – can be crashed by an offender who sends a large number of messages or queries to a system at the same time. This is called a *distributed denial-of-service attack* (DDoS). The result is that IT security becomes a priority.

As William C. Boni and Gerald L. Kovacich write: “Ironically, these I-Way robbers may do more to increase demand for I-Way security than any other force in the marketplace today.”²⁴ Some security operations managers will feel challenged by the opportunity to respond to security issues raised by the Net and e-commerce; others will be intimidated by the technical shift required to establish trusted IT security operations. But the issue cannot be ignored, due to both the ability of Net applications to enhance commerce and internal operations and the vulnerabilities created at the same time. Security operations managers must move up to the challenge of e-commerce and Net security issues, or step aside for others with the interest and competence.

Workplace Violence Prevention/Response

This issue has been at or near the top of every survey conducted among *Fortune* 1000 security directors. This discussion will concern workplace violence as it applies to employees in general and to security personnel in particular.

General Workplace Violence

The drama and significance of a violent act in the workplace is undeniable. In the past decade, violence in the workplace received exceptional attention from a variety of organizations, including the Office of Safety, Health and Working Conditions of the Bureau of Labor Statistics (BLS); the Occupational Safety and Health Administration; and the Centers for Disease Control and Prevention. In addition, organizations such as ASIS International and the Society for Human Resource Management have regarded workplace violence as a critical topic of interest for their memberships. Numerous insurance companies, trade organizations, and other state and local groups also have weighed in on the issue. Audiovisual materials have been produced and numerous books on the topic have been published.²⁵ Workplace attacks that result in death or serious injury are reported in the media often.

The workplace is becoming safer despite what the media might lead one to conclude (Figure 11.1). The US BLS measures work-related deaths from four causes: highway incidents, homicides, falls, and struck by object. Figure 11.1 demonstrates that these types of deaths collectively have decreased by over one-third since the high point of 1994. However, the most dramatic decrease has been for workplace homicides. In 1994, a high point of 1,080 homicides was recorded. By 2013, the number had fallen to 379, a decline of 64.9%. If the decline were calculated based on employment that grew during this period, the results

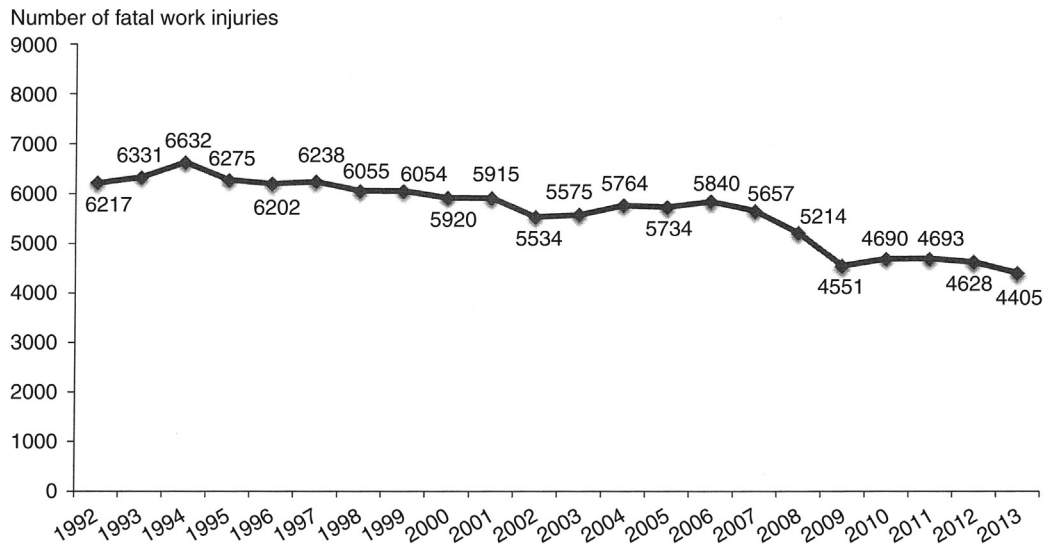


FIGURE 11.1 The declining trend of fatal work injuries. Fatal work injuries, 1992–2013. Workplace fatalities are measured from four types of incidents: highway, homicides, falls, and struck by object. From 1994 the number of workplace injury fatalities has declined 33.6% despite the fact that the number of workers has increased during this time. The decrease in workplace homicides has been greatest. (Preliminary total for 2013. Data for 2001 exclude fatal work injuries resulting from the September 11 terrorist attacks.) (Source: US Bureau of Labor Statistics, US Department of Labor, 2014, Washington, DC.)

would have been even more impressive. Still, such a decline is no excuse for complacency. Data for workplace fatalities emanate from the National Institute for Occupational Safety and Health (NIOSH), Centers for Disease Control and Prevention, BLS, and other sources.

- *Frequency of fatalities.* The frequency of homicides by shooting, stabbing, and other incidents, including bombings, has been similarly on the decline according to BLS reports through 2013. Regrettable as any number is a person's chances of being killed in a transportation accident while at work that are over four times greater than being a victim of homicide in the workplace (Table 11.1). Work-related deaths from homicides have trended down over the past two decades.
- *Risks for female workers.* In recent years three times as many male workers were murdered as female workers. However, homicide was the leading cause of job-related fatalities for women, accounting also for nearly half of women's work injuries. Security practitioners are aware that women in the workplace can be stalked and at risk from individuals who have threatened them in the past. Typically, a security program will require female employees to notify the department confidentially if they have an order of protection from someone who has threatened them or if other unsettling circumstances place them at risk while on the job.
- *Race and ethnicity.* Because of their occupations, not race or ethnicity *per se*, homicide was the leading cause of job-related deaths for African-Americans, Hispanics, Asians, and Pacific Islanders.

Table 11.1 Fatal Occupational Injuries from Transportation and Homicides, 2013

Occupation	Total	Transportation	
		Incidents	Homicides
Transportation and movers	1184	830	50
Construction	818	188	14
Executive and managerial	389	165	51
Installation and repair	356	84	13
Protective services	247	85	65
Police officers	79	39	26
Security guards	57	9	31
Building maintenance	242	56	6
Agricultural	225	85	4
Sales and related	211	42	98
Production jobs	210	31	7
Food preparation	70	4	29
Office and administration	70	28	10
Healthcare	59	30	7
Entertainment and media	50	30	5
Personal care	47	11	9
Financial and buyers	21	7	7
Education, librarian	19	5	4
Nurses and support aids	18	7	0
Social services	18	10	0
Legal	14	0	5
All other	137	42	13
Total	4405	1740	397

Source: Table A-6, Census of Fatal Occupational Injuries (CFOI)- Current and Revised Data. Washington, DC: Bureau of Labor Statistics. <<http://www.bls.gov/iif/oshcfoil.htm>> accessed 6/25/2015.

- *Risks for the self-employed.* Homicide was also the leading cause of job-related deaths for the self-employed.
- *Circumstances of job-related homicides.* In a study of 1024 job-related homicides that occurred in 1995, most (71%) of the incidents resulted from robberies or robbery attempts.²⁶ Typically, robbery victims were store personnel, gas station attendants, or taxicab drivers. Several workers were killed during carjackings, muggings, and robberies of goods and services. The frequent targets for robbery in this study are beer truck drivers, store personnel, gas station attendants, and cab drivers who are killed for their cash receipts.
- *Victimization by work associates.* One in six workplace homicide victims were killed by a current or former work associate. These incidents were most likely to be featured by the media.
- *Personal acquaintance of the victim.* Workers – primarily women – are killed as a result of domestic disputes that enter into the workplace.
- *Police and security victimization.* In 2013, 31 security personnel were homicide victims while 26 police officers died in the line of duty from homicides.

The strategy of mitigating possible workplace violence continues to evolve according to the type of industry. The highest danger of work-related homicide is faced by clerks at sales counters, managers and supervisors of food and lodging establishments, sales personnel and small business proprietors, and cashiers. These particular workplaces merit ongoing research to understand better the phenomenon and how working conditions could be improved to mitigate such possibilities.

More than half the nation works in offices. The specter of innocent workers being gunned down in their offices, say, by a disgruntled current or former employee, is sure to seize the nation's attention (Box 11.3). For that reason – in addition to the possibility that such incidents might produce copycat acts of violence – security operations managers must seek to improve vetting measures, identify workers who have previously made harsh

BOX 11.3 WORKPLACE VIOLENCE: WARNING SIGNS SOMETIMES MISSED

Research by Seungmug (Zech) Lee and the author identified 273 cases of workplace mass homicides (WMH) from 1986 to 2013. Data on *mass* homicides were collected instead of *all* workplace killings for the reason that more data were available. These incidents occurred an average of 2 per year, ranging from 0 to 4 events, and victims ranged from 0 to 27 deaths depending on the year.

An analysis of the cases allows a profile to be drawn indicating those above average as workplace killers and what the characteristics were of the workplaces where these WMH incidents occurred.

Workers present above-average risks if they are likely:

- To have been terminated recently or at any time in the past
- To be underperforming and facing a reprimand, negative evaluation, or termination
- To be argumentative with supervisors and coworkers
- To be described as possessing an “angry or loner personality”
- To have talked about perceived or actual slights by a supervisor or manager and who may have expressed the desire for revenge on the day of the incidence
- To have guns or previously to have served in the military
- To live alone

Such workplaces are likely:

- To possess weak security and HR protocols for disciplining and discharging subperforming employees
- To have weak controls on preventing formerly discharged employees from returning to and entering the workplace
- To have no active workplace violence mitigation plan
- To have supervisors and managers who are not alert to cues of angry, anxious, isolated, teased, or otherwise resentful employee behaviors

Source: Lee, S., McCrie, R., 2014. The violent vortex: appraising risk from workers who kill on-the-job. In: Gill, M. (Ed.), *The Handbook of Security*, second ed. Palgrave Macmillan, New York, NY.

or threatening comments about others in the workplace, support the Employee Assistance Program (EAP) initiatives, improve access control measures, and generally enhance the feeling of security.

Loss of Work Due to Injuries

Like the salutary reduction in workplace homicides, the total recordable nonfatal occupational injury and incident rate has also declined in private industry, 2009–2013 (Figure 11.2). By all measurements injury and illness incidence has trended down, dropping from an incidence rate per 100 full-time workers of 5.0 in 2003 to 3.3 in 2013, a decline of 34% in a decade. Research shows that the size of employment is related to this kind of injury or illness incidents. In a recent year, workplaces with 1–10 employees had the lowest rate of 1.7 per 100 full-time workers. Employers with 11–49 employees had an incidence of 3.1; those with 250–999, 3.5; those with 1000 or more employees, 3.6; and the highest incidence for workplaces with 50–249 employees, 4.0.

Business Continuity Planning/Organizational Resilience

Resilience is “ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, distraction, or loss.”²⁷ Protection of critical infrastructure to perform its mission or function is a fundamental duty of security. Security practitioners

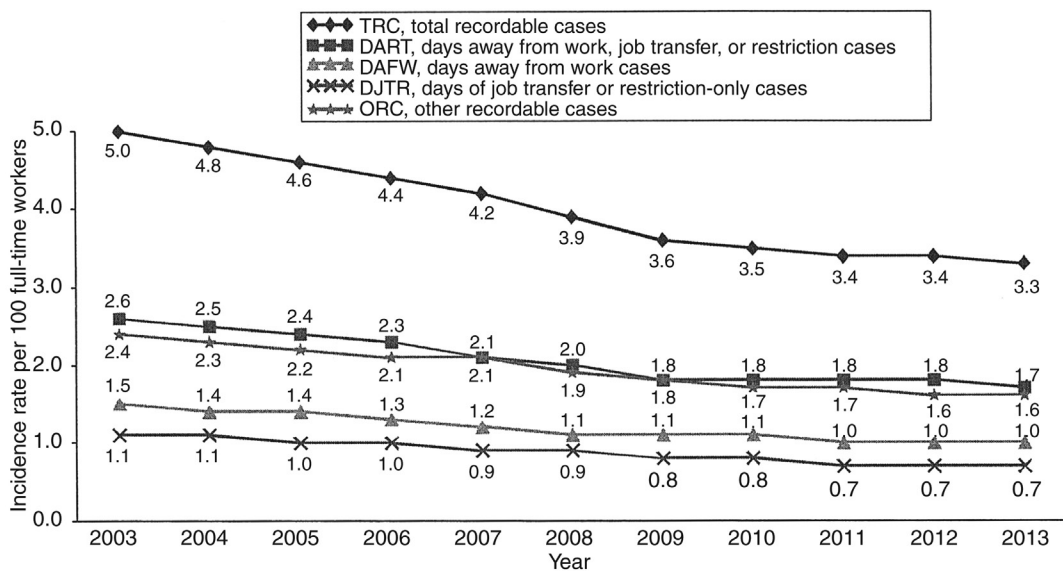


FIGURE 11.2 Declining trend in nonfatal work injury and illness. Nonfatal occupational injury and illness incident rates by case type in private industry, 2003–2013. During this study period, the incidence rate per 100 full-time workers dropped from 5.0 to 3.3 for total recordable cases. (Source: US Bureau of Labor Statistics, US Department of Labor, December 2014.)

think in terms of the likelihood of an initiating event to be expressed in a formula, as follows:

$$R = P_A \times SF \times C$$

where R , security risk; P_A , likelihood of the initiating event; SF , likelihood of system failure because of the initiating event; C , consequence associated with the failure.

A protection system assessment will depend on the likelihood of system failure. This will be estimated by 1.0 minus protection system effectiveness (P_E), as follows:

$$R = P_A \times (1.0 - P_E) \times C$$

Estimating the P_A for random events (weather, system decline, loss of utilities) can be undertaken. However, ascertaining the P_A for malevolent events (terrorist attacks, an extraordinary accident) is difficult.²⁸

Determining risk requires discernment and should be regarded as an approximation. Nonetheless, such a process is better than not undertaking it. The estimate of risks is likely to improve with the availability of the Infrastructure Resilience Analysis Methodology (IRAM) that can be applied to a wide variety of untoward conditions.

Employee Selection/Screening

Hiring the wrong employee leads to disappointment, financial loss, missed opportunity, and a sense of inadequate screening (vetting) measures. When employment is full and the need to fill key positions is high, the chances of failing to conduct a thorough preemployment credentials review increase.

Employers in high-tech industries may be particularly vulnerable to theft at the workplace. To achieve the desired results of a workforce with high integrity and reliability, security practitioners and human resources (HR) managers must work together, drawing from the skills that protection professionals know best regarding screening out candidates with undesirable prior work records or dishonest representations on résumés or application forms. (This process of preemployment verification and selection is discussed in detail in Chapter 3.)

Bias in hiring has been a central issue involving security and HR personnel in recent years. What is a “disability” remains an issue of contention. The Equal Employment Opportunity Commission (EEOC) has brought numerous suits against employers and has created a mindset that forces employers to evaluate if their reasons for rejecting a prospective employer are fair. Possession of a misdemeanor or felony conviction may not necessarily lead to exclusion from consideration for employment. The circumstances of the crime need to be evaluated as part of the process.

Vetting of prospective employees through social networks is increasingly being regarded as a justifiable, even necessary, process for some positions. Social networks generally work in favor of candidates. While privacy is eroded due to the ease of searches, the work and social interests of the applicant can establish credentials that corroborate the formal

application. Privacy matters and no sensible person has “nothing to hide.”²⁹ Applicants need to be aware that their Facebook profile and Twitter, LinkedIn, and Google+ accounts will be accessible to a prospective employer. Incriminating search results must never be assumed as factual. They serve as a means of raising discussion points with the candidate for employment prior to a final decision.

Workplaces are using services to check the background of not only their prospective employees but also contract workers.³⁰ “Good conduct” letters on applicants may be satisfactory if they come from genuine and recognizable third parties. If an employer rejects the applicant based on information collected, the right to an appeal exists. If the complaint is factual, the background screening company must investigate the dispute according to the Fair Credit Reporting Act (FCRA). If the other basis for an appeal is that an improper conclusion has been drawn due to the decision matrix, the workplace will need to review the matter.

Property Crime/External Theft/Vandalism

External theft, damage, vandalism, and sabotage cost organizations billions of dollars each year. Their prevention depends on a comprehensive security management program. Architectural design and space management concepts combined with the proper selection of building materials represent an important initial consideration in reducing property crime losses. This involves the concept of crime prevention through environmental design (CPTED), which can deter criminal and uncivil behavior (as discussed in Chapter 10).³¹ The appropriate use of hardware, software, and procedures aimed at reducing losses can result in further lowering the likelihood of loss. In the event that losses do occur, litigation pursuant to an investigation may recover some lost assets, reduce the pattern of loss, or both.

General Employee Theft

Theft of assets excludes fraud, intellectual property (IP), and electronic assets. Quantification of employee theft is difficult since definitions can vary. The cost of employee theft, time theft, and drug abuse on the job is an enormous cost to the American workplace. The indirect costs from such losses to the employer, government, and the general public add to the total risks (Box 11.4). Employee theft is mitigated by measures previously discussed, including appropriate vetting (Chapter 3), adequate supervision (Chapter 5), and discipline up to discharge and prosecution in the event of dishonesty (Chapter 7). Meanwhile, electronic systems may also discourage employee theft (Chapter 10).

Connected with employee deviancy are ethical lapses and sometimes addictive behaviors. Drug use and abuse in the workplace are issues that predate the Industrial Revolution. The media often refer to a “war on drugs”; however, alcohol and tobacco abuse are responsible for more deaths in the United States than all illegal drugs combined and yet no “war” is waged against them.³² Alcohol accounts for about 100,000 premature deaths per year and tobacco is linked to 400,000 demises, whereas illegal drugs are responsible

BOX 11.4 INDIRECT COSTS OF ECONOMIC CRIME

Determining economic losses from crime is difficult, as such offenses also produce indirect costs to the organization, including the following:

- *Increased cost effects on the organization:*
 - Increased security
 - Internal audit activities
 - Investigation and prosecution of suspects
 - Reduced profits
 - Increased selling prices and weakened competitive standing
 - Lower employee morale
 - Reduced productivity
 - Damage to business reputation and image
 - Deterioration in quality of service
 - Higher overhead due to theft
 - Lost business opportunity due to lack of needed items or concentration of resources in investigating and responding to the incident
 - Higher insurance premiums
- *Cost effects on local and national government:*
 - Criminal justice activities (investigating and prosecuting)
 - Correctional programs
 - Crime prevention measures
 - Policing and community security activities required
 - Loss of tax revenue (e.g., from loss of taxes due to the untaxed income of the perpetrator and due to deductible business losses producing less tax income)
- *Cost effects on the public:*
 - More expensive consumer goods and services to offset crime losses
 - Decreased investor equity
 - Higher taxes to pay for criminal justice costs
 - Reduced employment from business failures

Source: Cunningham, W.C., Strauchs, J.J., Van Meter, C.W., 1990. Private Security Trends 1970 to 2000: The Hallcrest Report II. Butterworth-Heinemann, Boston, MA, pp. 32–33.

for about 30,000 deaths. Excessive alcohol and tobacco use results in productivity losses, greater employers' health costs, and workplace accidents.

Such addictive substances as alcohol and tobacco, however, are not linked to the same extent to criminal propensities as some illicit drugs. For this and other reasons, drug use and abuse in the workplace are subject to federal programs, and policies that lead to a drug-free workplace are promoted.* Federal employment guidelines test for marijuana,

* For example, Executive Order 12564, September 1986, and the consequent 1998 US Department of Health and Human Services' "Mandatory Guidelines for Federal Workplace Drug Testing Programs."

opiates (heroin, morphine), cocaine, amphetamines and methamphetamines, and phen-cyclidine. Testing for such substances prior to an offer of employment or during employment is widely applied, as discussed in Chapter 3.

In addition to screening for drug use, security operations managers face different issues concerning workplace drug matters. Initially, a policy might be created and disseminated concerning a testing process at the workplace.³³ Legal issues, policy promotion strategy, testing methods, sample security protocols, and laboratory selection need to be considered. In the event an overt or undercover investigation must be conducted, procedures and personnel must be directed to collect facts. The investigative team, supported by protective management, will recommend subsequent actions to be taken to mitigate future incidents.

Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (Evacuation Potential)

The issues in this category are not necessarily related. Therefore, they will be discussed separately.

Crisis Management

This is the management process whereby potential emergencies or disasters are systematically identified and assessed for their frequency and criticality. Table 11.2 provides an overview of such processes and their consequences.

This is a formal process involving a comprehensive search for the likely crises that an organization actually or probably could experience.³⁴ Management usually seeks to mitigate such vulnerabilities – called risk reduction – with appropriate measures.

Table 11.2 The Strategy of Crisis Management

Process	Consequence
Risk reduction	Security managers identify significant risks to the organization that can be systematically reduced or eliminated. This may be achieved with appropriate programs. Sometimes, the risk can be shared with other organizations within the same entity or in the same geographical area. For example, an enterprise that fears operational losses from a computer crash may temporarily move operations to another location within the same establishment
Risk acceptance	This assumes that some losses will occur as a normal consequence of operations. Management concludes that the projected losses are acceptable and will be absorbed as a routine operating cost
Risk transfer	The organization accepts some risk, reduces it by various strategies but ultimately transfers an unacceptable risk level to an insurer
Risk elimination	Management determines that the risk is too great to accept and, therefore, elects to avoid the activity entirely by not commencing it, selling it off, or ceasing operations

Included here as part of crisis management, the process described in the table is a fundamental activity of security planning. Some risk is always accepted. Other risk must be transferred to an insurer or a mutual protection organization. Other risks make no good sense and should be eliminated. That leaves risk reduction as the center of activity in crisis mitigation or, for that matter, in corporate risk management.

Additionally, some small and predictable losses may be reducible by measures that are far more costly than the damages to be paid when they do occur. Therefore, management decides not to take exceptional risk reduction measures and accepts such risks. In still other cases, some risks are reduced and others are accepted, but an aggregate risk remains, such as damage from a major fire or natural disasters. These events such as severe windstorms, floods, earthquakes, and loss of utilities would be unacceptable should they actually occur due to the unlikely but possible major unplanned financial loss. Such risk is transferred to an insurer. Finally, in some cases, management will conclude that the risk cannot be accepted and the actual activity is not undertaken or is terminated. This process is termed “risk elimination” because the organization disassociates itself from the venture or activity.

Crisis management is an ongoing process in which the security operations manager is constantly engaged. Despite mitigation efforts, crises will occur. Emergencies and disasters must be responded to. Operations must resume as quickly as possible if the untoward event slows or stops the process of work. In years gone by, a crisis would be certainly regrettable and the marketplace would have sympathy for the harmed organization to get back in order. Not anymore. The sympathy factor has declined. Organizations are expected to have the means in place and available to bounce back from a crisis or disaster quickly – in hours, not days or weeks. The First Interstate Bank fire in Los Angeles in 1988 was a crisis, making the headquarters unusable (now Aon Tower). But a crisis management plan was put into place. And 1 full day later the institution made money because traders immediately traveled to satellite offices and bank customers were individually called to assure them of the stability of operations. The rule of thumb today: back to full operations within hours of a major crisis.

Further, security operations managers generally serve as coordinators of response and recovery activities. Contingency planning aids the organization to respond quickly to mitigate the effects of such incidents.

