

# Security Fundamentals *for the Safety Engineer*

By DAN. M. BOWERS

In many commercial, industrial and public organizations, facilities and institutions, the safety and security functions have been combined under a single manager. Since these are two distinct professional disciplines, the manager will likely require additional education in one area or the other. This article presents fundamental security principles for the safety engineer who has been given these dual responsibilities.

## WHO ARE THE SECURITY MANAGERS?

Most security managers have a background in law enforcement (e.g., retired or former police officers, FBI/Secret Service agents or corrections officers). In many cases, they don't hold a college degree and few are engineers; however, most have superior management skills and experience as well as an understanding of crime and criminals.

Many security professionals belong to the American Society of Industrial Security (ASIS). Similar in size and scope to ASSE, ASIS has 33,000 members, local chapters throughout the country, a certification process (the certified protection professional—CPP), and strong focus on education, standards and member interaction.

## WHAT DOES THE SAFETY ENGINEER DO?

Typically, a safety engineer's duties involve protecting employees and other people within a facility from injury and death; this encompasses accident hazards, hazardous materials and fire prevention/detection/suppression. Many of these activities are guided by regulations promulgated by agencies such as OSHA,

EPA and DOT and groups such as NFPA, ANSI and ASME. This is a principal difference between safety and security—no such statutory guides exist for the security manager. Security measures at a facility can range from minimal to Fort-Knox-class protection, based on management's discretion.

The guiding principles for security center on two considerations: 1) protection of a company's assets; and 2) due-diligence protection for facility inhabitants, which includes consideration of the legal liability for providing a level of protection that may later be judged inadequate. Methods for providing protection can lead to fundamental conflicts between the safety and security functions. For example, security is best served by strictly controlling both access and egress, while safety requires that immediate and unrestricted emergency egress be available.

## THE PROTECTION PROCESS

The first step is to perform a risk and threat analysis. Entire volumes have been written about this process and the step-by-step procedures for conducting it. (See the "For Further Reading sidebar and visit [www.asisonline.org](http://www.asisonline.org) for a listing of the many security references available).

Essentially, the analysis entails answering several key questions.

1) Who are the "bad guys" and what skills and tools do they have?

2) What do they want: business assets (money, drugs, salable commodities), company property (PCs, faxes, VCRs, office equipment, tools), employees' personal property?

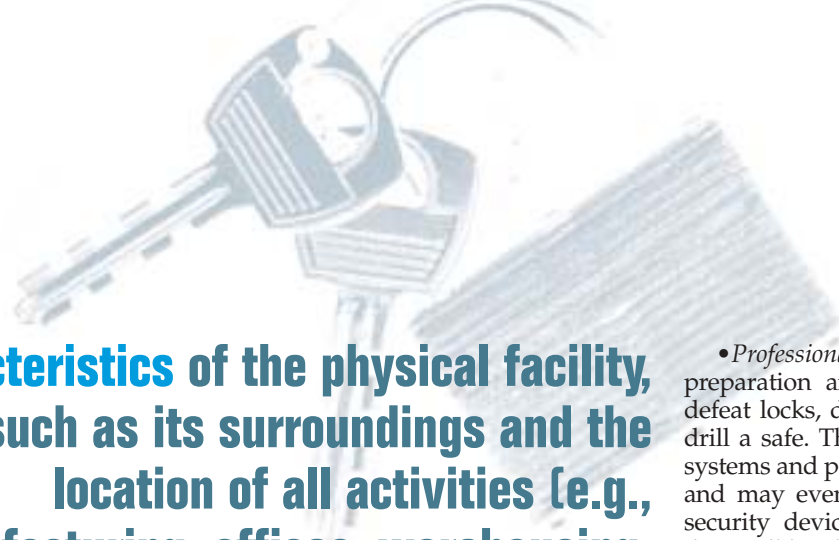
3) What protective tools are available?

4) What defenses are available against assaults on employees (e.g., revenge for dismissal or a poor performance review, family disputes that carry over into the workplace)?

5) How much protection is warranted for the particular facility?

The risk and threat analysis is based on a thorough examination of the company, its products, services and operations. Characteristics of the physical facility, such as its surroundings and the location of all activities (e.g., manufacturing, offices, warehousing, parking) are critical. Points of access and egress must be examined along with all associated life safety constraints. Locations of critical and valuable assets must be identified, and the need for movement of people—both employees and outsiders such as vendors and contractors—analyzed. Existing security equipment, personnel and procedures must also be assessed to

**Typically, a safety engineer's duties involve protecting employees and other people within a facility from injury and death.**



## Characteristics of the physical facility, such as its surroundings and the location of all activities (e.g., manufacturing, offices, warehousing, parking) are critical.

determine whether they should be incorporated into the new security plan.

Before assembling appropriate ingredients from which the total security system will be created, one must understand the protection process, which encompasses the following phases.

