Recent Developments in Nationwide Security Standards:

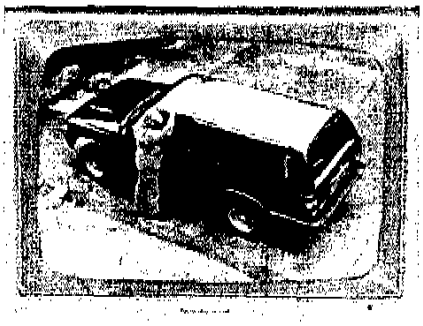
The General Security Risk Assessment Guideline

By Norman D. Bates, J.D.

The need for nationwide security standards and guidelines has never been more pronounced than in the wake of the September 11, 2001 terrorist attacks. Public awareness of security measures is high, whether during air travel, at concerts or sporting events, or on visits to office buildings or shopping malls. The average citizen is increasingly concerned about the quality of security programs and services provided by private industry to the consumer. This article explains the importance of security standards and guidelines and describe one set of guidelines, ASIS International's recently published General Security Risk Assessment Guideline.

Historically, the private security industry has been poorly regulated. Frequently, such regulation has only taken the form of limited state statutes that set forth licensing requirements –and on rare occasions, minimum training standards–– for contract security agencies or so-called guard companies. Proprietary security staff––individuals who are the direct employees of, for example, a hotel, shopping center, or office building— traditionally have not been regulated by states or municipalities.

Since the early 1970s, when the Connie Francis rape case against a motel in New



York received widespread publicity, there has been a multitude of civil litigation alleging inadequate security against privately owned businesses. With many verdicts of more than one million dollars and increased public awareness of this alternative remedy for victims of crime, business owners have become motivated to improve the quality of their security services to guests, tenants, visitors, and employees. Unfortunately, with a dearth of standards guiding property owners on how much or what type of security to provide, many of them failed to take the appropriate steps to properly analyze the risks of crime associated with their businesses. As a consequence, these businesses have failed to provide adequate protection for the public despite their legal duty to do so.

After thirty years of claims against property owners for poor security, a public outcry for nationwide security standards requiring some minimal measures to prevent crime would seem inevitable. In fact, during that thirty-year period, only a handful of technical standards were developed by such standard-setting organizations as the American National Standards Institute (ANSI) and the American Society for Testing and Materials (ASTM). However, these standards typically have been limited to technical items such as locks, fencing, safe construction, or lighting levels. There were no standards or guidelines for the management of security services or the use of security devices in any given application. This means that the landlord of an urban apartment building or the general manager of a downtown hotel would not be able to refer to a written standard regarding what type of locks should be installed on sliding glass doors. The liability of the motel in the Connie Francis case was predicated on the poor quality locks that were provided for the singer. She was raped in her room by an unknown intruder who gained access via a defective locking device on a sliding glass door.

As recently as the early 1990s, there was still opposition by three major industries to the development of any type of security standard or guideline. The apartment, hotel, and shopping-center industries, through their respective trade groups, fought an effort by ASTM to develop minimum guidelines for security measures in all types of privately owned businesses open to the public. A three-year effort to develop the guidelines dissolved with threats to the non-profit ASTM that it was working outside its charter. Although it is doubtful that there was any charter violation, the organization could not afford the cost of litigation and consequently disbanded the committee.

In late 2000 and early 2001, the National Fire Protection Association (NFPA), another standard-setting organization, made public its intentions to start the process of writing national security standards. However, NFPA was a fire-prevention-oriented organization which had no justifiable business entering the domain of the security industry. In February of 2001, this author wrote an article calling upon the private security industry, through its largest professional association - ASIS International (formerly called the American Society for Industrial Security)— to start the process of writing national standards and guidelines for all aspects of security.

ASIS Commission on Guidelines

In August of 2001, one month before the tragic events of September 11, the ASIS Commission on Guidelines was established. The twelve members of the Commission are appointed by the ASIS president and serve indefinitely. They represent a wide variety of interests and industries, including academia, information technology, and private-contract services. During the early stages of the Commission's work, it decided that its initial product would be in the form of guidelines (and not standards *per se*) to allow for the rapid development of useful materials for private industry. The Commission has been in the process of obtaining ANSI certification as a consensus standard-setting organization. Formal standards will come later.

Standards or Guidelines?

The difference between a standard and a guideline is to some degree a matter of semantics, and yet, there are distinctions. A standard usually refers to an adopted standard of practice for the construction, design, use, or application of a product or service. For example, there are national standards for the manufacturing of certain types of locking devices. An adopted standard usually goes through a time-consuming consensus-setting process where all interested parties have input on the content. Words such as "shall" are frequently used. Standards can be and are often adopted by municipalities in codes or ordinances, such as a building code.