Executive Protection

The safety and security of executives, indeed all employees, is a major concern for security operations managers. Executive protection often is related to workplace violence in that risks to the executive whenever he or she is working or traveling on behalf of the organization have security implications. However, few workplaces require special protective means such as employing executive protection personnel. M.J. Braunig states in the *The New Executive Protection Bible*: “Far fewer corporations hire executive protection agents than you might think, and the corporations [which] do hire them generally do so because of reaction to a specific incident, or because of specific threats, or in some cases simply as a prudent security measure.”³⁵ Yet the market is changing. Executive and celebrity protection is a growing concern on an individual level and also when senior managers travel to foreign lands where their security cannot be taken for granted.

Executive protection involves surveys of broad risk; specific evaluation of office, hotel, and residence dangers; and training for staff and family members on what to observe and

what to do under threatening circumstances.³⁶ The executive protection professional may complete extensive relevant training, possess good interpersonal skills, be physically fit and able to adapt to a wide variety of circumstances, and has analytical ability to identify risks and avoid them.³⁷ Risk reduction for the executive might involve countersurveillance operations that seek “to identify all possible attack points where the executive is vulnerable” and to eliminate or reduce exposure to them.³⁸

The consequences of inadequate executive protection can be profound, leading to liquidation or substantial reorganization of the firm when a significant and creative leader is struck down. One example is the gunning down of fashion mogul Gianni Versace in Miami Beach, Florida. Robert L. Oatman observes: “Executive protection has little to do with spinning tires and knocking people over, and everything to do with threat assessment, intelligence gathering, transportation, choreography, advance work, 10 minute medicine, resources, technology, and support.”³⁹

Terrorism

Since the blow of 9/11, plus those in London, Madrid, and elsewhere, life in economically advanced Western nations has never been the same. An act of terrorism occurs through the calculated use of violence to obtain political or social goals to instill fear, intimidation, or coercion. Terrorism usually involves a criminal deed meant as a symbolic activity to influence someone unrelated to the immediate victims. The efforts of terrorists have historically been against governments.⁴⁰ However, private organizations and their facilities may also be targets of or indirectly affected by a terrorist event (Box 11.5). Acts of domestic terrorism are infrequent in the United States and Canada despite the memory of 9/11. As a result, security operations managers assess the possibilities of terrorism to their operations in a wide global context. Predictions on the future course of terrorist events involve acumen. But complacency on domestic risks is never appropriate.

Governments prepare for the possibility of terrorism in a variety of ways. The first step is planning how to prevent or mitigate the effects of a terrorist act. Physical design, location, and construction methods influence the possibility of a particular facility or system being a target. Training, including mock exercises, helps organizations respond to the emergency. Appropriate emergency supplies and continuity resources are identified in case they should be needed. In 1980, an elite antiterrorist military group was created, called the Delta Force or Blue Light, and is based in Fort Bragg, North Carolina. The troops are trained to deal with terrorist incidents on land, sea, and air. In more recent years, the US and other governments plus institutions and the private sectors have collaborated on biennial collaborative exercises called TOPOFF (for top officials). Additionally states, cities, communities, and private enterprises have staged their own tabletop and full exercises. These measures seek to make society and its components more nimble in recovering from terrorism or other emergencies and disasters.

Terrorism need not be a dramatic event seeking to bring sweeping social change. It can be a local event capable of engendering fear or inconvenience. The Model Penal Code (Section 211.3) defines terrorism as threatening “to commit any crime of violence with

BOX 11.5 A STRIKE AT THE “HEARTLAND”: TERRORISM IN OKLAHOMA CITY, AND NEW YORK CITY AND BOSTON

At 9:02 a.m. on April 19, 1995, a detonation outside the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, changed the way millions of Americans thought about terrorism. The event occurred in the “heartland” of America, creating a sense of disbelief, anger, and fear unlike any other domestic disaster of its kind up to that point. The explosion immediately killed 167 persons, including children attending a nursery in the building. Extensive physical damage was sustained for several blocks from ground zero.

The explosion reminded security planners of the importance of car bombs as vehicles of destruction. In Beirut in 1983, an Islamic Jihad terrorist killed 241 US servicemen in a badly protected Marine barracks. (Moments later, another bomb in Beirut killed 58 servicemen at a nearby French barracks.) In London in 1982, an IRA car bomb exploded, killing eight and causing over \$1 billion in property damage. In New York City at the World Trade Center in 1992, a bomb killed 6 and injured around 1000. This was the “wake-up call” that terrorism had found its way to these shores. All of these instances of terrorism involved bombs composed mostly of natural materials or easily available explosives and were created with modest skill and at little cost. Perimeter control, CPTED, interior changes, and security systems enhancements are measures taken to deter these threats.

A survey by the US Marshal Service completed in the late 1990s identified over 1300 single or multitenant federal office buildings employing 750,000 federal employees. Such buildings, usually under the management of the General Services Administration, are divided into five categories according to number of employees, size, and criticality for federal service. Appropriate security measures are prescribed for buildings in each category. But some still wonder whether this level of security is sufficient.

At the same time, the Oklahoma City explosion made clear how uncommon domestic terrorism is. In the mainland United States, just two major incidents occurred in the 1990s. Both were targeted against important physical symbols of capitalism and government. These two incidents turned out not to be exceptional historical footnotes. The events of 9/11 signaled again a thesis of this book: vulnerability eventually will be exploited.

The first successful terror attack on American soil since 2001 occurred when the Boston marathon was bombed on April 14, 2014. Along with Al Qaeda-inspired attacks in Woolwich and Paris in 2013, religiously motivated terrorism in the West, and also in parts of Africa and Southeast Asia, threatened concepts of national security.

Sources: Coulson, D.O., Shannon, E., 1999. No Heroes. Pocket Books, New York, NY; Serrano, R.A., 1998. One of Ours: Timothy McVeigh and the Oklahoma City Bombing. W.W. Norton & Company, New York, NY; Dees, M., Corcoran, J., 1998. Gathering Storm: America's Militia Threat. HarperCollins, New York, NY; Security Letter, vol. 25, May 1, 1995, p. 1; Security Letter, May 17, 1995, p. 1; Ramakrishna, K., 2014. From 'old' to 'new' terrorism: history, current trends and future prospects. In: Gill, M. (Ed.), The Handbook of Security, second ed. Palgrave Macmillan, New York, NY.

purpose to terrorize another or to cause evacuation of a building, place of assembly, or facility of public transportation, or otherwise to cause serious public inconvenience, or in reckless disregard of the risk of causing such terror or inconvenience.” Security operations managers typically prepare for such risks as bomb threats, incidents, and kidnapping.⁴¹ However, other criminal forms of intimidation, such as cyberterrorism, can threaten the vitality of an organization and its people.

Unethical Business Conduct

Ethics are rules of conduct. They are practices that are applicable to organizations and members of a profession regarding their moral and professional obligations. As such, ethics have less force than legal requirements, although the organization must take them seriously. In some circumstances, ethical breaches may also constitute criminal behavior.

Employers have ethical obligations to employees, vendors, competitors, and society at large. Nearly all organizations have a code of conduct that delineates the principles of proper behavior. At the same time, organizations expect ethical behavior from their employees, vendors, competitors, and others.

Security practitioners encounter unethical business practices in a variety of contexts. In addition to domestic issues, the Foreign Corrupt Practices Act of 1977 requires that United States–based for-profit businesses operate ethically when conducting operations abroad. Bribes and kickbacks when offered in a seductive way for “consulting services” are certainly illegal, and possibly subject to criminal sanctions. Organizations may, for example, ethically collect publicly available information about competitors. Thus, sales literature, Web site information, comments by personnel made at trade shows, observations offered without prompting by vendors’ employees when seeking new employment, and technical papers presented at meetings may be collected, analyzed, and used to enhance an organization’s marketing and general management strategy.

Security personnel sometimes aid in the creation or management of such competitive information units. However, it is unethical and potentially a criminal violation for an organization to interview vendors’ employees solely for the purpose of collecting desirable competitive intelligence when no job with the interviewing organization is available. It is further unethical to hire such vendors’ employees as “consultants” on a project basis when the intention is to obtain critical details about such organizations rather than the employee’s skills for their own sake.

Apparent internal or external ethical violations require investigations to determine their veracity.⁴² Due diligence may be necessitated before domestic organizations deal with potential foreign partners. A thorough understanding of ethical obligations and risks reduces the possibility of violating ethics and legal practices in all countries involved.

Security practitioners frequently are given responsibilities for drafting and managing ethical policies and programs, and all major security organizations have a code of behavior or ethics. ASIS International, for example, has a Council on Business Practices and a Code

of Ethics, which can punish offenders with censure or dismissal from the organization (Appendix B). Masters of business administration also have a code of ethics, specifying expectations (Appendix C).

The status of ethics in the American workplace is mixed. That's why it so significantly is part of a security practitioner's concerns. According to the KPMG Forensic Integrity Survey, a majority of employees nationally – 73% – reported that they had observed misconduct in the previous 12-month period. More than half – 56% – reported that what they had observed could cause “a significant loss of public trust if discovered.”⁴³ The propensity to report misconducts to an ethics hotline has increased, according to the survey of more than 3500 employees in the United States. The prevalence of misconduct by industry during the previous 12 months in the five most reported sectors is as follows: consumer markets, 82%; government and public sector, 79%; chemicals and diversified industrials, 77%; pharmaceutical and life sciences, 76%; and real estate and construction, 77%. However, all industries reported misconduct.

Secure records retention and authenticity of certain financial documents have been required by two measures. The Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes–Oxley Act (SOX) have required a higher degree of circumspection than prior to the passage of these measures. HIPAA and SOX are important federal laws, not ethical guidelines. Yet, in many corporations these and other laws emphasize the existence of ethical behavior to support higher and broader standards of behavior. Security executives routinely have rates in policy setting and program management.

Litigation: Inadequate Security

As described in Chapter 3, litigation may occur if employers or their agents breach their duty and if such a breach results in direct harm to others. One question to be settled is how sufficient or proportional the effective protective measures are relative to the prescribed standards or measures. “Inadequate security” covers a wide range of inadvertent, intentional, and unintentional circumstances that could lead to a civil action in which the organization becomes a defendant. In such plaintiffs' actions, senior executives or managers, the director of security, and individual security personnel involved may be listed individually as defendants. While the employer may provide legal counsel for any employees, individuals frequently must consult lawyers privately for guidance at their own expenses.

Many charges of inadequate security relate to the failure of property owners and managers to adequately protect the public from the foreseeable criminal actions of others. For example, the appellate court of Pennsylvania ruled in a case:

*While we do not consider a landlord to be an insurer of its tenants, we hold that in all areas of the leasehold, particularly in the areas under his control, the landlord is under a duty to provide adequate security to protect its tenants from the foreseeable criminal actions of third persons.*⁴⁴

A wide variety of tort (civil wrong) actions due to inadequate security are conceivable. A fixed list of such actions cannot be created because of the changing nature of circumstances and the inventiveness of plaintiffs and their lawyers. Further, the nature of such charges varies according to the type of organization. The following are a few general examples of inadequate security charges that have been brought against organizations in the past:

- Alarms that are inadequate, missing, or broken
- Assaults
- Inadequate background checks (see the section “Litigation: ‘Negligent Hiring’”)
- Failure to prevent a crime
- Duty to protect not met
- Emotional distress
- Failure to make necessary repairs to security hardware
- Failure to anticipate crime
- Failure to warn
- Failure to adequately screen employee
- Failure to train security personnel adequately
- Failure to supervise security personnel adequately
- Failure to terminate an employee after illegal or unacceptable behavior
- Foreseeability of event not anticipated by the defendant
- Failure to maintain standards followed by comparable organizations
- Inadequate locks

Identity Theft

Each year over 10 million consumers suffer identity theft. The issue has become challenging for credit and debit card issuers, their customers and charge handlers, financial institutions, and the public involved. The FTC classified fraud within three categories. The categories of fraud listed as follows are from most to least serious:

- *New accounts and other frauds.* This category includes new accounts of loans for committing theft, fraud, or other crimes using the victim’s personal information.
- *Existing noncard accounts.* This category includes existing checking and savings accounts and existing loans and insurance, telephone, and utilities accounts.
- *Existing card accounts.* This category includes both the account numbers and the actual cards for existing credit and card-linked debit accounts.

Most victims who experience identity theft are in more than one of these categories.⁴⁵

Theft of the name and pertinent details leads to fraud. The fraudsters might steal identity on a retail level, that is, a few names at a time. Examples of this can be desperate request for money from someone facing an emergency. The fraudster has enough information to write a plausible appeal. Another approach is via the computer in which a genuine-looking appeal for information is really a fraudulent attempt to do the same. A wholesale, so to

speak, theft of names and identifications represents a much greater risk to the public. Such names are traded – sold like catalogue items – on foreign-based sites.

The credit and debit card issuers, processors, and clientele of retail users have routinely absorbed the cost of frauds.⁴⁶ This will change as solutions, including chips-in-cards and multifactor authentication, will reduce the frequency of crime as it is being committed currently. Thus, the United States will join countries in Western Europe that adopted the smart card beginning in 2010. Meanwhile, the industry is challenged to deal with cases of fraud with conventional investigative resources.

Other Issues Concerning Security Operations Managers

In addition to these top 10 concerns, many other issues come to the attention of security decision makers. These will evolve with time and circumstances. The important ones to test the abilities of a global security practitioner are given in the next subsections.

Sexual Harassment/Equal Employment Opportunity (EEOC) Concerns

Sexual harassment is defined as conduct directed at a specific person, usually of a different gender, causing substantial emotional distress. In 1994, 44% of women and 19% of men responding to a survey conducted by the US Merit Systems Protection Board said that they had experienced some form of unwanted sexual attention during the previous 2 years. Similar results were seen in a survey conducted 7 years earlier.⁴⁷ The survey gathered responses from employees in over 24 agencies. Nonetheless, few bothered to report the incidents. Only 6% of those in the 1994 survey who expressed being the target of sexually harassing behavior indicated that they took formal action in response. The unwanted attention included pressure for sexual favors, deliberate touching or cornering, sexual looks or gestures, letters or calls of a sexual nature, pressure for dates, and sexual teasing including jokes, remarks, or questions that were deemed offensive to the recipient.

Such behavior violates, in part, the federal Equal Employment and Opportunity Act of 1972, which bars discrimination based on race, color, religion, sex, and national origin. It also prohibits practices caused by statistically determined adverse impact, as well as intentional unequal treatment.[†] Implications of the Act encompass all private employers of 15 or more persons, educational institutions, government, employment agencies, labor unions, and joint labor-management committees established for apprenticeship and training. State regulations may not reduce federal measures, but may go further in specifically prohibiting behaviors covered in the Act. Sexual harassment occurs usually in situations of unequal power, although actionable charges involving parties of equal power occur.

[†] The legislation is enforced by the US EEOC, www.eeoc.gov. The act may be found at www.eeoc.gov/laws/vii.html.

Security practitioners normally have an obligation to investigate apparent or actual violations of these measures. If the investigation determines that offenses have occurred, disciplinary measures, including cautioning, counseling, or dismissal, may be considered, as discussed in Chapter 7. A single act of sexually oriented harassment does not necessarily meet the definition of ongoing harassment. The exact circumstances of the case determine whether a court proceeding will occur and can be sustained. These include the following: if management was informed of alleged abuse, and did nothing; how often the conduct occurs; how serious it is; if the behavior physically threatens the other party; and if the unwanted behavior interferes with work behavior. Failure of the employer to investigate and respond to charges in a timely fashion can lead to costly sanctions (Box 11.6). Some researchers have placed sexual harassment within a context of workplace violence and have related it to a global issue.⁴⁸

Smart managers concentrate on proactive measures that identify unwanted behavior in an effort to deter them from occurring. Similarly, employees may also learn how to respond to noisome comments directed at them by saying: “I’d like it better if you would comment on the quality of my work rather than how I look,” or “My name is ..., not ‘...’

BOX 11.6 SEXUAL HARASSMENT SANCTIONS ADD UP

For any organization, having an antiharassment policy is not enough. Organizations additionally may require customized training on sexual harassment awareness that spells out consequences for policy violations. The complaint procedure must be made clear. The following are some incidents in which employers were forced to pay for sexual harassment at the workplace:

- Mitsubishi Motors agreed to pay \$34 million in a sexual harassment settlement brought by some 300 current and former female workers at Mitsubishi’s Normal, Illinois, plant.
- The US unit of Sweden’s Astra Pharmaceuticals agreed to pay \$9.9 million to about 80 workers in a sexual harassment case.
- The Ford Motor Company paid \$7.5 million in damages and planned to spend about \$10 million more on training after 19 women at 2 Chicago-area plants complained to the EEOC. The women claimed that male workers often used sexually degrading words for them, placed explicit materials in their workplace, and even groped them.
- In 2006, New York City settled a lawsuit that the federal government filed 4 years earlier accusing the Giuliani administration of failing to safeguard women in workfare jobs against sexual and racial harassment by supervisors.
- A bank manager near Treviso, Italy, sought to kiss a cashier on the lips on Valentine’s Day. She forcefully resisted and took the manager to court. In 2006, an appeals court confirmed a lower court’s conditional punishment of 14 months in jail.

Sources: Miller, J.P., 1998. Mitsubishi will pay \$34 million in sexual-harassment settlement. Wall Street Journal, June 12, p. B4; McLaughlin, A., 1999. When others harass, now managers lose pay. Christian Science Monitor, September 10, p. 1; Barron, J., 2006. City settles workfare harassment lawsuit. New York Times, May 13, p. B-3; Stop ai baci rubati, sono un reato, 2006. America Oggi, June 10, p. 7.

(a term of endearment or an offense). Employees who believe they have been sexually harassed should feel free to discuss the issues with HR or security personnel. In unionized and nonunionized workplaces, a written complaint may be filed with the HR department. HR and security usually conduct the investigation. In unionized organizations, the offended worker may file a formal grievance.

Fraud/White-Collar Crime

The mantra among security practitioners is that more losses occur from fraud and so-called white-collar crime than from conventional internal or external theft. *Fraud* is the criminal offense of obtaining money or money equivalents by false pretenses, that is, the intentional perversion of truth. It usually does not involve property damage or threatened or actual physical injury. Fraud is an element in crimes such as forgery, counterfeiting, and embezzlement, in which cunning and unfairness are used to cheat people or organizations. The range of fraud is great, from petty cheating to large-scale looting of corporate or governmental assets. Frauds often are directed against individuals by others. This discussion, however, concentrates on circumstances in which the organization is itself victimized by individuals or entities.

White-collar crime is fraud committed by persons whose occupational status is executive, managerial, entrepreneurial, professional, or semiprofessional. The term, first used by Edwin H. Sutherland, was meant to encompass such business crimes as embezzlement, kickbacks, price fixing, antitrust violations, unfair labor practices, and war crimes.⁴⁹ Sutherland's work turned the attention of academics from poverty, class, and caste as factors that cause crime to values that lie within the social system and individual malfeasance as a criminogenic element. Some writers conclude that the level of crime among the wealthy and powerful can have an insidious effect on government, and vice versa, placing the social structure at risk when such depredations go unchecked.⁵⁰

For the security operations manager, dealing with internal and external fraud and white-collar crime usually takes the form of a reactive response, whereas a preventative response would be wiser and more cost-effective. Security practitioners usually are the best – or among the best – individuals in an organization to sense risks that are greater than their likely payoff or benefit to the organization. However, the nature of fraud is protean, and organizations reasonably well prepared to deter fraud may be victimized by the originality and daring of fraudsters. Further, some incidents involve offenders who appear to be making money for the organization, but in reality are doing the opposite. In such situations, the inquiring security practitioner or compliance officer will be rebuffed by managers protecting the supposed high-income producer because their bonuses and status are linked to those persons' success (Box 11.7).

Frequently, security practitioners learn about fraud after the fact and must move quickly to conduct an internal investigation. Such an investigation may be begun the moment an indication is received that the organization may have been victimized by fraudulent means. Before calling federal agents or local prosecutors, the organization usually seeks to

BOX 11.7 NICK LEESON AND THE FALL OF BARINGS BANK

Security practitioners and compliance officers often have the skills to identify risks that are too great relative to their potential payoff or that otherwise violate internal or regulatory standards. However, whether management will listen to their cautionary advice is another matter.

Sometimes, wild risks are taken clandestinely by people who appear to be making a profit for the organization, but actually are running it into the ground. An example of this is the collapse in 1995 of Barings Bank, a London-based international bank founded in 1762. The cause was a single individual operating without adequate controls, who was protected by his supervisors and managers who were ignorant of their subordinate's malfeasance. In this situation, Nicholas Leeson, a 28-year-old rogue trader for Baring Futures in Singapore, racked up huge unauthorized trading losses, hiding them in a mislabeled account.

Leeson appeared to be earning enormous profits for his accounts from buying and selling derivatives – future contracts linked to fluctuations in Japan's stock exchange. His reported “profits” earned him and his superiors substantial bonuses. By the time Leeson's scheme was discovered, he had racked up losses of £827 million. This exceeded the resources of the bank, which was liquidated as a result, ending the glorious history of an institution that helped finance, among other relationships, the expansion of the British Empire and the Louisiana Purchase by the United States from France in the nineteenth century.

Leeson was sentenced to 6.5 years in Changi Prison, Singapore, and was released 3 years later after a diagnosis of cancer, which he has survived.

Sources: Rawnsley, J.H., 1995. *Total Risk: Nick Leeson and the Fall of Barings Bank*. Harper Business, New York, NY. Also: Leeson, N., Whiteley, E., 1996. *Rogue Trader: How I Brought Down Barings Bank and Shook the Financial World*. Little, Brown & Company, Boston, MA; Security Letter, March 15, 1995, p. 1.

determine whether the indication of fraud is verifiable and, if so, how substantial the loss is to the entity.⁵¹ In the earliest phase in which fraud is suspected, criminality cannot be assumed. An internal investigation should collect facts that can be the basis of ascertaining the truth and facilitating future interaction with the criminal justice system. Normally, security practitioners confer with internal counsel before conducting an internal investigation. Staff investigators may be delegated to conduct the interviews needed to evaluate the situation. In the event that the organization does not have skilled personnel appropriate to the task, private investigators may be retained on a project basis.

Once the investigators establish the facts and the case is confirmed by the security operations head, the internal counsel may take the necessary steps that can result in arrest and prosecution of the offenders. Security practitioners may continue their efforts even after a case is transferred to federal, state, or local authorities. In some cases, security can achieve investigative goals better than government investigators because they understand their organization better and because incentives to protect the institutional reputation and possibly recover lost assets are present.

The twenty-first century has commenced with a series of major financial misappropriations from senior officials within organizations. Some of the malfeasance began even

earlier and resulted in severe losses or failure of such organizations. How can an organization be alert to these transgressions? Surveying recent “catastrophic fraud” incidents, Randolph D. Brock III, then executive vice president of risk oversight for Fidelity Investments, offered 15 lessons. These were presented to the General Audit Management Conference of the Institute of Internal Auditors in 2003:

- The easiest way to prevent theft is not to hire thieves.
- Past performance *is* a guarantee of future results.
- Climate is more than a weather report.
- Integrated control functions see more.
- Develop your senses and use them.
- Trust everyone, but cut the cards.
- Read the newspapers.
- No business ever failed because someone stole all its PCs.
- Aggressively question success.
- The more senior the perpetrator, the more serious the theft.
- Contingency planning should be an auditor core competency.
- Honest employees cannot be depended upon to blow the whistle.
- Asking the right questions isn’t enough.
- The most likely suspect probably did it.
- Suspect everyone all the time.