- **Anticipation** of likely threats is the first step. What objects or persons are likely to be targeted and why? What are possible routes of access? What everyday activities and traffic must be allowed to proceed without disruption? During this phase, the results of the risk and threat analysis are applied to a facility's geography and activities, and those features that will be included in the security system—physical measures, electronic systems, guards—are determined.

- **Deterrence** is a primary goal of the security system. If a prospective adversary can be made to believe that the system is invincible and, as a result, makes no attempt to defeat it, the battle is won before it even begins. Items such as alarms, lights, cameras, decals, warning signs, window bars and uniformed guards all provide deterrence.

- **Prevention** of unwanted acts, should deterrence measures, is a critical active measure. Strategies include walls, bars, locks and access controls. However, prevention really only provides delay since given enough time and the right tools, any physical barrier can be overcome—fences climbed or cut, locks picked, safes blown or drilled. Thus, it is vital to detect the beginning of an attempt to penetrate physical barriers and provide for appropriate response during the delay period.

- **Detection** of an attempt to penetrate the building, steal an object or engage in other criminal activity, is accomplished via electronic alarm systems; these may include fence intrusion detectors, motion

sensors and door-position sensors. Surveillance cameras are also useful, both for real-time observation and for after-the-fact analysis of perpetrator activity and identification.

- **Response** to the criminal activity detected, either immediately by in-house security staff or by an outside security company or police, is essential; otherwise, detection measures have no value. A delayed form of response is the after-the-fact use of information from surveillance tapes and logs from the alarm and access control systems.

### KNOW THE ENEMY

Many types of people can present threats to property or employees, and different kinds of security measures are appropriate for each. In planning the total security system, site management must decide what kinds of adversaries it is prudent to protect against and to what extent. Management must also recognize those adversaries against whom the system will provide less protection. The targets fall into the following categories:

- **Opportunists** are “passer-by” thieves. They will take readily accessible valuables left on desks or shelves, in store-rooms or cars; steal a car with the keys in the ignition; and perhaps damage or vandalize property. Minimal security measures, such as fences and ordinary locks, will typically keep them out.

- **Amateurs** are unsophisticated criminals who enter a premises with the intent to steal, vandalize or assault. They will climb fences, break windows and skylights, and break locks. Typically, these criminals do not have either the tools or skills to pick locks, duplicate keys or defeat an alarm system. Thus, good locks and other physical security features combined with elementary intrusion alarms are effective measures.

- **Professionals** have plans, training, preparation and equipment. They will defeat locks, duplicate or steal keys and drill a safe. These individuals will learn systems and procedures (“case the joint”) and may even thwart simple electronic security devices. Given sufficient time, they will be able to defeat or circumvent any physical security equipment. Thus, the only effective protection against this class of adversary is a total security system that combines locks and other physical security devices with electronics such as alarm systems and closed-circuit television (CCTV), along with an immediate response capability.

- **Insiders** are employees, contractors, delivery persons or repair personnel who have regular access to a facility whereby they can obtain knowledge about protective systems, their location and operation. However, a well-engineered total security system can provide protection against even those who understand it in every detail. For example, such a system should provide a log of all activities by name so that any crime can be reconstructed and correlated with a video record. For critical functions, a “two-man-rule” should be instituted, wherein two persons are required to perform a given task (e.g., open a safe).

- **Crazies** are people who are not in control of their faculties due to problems that may involve drugs, alcohol, mental instability and personal disputes. They can show up randomly and unleash an aggressive assault. Protection against this adversary is a challenge.

### THE PROTECTIVE RESOURCES

A considerable array of resources can be incorporated into a total security system.

- **Physical security** includes such obvious categories such as doors, turnstiles, door locks and strikes, walls, fences, vehicle barriers, moats, barbed wire, safes and vaults and hardened glass. It also includes lighting and signs, as well as special architectural features that can be used to improve protection.

- **Electronic security** is provided by several categories of equipment: access control systems, such as card readers, key-pads, electric locks and remote-control openers; alarm systems, including intrusion detection and article protection equipment, annunciation and reporting systems, central station monitoring; video surveillance systems, primarily CCTV;

## For Further Reading

Bintliff, R.L. *The Complete Manual of Corporate and Industrial Security*. Englewood Cliffs, NY: Prentice Hall, 1992.

Broder, J.F. *Risk Analysis and the Security Survey*. 2nd ed. Woburn, MA: Butterworth-Heinemann, 2000.

Cumming, N. *Security: A Guide to Security System Design and Equipment Selection and Installation*. 2nd ed. Woburn, MA: Butterworth-Heinemann, 1992.

Fay, J.J., ed. *Encyclopedia of Security Management*. Woburn, MA: Butterworth-Heinemann, 1993.

Fennelly, L.J., ed. *Handbook of Loss Prevention and Crime Prevention*. 3rd ed. Woburn, MA: Butterworth-Heinemann, 1991.

