2

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 antitheft 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 *U*niting and *S*trengthening *A*merica by *P*roviding *A*ppropriate *T*ools *R*equired to *I*ntercept and *O*bstruct *T*errorism (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 unlike 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.F., 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.F., 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>.