Business Espionage/Theft of Trade Secrets

For many organizations, theft of IP, including know-how and trade secrets, can far surpass losses from conventional theft. While larcenies can be overt, documented, and related to a monetary loss, the theft of information can be insidious and lead to the loss of market position and future opportunity without the victim organization perceiving the cause. According to an estimate by ASIS International years ago, espionage by foreign and domestic competitors costs US firms hundreds of billions per year.⁵² The total surely has continued to grow. While most offenders are likely to be competitors within the same industry, a few come from abroad and act with the support of their governments, increasingly benefitting from weak cyberspace security.⁵³

Security professionals seek to protect their organizations’ inherent intellectual capital by identifying what is most important and then restricting access to it. This involves broad information protection policies, requiring employees with need-to-know trade secrets to be aware of their importance for protection. As more know-how becomes accessible over the Net, protection of such systems becomes a priority, lest organizations become victims of cybertheft. A former National Security Agency expert, Ira Winkler, observes that countermeasures should include holding “fire drills” to simulate problems and their responses, and the periodic performance of vulnerability assessments with attempted penetration of systems.⁵⁴ Practitioners remain up to date about such risks by using independent consultants, surfing the Web, liaising with local sources, and studying material provided by US

cybersecurity programs. Corporations may retain the services of data services that search the Web for comments on the corporation and its products and services that may signal use of stolen trade secrets.

The ASIS Foundation sponsored by National Counterintelligence Executive periodically assesses threats to organizations. Their survey report concludes that as much as 75% of the market value of a typical US company resides in its IP assets. Yet firms rarely value these assets formally. If they are stolen and used against the proper owner, no credible basis of understanding the loss – and possibly suing for damages – exists. Passage of SOX makes such an IP inventory of assets desirable, if not compelling.

The management of competitive intelligence is linked to the protection against business espionage and the implementation of trade secret security as well as the legitimate collection of market information. The Society of Competitive Intelligence Professionals (SCIP) was founded in 1986 as a nonprofit organization that educates and provides liaison opportunities for managers of competitive intelligence programs.

Governments decide what's important for national interests and seek to protect it. In the United States classified information is divided into confidential, secret, and top secret categories. Individuals must be vetted by the government before being authorized to have access to such information. The National Classification Management Society consists of information security personnel who manage such programs by identifying and assigning security classification to information and materials to be protected in the national interest.

Litigation: “Negligent Hiring”

Employers have an obligation to conduct a reasonable investigation into a prospective employee's work experience, background, character, and qualifications. As David A. Maxwell writes, “The standard of care does not vary. The greater the risk of harm, the greater degree of care necessary to constitute ordinary care.”⁵⁵ The doctrine of negligent hiring and retention provides that:

*(A)n employer whose employees are brought into contact with members of the public in the course of the employer's business has a duty to exercise reasonable care in the selection and retention of his employees ... Negligent retention ... occurs when, during the course of employment, the employer becomes aware or should have become aware of problems with an employee that indicates his unfitness, and the employer fails to take further action such as investigating, discharge, or reassignment.*⁵⁶

The protection manager constantly evaluates personnel performance, asking whether particular behaviors should have been assessed and responded to. Failing to do so, has the workplace failed to meet the duty of care standard? Have such workers been counseled, retrained, reassigned, placed on temporary leave, or discharged? If appropriate measures are not taken in a timely fashion, the employer faces the possibility of a difficult defense in the event a plaintiff commences an action for such negligence.

Insurance/Workers' Compensation Fraud

Security practitioners frequently interact with an organization's risk manager, that is, the individual who directs an organization's nonhealth and benefits insurance coverage. When a security program reduces chances of loss, this information can be critical to the risk manager in negotiating lower premiums or improved coverage from the insurance carriers serving the property, liability, and other risks of the organization. Additionally, security directors may review or monitor insurance provided by protection-related vendors (e.g., for alarm monitoring, armored car, investigations, and security patrol services). Further, following an incident of some sort that triggers an insurance claim, a risk manager who is well informed on security measures in place can be more effecting in claim discussions with the insurer.

Apart from this interaction, security practitioners frequently are called to investigate workers' compensation fraud. Workers' compensation provides cash benefits for employees who are injured or otherwise incapacitated during the course of active employment. Also, in the event of a worker's death, a surviving spouse and family members may be entitled to benefits. State workers' compensation laws dictate the terms and conditions of benefits to claimants and the obligations to employers. In the event that an individual is unable to work because of a job-related injury or circumstance, benefits may also be awarded. In such cases, the worker may not sue the employer under the doctrine of negligence unless the court rules otherwise; that is, the rights and remedies granted to an employee arise out of and in the course of employment. For example, if a third party injures an employee while on the job, that employee normally may not be able to sue the employer for negligence, but will likely receive the limited recovery provided by the workers' compensation statute.⁵⁷

Security operations managers often must investigate incidents relative to routine workers' compensation claims. In other cases, however, former employees who are enjoying such benefits actually may no longer be ill or injured and should return to work and cease receiving such benefits. These can cost the employer over an extended period. Occasionally, former workers receiving benefits because they were injured on the job and can no longer work may in fact have returned to active health and may be working elsewhere while continuing to receive full benefits. In such cases, investigations seek to determine the facts of such incapacitation and to determine whether the benefits should be eliminated.⁵⁸

Cargo/Supply Chain Theft

The cost of cargo, transportation, and distribution theft is not known with any degree of precision. Periodic efforts made in Congress since the late 1960s to require that cargo theft losses be reported to a national registry have failed. Many cargo thefts are reported to police and are included in larceny statistics for the area where the crime occurred, but many others are not reported. In 1976, the Office of Transportation Security of the Department of Transportation estimated that \$1.5 billion per year was stolen from warehouses, shipping

and receiving platforms, storage areas, depots, terminals, and piers. Of the loss, 5% was from hijackings, 10% from breaking and entering, and 85% from internal theft, collusion, or unexplained shortage.⁵⁹

Emphasis on recruiting, screening, and training reliable personnel heads the agenda of cargo security practitioners. Technology and containerization help to cut losses from both internal and external crime.⁶⁰ Using bar codes, radio-frequency sensors, electronic seals, and asset-tracking technology helps organizations manage assets better, and also decreases the chances of merchandise being stolen or abused. Arms, cash and money equivalents, jewelry, pharmaceuticals, and microchips are low-weight/high-value cargo highly susceptible to theft, and are thus special targets for enhanced security. Cargo security practitioners learn to work with insurers, claim agents, and law enforcement – domestically and abroad – as part of their activities. To increase the confidence in those who work with cargo, a Transportation Worker Identification Card (TWIC) has been instituted and now constitutes an important identification in the industry.

Acts of terrorism, inclement weather, and strike action at critical ports put supply chains at risk. West Coast work slowdowns in 2014–2015 caused some workplaces to bring critical parts by air to continue manufacturing.

Kidnapping/Extortion

People have been seized, borne off, and held for ransom ever since the beginning of time.⁶¹ Greek mythology is full of examples, usually of females being carried off by males in acts of lust. In fact, familial disputes are still the causes of scores of domestic kidnappings each year. However, kidnappings for profit, or extortion, infrequently occur in the United States and Canada. Security practitioners with executives requiring protection in other nations, however, will find risks high under some circumstances. Charles P. Nemeth writes, “Kidnapping and false imprisonment actions are relevant to the security industry because of their executive protection and counter-terrorism roles.”⁶² Despite the unlikely event of a kidnapping, organizations rely on executive protection to make the possibility of such an attempt costly to the attackers, thus decreasing its likelihood.

Risks of kidnapping for profit are localized geographically. Only a few countries and parts of the world pose a serious risk for an executive being kidnapped. However, managerial personnel are traveling smarter than in the past – less showy, discreet security, and better informed. To aid security planners in reducing risks, resources are available. These include the Department of State’s Overseas Security Advisory Council (OSAC). Also, private intelligence services aid travel and related matters (Figure 11.3).

Kidnap and ransom (K&R) insurance requires a number of protective measures to be taken, including the agreement of the insured not to reveal that the organization has a K&R policy on the lives of its employees. K&R insurance coverage usually includes specialized services to support family members during the time a loved one is forcefully held. The same service interacts with local and national police officials and the kidnappers to negotiate a ransom, if permitted by local laws, and to obtain freedom for the victim bringing



FIGURE 11.3 Command centers can link global operations and risk mitigation. Executive traveling abroad require up-to-the-minute information on conditions in countries they are visiting, particularly risks. Organizations dedicated to collecting and analyzing developments on a real-time basis aid in the planning process. (Source: *iJET International*.)

him or her back safely. The success of these organizations in saving lives and recovering kidnapped and insured victims is excellent.

Political Unrest/Regional Instability

Commerce is global. Managing in an international environment demands sensitivity to issues such as relations with government, especially local police; sex roles in the workplace; and relations with customers and vendors. It also demands that management knows how to direct and control programs from a distance.

Sometimes, investment in foreign-based operations can be placed at risk for political or social reasons. In the worst of circumstances, executives and managers are kidnapped or assets are seized by a vengeful and corrupt foreign government. Security practitioners in global enterprises where substantial resources are allocated may be responsible for evaluating and reporting on changing political and social circumstances that conceivably could put people and capital at risk. The means by which managers stay informed of such circumstances include staying in touch with managers in distant locations, occasionally visiting such facilities and including courtesy calls to local governmental or police officials, and subscribing to services that provide information on changing political events around the world. Private intelligence services have emerged that provide extensive pertinent information and analysis about risks throughout the world on a real-time basis. Such services are useful for assessing foreign operations as well as making appropriate plans for executives traveling abroad. Additionally, the US government itself provides daily foreign intelligence geared toward the private sector. It is available free to those who participate in OSAC, mentioned above, or make use of private consulting services specializing in political risk analysis.

Product Diversion/Transshipment

Manufacturers sometimes have differential pricing policies for products. That is, the same product can cost different amounts in different countries. The reasons for this are because some governments set the price of products to be sold there and force manufacturers to meet it. Further, prices may be different due to local trading conditions and the sales strategy of the manufacturer. Companies may make products in one country and export them elsewhere, in which the price may be lower. An exporter purchases products at the lower price to market them abroad. Normally, such exporters agree not to sell products into the markets not covered by the purchase agreement. However, some unscrupulous exporters or shippers divert the product back to the original country and sell it into local channels at a discount. This deprives the manufacturer of conventional sales and profits.

Similar to this, domestic franchises may have an agreement to sell into one area but, somehow, their product is sold in a different franchise area. Frequently, this represents a deliberate violation of the franchise agreement for product distribution and can be harmful to the franchiser victimized by the cross-selling process. This is frequently a task for a security department to ascertain that products are being sold in the territories they are supposed to and to provide facts to the organization's internal counsel on deliberate or inadvertent violations.

The security practitioner learning of such a scam must be able to collect evidence to prove the suspicion. Investigations in the field must be conducted to ascertain whether products have been diverted from their intended destination. Fact-finders visit retailers, distributors, shippers, buyers, public markets, and elsewhere to check the reliability of the distribution program. If product diversion is confirmed, the investigators may seek to prepare an analysis of the profits lost and seek to receive lost profits from the exporters or distributors who have broken terms of the contract. Typically, audio products, computer chips and devices, new fashions, branded products, and pharmaceuticals are targets for diversionary fraud.

Product Tampering/Contamination

The security and safety of a product are sometimes elusive objectives. Generally, if a product has been contaminated, it is due to deficient production controls. On rare occasions, however, an empty container of a product may be used to store a caustic substance, and then instead of being discarded is reused in food service. In other cases, consumers can appear to have a reaction to a product for reasons unrelated to its purity. Nonetheless, the resulting reports of victimization may draw immediate and pervasive media attention. In other cases, however, the contamination is due to deliberate tampering, which can lead to deaths, injuries, and loss of immediate sales and market share for the product involved. The stock market valuation of a large, diverse organization can be affected deleteriously by a single criminal case.

In 1982, capsules of Tylenol, a popular analgesic made by McNeil Laboratories, a division of Johnson & Johnson, were laced with cyanide in a few Chicago area retailers.⁶³ Seven

persons died. The result was that a massive criminal investigation was launched, the product was recalled nationally and destroyed, and the organization sought to make future packaging tamper-resistant. The attack on Tylenol is the most dramatic case history of medical product contamination, and is remembered for the way in which the corporation demonstrated its security and safety measures to the public. Yet other cases of product contamination occur with less publicity.⁶⁴ In such circumstances, security practitioners must engage in supporting investigative efforts, coping with negative publicity, collecting and protecting recalled products, and helping to design procedures to avoid a recurrence of the incident. These measures have made products more difficult with which to tamper.

Organized Crime

The Federal Omnibus Crime Control Act of 1970 defines organized crime as “the unlawful activities of the members of a highly organized, disciplined association engaged in supplying illegal goods and services, including but not limited to gambling, prostitution, loan-sharking, narcotics, labor racketeering, and other unlawful activities of members of such organizations.” In effect, organized crime is crime that is organized. It should not be associated with any particular race, ethnicity, or national origin because the types of organized deviance and their perpetrators shift over time.

Dennis J. Kenney and James O. Finckenauer write: “Organized crime is not unique to the United States or American society. However, the wealth, the economic, social, and political structures, and the criminal opportunities available in the United States present a unique set of circumstances that enable organized crime to achieve its highest form here.”⁶⁵

Security practitioners in banking are concerned with the possibility of organized crime using financial institutions to launder money. In 1989, the Bank of Commerce and Credit International (BCCI) paid a \$50 million settlement after pleading guilty to conspiring to launder drug money. The bank subsequently ceased operations.⁶⁶ The US Department of Justice believes that the vast majority of cargo thefts are the result of organized crime. Businesses also have suffered from organized crime from product counterfeiting, product diversion, credit and insurance fraud, and labor racketeering. Each type of organized crime is somewhat different, as are the means of attacking it. Security operations managers work with law enforcement and other victims in quantifying the amount of loss and in qualifying the means by which such losses occur so that the offenses can be stopped. Despite the organization and determination of well-financed criminals, the grasp of organized crime can be loosened by concerted effort.⁶⁷

The strategy for controlling organized crime must increasingly be international in scope, particularly with the expansion of digital risks adding to criminal attractiveness.⁶⁸

The Future Direction of Security Operations

This book has emphasized origins of various security practices and institutions. It is certain that the pattern of rapid change will continue into the future, perhaps at a still faster pace. Technologically systems will be able to provide a higher degree of security, reliability,

and safety by enhanced supervision, tracking, and reporting. Management styles will continue to change. Science and technology are destined to drive development in the current workforce and larger society in the decades ahead. Such issues as inherent weaknesses of the Internet, terrorism, global instability, nanotechnology, climatic changes, constant innovation in the enterprise, and yet other indiscernible factors will all have implications for security operations.

Computer systems may lessen the burden of certain procedures and enhance decision making. Meanwhile, the role of security operations managers will also evolve. Separate security departments for individual tasks may be created, such as general patrol, investigations, competitive intelligence, IT protection, and emergency planning, response, and recovery. In other circumstances, managers may be expected to direct security programs as well as manage other activities not currently part of their job description. This could include specific programs such as institutional ethics or larger traditional work units such as HR, compliance, risk management, or general facilities operations. Surely, security operations management is a global, not parochial, challenge.⁶⁹

Senior management may also seek to eliminate, downsize, or outsource security programs to contractors and consultants. The likelihood of this occurring is related to the value perceived and demonstrated by the initiatives and success of extant security programs. Operating security managers who demonstrate the ongoing worth of their programs, through efficient operations, measurable benefits, and reliable services, will thrive.

Summary

Good planning is not enough. Carefully designed and supported strategies need to be brought to success through leadership. Increasingly, the need for security services is managed on a global basis. This calls for people who can absorb, respect, and work with those of different culture. Cyber security has risen as the top overall management concern. But conventional issues – business continuity planning, workplaces violence, employee selection, privacy concerns, and many others – continue to challenge the high-performing security operations manager.

Discussion and Review

1. While some people may be better leaders than others, all people can lead and all people can learn to lead better. Discuss some ideas of how leadership skills may be improved.
2. Can leadership exist without power? What kinds of power?
3. Why do security operations managers tempt to possess – or should endeavor to possess – exceptional discretion for workplace activities?
4. What is the philosophical essence of security as a management practice?
5. Workplace violence is a major concern among protection professionals in large industrial and commercial organizations. Why should this be so when the workplace – especially an office – is essentially one of the safest places for people to be?

6. Why does senior management expect security practitioners to head the organization's crisis management and contingency planning operations?
7. Why should security and risk managers collaborate regularly?
8. How does terrorism impact a local security manager? A global one?
9. Numerous challenges for security operations at the present involve the ability to direct and use technology and investigative services. Is the same person likely to have the skills for both corporate activities? If not, what are management's options?
10. What are some of the inherent points of possible conflict between a chief security officer and a chief information security officer? What are grounds for collaboration and mutual support?

Endnotes

- ¹ Jago, A., 1982. Leadership: perspectives in theory and research. *Manage. Sci.* 28, 315–336.
- ² Beck, J.D.W., Yeager, N.M., 1994. *The Leader's Window: Mastering the Four Styles of Leadership to Build High-Performance Teams*. John Wiley & Sons, New York, NY.
- ³ Brawer, R.A., 1998. *Fictions of Business: Insights on Management from Great Literature*. John Wiley & Sons, New York, NY.
- ⁴ Howarth, S., 1998. Leadership – fleets ahead of its time. *Financial Times*, August 1–2, p. IV.
- ⁵ Bryant, A., 1999. Talking management with: John Cleese – soldier of convention or agent of change? a rebuff to the ministry of silly bosses. *New York Times*, sec. 3, February 7, p. 1; Fisher, A., Cleese, J., 1998. Test: can you laugh at his advice? John Cleese, former Python and maker of the world's best-selling business videos, on confidence v. fear, where creativity comes from, and more. *Fortune*, July 6, p. 203.
- ⁶ Kotter, J.P., 1995. *The New Rules: How to Succeed in Today's Post-Corporate World*. Free Press, New York, NY.
- ⁷ Fiedler, F.E., 1996. Research on leadership selection and training: one view of the future. *Adm. Sci. Q.* 41, 243.
- ⁸ Scholtes, P.R., 1998. *The Leader's Handbook: Making Things Happen, Getting Things Done*. McGraw-Hill, New York, NY, pp. 18–19.
- ⁹ Cross, J., Gomez, R., Money, K., 2013. *The Little Black Book for Managers: How to Maximize Your Key Management of Power*. Capstone, North Mankato, MN.
- ¹⁰ Townsend, P.L., Gebhardt, J.A., 1997. *Five-Star Leadership*. John Wiley & Sons, New York, NY, pp. 64–75.
- ¹¹ Quoted in Rigby, R., 2011. In the US Marines, every member is trained to lead. *Financial Times*, October 24, p. 12.
- ¹² Conger, J.A., 1990. The dark side of leadership. *Organ. Dyn.* 19, 44–55.
- ¹³ Mintzberg, H., 2009. We're overled and undermanaged. *Businessweek*, August 17, p. 68.
- ¹⁴ Conger, J.A., 1990. The dark side of leadership. *Organ. Dyn.* 19, 55.
- ¹⁵ Durkheim, E., 1951. *Suicide: A Study in Sociology* (J.A. Spaulding, G. Simpson, Trans.). Free Press, New York, NY.
- ¹⁶ Hirschi, T., 1969. *Causes of Delinquency*. University of California Press, Berkeley, CA.
- ¹⁷ Sutherland, E.H., 1949. *White Collar Crime*. Dryden Press, New York, NY.
- ¹⁸ File, T., Ryan, C., 2014. *Computer and Internet use in the United States: 2013*. United States Census Bureau, Washington, DC.
- ¹⁹ <<http://www.internetworldstats.com/stats.htm>> (accessed 2/17/2015).

- ²⁰ Chang, L.Y.C., Grabosky, P., 2014. Cybercrime and establishing a secure cyberworld. In: Gill, M. (Ed.), *The Handbook of Security*, second ed. Palgrave Macmillan, New York, NY; Freund, J., Jones, J., 2015. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, Waltham, MA; Workman, M., Phelps, D.C., Gathegi, J.N., 2013. *Information Security for Managers*. Jones & Bartlett Learning, Burlington, MA.
- ²¹ Das, S.K., Kant, K., Zhang, N., 2012. *Handbook on Securing Cyber-Physical Critical Infrastructure – Foundations and Challenges*. Morgan Kaufmann, Waltham, MA; Olson, P., 2012. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Little, Brown and Company, New York, NY.
- ²² Wayner, P., 1998. From toy rings to sophisticated codes, a quest for security. *New York Times*, May 28, p. G9.
- ²³ Phleeger, C.P., 1997. *Security in Computing*, second ed. Prentice Hall PTR, Upper Saddle River, NJ.
- ²⁴ Boni, W.C., Kovachich, G.L., 1999. *I-Way Robbery: Crime on the Internet*. Butterworth-Heinemann, Boston, MA, p. 152.
- ²⁵ Ahrens, S.A., 2011. The role of standards in workplace violence prevention and response. *Security Magazine*, October, p. 23; Harrell, E., 2011. *Workplace Violence, 1993–2009*. US Department of Justice, Bureau of Justice Statistics, Washington, DC; Lee, S., McCrie, R., 2012. Mass homicides by employees in the American workplace. CRISP Report. ASIS Foundation, Alexandria, VA; Loomis, D., 2008. Preventing gun violence in the workplace. CRISP Report. ASIS Foundation, Alexandria, VA.
- ²⁶ Toscano, G., Windau, J., 1996. *National Census of Fatal Occupational Injuries, 1995*. Bureau of Labor Statistics, Washington, DC, p. 36.
- ²⁷ Biringer, B.E., Bugrin, E.D., Warren, D.E., 2013. *Critical Infrastructure System Security and Resiliency*. CRC Press, Boca Raton, FL.
- ²⁸ *Ibid.*
- ²⁹ Solove, D.J., 2011. Why privacy matters even if you have ‘nothing to hide’. *The Chronicle Review*, May 20, p. B11.
- ³⁰ Giles, F.G., 2010. Checking from a distance. *Security Management*, June, p. 104.
- ³¹ Atlas, R.I., 2008. *21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention*. CRC Press, Boca Raton, FL.
- ³² Normand, J., Lempert, R.O., O’Brien, C.P. (Eds.), 1994. *Under the influence? Drugs and the American work force*. National Academy Press, Washington, DC.
- ³³ Schur, P.B., Broder, J.E., 1990. *Investigation of Substance Abuse in the Workplace*. Butterworth-Heinemann, Boston, MA. Also: Abadinsky, H., 2001. *Drugs: An Introduction*, fourth ed. Wadsworth/Thompson Learning, Belmont, CA.
- ³⁴ Elliott, D., 2006. Disaster and crisis management. In: Gill, M. (Ed.), *The Handbook of Security*. Palgrave Macmillan, New York, NY, p. 532.
- ³⁵ Holder, P.T., Holley, D.L., 1998. *The Executive Protection Professional's Manual*. Butterworth-Heinemann, Boston, MA; Braunig, M.J., 2000. *The New Executive Protection Bible*, second ed. ESI Education Development Corporation, Aspen, CO, p. 221.
- ³⁶ NAI Executive Protection Manual, 1997. Noble & Associates, Tigard, OR.
- ³⁷ Johnson, D.L., 2009. *Advance: The Guide for Conducting a Protective Security Advance*. Varro Press, Shawnee Mission, KS; Oatman, R.L., 2006. *Executive Protection: New Solutions for a New Era*. Noble House, Alsea, OR; Mares, B., 1994. *Executive Protection: A Professional's Guide to Bodyguarding*. Paladin Press, Boulder, CO; Holder, P.T., Hawley, D.L., 1998. *The Executive Protection Professional's Manual*. Butterworth-Heinemann, Boston, MA.
- ³⁸ Autera, J., Scanlan, M., 1999. Seeing through enemy eyes. *Security Management*, April, p. 35.