Fennelly, L.J. *Effective Physical Security*. 2nd ed. Woburn, MA: Butterworth-Heinemann, 1997.

Fischer, R.J. and G. Green. *Introduction to Security*. 6th ed. Woburn, MA: Butterworth-Heinemann, 1998.

Floyd, W.R. *Security Surveys:*

*Guidelines for Evaluating Security*. Alexandria, VA: ASIS, 1995.

Konicek, J. and K. Little. *Security, ID Systems and Locks: The Book on Electronic Access Control*. Woburn, MA: Butterworth-Heinemann, 1997.

Pierce, C. *The Professional's Guide to CCTV: Application & Design of CCTV*. Alexandria, VA: ASIS, 1999.

Purpura, P.P. *Security and Loss Prevention: An Introduction*. 3rd ed. Woburn, MA: Butterworth-Heinemann, 1998.

Sennewald, C.A. *Effective Security Management*. 3rd ed. Woburn, MA: Butterworth-Heinemann, 1998.

Sennewald, C.A. and J.K. Tsukayama. *The Process of Investigation: Concepts and Strategies for Investigators in the Private Sector*. 2nd ed. Woburn, MA: Butterworth-Heinemann, 2001.

Tyska, L.A. and L.J. Fennelly. *Physical Security: 150 Things You Should Know*. Woburn, MA: Butterworth-Heinemann, 2000.

voice communications systems such as intercoms, loudspeakers and listening devices; covert surveillance (bugs) and related countermeasures; computer and communications security, encryption, data auditing, virus prevention and hacker detection; guard tour monitoring systems; and scanning and inspection systems for baggage, mail, parcels and people.

• **Systems and procedures** include education and training. The best security system will be ineffective if no one knows how to operate it properly.

• **Guards and patrols** include in-house security staff, private security services, armored cars and couriers.

• **Planning and investigation** include security consultants, personnel profiling, screening and interviewing services, and incident investigators.

• **Public resources** are broadly defined to include police forces, courts and the legal system, and insurance companies.

The crucial decision is to determine what level of protection will be provided. Often, this entails a compromise between the amount of risk that management is willing to assume and the amount of money it is prepared to spend. Protective resources can be defined in terms of the following three levels of protection.

• **Minimum security**, which is the minimum protection that can responsibly be provided with consideration of pertinent risks and threats.

• **Appropriate protection**, which is that level of protection which should be pro-

vided at this time in this location, and in keeping with normal practice of the professional security community.

• **Moat-and-drawbridge**, which involves extensive measures (Fort Knox should be so well protected).

### CALL ON THE EXPERTS

What has been described as comprising the "security" business is actually several enterprises. Physical security companies (fences and vehicle barriers) are typically not in the electronic or guard business, while electronic security companies do not offer fences and guards. Guard firms only provide personnel to perform guard and patrol functions. Investigation companies perform background checks and investigate incidents. Many other companies offer specialty products/services, such as armored cars, lighting, signage, safes and vaults, sweeps for eavesdropping devices, and risk and threat analysis.

In most settings, the safety engineer already has a challenging set of responsibilities and technologies as part of his/her basic job. Thus, it is not reasonable to suggest that s/he also master the intimate details of the many security constituents. Therefore, the best way to get the job done is to assemble a group of contractors that collectively can provide the required products and services. One manager cannot know it all nor can one contractor. The safety engineer cum security manager can act as the general contractor for this group; in some cases, however, it may be

best to engage a security consultant who will oversee the process, from the risk and threat analysis to security system design to contractor management.

Note that computer and networking security are not included among the security manager's many responsibilities. This field, which tackles problems are worms, viruses, hackers and electronic vandals, is a specialty that involves technology which is outside that normally required for by the safety/security manager. In the author's opinion, any organization that attempts to place responsibility for information security under physical security manager will likely face serious problems.

### THE TOTAL SECURITY SYSTEM

No whiz-bang, high-tech, one-size-fits-all protection method is available. Many large commercial and industrial security systems are flawed because management believes that since it has invested so much money in electronic security equipment, a high level of security will result. In essence, management is wearing a modern version of the emperor's new clothes—the appearance of security yet no actual protection.

Complete security is achieved only through a total system that incorporates equipment, people and procedures, and which is appropriate to risks and threats associated with a particular facility, its location, surroundings and operations. ■

*Dan M. Bowers is a security consultant and engineer in Red Lion, PA. He has worked for the federal government, as a research scientist for IBM and as vice president of Burns International Security. Bowers has authored many articles and books on security equipment, computer systems, general electronics and technology management.*

*This article is developed from material presented at the May 2001 meeting of ASSE's Chesapeake Chapter.*

### READER FEEDBACK

Did you find this article interesting and useful? Circle the corresponding number on the reader service card.

YES	00
SOMEWHAT	00
NO	00