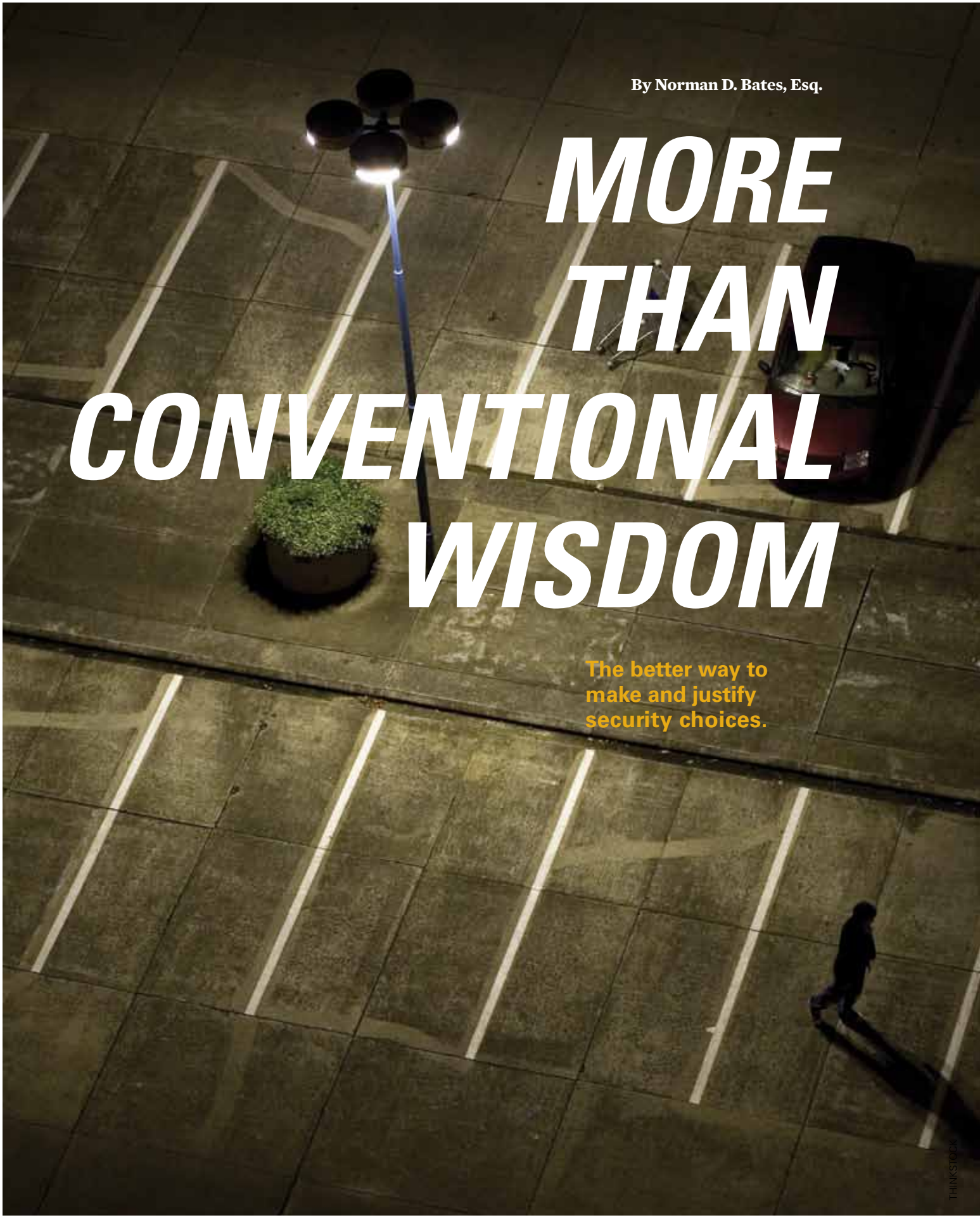
By Norman D. Bates, Esq.

MORE THAN CONVENTIONAL WISDOM

The better way to make and justify security choices.



THINKSTOCK

A woman went to an urban hospital to visit an ill friend. While walking to her car in the nearby parking garage, she was stabbed and robbed by an unknown assailant. A year later, the garage manager finds himself sitting in a deposition that is being taken by the woman's attorney. The attorney has many questions, but, in particular, wants to know how that manager determined how much and what type of security measures to provide in that garage at the time his client was attacked.

If you were that manager, would you be able to answer the following questions?

- How did you arrive at the decision to have only the local police randomly patrol that garage and not retain the services of a security company dedicated to the facility?
- On what basis was the decision made to place closed-circuit television cameras only at the vehicle entrances and not inside the garage as well?
- Was any kind of security risk analysis conducted, and is that analysis acceptable in the parking industry?

In short, the attorney for the victim wants to determine how the manager can support his decisions about the type of security program the garage provided its customers.

Security programs often develop and grow over a period of years, with changes made in response to certain incidents (e.g., a rash of thefts from vehicles) or when crime in the neighborhood has increased. What the garage facility may have needed 10 years ago may be far different from its current needs. But all too often, the current manager will have difficulty explaining the rationale for certain decisions about staffing levels and the use of security technology. Sometimes, the reasons for doing something may reflect what a manager thinks is needed or are the result of the influence of various constituencies, such as customers or employees.

For example, if customers parking in the garage do not feel safe walking to their vehicles at night, then garage management might respond by increasing the lighting levels. However, one consideration is whether increased lighting will actually make a place safer. Based upon a number of studies published to date, there is no absolute proof that increased lighting actually reduces the occurrence of crime. Given this fact, how does the garage manager justify the decision to increase lighting levels versus using other security measures such as increased security patrols?