- ³⁹ Oatman, R.L., 1998. The challenge of protecting the chief. *Security Management*, June, p. 40.
- ⁴⁰ Falkenrath, R.A., Newman, R.D., Thayer, B.A., 1998. *America's Achilles' Heel*. MIT Press, Cambridge, MA; Heymann, P.B., 1998. *Terrorism and America*. MIT Press, Cambridge, MA.
- ⁴¹ Bolz Jr., F., Dudonis, K.J., Schulz, D.P., 1990. *The Counter-Terrorism Handbook*. Elsevier Science Publishing, New York, NY.
- ⁴² Hollstein, B.R., 1998. Don't do as the Romans do. *Security Management*, February, pp. 56–57.
- ⁴³ KPMG Forensic, 2013. *Integrity Survey 2013*. KPMG, New York, NY.
- ⁴⁴ Vaughan, J.F. (Ed.), 1999. *Avoiding Liability in Premises Security*, fourth ed. Strafford Publications, Atlanta, GA, pp. 2–3.
- ⁴⁵ Javelin Strategy and Research, 2014. 2014 identity fraud report. Javelin Strategy and Research, Pleasanton, CA.
- ⁴⁶ Pontell, H.N., Geis, G., 2014 Identity theft. In: Martin, G. (Ed.), *The Handbook of Security*, second ed. Palgrave Macmillan, New York, NY, p. 302.
- ⁴⁷ U.S. Merit Systems Protection Board, 1995. *Sexual Harassment in the Federal Workplace: Trends, Progress, and Continuing Challenges*. Government Printing Office, Washington, DC, p. viii. While most cases of sexual harassment have been filed by or on behalf of women, men also account for about one-fifth of the cases. Greenwald, J., 2010. More men filing sexual harassment, bias claims. *Business Insurance*, August 30, p. 3.
- ⁴⁸ Licu, E., Fisher, B.S., 2006. The extent, nature and responses to workplace violence globally: issues and findings. In: Martin, G. (Ed.), *The Handbook of Security*, second ed. Palgrave Macmillan, New York, NY, p. 229.
- ⁴⁹ Sutherland, E.H., 1983. *White-Collar Crime: The Uncut Version*. Yale University Press, New Haven, CT.
- ⁵⁰ Nolan, J., 1999. *Confidential*. Harper Business, New York, NY; Poveda, T.G., 1994. *Rethinking White-Collar Crime*. Praeger, Westport, CT.
- ⁵¹ Magnuson, R.J., 1992. *The White-Collar Crime Explosion*. McGraw-Hill, New York, NY, pp. 100–109.
- ⁵² Silverman, R.E., 1999. Stop, thief! *Wall Street Journal*, January 4, p. R50.
- ⁵³ Office of the National Counterintelligence Executive, 2011. *Foreign spies stealing US secrets in cyberspace*. Office of the National Counterintelligence Executive, Washington, DC.
- ⁵⁴ Winkler, I., 1997. *Corporate Espionage*. Prima Publishing, Rocklin, CA.
- ⁵⁵ Maxwell, D.A., 1993. *Private Security Law: Case Studies*. Butterworth-Heinemann, Boston, MA, p. 8.
- ⁵⁶ Vaughan, J.F. (Ed.), 1999. *Avoiding Liability in Premises Security*, fourth ed. Strafford Publications, Atlanta, GA, pp. 221–222.
- ⁵⁷ *Ibid.*, p. 166.
- ⁵⁸ Wallace, S.L., 1997. Curing a claims crisis. *Security Management*, October, pp.72–75; Schmedlen, R.H., 1997. Heading off the liability headache. *Security Management*, August, p. 79.
- ⁵⁹ National Advisory Committee on Criminal Justice Standards and Goals, 1976. *Report of the Task Force on Private Security*. Government Printing Office, Washington, DC, p. 59. See also Mueller, G.O.W., Adler, E., 1985. *Outlaws of the Ocean*. Hearst Marine Books, New York, NY.
- ⁶⁰ Tyska, L.A., Fennelly, L.J. (Eds.), 1983. *Controlling Cargo Theft*. Butterworth-Heinemann, Boston, MA.
- ⁶¹ Moorehead, C., 1980. *Hostages to Fortune*. Atheneum, New York, NY.
- ⁶² Nemeth, C.P., 1995. *Private Security and the Law*, second ed. Anderson Publishing, Cincinnati, OH, p. 219.
- ⁶³ *Security Letter*, vol. XII, October 4, 1982, p. 1; *Security Letter*, vol. XIV, February 15, 1986, p. 1.
- ⁶⁴ *Security Letter*, vol. XX, May 15, 1990, p. 3; *Security Letter*, vol. XXIX, July 1, 1999, p. 1.

- ⁶⁵ Kenney, D.J., Finckenauer, J.O., 1995. *Organized Crime in America*. Wadsworth Publishing, Belmont, CA, p. 371.
- ⁶⁶ Silver lining, 1998. *Economist*, June 27, pp. 74–75.
- ⁶⁷ Jacobs, J.B., Friel, C., Radick, R., 1999. *Gotham Unbound*. New York University Press, New York, NY.
- ⁶⁸ Levi, M., 2014. Fighting organized crime and the threats to business. In: Martin, G. (Ed.), *The Handbook of Security*, second ed. Palgrave Macmillan, New York, NY, p. 256.
- ⁶⁹ Gates, M., 2015. Required: license to operate. *Security Management*, February, p. 34.

Additional References on Leadership

- Cottrell, D., 2002. *Monday Morning Leadership*. CornerStone Leadership Institute, Dallas, TX.
- Denton, D.K., Wisdom, B.L., 1989. Shared vision. *Business Horizons* 32 (4), 67–69.
- Gardner, J.W., 2003. *Living, Leading, and the American Dream*. Jossey-Bass, San Francisco, CA.
- Garone, S.J., 1999. Concepts for the new leadership. In: Conference Report 1231-99-CH. Conference Board, New York, NY.
- Johnstone, R.W., 2006. *9/11 and the Future of Transportation Security*. Praeger Security, Westport, CT.
- Katz, D.S., Caspi, I., 2003. *Executive's Guide to Personal Security*. John Wiley & Sons, Hoboken, NJ.
- Walden, J.L., 2006. *Velocity Management in Logistics and Distribution*. CRC Press, Boca Raton, FL.
- Zaleznik, A., 1992. Managers and leaders: are they different? *Harvard Business Review*, vol. 70, issue 2, March–April, pp. 126–135.

Additional References on Current Security Challenges

- Bichler, G., Malm, A.E. (Eds.), 2015. *Disrupting Criminal Networks: Network Analysis in Crime Prevention*. Crime Prevention Studies, vol. 28. First Forum Press, Boulder, CO.
- Caputo, A.C., 2014. *Digital Video Surveillance and Security*, second ed Butterworth-Heinemann, Waltham, MA.
- Conti, G., 2009. *Googling Security: How Much Does Google Know About You?* Pearson Education, Boston, MA.
- Cubbage, C.J., Brooks, D.J., 2013. *Corporate Security in the Asia-Pacific Region*. CRC Press, Boca Raton, FL.
- D'Addario, F.J. (Contr. Ed.), 2014. *Personal Safety and Security Playbook: Risk Mitigation Guidance for Individuals, Families, Organizations, and Communities*. Security Executive Council, Elsevier, Waltham, MA.
- Doherty, E.P., 2013. *Digital Forensics for Handheld Devices*. CRC Press, Boca Raton, FL.
- Fennelly, L.J., Perry, M.A. (Eds.), 2014. *The Handbook for School Safety and Security*. Butterworth-Heinemann, Waltham, MA.
- Freund, J., Jones, J., 2015. *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, Waltham, MA.
- Gonzalez, D., 2015. *Managing Online Risk: Apps, Mobile, and Social Media Security*. Butterworth-Heinemann, Waltham, MA.
- Greenberg, A., 2012. *This Machine Kills Secrets: How Wikileakers, Cyberpunks, and Hactivists Aim to Free the World's Information*. Penguin Group, New York.
- Johnson, R., 2013. *Antiterrorism and Threat Response*. CRC Press, Boca Raton, FL.

- Kirschner, Jr., R., 2014. Surveillance and Threat Detection: Prevention Versus Mitigation. Butterworth-Heinemann, Waltham, MA.
- Law Enforcement – Private Security Consortium, 2009. Operation Partnership: Trends and Practices in Law Enforcement and Private Security Collaborations. US Department of Justice, Office of Community Oriented Policing Services, Washington, DC.
- Layne, S.P., 2014. Safeguarding Cultural Properties: Security for Museums, Libraries, Parks, and Zoos. Butterworth-Heinemann, Waltham, MA.
- Macaulay, T., 2009. Critical Infrastructure: Understand its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies. CRC Press, Boca Raton, FL.
- Park, P., 2009. Voice Over IP Security. Cisco Press, Indianapolis, IN.
- Smith, E.N., 2014. Workplace Security Essentials: A Guide for Helping Organizations Create Safe Work Environments. Butterworth-Heinemann, Waltham, MA.
- Timm, P., 2015. School Safety: How to Build and Strengthen a School Safety Program. Butterworth-Heinemann, Waltham, MA.
- Wimmer, B., 2015. Business Espionage: Risks, Threats, and Countermeasures. Butterworth-Heinemann, Waltham, MA.
- Winkler, V.(J.R.), 2011. Securing the Cloud: Cloud Computing Security Techniques and Tactics. Syngress, Waltham, MA.



Appendix A

Contact Information for Security Organizations

Academic, Trade, and Professional Associations

Organization, Year Founded	Web Site
Academy of Criminal Justice Science, 1963	www.acjs.org
American Fire Sprinkler Association, 1981	www.sprinklernet.org
American Institute of Certified Public Accountants, 1887	www.aicpa.org
American Management Association, 1923	www.amanet.org
American Polygraph Association, 1966	www.polygraph.org
Associated Licensed Detectives of New York State, 1950	www.aldonys.org
ASIS International, 1955	www.asisonline.org
ASTM International, 1898	www.astm.org
Business Software Alliance, 1988	www.bsa.org
Central Station Alarm Association, 1950	www.csaaul.org
Communications Fraud Control Association, 1985	www.cfca.org
Computer Security Institute, 1974	www.gocsi.com
Conference Board, 1916	www.conference-board.org
Fire and Emergency Manufacturers & Services Association, 1966 (ISC) ²	www.femsa.org www.isc2.org
Independent Armored Car Operators Association, 1971	www.iacoa.com
Institute of Internal Auditors, 1941	www.theiia.org
Institute of Nuclear Materials Management, 1958	www.inmm.org
International Association for Healthcare Security And Safety, 1968	www.iahss.org
International Association of Chiefs of Police, 1893	www.theiacp.org
International Association of Campus Law Enforcement Administrators, 1958	www.iaclea.org
International Association of Personal Protection Agents, 1989	www.iappa.org
International Association of Professional Security Consultants, 1984	www.iapsc.org
International Foundation for Protection Officers, 1984	www.ifpo.org
International Security Management Association, 1982	www.isma.com
International Systems Security Association, 1984	www.issa.org
Jewelers' Security Alliance of the United States, 1883	www.jewelerssecurity.org
National Association of Security Companies, 1972	www.nasco.org
National Burglar and Fire Alarm Association, 1948	www.alarm.org
National Classification Management Society, 1964	www.classmgmt.com

National Fire Protection Association, 1896
 Operations Security Professionals Society, 1990
 Risk and Insurance Management Society, 1950
 Security Industry Association, 1969
 Society for Human Resource Management, 1948
 Underwriters Laboratories, 1924

www.nfpa.org
www.opsec.org
www.rims.org
www.siaonline.org
www.shrm.org
www.ul.com

Federal Contacts

Organization	Web Site
Central Intelligence Agency	www.cia.gov
Chemical Safety and Hazard Investigation Board	www.chemsafety.gov
Consumer Product Safety Commission	www.cpsc.gov
Cyber Threat Intelligence Integration Center	Information
Department of Defense	www.defenselink.mil
DoD Security Institute	www.dtic.mil/dodsi
Defense Nuclear Facilities Safety Board	www.dnfsb.gov
Department of Energy	www.energy.gov
Department of Homeland Security	www.dhs.gov
US Customs & Border Protection	www.cbp.gov
Immigration & Customs Enforcement	www.ice.gov
Federal Emergency Management Agency	www.fema.gov
Secret Service	www.secretservice.gov
Department of Justice	www.usdoj.gov
Alcohol, Tobacco & Firearms	www.atf.gov
Community Oriented Policing Services	www.cops.usdoj.gov
Federal Bureau of Investigation	www.fbi.gov
National Counterintelligence Executive	www.ncix.gov
National Transportation Safety Board	www.nts.gov
Nuclear Regulatory Commission	www.nrc.gov
Department of Labor	www.dol.gov
Occupational Safety & Health Administration	www.osha.gov
Department of State	www.state.gov
Overseas Security Advisory Council	www.osac.gov
Department of Transportation	www.dot.gov
Federal Aviation Administration	www.faa.gov
Maritime Administration	www.marad.dot.gov
National Highway Traffic Safety Administration	www.nhtsa.dot.gov
Department of the Treasury	www.ustreas.gov

Other Security-Related Contacts

Another security-related contact is the Transportation Research Board of the National Academies (www.trb.org).



Appendix B

Code of Ethics of ASIS International

Preamble

Aware that the quality of professional security activity ultimately depends upon the willingness of practitioners to observe special standards of conduct and to manifest good faith in professional relationships, ASIS adopts the following Code of Ethics and mandates its conscientious observance as binding condition of membership in or affiliation with ASIS:

Article I

A member shall perform professional duties in accordance with the law and the highest moral principles.

Ethical Considerations

- 1-1** A member shall abide by the law of the land in which the services are rendered and perform all duties in an honorable manner.
- 1-2** A member shall not knowingly become associated in responsibility for work with colleagues who do not conform to the law and these ethical standards.
- 1-3** A member shall be just and respect the right of others in performing professional responsibilities

Article II

A member shall observe the precept of truthfulness, honesty, and integrity.

Ethical Considerations

- 2-1** A member shall disclose all relevant information to those having the right to know.
- 2-2** A “right to know” is a legally enforceable claim or demand by a person for disclosure of information by a member. This right does not depend upon prior knowledge by the person of the existence of the information to be disclosed.
- 2-3** A member shall not knowingly release misleading information, nor encourage or otherwise participate in the release of such information.

Article III

A member shall be faithful and diligent in discharging professional responsibilities.

Ethical Considerations

3-1 A member is faithfully when fair and steadfast in adherence to promises and commitments.

3-2 A member is diligent when employing best efforts in an assignment.

3-3 A member shall not act in a matters involving conflicts of interest without appropriate disclosure and approval.

3-4 A member shall represent services or product fairly and truthfully.

Article IV

A member shall be competent in discharging professional responsibilities.

Ethical Considerations

4-1 A member is competent who possesses and applies the skills and knowledge required for the task.

4-2 A member shall not accept a task beyond the member's competence nor shall competence be claimed when not possessed.

Article V

A member shall safeguard confidential information and exercise due care to prevent its improper disclosure.

Ethical Considerations

5-1 Confidential information is nonpublic information, the disclosure of which is restricted.

5-2 Due care requires that the professional must not knowingly reveal confidential information or use a confidence to the disadvantage of the principal or to the advantage of the member or a third person unless the principal consents at the full disclosures of all the facts. This confidentiality continues after the business relationship between the member and his principal has terminated.

5-3 A member who receives information and has not agreed to be bound by confidentiality is not bound from disclosure it. A member is not bound by confidential disclosures of acts or omissions that constitute a violation of the law.

5-4 Confidential disclosure made by a principal to a member are not recognized by the law as privileged in a legal proceeding. In an legal proceeding, the member may be required to testify to information received in confidence from his principal over the objection of his principal's counsel.

5-5 A member shall not disclosed confidential information for personal gain without appropriate authorization.

Article VI

A member shall not maliciously injure the professional reputation or practice of colleagues, clients, or employers.

Ethical Considerations

6-1 A member shall not comment falsely and with malice concerning a colleague's competence, performance, or professional capabilities.

6-2 A member who knows, or has reasonable grounds to believe, that another member has failed to conform to code of ethics of ASIS should inform the Ethical Standards Council in accordance with Article VIII of the Bylaws.



Appendix C

The MBA Oath

Preamble

As a manager, my purpose is to serve the greater good by bringing together people and resources to create value that no single individual can build alone. Therefore I will seek a course that enhances the value my enterprise can create for society over the long term. I recognize that my decisions can have far-reaching consequences that affect the well-being of individuals inside and outside my enterprise, today and in the future. As I reconcile the interests of different constituencies, I will face difficult choices.

Therefore I promise:

1. **I will act with utmost integrity and pursue my work in an ethical manner.** My personal behavior will be an example of integrity, consistent with the values I publicly espouse.
2. **I will safeguard the interests of my shareholders, coworkers, customers and the society in which we operate.** I will endeavor to protect the interests of those who may not have power, but whose well-being is contingent on my decisions.
3. **I will manage my enterprise in good faith, guarding against decisions and behavior that advance my own narrow ambitions but harm the enterprise and the people it serves.** The pursuit of self-interest is the vital engine of a capitalist economy, but unbridled greed can be just as harmful. I will oppose corruption, unfair discrimination, and exploitation.
4. **I will understand and uphold, both in letter and in spirit, the laws and contracts governing my own conduct and that of my enterprise.** If I find laws that are unjust, antiquated, or unhelpful I will not brazenly break, ignore or avoid them; I will seek civil and acceptable means of reforming them.
5. **I will take responsibility for my actions, and will represent the performance and risks of my enterprise accurately and honestly.** My aim will not be to distort the truth, but to transparently explain it and help people understand how decisions that affect them are made.
6. **I will develop both myself and other managers under my supervision so that the profession continues to grow and contribute to the wellbeing of society.** I will consult colleagues and others who can help inform my judgment and will continually invest in staying abreast of the evolving knowledge in the field, always remaining open to innovation. I will mentor and look after the education of the next generation of leaders.

7. **I will strive to create sustainable economic, social, and environmental prosperity worldwide.** Sustainable prosperity is created when the enterprise produces an output in the long run that is greater than the opportunity cost of all the inputs it consumes.
8. **I will be accountable to my peers and they will be accountable to me for living by this oath.** I recognize that my stature and privileges as a professional stem from the respect and trust that the profession as a whole enjoys, and I accept my responsibility for embodying, protecting, and developing the standards of the management profession, so as to enhance that trust and respect.

This oath I make freely, and upon my honor.

Source: mbaoath.org.



Appendix D

Selected Security Standards

Standards are voluntary agreements that specify that a product, system, or service meets mutually agreed-to specific criteria and requirements. They are produced by consensus from standards-setting organizations like the ones listed in the following. Standards are proven, recognized, reliable, repeatable, fair, transparent, and globally accepted, and possess assured accountability.

Most standards in the United States are set by government, primarily for military contract purchases. However, most of the standards in this section have no enforcement power – except for the action of a standards-setting organization to make clear that products, systems, or services not meeting standards have untested risk to them. That does not make standards impotent. If harm occurs and a product, system, or service does not meet standards available for them, this omission could be a negative factor in a civil lawsuit filed in order to redress the harm.

This appendix mentions a selected list of security standards. In some industries important standards exist but are not listed here because of their restricted application. Indeed some organizations with relevant standards for security, safety, and fire prevention are not mentioned. However, citations for them are included at the end of this section.

The American National Standards Institute (ANSI) designation that appears before some standards means that the particular standards have been approved by this comprehensive standards review group, raising its level of significance.

ASIS International

ASIS International has developed a series of standards to support accountability for the following: Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict (09/2008); International Code of Conduct for Private Security Service Providers (11/2010). These are aligned with globally accepted standards on quality management, organizational resilience, and other topics.

ANSI/ASIS CSO.1-2013: *Chief Security Officer (CSO) – An Organizational Model*

ANSI/ASIS PSC.1-2012: *Management System for Quality of Private Security Company Operations – Requirements with Guidance* (available in Spanish)

ANSI/ASIS PSC.2-2012: *Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations*

ANSI/ASIS PSC.3-2013: *Maturity Model for the Phased Implementation of a Quality Assurance Management System for Private Security Service Providers*

ANSI/ASIS PSC.4-2013: *Quality Assurance and Security Management for Maritime Private Security Companies Operating at Sea – Guidance*

ANSI/ASIS/SHRM WVP1-1-2011: *Workplace Violence Prevention and Intervention* (available in Spanish)

ANSI/ASIS SPC.1-2009: *Organizational Resilience: Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use* (available in Spanish)

ANSI/ASIS SPC.2-2014: *Auditing Management Systems: Risk, Resilience, Security, and Continuity – Guidance for Application* (available in Spanish)

ANSI/ASIS SPC.4-2012: *Maturity Model for the Phased Implementation of the Organizational Resilience Management System*

ANSI/ASIS/BSI BCM.1-2010: *Business Continuity Management Standard*

ANSI/ASIS PAP.1-2012: *Security Management Standard: Physical Asset Protection* (available in Spanish)

ANSI/ASIS SCRM.1-2014: *Supply Chain Risk Management: A Compilation of Best Practices*

ASIS International – Under Development

Continuity Resilience (SPC.5)

Management System for Quality of Private Security Company (PSC) Operations – Requirements with Guidance

Managing the Investigative Process – Guidance (INV)

Resilience in the Supply Chain Standard (SPC.3)

Risk Assessment Standard (RA)

Supply Chain Risk Management Standard: A Compilation of the Best Practices (SCRM)

To order standards: www.asisonline.org

National Fire Protection Association (NFPA)

NFPA 1: Fire Prevention Code

NFPA 10: Portable Fire Extinguisher

NFPA 13: Installation of Sprinkler System

NFPA 13A: Care and Maintenance of Sprinkler System

NFPA 70: National Electrical Code

NFPA 72®: Four-Wire Smoke Detector Installation

NFPA 101: Exit Safety for Building Occupants

NFPA 600: Private Fire Brigades

NFPA 601: Guard Service in Fire Loss Prevention

NFPA 730: Premises Security

NFPA 731: Installation of Electronic Premises Security Systems

NFPA 910: Protection of Libraries and Library Collections

NFPA 911: Protection of Museums and Museum Collections

To order standards: www.nfpa.org

National Institute of Justice (NIJ)

NIJ 0108.01 and EN 1063: No Spall Bullet Resistant Laminates (see also UL 752)

To order standards: www.nij.gov

Security Industry Association (SIA) Standards

ANSI/SIA CP-01-2014: Control Panel Standard – Features for False Alarm Reduction

ANSI/SIA DC-09-2007: SIA DCS – Internet Protocol Event Reporting

ANSI/SIA MSD-01-2000: MSD Monitoring Practices Standard

ANSI/SIA PIR-01-2000: PIR False Alarm Immunity Standard

SIA: Open Supervised Device Protocol (OSDP)