Guidelines are generally less restrictive than standards, using language such as "it is recommended" or "courses of action may include." By definition, guidelines are meant to provide guidance to the end user—the private business owner or manager—who needs help in identifying options that may be available for a certain type of application.

The legal implications of a standard versus a guideline are somewhat blurry. While a standard is developed over a longer period of time and goes through a more rigorous process, the effect in the courtroom of invoking standards or guidelines is not likely to be very different. For the plaintiff who is introducing a guideline, the objective is to show a jury that there was a business practice that, arguably, the defendant company should have followed in this case. The alleged failure to adhere to that practice or guideline becomes evidence of negligence in most jurisdictions.

Why Have Security Standards?

At least two views have emerged on whether standards or guidelines that attempt to regulate the security of private organizations should be adopted. The more conservative view is that no standards or guidelines can be written to fit all circumstances. The "one-size-does-not-fit-all" argument has been made numerous times, including during the early 1990s ASTM effort. However, this argument is misleading. It fails to recognize that many efforts can be undertaken by any size organization to improve the quality of its security program.

The more progressive view on standards development is that they are necessary to ensure a higher level of professionalism within the security industry and to render a more consistent approach to the provision of security measures in any private-sector application. Security standards or guidelines can be written to apply in any given setting or circumstances, a fact which is well illustrated by the "General Security Risk Assessment Guideline" written by the ASIS International Guidelines Commission and approved on November 13, 2002.

General Security Risk Assessment Guideline

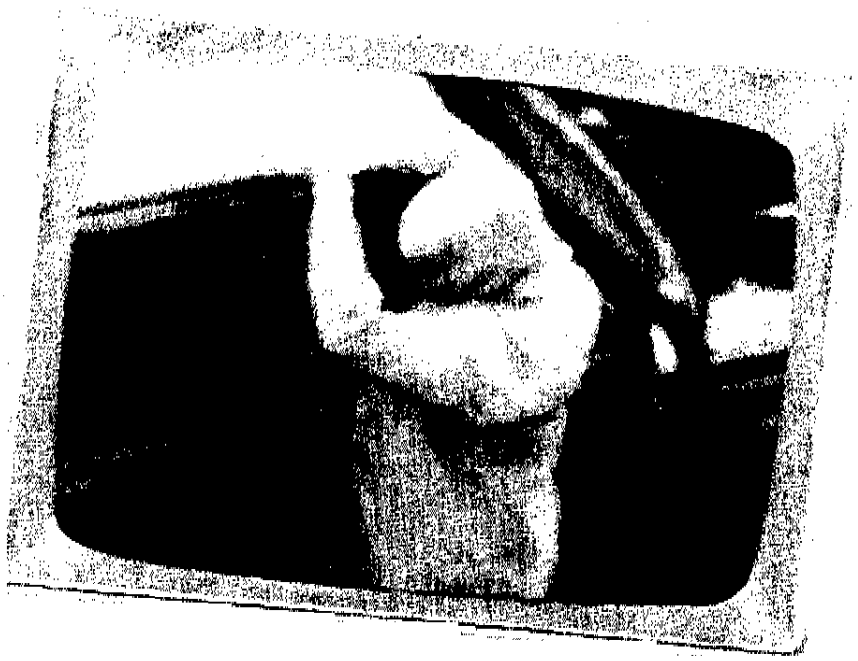
The General Security Risk Assessment Guideline was written by the members of the Guidelines Commission over a one-year period starting in the fall of 2001. The Commission recognized that the best starting point for the development of security standards and practices was with a practice guide that addressed the most basic of issues for private industry. The obvious place to start was by developing a standardized approach to conducting security risk assessments. Regardless of the application or the business or organization type, there is a long-recognized, logical method of analyzing security risks and identifying the options that are available to manage security-related problems. The General Security Risk Assessment Guideline seeks to outline this method. (The Guideline is available free on-line at *www.asisonline.org.*)

The Guideline describes itself as being "applicable in any environment where people and/or assets are at risk for a security-related incident or event that may result in human death, injury, or loss of an asset." The phrase "a security-related incident or event" is not limited to criminal activity. It also includes natural disasters, war, and other activities that could result in a loss of life or property.

The Guideline is a "seven step process that creates a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions." (It also includes definitions, a flow chart, appendices, and a bibliography.) The Guideline's seven-step framework for conducting a security risk assessment is broken down as follows:

Understand the Organization and Identify the People and Assets at Risk

The first objective for a security practitioner in the risk-assessment process is to understand the nature of the organization being evaluated, including its peculiarities, business purpose, methods of operating, and corporate goals. In addition, the nature of the assets and the



type of people at risk are essential pieces of information in a proper risk assessment. The Guideline's appendices include two sections: a qualitative approach to risk assessment and a quantitative approach. In the first appendix—which addresses the qualitative approach that will be described further in this article—there are numerous examples used to illustrate such issues as what constitutes an "asset" or the type of "people" that the practitioner should consider when making the assessment.