Security programs are frequently based on someone's intuitive feeling about the needs of the facility, an increase or decrease in criminal activity, or fluctuations in business levels due to seasonal changes. Frequently though, security programs are not evaluated in their entirety in light of crime trends over a greater period of time, such as one to three years.

In recognition of the need to conduct regular security assessments that are based on a logical approach, the private security industry has developed a variety of peer supported methodologies. One of these methodologies is the "General Security Risk Assessment Guideline," published by ASIS International (the largest security industry professional association) in 2002 as a tool for managers to use when conducting a security risk and needs analysis. While this guideline is only one tool among others that have been developed, it provides managers with some direction when analyzing security risks as well as a means to consider the various available security measures.

The Guideline includes seven distinct steps, regardless of the business or organization type, whereby the practitioner can analyze crime risk and evaluate whether the various security measures available are practical and cost-effective:

1. Understand the Organization and Identify the People and Assets at Risk.

The first objective in the risk assessment process is to understand the nature of the organization being evaluated, including its peculiarities, business purpose, method of operating, and business goals. The nature of the assets and the type of people (e.g., customers and employees) at risk are essential information if a proper risk assessment is to be conducted. Assets include tangible items such as property in vehicles and the vehicles themselves.

2. Specify Loss Risk Events/Vulnerabilities.

This step in the Guideline addresses incidents that are likely to occur at a site based on a history of such events at or around the facility, among other factors. The risk of an incident can also be affected by the value of assets present at a facility. The existence of prior criminal activity at the garage and/or immediate vicin-

Security programs are frequently based on someone's intuitive feeling about the needs of the facility, an increase or decrease in criminal activity, or fluctuations in business levels due to seasonal changes.

ity, and crimes that may be inherently common to that type of industry (e.g., robberies at convenience stores, burglaries in apartment communities, etc.) should also be taken into account.

The local law enforcement agency can be very helpful to the garage manager in understanding the nature and frequency of crime both at and around the garage. The manager can contact the agency and speak with the law enforcement officer assigned to act as liaison with the business community to get such details and also obtain a list of calls to the department for incidents reported to have occurred at and around the property.

According to the U.S. Department of Justice Bureau of Justice Statistics, analysis of crime victimization in 2008 (the most recent year for such data), showed that 10.5 percent of all violent crimes involving strangers was reported to have occurred in parking garages.

3. Establish the Probability of Loss Risk Events and Frequency of Events.

Probability of loss is a concept that considers such issues as the occurrence of prior incidents, crime trends, or other threats. Probability is not necessarily based on some mathematical certainty, but simply the consideration of the likelihood that an event will occur based on historical data, events at similar establishments, crime in the immediate vicinity, social and economic conditions (i.e., a poor economy), and other factors.

Frequency of events relates to the regularity of the potential loss event. For example, if the threat is the robbery of patrons in a parking garage, the frequency of exposure to the potential crime would be the number of times customers park in a garage and walk to and from their vehicles.

4. Determine the Impact of the Events.

The impact of an event refers to the financial, psychological, and other related/potential costs of the loss of the assets of an organization. Financial costs would include the value of an item stolen, increased insurance premiums due to a history of claims, deductible expenses on insurance policies, labor costs for an increase in security coverage after an incident has occurred, lost management time to deal with the aftermath of a serious incident (e.g., rape/abduction from the garage), and damage awards not covered by the facility's insurance policy.

Indirect costs include negative media coverage and the consequential decline in business, poor consumer perception, the inability to obtain insurance coverage, and poor employee morale that affects worker productivity.

5. Develop Options to Mitigate Risks.

It is well understood in the security industry that one cannot eliminate all risks nor prevent all losses. However, there are often several different options or security measures that can be taken to address a particular security problem or crime risk. Those options may include security personnel and security equipment such as card access systems, alarm systems, and locking devices. The financial risk of loss can be transferred through insurance coverage, indemnification agreements with security service providers, and any one of a number of creative approaches to address the problem.

6. Study the Feasibility of Implementation of Options.

Feasibility is whether or not certain security measures available are practical within the realm of the organization's operation and do not substantially interfere with that operation. For example, if there has been a series of automobile thefts from a parking garage, one possible "solution" would be to simply lock all the doors of the garage. In doing so, the thieves would be prevented from stealing the vehicles, but legitimate customers would also be unable to park their vehicles in the facility and the garage would go out of business. Feasibility is the consideration of various security options and a determination of whether any of those options makes it impractical to operate the business.

7. Perform a Cost/Benefit Analysis.

The impact of a loss, whenever it involves people, can be substantial in a variety of ways, from the obvious emotional loss up to and including economic loss caused by the death or serious injury of key employees. Some property losses, however, are more bearable than others and, as such, the manager would be expected to compare the cost of the various options against the cost of the potential loss. While some people would insist that no cost is too great to save a human life, others would argue that it makes no sense to spend $100,000 in security equipment to prevent the loss of $1,000 worth of property.

Conclusion

The methodology found in this Guideline provides an approach to considering what constitutes a security risk and a manner to evaluate the various options available to management.

The critical point for the garage manager conducting a security risk assessment is the ability to justify the methodology and thought process used when making decisions about the facility's security program. Following this approach or a comparable one will help managers justify their decisions about security.

NORMAN D. BATES, Esq., is president and founder of Liability Consultants, Inc., and a nationally-recognized expert in security and the law. He can be reached at info@liabilityconsultants.com or 978.779.9906.