SIA AC-01-1996.10: Access Control – Wiegand

SIA AC-03-2000.06: Access Control Badging Guideline

SIA AV-01-1997.11: Audio Verification – 2 Way Voice Standard

SIA BIO-01-1993.02 (R2000.06): Biometric Vocabulary Standard

SIA DC- 01-1988 (R2001.4): DCS Computer Interface (CIS-1) Technical Report

SIA DC-02-1992.02 (R2000.05): DCS Generic Protocols Technical Report

SIA DC-03-1990.01 (R2003.10): DCS SIA Format Standard

SIA DC-04-2000.05: DCS SIA 2000 Standard

SIA DC-05-1999.09: DCS Ademco Contract ID Standard

SIA DC-07-2001.04: DCS Computer Interface (CIS-2) Standard

SIA GB-01-1994.12: Glassbreak False Alarm Reduction Standard

SIA GB-01-1996.07: Glassbreak False Alarm Sounds Technical Report

SIA PID-01-1995.12 (2000.06): Point ID Sensor Multiplex Protocol Standard

SIA RF-01-1997.04: Short Range RF Definitions Standard

SIA TVAC-01-2001.04: TVAC – CCTV to Access Control Standard

SIA/IAPSC AG-01-1995.12 (R2000.03): Architectural Graphics – CAD Standards

To order standards: www.siaonline.org

Underwriters Laboratories (UL)

ANSI/UL 140: Relocking Devices for Safes and Vaults

ANSI/UL 291: Automated Teller Systems

ANSI/UL 294: Access Control Units

ANSI/UL 365: Police Station Connected Burglar Alarm Units and Systems

ANSI/UL 608: Burglary Resistant Vault Doors and Modular Panels

ANSI/UL 609: Local Burglary Alarm Units and Systems

ANSI/UL 634 Connectors and Switches for Use with Burglar-Alarm Systems

ANSI/UL 636: Holdup Alarm Units and Systems

ANSI/UL 639: Intrusion Detection Units

UL 681: Installation and Classification of Burglar and Holdup Alarm Systems

ANSI/UL 752: Bullet-Resisting Equipment
ANSI/UL 872 Central-Station Alarm Services
ANSI/UL 985: Household Fire Warning System Units
ANSI/UL 1023: Household Burglar-Alarm System Units
ANSI/UL 1037: Anti-Theft Alarms and Devices
ANSI/UL 1610: Central-Station Burglar-Alarm Units
ANSI/UL 1635: Digital Alarm Communicator System Units
ANSI/UL 1641: Installation and Classification of Residential Burglar Alarm Systems
ANSI/UL 1981 Central-Station Automation Systems
ANSI/UL 2044 Commercial Closed-Circuit Television Equipment
To order UL standards: www.ul.com

Other groups that provide standards, training, and best practices for security-oriented organizations not discussed here are as follows:

ABA: American Bankers Association, Accredited Standards Committee (www.aba.com and www.x9.org)
AFAA: The Automatic Fire Alarm Association (www.affaa.org)
ASTM: American Society for Testing and Materials (www.astm.org)
BOCAI: BOCA International (www.bocai.org)
CSAA: The Central Station Alarm Association (www.csaintl.org)
FM: Factory Mutual (www.fmglobal.com)
ISO: International Organization for Standardization (www.iso.org)
ISO: Insurance Services Office
NBFAA: National Burglar and Fire Alarm Association (www.alarm.org)
NIST: National Institute of Standards and Technology (www.nist.gov/aes)
SFPE: The Society of Fire Protection Engineers (www.sfpe.org)

The Office of Physical Security Programs of the U.S. Department of State promulgates standards to protect personnel serving abroad and embassies and consulates. These standards have influenced private sector and other public sector organizations in security planning. (www.state.gov/documents/organization/88382.pdf)



Glossary

- ABC technique:** A time management concept in which the adherent categorizes items to be done according to their vital importance, nominal importance, and unimportance.
- Acceptance theory:** A concept advanced by Chester Barnard holding that subordinates will cooperate in the goals of the organization and assent to authority when certain conditions were met.
- Adverse impact:** Having an opposed or contrary effect on members of the public who are protected by legislation. For example, an individual with a physical disability may be able to perform all the duties of a security receptionist or alarm monitoring agent except that the computer keyboard is difficult to reach, creating an adverse impact. Cutting a semicircular area from the counter would be an appropriate accommodation.
- Amortization:** The allocation and charge to expense of the cost or other basis of an intangible asset over its estimated useful life. Intangible assets such as goodwill are not amortizable. Examples of amortizable intangibles include capital costs, leasehold improvements and interests, patents, and copyrights.
- Analysis:** The process of separating a problem into its constituent parts or basic principles so as to determine the nature of the whole and to examine it methodically. Related to planning.
- At-will employment:** The concept that an employee may be fired at any time for good cause, bad cause, or no cause at all. Originated by Horace G. Wood in 1877. The at-will concept of employment was less common in the second half of the twentieth century, but still is the basis of employment for most private sector and institutional employees.
- Auditor:** See *independent auditor*.
- Baseline:** Readings on a polygraph chart that form a point of comparison for the psychological responses to polygraph questions.
- Behaviorally Anchored Rating Scale (BARS):** A behaviorally oriented scale sometimes used to assess performance.
- Biometric:** A security identification system that uses a physical feature and measures it automatically. The information from the physical feature is translated into a digital register, which is then compared with the values found in the approved database list.
- Break-even:** The point at which fixed costs and variable costs equate with sales or revenues volume.
- Budget:** A financial statement prepared prior to an accounting period containing the financial plans to be achieved during that period.
- Bureaucracy:** An organization with the following traits: a chain of command with fewer people at the top than at the bottom, well-defined positions and responsibilities, generally inflexible rules and procedures, and delegation of authority from the top down. Considered the most rational form of organization by Max Weber.
- Capital expenditures:** The cost of purchasing or improving a fixed asset, which will be depreciated over the estimated useful life of that asset.
- Cash flow:** A measurement of the inflow and outflow of cash and cash equivalents over a financial period.
- Certificate of good conduct:** A written document that determines whether a person is law-abiding at that time in the area in which the document is produced.
- Certificate of relief:** An order by a civilian or military judge in which an offender's criminal record may be sealed from public scrutiny or consideration in employment circumstances. It may be lifted in cases of employment consideration by government.
- Charge-coupled device:** A camera that uses a semiconductor microchip as the imaging device.
- Chief financial officer (CFO):** The senior official in an organization responsible for financial activities.

Claims-made coverage: This is a type of general liability insurance. It protects the insured only when both the alleged incident and the resulting claim happen during the time the policy is in force. See *occurrence coverage*.

Collusion: A conspiracy between two or more persons to defraud a person or persons of their rights by fraudulent means. When one fraudster is an employee and another is outside the organization, the effects from the secret combination can be deep and costly.

Concentric circles of protection: The notion that all countermeasures to crime and disorder have their limitations; therefore, numerous countermeasures need to be designed and implemented to protect a facility or program. Also called layered security.

Contingency: Something that may or may not happen; a possibility. In emergency planning, the term refers to an emergency or casualty.

Contingency management: See *crisis management*.

Contracting out: The process of transferring responsibility for certain tasks or duties to another party or organization.

Cost-benefit analysis (CBA): One of the steps in management decision making: identification of problem, problem assessment, problem management with options, CBA, and decision making about program implementation.

CRAVED: The acronym in situational crime prevention to identify hot products that are attractive to thieves. It stands for concealable, removable, available, valuable, enjoyable, and disposable.

Crime prevention through environmental design (CPTED): The concept of defensible space attributed to criminologist C. Ray Jeffrey.

Crisis management: The process of dealing with an event or set of circumstances that can lead to loss to persons or an organization; a critical point that demands resolute action.

Cross-training: When an employee in one primary job task is trained in another or other tasks.

Cybercrime: A variety of offenses related to information technology. They include extortion, boiler room investment and gambling fraud, and fraudulent transfers of funds. The term was coined by Donn B. Parker.

Delegation: The giving of authority by one person to another; for example, a manager delegates responsibility to employees.

Denial-of-service (DoS) attack: An attack on a Web site that usually crashes the system. It is one of the most harmful types of cybercrime. The attacker triggers a large number of distributed simultaneous demands on a system from computers that have been taken over. For this reason it is also sometimes called a *distributed denial-of-service (DDoS)* attack.

Depreciation: The cost of the economic benefits of a tangible fixed asset that has been consumed over a financial period.

Deputizing: The process of selecting personnel to manage or direct an operational plan.

Diligence: A measure of prudence or activity that is to be expected from a reasonable and prudent person under the particular circumstances; it is not measured by an absolute standard, but is dependent on circumstances of a particular case. Also referred to as due diligence.

Director: A person appointed or elected according to law and authorized to manage and direct the affairs of a corporation or company. Inside directors are employees, like the CEO or CFO; outside directors are not employees, but may be officers of other corporations and possess skills and experience believed to be valuable in directing the affairs of the corporation.

Discipline: The process of controlling behavior (e.g., in a workplace).

Disguised-purpose test: A test instrument that seeks to determine characteristics of deviance or unreliability without asking direct questions. Also called a covert test instrument.

Dividends: The distribution of current or accumulated earnings to the shareholders of a corporation *pro rata* based on the number of shares owned.

Embezzlement: The willful taking or converting to one's own use the assets of another that the wrongdoer acquired possession of lawfully during the course of office, employment, or reasons of trust.

Embezzlement differs from larceny in that the original taking of property was lawful or with the consent of the owner; in larceny, the felonious intent must have existed at the time of the initial taking.

Equity: The extent of a stockholder's proportionate ownership interest in the corporation's capital stock and surplus; the extent of ownership interest in a venture. Also refers to injustice as a concept of fairness as contrasted with strictly formulated rules of common law.

Ethics: Relating to moral action, conduct, motive, or character; professionally right or befitting conduct, conforming to professional standards of conduct.

False-negative: An erroneous decision that a person is not deceptive when she or he actually is deceptive. Also called Type I or A.

False-positive: An erroneous decision that a person is being deceptive when she or he actually is being truthful. Also called Type II or B.

Firewalls: A network security system used to monitor and restrict external and internal traffic.

Fraud: The criminal offense of intentionally deceiving another person or persons to obtain financial or monetary gains. Fraud usually does not involve property damage or threatened or actual physical injury to another.

Functional foremanship: A concept introduced by Frederick W. Taylor that when different responsibilities are understood, managerial or supervisory employees can change without affecting production by workers.

Generally accepted accounting principles (GAAP): Standards and concepts followed by accountants in measuring, recording, and reporting transactions.

Graphic user interface (GUI): A system whereby a user may direct a computer program by touching or clicking on symbols located on the monitor screen.

Grievance: A complaint filed by an employee, or by his or her union representative, regarding working conditions to seek resolution for which procedural measures are available in the union agreement.

Gross domestic product (GDP): The economic activity of a country during a particular calendar year; an international convention aggregating economic activity.

Gross national product (GNP): GNP includes the GDP plus net income transfer from international economic activity.

Halo effect: The tendency of some evaluators to judge workplace performance of subordinates as consistently superior, despite evidence to the contrary in some situations.

Hawthorne investigations: Investigations conducted by Elton T. Mayo and others at the Western Electric company's plant in Hawthorne, Illinois. The research seemed to establish that paying attention to workers affected production output more than extrinsic factors did.

Hierarchy of human needs: Proposed by Abraham Maslow, this hierarchy identifies five levels of needs, with a lower one having to be satisfied before the next higher one can become important. Also called Maslow's pyramid or ladder.

Independent auditor: Usually a firm or corporation retained by a corporation to check and attest to the accuracy, fairness, and general acceptability of accounting records and statements. Usually performed by a certified public accountant.

Informed consent: A person agrees in writing to allow something to happen (e.g., a check of credit records) based on disclosure of relevant facts relating to the procedure.

Inspector-general: Government personnel whose primary function is to conduct and supervise audits and investigations relating to programs and operations of the particular agency. May investigate allegations by whistle-blowers.

Job description: A statement of facts about a particular job that can be used to determine job requirements (skill, knowledge, physical and mental efforts), responsibility, and working conditions. It sets out the requirements that applicants should be able to meet.

Knowledge workers: A term coined by Peter F. Drucker referring to executives, managers, and individual professionals who, through their knowledge or positions, make decisions that have a significant impact on the performance and results of the whole group or organization.

Larceny: The unlawful taking and removal of another's property with the intent to convert it or deprive the owner of its use.

Liabilities: An obligation to transfer economic benefit as a result of a passed transaction.

Likert scale: The scale used in certain tests that ask test takers to judge a question on a scale of 1–7, in which 1 and 7 represent the extremes and 4 represents the midpoint, and the numbers between the extremes represent degrees of difference.

Line item: An expense planned on an ongoing basis, such as a position.

Local area network (LAN): A collection of computing resources (e.g., PCs, printers, minicomputers, and mainframes) linked by a common transmission medium such as a coaxial cable.

Management by objectives (MBO): A popular management strategy in which employees and supervisors set mutually agreed-upon goals and endeavor to reach them. Proposed by Peter F. Drucker and Douglas McGregor in the 1950s.

Middle management: Managers who supervise first-line managers and some nonmanagement personnel. They coordinate tasks and do some planning to achieve organizational goals.

Model penal code: A codification of the principles of criminal law published by the American Law Institute in 1962. It served to unify state codes following its publication.

Moonlighting: Working at a second job after regular working hours. Some police officers moonlight as private security officers.

National Labor Relations Act: This 1935 law requires organizations to recognize and bargain with the union if that union has been legally established by the organization's employees. Section 9(b)(3) permits employers the right to terminate voluntary recognition of nonguard unions to perform security services. Also called the Wagner Act.

Negligence: The failure to do something that a reasonable person, guided by ordinary considerations, would do; the failure to use such care as a reasonably prudent and careful person would use under similar circumstances. The opposite of diligence. Negligence varies in significance from slight negligence (a failure to exercise great care) to gross negligence (the intentional failure to perform a manifest duty in reckless disregard of consequences affecting the life or property of others).

Occurrence coverage: This type of general (commercial) liability coverage protects the policy holder from any covered incident that "occurs" during the policy period, regardless of when the claim is filed. Such a policy pays for defense costs and settlement or judgment indemnification.

Organizing: The process of amassing critical resources needed in a plan so that the action aspect of the plan may get under way.

Outsourcing: See *contracting out*.

Overt integrity test: An employment test that raises specific questions about the test taker's past deviant behavior as well as attitudes toward such behavior in others. See *disguised-purpose test*.

Pareto principle: A rule that posits that 80% of business activity comes from about 20% of the customers or clients. Named for Vilfredo Pareto, an Italian economist.

Peace Officer Standards of Training (POST): Training requirements whereby someone is trained following the statute of a particular state in the legal basis of making arrests. Some security officers are trained as peace officers with supplemental training that requires an average of 40 hours of classroom instruction.

Performance standards: These standards compare the actual work of an employee with a standard rate of work.

Peter Principle: This idea stipulates, semiseriously, that employees rise to the level of their incompetence. Proposed by Lawrence J. Peter and Raymond Hull.

Piece-rate: A form of financial incentive, proposed by Frederick W. Taylor, that provided for higher compensation to workers who produced at rates above the expected level.

Plaintiff's action: Such cases are usually in civil cases in which a complainant seeks redress for alleged grievances and harms. Negligent hiring and retention may be the basis for such a case.

- Planning:** The process of determining how a problem or opportunity may be responded to. Involves identifying problems or opportunities, analyzing relevant characteristics of the circumstances, organizing the formal response, deputizing a leader to head the response effort, and supervising the person(s) selected.
- Privatization:** The process whereby a public entity, usually a government, contracts out for services or materials to the private sector that the public sector might formally have managed for itself.
- Profit:** A reward to that factor of production known as enterprise; the residual figure in payment for risk bearing; the money remaining after all expenses, amortization, taxes, and other charges have been subtracted.
- Proprietary:** Refers to property ownership; possessorship of assets or opportunity. In a proprietary security department, all employees are normally full-time, not contract, employees.
- Proximate cause:** A natural and continuous sequence that produces a direct result.
- Publicly held corporations:** Corporations whose stock is held by and available to the public. Such shares are usually traded on a securities exchange or over-the-counter.
- Pygmalion effect:** Named for the George Bernard Shaw play in which a simple flower girl was transformed into a refined socialite; a kind of self-fulfilling prophecy.
- Quality circles:** Employees' committees that analyze and solve quality problems. An outgrowth of the work conducted by W. Edwards Deming.
- Relevant/irrelevant technique:** An examination technique that uses two types of questions – relevant questions and neutral questions – to assess the subject's baseline response.
- Relevant questions:** Polygraph test questions about the topic or topics under investigation.
- Reliability (in preemployment tests):** Implies that the same test will produce about the same results if administered at a later time.
- Request for proposal (RFP):** The process by which an organization formally requests that bidders indicate how they will provide the services required by a client and their proposed fee.
- Respondeat superior:** The doctrine that states that the master (employer) is liable in certain cases for the wrongful acts of servants (employees) and is a principal for these agents.
- Return on equity (ROE):** An accounting ratio in which the net income is expressed as a percentage of capital employed.
- Return on investment (ROI):** An accounting ratio in which the net income is expressed as a percentage of capital employed plus cost of capital.
- Risk management:** The process of identifying hazards of property insured; the casualty contemplated in a specific contract of insurance; the degree of hazard; a specific contingency or peril. Generally not the same as security management, but may be related in concerns and activities. Work is done by a risk manager.
- SARA:** An acronym from situational crime prevention that identifies the process through which a practitioner should go when faced with a crime problem: scan, or identify the problem; analyze it in a detailed way; response from the plan created from the analysis; and assess to assure objectives are being reached.
- Security design:** The process by which a new facility or retrofit is designed and engineered with protective principles considered, usually from the earliest stages of planning.
- Senior management:** Usually refers to headquarters staff officers.
- Shareholder:** A person who owns shares or stocks in a corporation or joint-stock company. Also called stakeholder, stockholder, or stock owner.
- Shareholders' equity:** The asset value in the organization belonging to shareholders, plus any reserves.
- Situational crime prevention (SCP):** The primary theoretical basis for understanding and manipulating aspects of crime reduction. The elements are a motivated offender, a suitable reward or goal, and the absence of appropriate control. If any one of these factors is changed, the likelihood of loss also will change.
- Supervising:** The process whereby a manager responsible for an operation ascertains the progress of the intended plan, including ongoing evaluation of the persons specifically responsible for carrying out the plan. See *deputizing*.

Tempest: The technology and processes of illuminating undesirable electronic emanations.

Theory X and Theory Y: Two management theories described by Douglas McGregor that reflect opposite ways management has of viewing the workforce. The Theory X manager favors authoritarian leadership with centralized decision making and close supervision of work activities. The Theory Y manager favors participatory decision making, a decentralized authority structure, and less emphasis on coercion as a motivator.

Theory Z: Proposed by William Ouchi at a time when market share in some industries was lost to Japanese competitors. Theory Z incorporates aspects of American and Japanese styles of management.

Uniform Crime Reports (UCR): A national report of “serious crime,” or Type I incidents, compiled by the Federal Bureau of Investigation. Includes four violent incidents (non-negligent homicide, rape, robbery, and aggravated assaults) and four property crimes (burglary, larceny, vehicular theft, and arson).

Uninterrupted power supply (UPS): A device that stores energy during normal operations so that it can provide backup energy if power fails.

Validity (in preemployment test): Implies that the test measures what it is supposed to.

Vetting: The process of ascertaining the accuracy and completeness of information. Often refers to pre-employment screening.

Whistle-blower: An individual who informs on an employee’s or employer’s misconduct. In federal and state statutes, public employees are protected from retaliation for such disclosures. Some states also protect private sector whistle-blowers.

White-collar crime: Unlawful, nonviolent conduct by corporations and individuals, including theft or fraud and other violations of trust occurring during the time of the offender’s occupation. White-collar crime is a frequent focus of internal investigations within the organization. A term devised by the sociologist Edwin Sutherland. See also *embezzlement*.



Subject Index

A

- ABC technique, 166–171
- Acceptance theory, 13
- Access control equipment, 58
- Access control systems, 346
 - biometric features, 348–349
 - ID cards and tokens, 347–348
 - ID numbers and passwords, 347
 - radio-frequency identification, 349
- Accounting controls, 251–283
 - financial controls, 251–266
 - change in auditors, 262
 - consolidated balance sheets, 253–259
 - evolution of, 252–253
 - independent auditor statement, 261–262
 - manipulation of financial statements, 263–265
 - notes to statement of operations, 259–261
 - not-for-profit organizations, 265–266
 - overview, 251–252
 - Securities and Exchange Commission (SEC), 263
 - forensic safeguards to internal fraud, 279–283
 - fraud, embezzlement, and security, 281
 - generally accepted accounting principles (GAAP), 279–281
 - overview, 279
 - separating tasks, 281–283
- Accounting policies, 259
- ADA. *See* Americans with Disabilities Act (ADA)
- Addictive substances, 382
- Administrative expenses, 258
- Administrator, 4
- Advanced security programming course, outline of, 129–130
 - attack methods, 129
 - authentication, 129
 - cryptography, 130
 - firewall architecture, 129
 - firewall components, 129
 - intrusion detection and response, 130
 - security assessment, 129
 - security implementation policy, 129
- Adverse impact, 390
- Alarm contract, 320–322
 - install and monitor alarm signals, 320
 - notification for termination, 321
 - security system
 - burden of customer, 321
 - daily testing, 321
 - liability for negligence, 322
 - maintenance of, 321
 - obligations of subscriber, 322
 - ownership of, 321
 - suitability, 321
 - telephonic signals, interruption of, 321
 - terms of agreement, 321
 - typical aspects, 320
- Alarm monitoring, 151
 - operators, 150
- Alarm services, 278
 - contracting, 320–322
- Alcohol abuse, 247
- Alert Management Systems, Inc., 44
- AlliedBarton Academy, 134
- Allied International Union, 54
- American Management Association, 137
- American management concept, 6
 - analysis and planning in, 7
 - criticize, 7
 - deputize, 7
 - organizing, 7
 - supervise, 7

American Psychological Association (APA), 95
 American Society for Industrial Security-
 International (ASIS-International),
 16, 18, 41, 137
 members of, 41
 Private Security Officer Training
 Guidelines, 123
 Americans with Disabilities Act (ADA), 84, 85
 American Telephone and Telegraph (AT&T),
 172
 American workplace, 160
 Ames, Aldrich, 96
 Amortization, 256
 Analytical directors, 289
 Ancillary costs, 318
 Annual budgeting process, 266
 Annual reports, corporation's, 260
 APA. *See* American Psychological
 Association (APA)
 Application, and vetting process, 82–86
 Appraisal document, 187, 189–193
 Appraisal interview, 199–202
 Appraisals. *See* Performance appraisals
 Armed security guards
 training for, 124
 classroom-based training, 124
 range-based training, 124
 Armored car industry, 124
 Armored car personnel, 150
 Armored car services, 57
 ASIS-International. *See* American Society for
 Industrial Security-International
 Assets, 5
 Association of Certified Fraud Examiners,
 296, 297
 Association of Test Publishers (ATP), 102
 ATMs. *See* Automated teller machines (ATMs)
 ATP. *See* Association of Test Publishers (ATP)
 AT&T. *See* American Telephone and Telegraph
 (AT&T)
 At-will employment, 230–233
 Audio alarm, 346
 Audiovisual (AV) materials, 130–131
 Audit committee, 26
 Audit firms, 280

Auditors, 262, 281
 independent statement, 261–262
 Authentication, 129
 Automated teller machines (ATMs), 57
 Automatic access control, 373
 Automatic sprinkler systems, 357
 Average tendency, 197
 AV materials. *See* Audiovisual (AV) materials