Specify Loss Risk Events/Vulnerabilities

The Guideline defines risks or threats as "those incidents likely to occur at a site, either due to a history of such events or circumstances in the local environment. They can also be based on the intrinsic value of assets housed or present at a facility or event." For clarification of this definition, the reader can again refer to the appendices. For example, the concept of "loss risk" events includes prior crimes at the site or in the immediate vicinity and crimes that may be common to that type of industry (*e.g.*, robberies in convenience stores or burglaries in apartment communities). Loss risk events are not just crime or security-related problems. They also include non-criminal events such as human-made or natural disasters such as storms, power outages, and labor disputes.

Establish the Probability of Loss Risk Events and Frequency of Events

In establishing the probability of loss, one should consider such factors as prior incidents, trends, warnings, and threats. The probability is not based on mathematical certainty, but simply a consideration of the likelihood that an event will occur, based on historical data, events at similar establishments, and so forth. For instance, it is well known within the industry that convenience stores are targets for armed robbery. This is primarily because they are cash businesses, often are open twenty-four hours a day, frequently have only one clerk, and commonly are located at major intersections where there are more escape routes for the criminal. The security practitioner would take this "inherent risk" into account when assessing the probability of future robberies in similar establishments and would provide the appropriate recommendations.

Determine the Impact of the Events

The impact of an event refers to financial,

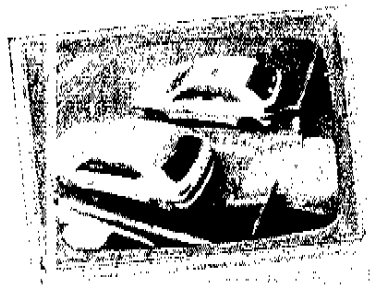
psychological, and other related costs incurred by an organization. "Other related costs" may not be so obvious. The appendix describes a number of issues raised by certain loss events, such as negative media coverage, poor consumer perception, the inability to obtain insurance coverage (*e.g.*, in the wake of the recent terrorist attacks), or poor employee morale which affects worker productivity.

Develop Options to Mitigate Risks

It is understood and accepted within the security industry that one cannot eliminate all risks or prevent all losses. Frequently, however, there may be several options or security solutions that can be applied to the same set of factors. Examples of security solutions include staffing, security equipment (*e.g.*, card access systems, closed-circuit television cameras, alarms, lighting, and locks), transferring the financial risk of loss through insurance coverage, indemnification agreements with security service providers, and a number of creative approaches to address a problem. Security solutions often involve a compromise arising out of the long-standing conflict between security and "convenience." Convenience is the argument that "we have always been doing it that way and it wouldn't be convenient to change the way we operate." The example of forcing employees to use a single entrance to a facility to enhance access control illustrates the problem.

Study the Feasibility of Implementation of Options

The questions are whether the security measures available are feasible for an organization and whether the measures would



substantially interfere with the organization's operation. If they do substantially interfere, the security measures may not be practical. As an absurd example, if a retail store had severe shoplifting problems, one possible "solution" would be to simply lock the doors of the store. In doing so, the shoplifters would be prevented from stealing the merchandise. Of course, legitimate shoppers would also be prevented from purchasing the merchandise and the store would go out of business. The "solution" here would obviously substantially interfere with the operation.

Perform a Cost/Benefit Analysis

Security measures should be proportional to the risks against which they are designed to protect. The impact of a loss that involves the death or injury of people can be substantial in a variety of ways—from the obvious emotional costs to the economic harm caused by the loss of key employees. On the other hand, some property losses are more bearable than others and as such, the security practitioner would be expected to compare the cost of the various options against the cost of the loss. While many people would insist that no cost is too great to save a human life, most would also concede that it makes no sense to spend $100,000 on security equipment to prevent the loss of $1,000 dollars of property.

Conclusion

The methodology found in the General Security Risk Assessment Guideline is not new. Research conducted by this author over the last several years has revealed similar approaches in a number of publications, ranging from basic security texts to Department of Justice guidelines on assessing security risks in federal buildings. Several of these publications are cited in the bibliography provided in the Guideline.

The fundamental question is: who benefits from the development of security standards and guidelines? The answer, first and foremost, is the public. We all benefit. Private organizations have incentives to minimize their losses, and now, more than ever, the public is concerned about security and having safer places to live, work, and spend their free time. Ultimately, security standards will help ensure that these mutually inclusive goals are achieved.

Norman D. Bates, J.D., is the president of Liability Consultants, Inc. in Sudbury, MA, a member of the ASIS International Commission on Guidelines, and a charter member of the National Crime Victim Bar Association. For more information, visit www.liabilityconsultants.com.