B

Badges, 70
 Balance sheet, 252
 Bank Crime Statistics Reports, 160
 Bank of Commerce and Credit International
 (BCCI), 400
 Bank Security Act of 1968, 46, 47
 Bank tellers, 247
 Ban the box, 86–87
 Barefoot, J. Kirk, 20
 Barnard, Chester, 12
 Barriers, as security countermeasure, 334–335
 Barry, Joseph, 325
 BARS. *See* Behaviorally Anchored Rating Scale
 (BARS)
 Baseline, 273
 BCCI. *See* Bank of Commerce and Credit
 International (BCCI)
 Becker, Gavin de, 247
 Behaviorally Anchored Rating Scale (BARS), 189
 Behaviorally oriented screening process, 97
 Behavioral measurement, 189
 Benevolent authoritative, 15
 Bernardin, H. John, 101
 Biometric features, 348–349
 Biometrics, to time and attendance, 301
 Biometric systems, 348
 Blanchard–Johnson human relations strategy,
 155, 158, 159
 Blanchard–Johnson thesis, 159
 BLS. *See* Bureau of Labor Statistics (BLS)
 Board committees, 26
 Board membership, 24
 Board of directors, 212, 281
 Bomb-detection system, 355
 Bomb threat analysis, 351

- Boni, William C., 375
- Bookkeeping, 252
- Bottom-up appraisals, 187
- Bow Street Runners, 41
- Braunig, M. J., 384
- Brock, Randolph, D. III, 283, 394
- Budget approval process, 266
- Budgeting, 266–270
 - profits, 270–277
 - capital budgeting for, 275–277
 - return on equity (ROE), 272
 - return on investment (ROI), 272–275
 - purposes of, 266
 - security as profit center, 278
 - for security department, 266–270
 - overview, 266–268
 - process of budget creation, 268–270
 - senior management seeks to cut security spending, 277–278
- Bureaucracy, 12–13, 205
- Bureau of Labor Statistics (BLS), 375
- Burglar alarm certificates, 349, 350
- Burglar resistance, 340
- Burns, James MacGregor, 363
- Buros Center for Testing, 102
- Buros Institute of Mental Measurements, 102
- Business espionage, 33, 394–395
- Business Espionage Controls and Countermeasures Association, 33
- Business services and insurance, 65
- Butcher, J.N., 98
- C**
- Cameras, 341
- Candidate assessment, 107
- Capital budgeting, 275–277
 - initial-investment rate of return (IIRR)
 - method, 276
 - other managerial options, 277
 - payback method, 276
 - time-adjusted rate of return (TARR)
 - method, 276
- Capital expenditure budgets, 267
- Cardiopulmonary resuscitation/automated external defibrillator (CPR/AED), 136
- Cargo/supply chain theft, 396–397
- Carnegie, Andrew, 183
- Cash-based accounting, 263
- Cash flows, 276
- Cash penalties, 318
- Casinos, security for, 123
- Cathode ray tubes (CRTs), 341
- CCD. *See* Charge-coupled device (CCD)
- CC/IPTV. *See* Closed circuit/Internet Protocol television (CC/IPTV) system
- CCTV. *See* Closed-circuit television (CCTV)
- Centers for Disease Control and Prevention, 375
- Central Intelligence Agency (CIA), 96
- Central station services, 57
- CEO. *See* Chief executive officer (CEO)
- Certification, 137
 - in protection field, 138
- Certified Forensic Interviewer (CFI), 139
- Certified Fraud Examiner™ (CFE), 138
- Certified Healthcare Protection Administrator (CHPA), 138
- Certified Information Systems Security Professional® (CISSP), 138
- Certified Institutional Protection Specialist (CIPS), 139
- Certified Protection Professional™ (CPP)
 - designation, 138
- Certified public accountants (CPAs), 251
- CFE. *See* Certified Fraud Examiner™ (CFE)
- CFI. *See* Certified Forensic Interviewer (CFI)
- CFO. *See* Chief financial officer (CFO)
- Charge-coupled device (CCD), 341
- Check authorization, 282
- Check preparation, 282
- Chief executive officer (CEO), 21, 52, 145, 212
 - history and welcome, 153
 - performance evaluations of, 212
- Chief financial officer (CFO)
 - responsibilities, 251
- Chief operating officer (COO), 21, 145
- Chief security officer (CSO), 29, 113, 145, 371
- Chip cameras, 341
- Chips-in-cards, 390
- CHPA. *See* Certified Healthcare Protection Administrator (CHPA)

- CIA. *See* Central Intelligence Agency (CIA)
- CIPS. *See* Certified Institutional Protection Specialist (CIPS)
- CISSP. *See* Certified Information Systems Security Professional® (CISSP)
- Civil investigations, 294
- Civil record searches, 90
- Civil Rights Act of 1964, 83
- Civil Service procedures, 231
- Civil wrong actions, 389
- Clarke, Ronald V., 17
- Clark–Hollinger study, 31
- Clark, John P., 31, 279
- Classical management theorists, 11–13
- Classroom instruction, 120
- Classroom-style training, 126
 - disadvantage of, 127
 - with learner participation, 126–127
- Clear purpose test, 99–100
- Client review appraisals, 187
- Closed circuit/Internet Protocol television (CC/IPTV) system, 45
 - equipment, 58
- Closed-circuit television (CCTV), 322, 327
 - cameras, 341
 - installation, 304
 - monitors of, 342–343
 - recording devices and media, 343–344
 - technical features, 344–345
 - video surveillance trends, 344
- Coaxial cable, 343
- Code of Ethics, 32
- Code of Hammurabi, 252
- Codes, 58
- Code sheets, 190
- Coelho, S.A., 98
- Cold War protectionism, 41
 - implications of, 41
- Cole, Richard B., 245
- Colleague Confidential Evaluation form, 193, 196
- Collusion, 281, 287
- Commercial telephone service, 352
- Commission on Accreditation for Law Enforcement Agencies (CALEA), 116
- Communications, 40
- Community Oriented Policing Services (COPS), 51, 116
- Compensation, 396
- Complex security department structure, 29–30
- Computer-aided instruction
 - disadvantages of, 128
- Computer-aided interactive instruction, 128–130
- Computer-based employment screening system, 104
- Computer crime, 373
- Computer security equipment, 58
- Concentric circles of protection, 332
- Confrontations, reducing risk in, 135
- Conger, Jay A., 370
- Consent, informed, 108
- Consolidated balance sheets, 253–259
- Constant critical analysis, 10
- Consultants, 278
 - retaining services, 320
 - and services, 57–58
- Containers. *See* Locks, keys, and containers
- Contamination, 399–400
- Contemporary management, holy grail of, 7
- Contemporary organizations, 10
- Contemporary security programs, 44
 - accreditation requirements, 46
 - bureaucratic requirements, 46
 - cost savings, 44
 - crime, 45
 - fear, 45
 - income generation, 45
 - insurance against liabilities/negligence, 46
 - legal mandates, 46
 - litigation, 46
 - risk mitigation, 44
- Contingencies, 268
- Contraband detection
 - drug detection, 355
 - explosive, 355
 - heat detectors, 357
 - metal detectors, 356
 - X-ray technology, 354
- Contract award, 314

- Contractee appraisals, 187–188
- Contracting, for alarm monitoring services, 320
- Contract security officers
 - in the leader's organization, 369
- Contract security services, 293, 302
 - employee leasing, concept of, 303
 - factors affects
 - amendments to RFP, 307
 - client contact person, 307
 - discussion with proposers, 308
 - fairness/ethics, 308
 - late proposals/withdrawals/
 - modifications, 307
 - letter of intent, 307
 - modification/withdrawal of proposals, 307
 - payment policy, 307
 - postopening withdrawals, 307
 - procurement policy rules, 308
 - proposer's conference, 307
 - proposers' right of appeal, 307
 - statement of purpose, 306
 - submission, 307
 - submission requirements, 307
 - large, complex security programs, 306
 - process of selecting, 305
 - small, simple programs, 305
- Contract security trends, 299
- Control center, 342
- Control theory, 371
- COO. *See* Chief operating officer (COO)
- Cooke, Donna K., 101
- Cooperative process, 204
- Cooperative system, 13
- Cooper, Dan B., 48
- COPS. *See* Community Oriented Policing Services (COPS)
- Core competencies, 37–66
 - contemporary security services evolution, 42–43
 - history of growing field, 40–42
 - industry concerns, 64–66
 - finance and insurance, 65
 - manufacturing, 64–65
 - retail trade, 65
 - utilities, 65–66
 - modern protective industry growth, 55–60
 - security services, 56–59
 - and products as global business, 59–60
 - security executives, how priorities ranked by, 60–64
 - of security operations, 37–40
 - initiating and managing security programs, 37–40
 - security operations, driven by, 44–55
 - 9/11 and consequences, 49–52
 - laws influencing growth, 47–48
 - other legal measures affecting security, 53
 - Patient Protection and Affordable Care Act (PPACA), 52–53
 - role of unions in, 53–55
 - Sarbanes–Oxley Act (SOX), 52
- Corporate organizational chart, security functions of, 23
- Corporate pay policy, 72
- Corporate security directors, 29, 43
- Corporations
 - annual reports for, 260
 - board of directors, 212
 - publicly held, 21
- Corrective discipline, 224
- Cost of sales, 257
- Cost savings, 262
- Council on Business Practices, 387
- Courage, 367
- Covert tests, 100
- CPAs. *See* Certified public accountants (CPAs)
- CPP. *See* Certified Protection Professional™ (CPP) designation
- CPR/AED. *See* Cardiopulmonary resuscitation/automated external defibrillator (CPR/AED)
- CPTED. *See* Crime prevention through environmental design (CPTED)
- Creative incompetence, 215
- Credit/debit card, 374
- Credit header, 89
- Credit reports, use of, 89
- Crime
 - root causes of, 326
 - in the suites, 371

Crime Control, Inc., 260–261
 Crime prevention through environmental
 design (CPTED), 326, 327, 381
 Criminal conviction, 92
 Criminal history, 90
 Criminal incidents, number of, 38
 Criminal investigations, 294
 Criminal justice database, 90
 Criminal justice programs, 325
 Criminal records, 91
 Crisis management, 383, 384
 Crisis Management Centers, 74
 Crisis Management Controller, 74
 job description for, 74
 Critical incident methods, 189
 Critical infrastructure, 379
 CRTs. *See* Cathode ray tubes (CRTs)
 Cryptography, 130
 CSO. *See* Chief security officer (CSO)
 “C-suite”, 24
 CTIIC. *See* Cyber Threat Intelligence
 Integration Center (CTIIC)
 Current assets, 253–255
 Current liabilities, 256
 Customer review appraisals. *See* Client review
 appraisals
 Customer’s check, 372
 Cyber-communications security, 65, 372–375
 Cybercrime, 298, 374
 cOmplic@t3d passwords, creation, 374
 keep tabs on accounts, 374
 stay alert online, 374
 think and act defensively, 374
 Cybersecurity technology, 42
 Cyber Threat Intelligence Integration Center
 (CTIIC), 373

D

Daily testing, 321
 Dalton, Dennis R., 286, 289
 Data collection, 94
 Data Encryption Standard (DES), 373
 Davidson, Charles “Sandy” H., 18, 19
 DDoS. *See* Distributed denial-of-service attack
 (DDoS)
 Debits and credits bookkeeping, 253

Decisiveness, 367
 Defensible space theory, 326
 Deferred charges, 255
 Deferring costs, 265
 Deister Electronics, 338
 Delegating, 168
 Deming, W. Edwards, 365
De minimis payment, 322
 Demonstrations, 131
 Department of Defense, 49, 95
 Department of Energy, 335
 Department of Homeland Security (DHS),
 49, 87
 net effect of, 49
 Department of Justice (DOJ), 51
 Dependability, 367
 Depreciation, 256, 274
 dabbling with, 265
 Depth interview, 105
 Deputizing, 9
 DES. *See* Data Encryption Standard (DES)
 Designing systems
 importance of, 14
 Detectives, 293
 Developmental expenses, 270
 DF. *See* Discount factor (DF)
 DHS. *See* Department of Homeland Security
 (DHS)
 Didactic techniques, 133
 Digital monitors, 342
 Digital video recorders (DVRs), 343
 Diligence, 262
 Directors, 5
 Directory-type information, 90
 Disability, definition of, 85
 Discharge
 categories of, 240
 economic downturn; retrenchment, 240
 poor work and misconduct, 241
 defined, 240
 and disgruntled employee, 242–246
 exit interview, 241–242
 insurance against wrongful termination,
 238–239
 legal cases of proper and improper,
 236–238

- legal issues for wrongful, 229–235
 - at-will employment, 230–233
 - overview, 229
- procedures at time of, 239–241
- special defenses against, 234–235
- T.I.M.E. (Threats, Intimidation, Manipulation, and Escalation syndrome), 247–248
- workplace bullying and disruptive behavior prevention, 246
- Discipline, 219–248
 - employees fail to achieve desired standards, 219–221
 - explanations for poor performance, 220–221
 - human relations-oriented managers, 223–224
 - minor worker misconduct, 228
 - progressive, 224–229
 - progressive to save weak workers, 224–229
 - psychological basis of non-compliance, 221–222
 - reason for, 229
 - stepwise procedure, 225
 - substandard worker performance, 227
 - supervisors' failure to provide, 222–223
 - US postal service disciplinary infractions, 230
- Discount factor (DF), 274
- Disgruntled employee, 242–246
- Disguised-purpose test. *See* Covert tests
- Dismissal, 239–241
- Distance learning, 137
- Distributed denial-of-service attack (DDoS), 375
- Distribution theft, 396
- Dividends, 28, 251, 256
- Documentation, and performance appraisals, 197–198
- Dogs, as guard, 334
- DOJ. *See* Department of Justice (DOJ)
- Domestic franchises, 399
- Double-entry bookkeeping, 252
- Drones, for security use, 352
- Drucker, Peter F., 6, 204
- Drug-Free Workplace Act of 1988, 107
- Drug-screening laboratories, 108
- Drug test policies, 107
- Durkheim, Emile, 371
- Duties of employees, 164–165
- Duty of care, 395
- DVRs. *See* Digital video recorders (DVRs)
- E**
- EAP. *See* Emergency Action Plan (EAP)
 - director; *See also* Employee assistance programs (EAP)
- Earnings, from continuing operations, 258
- Earnings (loss) per share (EPS), 259
- EAS. *See* Electronic article surveillance (EAS) systems
- E-commerce, 375
- Economic crime, indirect costs, 382
- E-DRM. *See* Enterprise digital rights management (E-DRM)
- Educational records, 92
- Edwards, W., 365
- EEOC. *See* Equal Employment Opportunity Commission (EEOC)
- Effectiveness of training, 139–141
- Efficiency, 140
- Egyptian pin lock, 338
- 80/20 rule. *See* Pareto principle
- Electronic and mechanical security products and systems, 56
- Electronic article surveillance (EAS) systems, 58, 273
- Electronic assets, 381
- Electronic collection, of information, 354
- Electronic data, 374
- Electronic locking systems, 336
- Electronic monitoring, door, 339
- Electronic numerical integrator and computer (ENIAC), 372
- Electronic security equipment and systems, 58
 - access control equipment, 58
 - biological, nuclear, and chemical detection, 58
 - CC/IPTV equipment, 58
 - computer security equipment, 58
 - electronic article surveillance (EAS) systems, 58
 - fire detection equipment, 58

- Electronic security equipment and systems (*cont.*)
 - intrusion detection equipment, 58
 - metal detection equipment, 58
 - secure telephone equipment, 58
 - vehicle security systems, 58
 - X-ray inspection equipment, 58
 - Embezzlement, 281
 - Emde, Eduard J., 19
 - Emergency Action Plan (EAP) director, 136
 - Emergency lighting, 341
 - Emergency response, fire and smoke, 292
 - Emergency, training for, 135–136
 - EMIT. *See* Enzyme multiplied immunoassay technique (EMIT)
 - Employee assistance programs (EAP), 247
 - for aiding workers, 247
 - Employee Polygraph Protection Act (EPPA) of 1988, 84, 95, 96
 - meeting conditions of, 96
 - Employee Retirement Income Security Act (ERISA) of 1974, 84
 - Employees
 - leasing, 303
 - progress report form, 202
 - selection/screening, 380–381
 - theft, 381–383
 - Employers
 - ethical obligations, 387
 - Web site, 82
 - Employment application, 83
 - Employment Nondiscrimination Act (ENDA), 85
 - Employment process, 109
 - Employment screening services, 187
 - Employment verification and continuity, 88–93
 - Encryption, 354
 - ENDA. *See* Employment Nondiscrimination Act (ENDA)
 - Endurance, 367
 - ENIAC. *See* Electronic numerical integrator and computer (ENIAC)
 - Enterprise digital rights management (E-DRM), 354
 - Enthusiasm, 367
 - Entrapment, 299
 - Entry-level operational personnel, 126
 - Enzyme multiplied immunoassay technique (EMIT), 108
 - E&O. *See* Errors and omissions (E&O)
 - EPPA. *See* Employee Polygraph Protection Act (EPPA) of 1988
 - EPS. *See* Earnings (loss) per share (EPS)
 - Equal Employment and Opportunity Act of 1972, 390
 - Equal Employment Opportunity Commission (EEOC), 64, 85, 86, 146, 380
 - concerns, 390–392
 - ERISA. *See* Employee Retirement Income Security Act (ERISA) of 1974
 - Errors and omissions (E&O), 304
 - Estimated revenues, 266
 - Ethical Standards Committee, 32
 - Ethics and security operations, 30–33
 - Ethnicity, 376
 - Evaluation process, 82, 193
 - Evaluators, 141, 197
 - E-verify, 87
 - Executive Orders, 84
 - Executives
 - development and education for, 137–139
 - loss prevention, certifications for, 137–139
 - protection, 384–385
 - purpose of, 6
 - Exit interview, 241–242
 - Expenditure, capital, 267
 - Expense budget, 267
 - Exploitive authoritative, 15
 - External auditors, 281
 - External theft, 61, 381
 - Extortion, 397–398
 - Extraordinary item, 259
- F**
- FAA. *See* Federal Aviation Administration (FAA)
 - Fabricatore, J.M., 99
 - Facebook, 380
 - Facility design, 333

- Fact-finding process, 8
- Fair Credit Reporting Act (FCRA), 84, 89, 381
- Fair Labor Standards Act (FLSA) of 1938, 83
- False-negative errors, 95, 349
- False-positive errors, 95, 349
- Family Educational Rights and Privacy Act (FERPA), 93
- Fatalities, frequency, 376
- Fatal occupational injuries, by industry sector, 161
- Fatal work injuries, 376
- Fay, John J., 293, 331
- Fayol, Henri, 11, 12, 219
- FCRA. *See* Fair Credit Reporting Act (FCRA)
- FDNY. *See* Fire Department of the City of New York (FDNY)
- Federal Aviation Administration (FAA), 46
- Federal Bureau of Investigation (FBI), 41, 92, 157
 - Bank Crime Statistics Reports, 160
- Federal contractor
 - screens in haste and lapses result, 78
- Federal employment guidelines test, 382
- Federal Housing Finance Agency (FHFA), 235
- Federal laws, 83
- Federal Omnibus Crime Control Act of 1970, 400
- Federal Trade Commission (FTC), 374
- Female workers, risks, 376
- FERPA. *See* Family Educational Rights and Privacy Act (FERPA)
- FHFA. *See* Federal Housing Finance Agency (FHFA)
- Fibonacci, 252
- Fiedler, Fred E., 364
- Field review, 210–211
 - visits for, 211–212
- File review, 103
- Final employment interview, 103–107
- Final offer of employment, 109
- Finance charge, 258
- Finance department, 251
- Financial controls, 251–266
 - change in auditors, 262
 - consolidated balance sheets, 253–261
 - notes to, and statement of operations, 259–261
 - evolution of, 252–253
 - independent auditor statement, 261–262
 - manipulation of financial statements, 263–265
 - notes to statement of operations, 259–261
 - not-for-profit organizations, 265–266
 - overview, 251–252
 - Securities and Exchange Commission, 263
- Financial director, 271
- Financial incentives, 14
- Financial Institution Reform, Recovery, and Enforcement Act (FIRREA), 235
- Financial policies, 251
- Financial statements, 260
 - manipulation of, 263–265
- Finckenauer, James O., 400
- Finding applicable test instruments, 102
- Finding investigators, 293
- Finnegan, Patrick, 325
- Fire alarm systems
 - in homeless shelters, coordinator of, 136
 - inspection and testing, certifications in, 139
 - supervision of, 135
- Firearms, criticality of, 132–133
 - armored car personnel, 125
- Fire Department of the City of New York (FDNY), 135
- Fire detection equipment, 58
- Fire drills, 394
- Fire guard, 135
- Fire prevention, training for, 135–136
- Fire safety director (FSD), 136
- Fire safety manager
 - construction site, 136
- Firewall
 - architecture, 129
 - components, 129
- FIRREA. *See* Financial Institution Reform, Recovery, and Enforcement Act (FIRREA)
- Fitness for work, 102–103
- Fitzgerald, Thomas H., 177
- Fixed assets, 255

Fixed focal length (FFL), 344
 Flanagan's Tests of General Ability (ToGA), 176
 FLSA. *See* Fair Labor Standards Act (FLSA)
 Forced-choice method, 198
 Foreign-based operations, 398
 Foremanship, 14
 Forensic investigators, 281
 Forgery, 392
 Formal appraisal processes, 185
 Formal employee performance evaluation, 189
 Formal written approbation, 156
 For-profit corporations, 21–28
 organizational chart of, 26
 For-profit organizations, 270
 Four-fifths rule, 107
 Fraternalization, 287
 Frauds, 281, 392–394
 forensic safeguards to internal fraud,
 279–283
 fraud, embezzlement, and security, 281
 generally accepted accounting principles
 (GAAP), 279–281
 overview, 279
 separating tasks, 281–283
 and security, 281
 and white-collar crime, 62
 workers' compensation, 396
 FSD. *See* Fire safety director (FSD)
 FTC. *See* Federal Trade Commission (FTC)
 Functional foremanship, 14
 Future of security operations, 363

G

GAAP. *See* Generally accepted accounting
 principles (GAAP)
 Gas chromatography/mass spectrometry
 (GC/MS), 108
 GC/MS. *See* Gas chromatography/mass
 spectrometry (GC/MS)
 GDP. *See* Gross domestic product (GDP)
 Gebhardt, Joan E., 366, 369
 Geese, 333
 General Audit Management Conference of the
 Institute of Internal Auditors, 393
 General employee theft, 61

General liability insurance, 319
 Generally accepted accounting principles
 (GAAP), 263, 279–281
 General management organizations, 137
 Genetic Information Nondiscrimination Act
 (GINA) of 2008, 85
 Gilbreth, Frank, 14
 Gilbreth, Lillian, 14
 GINA. *See* Genetic Information
 Nondiscrimination Act (GINA)
 of 2008
 Global positioning satellite (GPS) system, 168
 Global security operations, managers of, 60
 Goldman Sacks, 74
 Google+, 380
 Government employment background
 investigators, 92
 Government security operations, 28
 GPS. *See* Global positioning satellite (GPS)
 system
 Graphic user interfaces (GUIs), 358
 Gray crime, 371
 Gross domestic product (GDP), 55
 Gross profit, 258
 Grove, Andrew S., 169, 211
 Guardianship, 336
 Guard licensing process, 90
 GUIs. *See* Graphic user interfaces (GUIs)

H

Hair testing, 108
 Hallcrest Report II, 37
 Halo effect, 197
 Harrison, Edward L., 222
 Hawthorne plant, 172
 Hazardous materials, 153
 Header information, 89
 Health and Working Conditions of the Bureau
 of Labor Statistics (BLS), 375
 Health Insurance Portability and
 Accountability Act (HIPAA), 247, 388
 Heat detectors, 357
 Herzberg, Frederick, 174
 Heskett, Sandra L., 245
 Hiding inventory, 265

- Hierarchical organization, 186
- Highjacking, 48
- High-performance executives
 - personal characteristics, 40
- High-performance managers, 81
- High-performance security operations, 38
- High-performing security programs, 116, 133
- High-security lock, 338
- HIPPA. *See* Health Insurance Portability and Accountability Act (HIPAA)
- Hire off-duty police officers, for part-time duty, 293
- Hirschi, Travis, 371
- Hollinger, Richard C., 31, 279
- Homeland Security Act of 2002, 49
- Homeland Security Presidential Directive/ HSPD-5, 49
- Homicides, 377
 - job-related, 377
- Hoover, John Edgar, 157
- House Committee on Government Operations, 95
- Hull, Raymond, 214
- Human needs, hierarchy of, 173–174
- Human relations–oriented managers, 223–224
- Human resources (HR)
 - managers, 242, 380
 - vetting program, 75
- Humphrey, Albert, 16
- “Hygiene” factors, 174
- Hypothetical test, 107
- I**
- IACP. *See* International Association of Chiefs of Police (IACP)
- Identification (ID) cards and tokens, 347–348
- Identification (ID) numbers and passwords, 347
- Identity theft, 389–390
- IIRR. *See* Initial-investment rate of return (IIRR) method
- iJet International, 398
- Illness incidents, 379
- Immigration Reform and Control Act (IRCA) of 1986, 84
- Impairment charges, 259
- Inadequate security charges, 389
- Incident reports, 310
- Income statement, 257
- Income taxes
 - earnings before, 258
 - provision for, 258
- Independent auditors, 261–262
- Industrial Age, 10
- Industrialization, 11
- Industry concerns, 64–66
 - finance and insurance, 65
 - manufacturing, 64–65
 - retail trade, 65
 - utilities, 65–66
- Information Age, 117
- Information security systems, 353–354
 - other considerations, 354
 - physical security, 353
 - systems security, 353–354
 - UPS for, 353
- Information technology (IT), 60
 - assets, 373
 - protection, 401
 - security, 374, 375
- Informed consent, 108
- Infractions, categories of, 229
- Infrastructure Resilience Analysis
 - Methodology (IRAM), 380
- Inherent intellectual capital, 394
- Initial-investment rate of return (IIRR)
 - method, 276
- Initiative, 367
- Innovator, 369
- in organizational hierarchy, 29
- In-person prescreening, 82
- Inspectors, and tests, 312
- Institute of Finance and Management, 56
- Instructors, 291
- Insurance, 396
 - for terminated employees, 241
 - against wrongful termination, 238–239
- Intangibles, 256
- Integrity, 366
- Intellectual property (IP), 381

- Interest expense, 258
 - Internal financial officer, 281
 - Internal rate of return (IRR), 274, 275
 - International Association for Healthcare Security and Safety, 33
 - International Association of Chiefs of Police (IACP), 51, 116
 - International Security Conference, 137
 - International Security Management Association (ISMA), 16, 116
 - Internet
 - access control, 373
 - freedom of communications, 372
 - proposals, purchasing security services through, 322
 - Internet Protocol (IP), 328
 - Internet service provider (ISP), 372
 - Interview
 - categories, 105
 - depth, 105
 - panel, 105
 - stress, 105
 - structured, 105
 - unstructured, 105
 - depth, 105
 - for performance appraisals, 199–202
 - process, 105, 201
 - questions, 104
 - Intrusion
 - detection and response, 130
 - detection equipment, 58, 345
 - Investigations
 - civil, 294
 - and contractual, 294
 - criminal, 294
 - diversionary fraud, 295
 - to find facts, 293
 - fraud and abuse, 297
 - investigator, nonexpectations of, 299
 - IT crimes, importance, 298
 - private investigations, to enhance law enforcement, 296
 - Investigative services, 278
 - Investigators, 150
 - to find facts, 293
 - finding, 293
 - nonexpectations of, 299
 - private, retaining services, 320
 - Ionization detectors, 357
 - IP. *See* Intellectual property (IP)
 - IP/CCTV, on mobile device, 351
 - IRAM. *See* Infrastructure Resilience Analysis Methodology (IRAM)
 - IRCA. *See* Immigration Reform and Control Act (IRCA) of 1986
 - IRR. *See* Internal rate of return (IRR)
 - ISMA. *See* International Security Management Association (ISMA)
 - ISP. *See* Internet service provider (ISP)
 - I-Way security, 375
- J**
- Jacobson, Lenore, 176
 - Jago, Arthur, 363
 - JCAHO. *See* Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)
 - JIT. *See* Just in-time (JIT) planning
 - Job descriptions, 72–74, 213
 - for crisis management center controller, 74
 - Job dissatisfiers, 175
 - Job-related skills testing, 102
 - Job satisfiers, 175
 - job security, 157
 - Johnson & Johnson, 399
 - Joint Commission on the Accreditation of Healthcare Organizations (JCAHO), 46
 - Journal bookkeeping, 253
 - Judgment, 368
 - Justice, 367
 - Just in-time (JIT) planning, 146
- K**
- Kakalik, James S., 42
 - Katzenbach, Jon, 368
 - Keeler, Leonarde, 94
 - Kelleher, Michael D., 244
 - Kenney, Dennis J., 400
 - Kenney, Joseph A., 248

Key-operated locks, 336–338
 Keypad, 347
 Keys. *See* Locks, keys, and containers
 Kidnap and ransom (K&R) insurance, 397
 Kidnapping, 397–398
 Knowledge, 367
 based content, 137
 related activities, 5
 workers, 6
 Kotter, John, 366
 Kovacich, Gerald L., 375
 Ktalav Promotion and Investment Ltd.
 (KPI), 45

L

Labor resources, 71
 Langdell, Christopher Columbus, 126
 LANS. *See* Local area networks (LANs)
 Larceny, 38
 Large, complex security programs, 306
 comprehensive request for proposal (RFP),
 308–318
 continuous supervision, 319
 final costs determination, 318
 other considerations, 318–319
 Larson, John A., 94
 Later bloomers, 176
 Law enforcement agencies, 49, 96
 Law Enforcement Assistance Administration
 (LEAA), 42, 43
 Layers of management, 29
 LCD. *See* Liquid crystal display (LCD)
 LEAA. *See* Law Enforcement Assistance
 Administration (LEAA)
 Leadership, 40
 critical issues for security operations
 managers, 371
 business continuity planning/
 organizational resilience, 379–380
 business espionage, 394–395
 cargo/supply chain theft, 396–397
 crisis management and response, 383–384
 cyber/communications security, 372–375
 employee selection/screening, 380–381
 employee theft, 381–383

equal employment opportunity (EEOC)
 concerns, 390–392
 executive protection, 384–385
 extortion, 397–398
 fraud, 392–394
 future direction, 400–401
 identity theft, 389–390
 insurance, 396
 kidnapping, 397–398
 litigation, inadequate security, 388–389
 litigation, negligent hiring, 395
 organized crime, 400
 political unrest/regional instability, 398
 product diversion/transshipment, 399
 product tampering/contamination,
 399–400
 property crime/external theft/vandalism,
 381
 sexual harassment, 390–392
 terrorism, 385–387
 theft of trade secrets, 394–395
 unethical business conduct, 387–388
 white-collar crime, 392–394
 workers' compensation fraud, 396
 workplace violence prevention/response,
 375–379
 distinction of, for security operations,
 370–371
 learning about, 363
 importance of discretion, 369
 and power, 366
 problems with, 369–370
 traits, 366
 bearing, 367
 courage, 367
 decisiveness, 367
 dependability, 367
 endurance, 367
 enthusiasm, 367
 initiative, 367
 integrity, 366
 judgment, 368
 justice, 367
 knowledge, 367
 loyalty, 368

Leadership (*cont.*)
 tact, 367
 unselfishness, 367
 for optimal security operations, 363–401
 quality improvement, 365
 Learning, application of, 140
 Ledger bookkeeping, 253
 Lee, Seungmug (Zech), 163
 Leeson, Nick, 393
 Legal issues, for discharge, 229–238
 Legality, in pre-employment tests, 101
 Legal measures affecting security, 53
 Leniency tendency, 197
 Letter of intent, 314
 Levinson, Harry, 213
 Liabilities, 256
 insurance, 238, 319
 coverage, 285, 303
 professional, 319
 specialized, 287
 for negligence, 322
 Liberty Mutual Insurance Company, 115
 Licensed security guard companies and
 investigators, 42
 Life Safety Code (NFPA #101), 357
 Likert, Rensis, 15
 Likert Scale, 15
 Likert's system 4 categories, 15
 Line-item budgets, 269
 capital budget, 268
 emergencies and contingencies, 268
 expenses, 268
 personnel costs, 268
 LinkedIn, 380
 Linking key control, 338
 Linking management
 to authority and responsibility, 206
 Liquidated damages, 316, 318
 Liquidation, 385
 Liquid crystal display (LCD), 343
 Litigation
 inadequate security, 388–389
 negligent hiring, 395
 Local area networks (LANs), 242, 353
 Local law enforcements, 291

Locks, keys, and containers, 336
 key-operated locks, 336–338
 lock hardware and mountings, 338–339
 overview, 336
 vaults and safes, 339–340
 Lombroso, Cesare, 94
 Longenecker, Clinton O., 167
 Long-term liabilities, 256
 Loss prevention departments, 29
 Loss prevention staff
 assess security technology, 40
 contract services management, 40
 expectations, 40
 private investigations, 40
 tasks for, 40
 Lost cards, 348
 Loyalty, 368

M

Magnetic field, 356
 Management by objectives (MBO), 204–209
 advantages, 209
 criticism of, 209
 examples in security applications, 207–209
 principles, 204
 Management layers, 29
 Management security operations, 1–34
 complex security department structure,
 29–30
 contemporary management, holy grail of, 7
 corporate organizational chart, security
 functions of, 23
 ethics and security operations, 30–33
 executives, purpose of, 6
 government security operations, 28
 key assets and risks, 22
 management layers, 29
 management strategy, 6–10
 modern organization characteristics, 10–13
 classical management theorists, 11–13
 scientific management pioneers, 13–16
 security management precedent setters,
 16–20
 in organizational hierarchy, 29
 organizations and managers, 4–5

- chief security officer (CSO), 29
 - convictions of effective managers, 24–25
 - manager/director, 5
 - organization defined, 4–5
 - security manager, 5
- organization structure, 21–28
 - for-profit corporations, 21–28
 - not-for-profit (NFP) corporations, 28
 - other types of organization, 31
 - staff relates to operating units, 27
 - work relationships of, 30
- overview, 3–4
- situational crime prevention, 18, 325–327
- Management strategy, 6–10
 - critical incident review, 209–210
 - “field review”, 210–212
 - management by objectives (MBO), 204–206
 - examples of, 207–209
 - problem-solving ability, 210
- Managers, 116–117, 369
 - assertiveness, 364
 - decisiveness, 364
 - development and education for, 137–139
 - directors, 5
 - effective, convictions of, 24–25
 - forcefulness, 364
 - integrity and diplomacy, 365
 - motivating, 364
 - results-and bottom-line-oriented, 364
 - of security programs, 132
 - task-oriented, 365
 - tasks performed by, 7–10
 - time management for, 166–171
 - willfulness, 364
- Managing general agent (MGA), 303
- Maslow, Abraham H., 173, 174
- Master keys, 304, 337
- Master List Tasks, 192
- Master Security Officer (MSO), 134
- Maxwell, David A., 115, 395
- Mayo, Elton T., 172
- MBO. *See* Management by objectives (MBO)
- McGregor, Douglas, 170–171, 204
- Mechanical security hardware, 58–59
- Medical test, 109
- Memory of 9/11, 385
- Memos, 168
- Mercer LLC National Survey of Employer-Sponsored Health Plans, 247
- Merton, Robert K., 175, 176
- Metal detectors, 58, 356
- MGA. *See* Managing general agent (MGA)
- Michelman, Bonnie S., 20
- Military history, employee's, 89–90
- Minimum Security Devices and Procedures, 47
- Minimum-security lighting standards, 340
- Minnesota Multiphasic Personality Inventory (MMPI-2), 97, 98, 166
- Mintzberg, Henry, 370
- Mixed standard scale (MSS), 189
 - average performance, 189
 - high performance, 189
 - low performance, 189
 - for patrol performance, 190
- MMIP-2. *See* Minnesota Multiphasic Personality Inventory (MMPI-2)
- Modern organization characteristics, 10–13
 - classical management theorists, 11–13
 - scientific management pioneers, 13–16
 - security management precedent setters, 16–20
- Modern protective industry growth, 55–60
 - security services, 56–59
 - and products as global business, 59–60
- Money as motivator, 175
- Money society, 175
- Monitors in CCTV system, 342–343
- Moonlighting, 120
- Moral conduct, 30
- Motivation, 169–170
 - complexity of, 171–177
 - Hawthorne investigations, 172–173
 - hierarchy of needs, 173–174
 - manipulated self-motivation, 175–177
 - money as motivator, 175
 - motivational-hygiene factors, 174–175
 - research, limitations of, 177–179
 - Theory X and Theory Y, 170–171
 - Theory Z, 171

Motivational-hygiene factors, 174–175
 Motor vehicle reports (MVRs), 90
 MSO. *See* Master Security Officer (MSO)
 MSS. *See* Mixed standard scale (MSS)
 MVRs. *See* Motor vehicle reports (MVRs)

N

Narrative form, 198
 NASCO. *See* National Association of Security Companies (NASCO)
 National Advisory Commission on Criminal Justice Standards and Goals, 121
 National Advisory Committee, 43
 National Armored Car Association, 125
 National Association of Security Companies (NASCO), 116, 305, 321
 National Commission on Terrorist Attacks, 50
 National Council of Investigation and Security Services (NCISS), 16, 33, 305, 321
 National Crime Information Center (NCIC) database, 92
 National Crime Victimization Survey, 162
 National Fire Protection Association, 340
 National Incident Management System (NIMS), 49
 National Infrastructure Protection Plan (NIPP), 49
 National Institute for Occupational Safety and Health (NIOSH), 375
 National Institute of Standards and Technology (NIST), 374
 National Labor Relations Act, 53, 231, 287
 National Labor Relations Board (NLRB), 53, 238
 National Policy Summit in 2004, 51
 National Response Plan (NRP), 49
 National Rifle Association (NRA), 133
 National Security Act of 1947, 49
 National Security Agency, 78, 394
 Natural defense characteristics, 333
 NCIC. *See* National Crime Information Center (NCIC) database
 NCISS. *See* National Council of Investigation and Security Services (NCISS)
 Negligent hiring litigation, 75–77

verifying indications of integrity, 76
 background, 76–77
 deficient preemployment process, 77
 lesson, 77
 Nemeth, Charles P., 397
 Net earnings, 259
 Net expenses, 258
 Net present value (NPV), 274
 Net revenues, 257
 Net security issues, 375
 Network interfaces, 39
 Newark International Airport, 49
 New Deal legislation, 53
 Newman, Oscar, 326
 New York City Police Department (NYPD), 51
 New York City's Health and Human Resources Administration, 115
 New York State Organized Crime Task Force, 54
 NFP. *See* Not-for-profit (NFP) organizations
 NIMS. *See* National Incident Management System (NIMS)
 9/11, and consequences, 49–52
 NIOSH. *See* National Institute for Occupational Safety and Health (NIOSH)
 NIPP. *See* National Infrastructure Protection Plan (NIPP)
 NIST. *See* National Institute of Standards and Technology (NIST)
 NLRB. *See* National Labor Relations Board (NLRB)
 No arrest policy, 312
 Noncriminal emergencies, number of, 39
 Nonmanagerial employee performance evaluation form, 191
 Nonsecurity personnel, training for, 136
 Nonviolent financial crimes, 371
 Not-for-profit (NFP) organizations, 4, 28, 251, 265–266, 296
 NPV. *See* Net present value (NPV)
 NRA. *See* National Rifle Association (NRA)
 NRP. *See* National Response Plan (NRP)
 Nuclear Regulatory Commission, 15
 NYPD. *See* New York City Police Department (NYPD)

O

Oatman, Robert L., 385
 ObamaCare. *See* Patient Protection and Affordable Care Act (PPACA)
 Obligations, of subscriber, 322
 Occupational Safety and Health Act (OSHA) of 1970, 47, 84
 Occupations
 with high fatal work injury rates, 161
 of victims from nonfatal workplace violence, 162
 Office of Compensation and Working Conditions, 302
 Office of Field Operations, 302
 Office of Safety, 375
 Office of Technological Assessment (OTA), 95
 report, 101
 Office of Technology and Survey
 Processing, 302
 Omnibus Drug Initiative Act of 1988, 107
 One-time gains, 265
 Ongoing evaluation, 140
 Ongoing “in-service” training, 133–134
 On-the-job (OTJ) training, 119, 127, 131, 149
 instructor, 127
 Operating security programs, 16
 Operational-level security staffers, 145
 Ordeal of the Red-Hot Stones, 93
 Organizational design, 206
 Organizations
 appraisals schedule, 186
 chart, 153
 defined, 4
 hierarchical structure of, 29
 and managers, 4–5
 chief security officer (CSO), 29
 convictions of effective managers, 24–25
 manager/director, 5
 organization defined, 4–5
 security manager, 5
 periodic statements, 253
 role migration, 4
 structure, 21–28
 for-profit corporations, 21–28
 not-for-profit (NFP) corporations, 28

 other types of organization, 31
 staff relates to operating units, 27
 work relationships of, 30
 Web sites, 369
 Organized crime, 400
 Orientation, 118–119
 overview, 118–119
 training content, 118–119
 OSHA. *See* Occupational Safety and Health Act (OSHA) of 1970
 OTA. *See* Office of Technological Assessment (OTA)
 OTJ. *See* On-the-job (OTJ) training
 Ouchi, William G., 171
 Outcontracting process, 29
 Outplacement program, 226, 245
 Outside directors, 24
 Outsourcing, 34
 Overhead costs, 270
 Overtime pay policy, 313
 Overt integrity test, 99
 Owners’ equity, 256
 Ownership, of security system, 321

P

Pacioli, Luca, 252
 Palmer, Walter E., 273
 Paltry security, 45
 Pan Am World Airways, 44, 45
 Panel interview, 105
 Paper-and-pencil instruments, 99
 Pareto principle, 166–167
 Parking revenues, 278
 Pascal, Blaise, 372
 Passcode, 347
 Passive infrared (PIR) sensor, 346
 Paterson, Richard D., 19
 Patient Protection and Affordable Care Act (PPACA), 52–53
 Patriot Act of 2001, 49
 Pavlovian methods, 334
 Payback method, 275, 276
 Payback period, 274
 Payments, 255
 Pay scales, 72

PCI. *See* Professional Certified Investigator™ (PCI)

PDAs. *See* Personal digital assistants (PDAs)

Peace officers

- characteristics, 291
- contribute to security procedures, 291
- instructors, 291
- uses, 291

Peace Officer Standards of Training (POST), 115

Peer reviews, 193

- appraisals, 187

Pension option, 241

Percentage of completion, 265

Performance appraisals, 185–216

- for all levels and by all levels, 186–188
- aspects of, 185
- assessing performance among different employment levels, 203–204
- average tendency, 197
- difficulties of, 185–186
- documentation, 197–198
- evaluation needs, 188–189
- evaluation types preferred by workers, 188
- formal appraisal document, 189–193
- halo effect, 197
- interview, 199–202
- job performance rating, 193–196
- leniency tendency, 197
- levels of workplace, 188–189
- limitations of, 213
- management strategies, 203–212
 - critical incident review, 209–210
 - field review, 210–211
 - management by objectives (MBO), 204–209
 - problem-solving ability, 210
- methods of, 186–188
- overview, 185
- rating colleagues objectively in, 197
- for senior management, 212
- specific language in, 200–201
- strictness tendency, 197
- written appraisal techniques, other, 198

Performance evaluation, 198

Personal acquaintance, 377

Personal digital assistants (PDAs), 344

Personality psychological tests, 99

Personnel

- budgets, 268
- cash handling back-office, 150
- future requirements, 72
- hiring for security positions, 69
- labor resources, 71
- monitor internal resources, 71
- planning, 69–72
- procedures, 75
- process, 78
- resources identification, 71
- strategies, 72

Personnel-based services

- categories, 57
 - armored car services, 57
 - central station services, 57
 - consultant and services, 57–58
 - electronic security equipment and systems, 58
 - mechanical security hardware, 58–59
 - private investigation services, 57
 - security guard services, 57

Personnel-intensive programs

- combined proprietary, 289
- comprehensive request for proposal (RFP), 308–318
- contract staffs, 289
- final costs determination, 318
- internet proposals, purchasing security services through, 322

large, complex security programs

- continuous supervision, 319
- final costs determination, 318

proprietary/contract employee debate, 285

- administrative ease, 286
- collusion/fraternization, less likelihood, 287
- cost savings, 289
- criminal records screening, 286
- emergency/short-term staff available, 288
- employee
 - greater quality perception, 288

- employer
 - greater loyalty, 288
 - greater site knowledge, 288
 - less total cost, 285
 - more flexible controls, 288
 - personnel retention, 288
 - personnel scheduling flexibility, 287
 - recruiting/vetting transferred, 287
 - reliability of service, 288
 - specialized liability insurance, 287
 - specialized protective experience, 287
 - supervision transferred, 287
 - training transferred, 287
- security officer's job, design of, 319
- Peter, Lawrence J., 214
- Peter principle, 214–215
- Photoelectric detectors, 357
- Photoelectric smoke detectors, 357
- Physical- and technology-centered programs
 - alarm systems, 349–351
 - contraband detection
 - drug detection, 355
 - explosive, 355
 - heat detectors, 357
 - metal detectors, 356
 - X-ray technology, 354
- form to plan security alarm costs, 359
- needs for, 331
- risk *vs.* cost ratio, 327, 329
- security conditions and management
 - advanced security, 330
 - dealing with managers, 330
 - fail-safe security, 330
 - high-level security, 328
 - low-level security, 328
 - medium security, 328
 - minimum security, 328
 - protectionless places, 328
- security countermeasures, to reduce loss, 332
 - access control systems, 346–347
 - animals, 333–334
 - barriers, 334–335
 - biometric features, 348–349
 - communications, 352–353
 - contraband detection, 354–356
 - drones, 352
 - drug detection, 355
 - explosive, 355
 - facility design, 333
 - fire detection, 356–358
 - glazing, 335–336
 - heat detectors, 357
 - ID cards and tokens, 347–348
 - identification numbers and passwords, 347
 - information security systems, 353–354
 - internet protocol/closed-circuit television, 341–342
 - intrusion detection systems, 345–346
 - IP/CCTV displays, monitors of, 342–343
 - key-operated locks, 336–338
 - life safety, 356–358
 - lighting systems, 340–341
 - lock hardware, 338–339
 - locks, keys, and containers, 336
 - metal detectors, 356
 - mountings, 338–339
 - power backup, needs, 340–341
 - radio-frequency identification, 349
 - recording devices and media, 343–344
 - robotic systems, 351–352
 - strengths and relative cost, 332
 - technical features, 344–345
 - vaults/safes, 339–340
 - video surveillance trends, 344
 - warning signs, 336
 - X-ray technology, 354
- security operations planners, 331
- security system design, 358–360
- situational crime prevention, 18, 325–327
 - crime reduction, strategy of, 325
- Physical security, 331
 - countermeasures, 332
- Physical Security Professional™ (PSP)
 - certification, 138
- Pinkerton Agency, 76, 77, 302
- Pin tumbler lock security, 337
- Placement, 146–159
- Plaintiff's action, 75

- Planning
 - and development requirements, 117–118
 - manager, 9
- Police
 - departments, conflicts, 293
 - victimization, 377
- Policy direction, 213
- Political unrest/regional instability, 398
- Polycarbonate, 335
- Polygraph, 93–97
 - beating, Aldrich Ames case, 96
 - testing, scientific basis for, 97
- Polyvinyl butyral (PVB), 335
- Poor performance explanations, 220–221
- Poor preemployment screening, perils of, 70
- Porter, Michael, 16
- Positive socialization, 173
- POST. *See* Peace Officer Standards of Training (POST)
- Posttraumatic stress disorder (PTSD), 246
- PowerPoint, 130–131
- PPACA. *See* Patient Protection and Affordable Care Act (PPACA)
- Pre-employment
 - drug screening, 107–109
 - integrity screening methods, 100
 - reference sheet, 106
 - screening instruments, 99
 - screening process, 107
 - testing, 97
- Pre-emptory discharge, 229
- “Preferred” guarantee, 256
- Pregnancy Discrimination Act of 1978, 84
- Present value (PV), 274
- Pricing policies, 399
- Private guard, 299
- Private intelligence services, 398
- Private investigation services, 57
- Private investigators, retaining services, 320
- Private security, 5
 - 8-H preassignment training course, 120–121
 - 32-H preassignment training course, 122–123
 - personnel, 132
 - services, 116
 - services demand, 56
- Private Security Task Force (PSTF), 43
- Probationary period, 186, 193
- Problem
 - identification, 7
 - analyzing and planning, 8
 - criticizing results, 10
 - deputizing, 9
 - organizing, 8–9
 - supervising, 9–10
- Product
 - diversion/transshipment, 399
 - tampering/contamination, 399–400
- Professional Certified Investigator™ (PCI), 138
- Professional liability insurance, 319
- Professional security, origins of, 41
- Profits, 270–277
 - achievement of, 270
 - capital budgeting for, 275–277
 - initial-investment rate of return (IIRR) method, 276
 - other managerial options, 277
 - payback method, 276
 - time-adjusted rate of return (TARR) method, 276
 - fixed and variable costs, 271
 - making organizations, 204
 - return on equity (ROE), 272
 - return on investment (ROI), 272–275
 - smoothing of, 265
- Program operator, 369
- Progressive discipline, 224–229
- Promotion, 156, 159
 - difficulties of, 214–215
 - importance of, 215–216
 - process, 213
- Property crime/external theft/vandalism, 381
- Proposals submitting, guidelines, 314
- Proprietary security
 - directors, 55
 - strategy, 299
 - compensation, 302
 - insurance, 303
 - liability insurance, 304
 - personnel needs for posts, 301–302
 - salary, 302

scheduling requirements, 300–301
 security services business, 304
 trends, 299
 Protection, defined, 5
 Protectionless behavior, 328
 Protective program, 37
 Prudent operational management, 75
 PSP. *See* Physical Security Professional™ (PSP)
 certification
 PSTF. *See* Private Security Task Force (PSTF)
 Psychological or behavioral stability, 97–99
 Psychological personality test, 98, 99
 Psychometric testing methods, 97
 PTSD. *See* Posttraumatic stress disorder
 (PTSD)
 Public corporations, guide to financial
 performance of, 264
 Public employees, 234
 Public law enforcement, 121, 160
 “Pure guard” unions, 54
 PV. *See* Present value (PV)
 PVB. *See* Polyvinyl butyral (PVB)
 Pygmalion effect, 175, 177
 in management, 176

Q

Quality circle, 365
 Quick Response code, 348

R

Race, 376
 Radio-frequency identification (RFID), 349
 tags, 349
 Rae, Leslie, 139
 Rand Corporation, 42
 Rand Report, 42, 43
 Ranking, 198
 Recording devices and media, 343–344
 Record-keeping process, 92
 Recruiting, 79–82
 Recruitment sources, 81
 Redundancy, time of, 240
 References, 87–88
 Refresher training, 114, 115
 Registration, 263
 Rehabilitation Act of 1973, 84

Relevant/irrelevant technique, 94
 Reliability, in pre-employment tests, 101
 Report of the Private Security Task Force, 14,
 117
 Request for Educational Verification, 92
 Request for proposal (RFP), 9
 comprehensive elements, 308–318
 contract security services, amendments,
 307
 Reservation, 315
 Respondeat superior, 75
 Retail trade, 65
 Retained earnings, 256
 Retaining services
 private investigators and consultants, 320
 Retrospective analysis, 140
 Return on equity (ROE), 272
 Return on investment (ROI), 272–275
 Revenues
 budgets, 267
 reporting variably, 265
 RFID. *See* Radio-frequency identification
 (RFID) tags
 RFP. *See* Request for proposal (RFP)
 Right to audit, 313
 Risk mitigation, 398
 Risks of kidnapping, 397
 Risk Versus Cost Ratio, 327
 Robotic systems, 351–352
 ROE. *See* Return on equity (ROE)
 ROI. *See* Return on investment (ROI)
 Rosenthal, Robert, 176
 Rule of thumb, 80, 153

S

Safes, 339–340
 Sakai, Toshiyuki, 239
 Salary, 302
 Sample personal conduct policy, 232–233
 Sandia National Laboratories, 335
 Sarbanes–Oxley Act (SOX), 52, 212, 262, 388
 SARS. *See* Severe acute respiratory
 syndrome (SARS)
 Scheduling, 156
 Scholtes, Peter R., 364, 365
 Scientific management approach, 15

Scientific management pioneers, 13–16

 Likert's system 4 categories, 15

 SWOT matrix analysis, 16

SCIP. *See* Society of Competitive Intelligence Professionals (SCIP)

Screening test, 108

“Screen out” assessment strategy, 98

SEC. *See* Securities and Exchange Commission (SEC)

Secure telephone equipment, 58

Securitas/Pinkerton survey, 61, 372

Securitech Group, 339

Securities Act of 1933, 263

Securities and Exchange Commission (SEC),
 26, 52, 259, 263

Securities Exchange Act of 1934, 263

Security, 281

 assessment, 129

 countermeasures, to reduce loss, 332

 access control systems, 346–347

 animals, 333–334

 barriers, 334–335

 biometric features, 348–349

 communications, 352–353

 contraband detection, 354–356

 drones, 352

 drug detection, 355

 explosive, 355

 facility design, 333

 fire detection, 356–358

 glazing, 335–336

 heat detectors, 357

 ID cards and tokens, 347–348

 identification numbers and passwords, 347

 information security systems, 353–354

 internet protocol/closed-circuit
 television, 341–342

 intrusion detection systems, 345–346

 IP/CCTV displays, monitors of, 342–343

 key-operated locks, 336–338

 life safety, 356–358

 lighting systems, 340–341

 lock hardware, 338–339

 locks, keys, and containers, 336

 metal detectors, 356

 mountings, 338–339

 power backup, needs, 340–341

 radio-frequency identification, 349

 recording devices and media, 343–344

 robotic systems, 351–352

 strengths and relative cost, 332

 technical features, 344–345

 vaults/safes, 339–340

 video surveillance trends, 344

 warning signs, 336

 X-ray technology, 354

defined, 5

essential for, 40

leaders, 40

loss prevention programs, 4

management, 248

management precedent setters, 16–20

management programs, 38

minded employers, 241

products, 55

professionals, 394

as profit center, 278

training, 125, 139

victimization, 377

window film, 335

Security departments

 budgeting for, 266–270

 overview, 266–268

 process of budget creation, 268–270

 rules and regulations of, 165

Security directors, 8, 41, 64, 281

Security employees, 133

 content for, 119–125

Security executives, how priorities ranked
 by, 60–64

Security Guard Act of 1992, 133

Security guards

 homicides of, 160

 regulations, statutory requirements of, 114

 services, 57

Security implementation policy, 129

Security industry, 42, 55

Security Industry Association (SIA), 16, 116

Security managers, 3, 5, 54

Security officer

- job description for, example of, 73–74
 - job performance evaluation form, 194, 195
- Security officer nonexpectations, 291
- Security officers, 120, 124, 149, 150
 - expectations, 289
 - delay, 290
 - detect, 290
 - deter/prevent harm to people, 289
 - honesty and integrity, 290
 - obligations, 289
 - protective personnel, 290
 - report, 290
 - respond, 290
 - master list tasks and standards, for
 - examples, 192
 - training of, 115
- Security operations, 37–40, 66
 - driven by, 44–55
 - 9/11 and consequences, 49–52
 - laws influencing growth, 47–48
 - other legal measures affecting security, 53
 - Patient Protection and Affordable Care Act (PPACA), 52–53
 - role of unions in, 53–55
 - Sarbanes–Oxley Act (SOX), 52
 - initiating and managing security programs, 37–40
- Security operations managers, 371, 384, 385, 396
 - internal and external controls, 370
- Security-oriented programs, 117
- Security-oriented vetting process, stages of, 79
- Security personnel, 109, 210
 - employers of, 81, 92
 - training factors for
 - extensive basic training, 123
 - firearms training, 124
 - ongoing training, 125
 - preassignment training, 119–123
 - training for investigators, 125
- Security practitioners, 60, 113, 391, 393
- Security programs, 3, 271
 - directory-type information, 189
 - formation of, 53
 - managers, 80
 - requirements of, 37
- Security recruitment productivity
 - worksheet, 80
- Security robotics, 351
- Security services, 56–59
 - contemporary, evolution of, 42–43
 - insurance, 303
 - and products as global business, 59–60
 - workers, 151
- Security supervisor, 163
- Security systems designing, 358
 - bidding/negotiation, 358
 - construction phase, 358
 - design approach, 358
 - operational phase, 360
 - preliminary, 358
 - testing/training phase, 358
- Security technicians, 151
- Security threats and management, 60
 - bombings/bomb threats, 63
 - Business continuity planning/
 - organizational resilience, 60
 - business espionage/theft of trade secrets, 63
 - computer/communications security, 60
 - crisis management and response
 - domestic terrorism, 62
 - international terrorism, 63
 - kidnapping and extortion, 64
 - political unrest/regional instability/
 - national disaster, 62
 - employee selection/screening, 60
 - environmental/social
 - pandemics, 62
 - privacy concerns, 61
 - robberies, 63
 - executive protection, 63
 - fraud/white-collar crime, 62
 - general employee theft, 61
 - global supply chain security, 63
 - identity theft, 62
 - insurance/workers' compensation fraud, 63
 - intellectual property/brand protection/
 - product counterfeiting, 63
 - issues, 60–64
 - labor unrest, 64
 - litigation

- Security threats and management (*cont.*)
 - inadequate security, 62
 - negligent hiring/supervision, 63
 - organized crime, 64
 - product diversion, 64
 - product tampering/sabotage, 64
 - property crime, 61
 - Severe acute respiratory syndrome (SARS), 62
 - sexual harassment/Equal Employment Opportunity Commission (EEOC), 64
 - substance abuse, 63
 - Unethical business conduct, 62
 - Workplace violence prevention/
 - response, 60
- Self-fulfilling prophecy, 175
- Senior management, 210
 - seeks to cut security spending, 277–278
- Sensors, 346
- September 11, 2001, 114
- Service activities, number of, 39
- Service businesses, types of, 41
- Severe acute respiratory syndrome (SARS), 62
- Sexual harassment, 390–392
- SFAS. *See* Statement of Financial Accounting Standards (SFAS)
- Shareholders, 21
- SIA. *See* Security Industry Association (SIA)
- SIMS card, 373
- Single focal length (FL), 344
- Situational crime prevention, 18, 325–327
- Sixteen Personality Factor Questionnaire (16PF), 97
- Skyjacking, 44, 48
- Smart card, 373
- Smoke, 357
- Social media collection, 86
- Social networks, 380
- Social Security Administration (SSA), 87
- Social Security Number (SSN), 83
 - importance of, 89
 - verification, 88
- Society of Competitive Intelligence Professionals (SCIP), 395
- Software packages, 301
- Software programs, 133
- human resources services, 300
- management's support, 301
- and services, 300
- Solicitation Summary, 306, 308, 314
- Somerson, Ira, 30
- Southwest Airlines, 147
- SOX. *See* Sarbanes–Oxley Act (SOX)
- Spadanuta, Laura, 248
- Sprinkler systems, 136
- SSA. *See* Social Security Administration (SSA)
- SSN. *See* Social Security number (SSN)
- Stack, Michael J., 18
- Staffing, 69–110
 - disability, definition of, 85
 - employment application, 83
 - federal contractor screens in haste and lapses result, 78
 - implementation, 75
 - job descriptions, 72–74
 - acrisis management center controller, 74
 - a security officer, example of, 73–74
 - negligent hiring
 - litigation, 75–77
 - verifying indications of integrity, 76
 - background, 76–77
 - deficient preemployment process, 77
 - lesson, 77
 - personnel planning, 69–72
 - polygraph, beating
 - Aldrich Ames case, 96
 - poor preemployment screening, perils of, 70
 - preemployment integrity screening
 - methods, 100
 - security-oriented vetting process, stages of, 79
 - security recruitment productivity worksheet
 - comparison, 80
 - vetting process, 78–109
 - application, 82–86
 - ban the box, 86–87
 - candidate assessment, 107
 - clear purpose test, 99–100
 - employment verification and continuity, 88–93
- E-verify, 87
- file review, 103

- final employment interview, 103–107
 - final offer of employment, 109
 - finding applicable test instruments, 102
 - fitness for work, 102–103
 - in-person prescreening, 82
 - job-related skills testing, 102
 - medical test, 109
 - other tests, 100–101
 - polygraph, 93–97
 - pre-employment drug screening, 107–109
 - preemployment reference sheet, 106
 - preemployment testing, 97
 - psychological or behavioral stability, 97–99
 - recruiting, 79–82
 - references, 87–88
 - testing the tests, 101–102
 - Staff officers, 24
 - Stakeholders, 21
 - Standpipe systems, 136
 - State and federal employment regulations, 104
 - Statement of Financial Accounting Standards (SFAS), 260
 - Statement of operations, 257
 - State-of-the-art systems, 45
 - Strengths, weaknesses, opportunities, and threats (SWOT) analysis, 16
 - matrix, 16
 - Stress interview, 105
 - Strictness tendency, 197
 - Structured interview, 105
 - Sub-master keys, 304
 - Substandard protection service providers, 43
 - Summary judgment, 75
 - Supervision, by contractor, 312
 - Supervisors, 137
 - to be a supervisor, 163–164
 - characteristics, 163
 - definition of, 146
 - duties of employees to workplace, 164–165
 - failure to provide discipline, 222–223
 - feedback from, 155
 - not to be a supervisor, 164
 - placement, 146–159
 - principles, 147–159
 - responsibility of, 160–163
 - and staff, 145–179
 - motivating, 165
 - supporting, 145–159
 - time management for, 166–171
 - ABC technique, 166–171
 - clean desk *vs.* messy, 169
 - delegating everything delegable, 168
 - motivation matters, 169–170
 - Theory X and Theory Y, 170–171
 - Theory Z, 171
 - Pareto principle, 166–167
 - slow down to S.T.O.P. to move ahead, 167–168
 - using technology for greater efficiency, 168–169
 - Surveillance, 344
 - Surveying, 393
 - Sutherland, Edwin H., 62
 - SWOT analysis. *See* Strengths, weaknesses, opportunities, and threats (SWOT) analysis
 - System 4 concept, 15
 - Systems match services, 59
- T**
- Taft–Hartley Act, 53
 - TARR. *See* Time-adjusted rate of return (TARR) method
 - Task Force on Private Security, 119, 121
 - Taylor, Frederick W., 13–15, 166, 175
 - Technology-based learning, 117
 - Technology, using for greater efficiency, 168–169. *See also* Physical- and technology-centered programs
 - Tempest programs, 354
 - Temporary workers, 80
 - Territoriality, 326
 - Terrorism, 385–387
 - Test-scoring variations, 99
 - “T” groups (sensitivity training), 131
 - Theft, of trade secrets, 394–395
 - Threats, Intimidation, Manipulation, and Escalation syndrome (T.I.M.E.), 247–248

- Three Mile Island, 15
- T.I.M.E. *See* Threats, Intimidation, Manipulation, and Escalation syndrome (T.I.M.E.)
- Time-adjusted rate of return (TARR) method, 276
- Time management
 - ABC technique, 166–171
 - clean desk *vs.* messy, 169
 - delegating everything delegable, 168
 - motivation matters, 169–170
 - Theory X and Theory Y, 170–171
 - Theory Z, 171
 - Pareto principle, 166–167
 - slow down to S.T.O.P. to move ahead, 167–168
 - using technology for greater efficiency, 168–169
- Titles, 5
- Tobacco abuse, 381
- ToGA. *See* Flanagan's Tests of General Ability (ToGA)
- Top-down appraisals, 186–187
 - advantage of, 186
- Total assets, 256
- Total liabilities, 256
- Tour limitation rule, 312
- Townsend, Patrick L., 366
- Trade secrets, 394
- Trainers, 137
 - skills, 140
- Training, 113–142
 - accommodations, 140
 - advanced security programming course,
 - outline of, 129–130
 - attack methods, 129
 - authentication, 129
 - cryptography, 130
 - firewall architecture, 129
 - firewall components, 129
 - intrusion detection and response, 130
 - security assessment, 129
 - security implementation policy, 129
 - agreement, 313
 - amount of, 139
 - for armed security guards, 124
 - classroom-based training, 124
 - range-based training, 124
 - assessors, 141
 - confrontations, reducing risk in, 135
 - content of, 139
 - correspondence and online courses, 134
 - defined, 118
 - development and education for managers and executives, 137–139
 - loss prevention, certifications for, 137–139
 - emergency and fire prevention, 135–136
 - facilities, 292
 - firearms, criticality of, 132–133
 - armored car personnel, 125
 - importance of, 113–116
 - learning transfer, 140
 - length and pace of, 140
 - manager, 116–117
 - measuring effectiveness of, 139–141
 - method of, 139
 - new security employees, content for, 119–125
 - for nonsecurity personnel, 136
 - objectives, 140
 - omissions, 140
 - ongoing “in-service”, 133–134
 - orientation, 118–119
 - overview, 113
 - planning and development requirements, 117–118
 - private security
 - 8-H preassignment training course, 120–121
 - 32-H preassignment training course, 122–123
 - relevance, 140
 - security for casinos, 123
 - security guard regulations, statutory requirements of, 114
 - standards, 291
 - techniques, 126–133
 - audiovisual (AV) materials and Power Point, 130–131
 - classroom style with learner participation, 126–127

computer-aided interactive instruction,
128–130
demonstrations, 131
on-job (OTJ) training, 127
other techniques, 132
role playing, 131
“T” groups (sensitivity training), 131
for trainers and supervisors, 137
Training Committee of the National Armored
Car Association, 124
Trait analysis, 188
Transparent film, 335
Transportation, 377, 396
Transportation Worker Identification Card
(TWIC), 397
Transshipment, 399
Tumbler mechanisms, 336
TWIC. *See* Transportation Worker
Identification Card (TWIC)
Twitter, 380
Tzu, Sun, 363

U

UCR. *See* Uniform Crime Reports (UCR)
UL. *See* Underwriters Laboratories (UL)
Underwriters Laboratories (UL), 339
Unethical business conduct, 387–388
Uniform Crime Reports (UCR), 63
Uninterruptible power supply (UPS), 353
for information systems, 353
Unionized employees, 242
Unions, 242
role of, 53–55
Uniting and Strengthening America by
Providing Appropriate Tools Required
to Intercept and Obstruct Terrorism
(USA PATRIOT) Act of 2001, 49
Unselfishness, 367
Unstructured interview, 105
UPS. *See* Uninterruptible power supply (UPS)
USA PATRIOT. *See* Uniting and Strengthening
America by Providing Appropriate
Tools Required to Intercept and
Obstruct Terrorism (USA PATRIOT)
Act of 2001

US Bureau of Labor Statistics, 161
USCIS. *See* US Citizenship and Immigration
Services (USCIS)
US Citizenship and Immigration Services
(USCIS), 87
US Department of Labor, 161
US intelligence system, 96
US Labor Code, 53
US Postal Service, 229, 230
Utility, in pre-employment tests, 101

V

Valiant Solutions, 301
Validity
in pre-employment tests, 101
scale tests, 98
Van Dersal, William R., 145
Variable budgets, 267
Variable expense, 267
Variable focal length (VFL) lenses, 344
Vaughan, Jennifer F., 69
Vaults, 339–340
VCRs. *See* Video cassette recorders
(VCRs) record
Vehicle security systems, 58
Vendor responsibility, 310
Versace, Gianni, 385
Vetting process, 78–83, 103, 109
application, 82–86
ban the box, 86–87
candidate assessment, 107
clear purpose test, 99–100
employment verification and continuity,
88–93
E-verify, 87
file review, 103
final employment interview, 103–107
final offer of employment, 109
finding applicable test instruments, 102
fitness for work, 102–103
in-person prescreening, 82
job-related skills testing, 102
medical test, 109
other tests, 100–101
polygraph, 93–97

Vetting process (*cont.*)

- pre-employment drug screening, 107–109
- preemployment reference sheet, 106
- preemployment testing, 97
- psychological or behavioral stability, 97–99
- recruiting, 79–82
- references, 87–88
- testing the tests, 101–102

VEVRRRA. *See* Vietnam Era Veterans' Readjustment Assistance Act (VEVRRRA) of 1974

VFL. *See* Variable focal length lenses

Victimization, by work associates, 377

Video cassette recorders (VCRs) record, 343

Video motion detection (VMD), 345

Video surveillance trends, 344

Vietnam Era Veterans' Readjustment Assistance Act (VEVRRRA) of 1974, 84

Violence. *See* Workplace violence

VMD. *See* Video motion detection (VMD)

Voice over Internet Protocol (VoIP), 352

VoIP. *See* Voice over Internet Protocol (VoIP)

Vollmer, August, 94

Voluntary ethical standards, 32

Voluntary nonprofit organization, 349

W

Wages, 72

Wagner Act, 53

Walk-through detectors, 355

WANs. *See* Wide area networks (WANs)

Warning signs, 378

Wasting asset, 255

Weapon proficiency requirements, 124

Web-based interactive training, 125

Weber, Max, 12

Web sites, organization, 369

Welch Manufacturing, 76

Western Electric Company, 172

Whistle-blower suits, 234–235

White-collar crime, 392–394

Wicklander-Zulawski, 106, 107

Wide area networks (WANs), 353

Wi-Fi®. *See* Wireless Fidelity (Wi-Fi®)

Wildhorn, Sorrel, 42

Winkler, Ira, 394

Winston, Stephanie, 169

Wireless Fidelity (Wi-Fi®), 352

local area network (WLAN), 352

WLAN. *See* Wi-Fi local area network (WLAN)

Wood, Horace G., 230

Workers' compensation, 396

Workplace

demands, categories, 203

security and safety issues

rationale and methods of, 136

Workplace violence, 162, 242–246, 378

prevention/response, 375–379

Work safety, 160–163

World security services, 59

World Trade Center attack, 50–51

Writing off exceptional expenses, 264

Written appraisal techniques, 198

Written approbation, 156

Written communications, 156

Written employment contract, 231

Wrongful discharge, 229–235

X

X-ray, 309, 310, 354–355

inspection equipment, 58

Y

Yeffet, Isaac, 338

Z

ZBB. *See* Zero-based budgets (ZBB)

Zero-based budgets (ZBB), 267–268

Zoom lens, 344