

June 15, 2001

Critical issues for security directors

Professionals discuss workplace violence, overseas travel, cost-effective security

For a company, the impact of a security breach extends beyond the immediate costs of theft or violence. The kidnapping or loss of top executives can imperil the company's future. The loss of proprietary secrets risks a competitive edge. An incident overseas can affect the ability to compete globally. Shareholder value can plunge after a serious incident. Workplace violence costs American business more than \$35 billion a year, according to researchers, including lost time, lower productivity and legal liability.

The strategies corporate security directors propose and the forces they deploy help determine whether employees, customers and property are safe and whether investors are confident.

At a series of private sessions conducted by security experts and in interviews, corporate security directors shared their foremost concerns. Among them were workplace violence, international travel and the pressures of cost-cutting. This issue of The Lipman Report highlights those concerns and presents possible solutions.

Workplace violence

Workplace violence remains a primary concern. An especially violent incident like the December massacre in a Boston suburb last year draws renewed attention to the problem. In that case, a software worker embroiled in a tax dispute carried several weapons to work and killed seven co-workers. These cases from the last two years show the scope of the problem:

- A former employee at a Chicago-area manufacturer killed four employees and himself.
- A housekeeper shot and killed five co-workers at a Tampa hotel.
- A copier repairman in Honolulu fatally shot seven people at his office.
- A day trader killed nine people at two Atlanta brokerage offices and then killed himself.

Recent economic performance adds to the concern. "Economic trouble increases the threat of workplace violence," said a veteran security professional. He pointed out that some companies add security when business is good and cut secu-

rity during a downturn, the opposite of what they should do. Laid-off employees might strike back. Remaining employees, fearing they could be next, might take proprietary information.

The latest economic figures point to a slowing economy. Gross Domestic Product (GDP) increased at an annual rate of only 1.3 percent in the first quarter of 2001. Durable goods orders are down, and the National Association of Purchasing Management survey declined in May.

Although unemployment dipped slightly to 4.4 percent in May, the latest Employment Outlook Survey shows that hiring will continue to slow down, especially in manufacturing. According to a Chicago outplacement firm, so far this year companies have announced 570,000 layoffs. Businesses are definitely tightening their belts, and workplace tension is bound to increase.

Alert security directors know that now is the time for increased vigilance. As one supporter of a zero-tolerance policy put it: "Never ignore angry talk like 'You haven't heard the last of this!'" The costs of workplace violence are too high to ignore warning signs.

On-the-job homicides

In 1999, the latest year surveyed by the Bureau of Labor Statistics, 645 homicides occurred in workplaces. That represents a 40 percent decline from the high of 1,080 on-the-job homicides in 1994. Increased security and a growing economy during the 1990s may be responsible for the decline, but the toll is still high. After years at number two, homicides are now the third leading cause of on-the-job deaths, trailing highway crashes and workplace falls.

The National Crime Victimization Survey of 46,000 households estimates that 2 million people a year suffer non-fatal injuries at work. Most definitions of workplace violence include threats, coercion and harassment.

(continued on next page)

Critical issues for security directors

Professionals discuss workplace violence, overseas travel, cost-effective security

(continued from preceding page)

An academic report published in February listed these categories of workplace violence:

- *Criminal (85% of workplace homicides)*—The perpetrator is committing a crime, such as robbery, along with the violence.
- *Customer/client/patient (3%)*—The perpetrator becomes violent while being served by the business. A large number occur in the health care industry.
- *Worker on worker (7%)*—An employee or former employee attacks another employee in the workplace.
- *Personal (5%)*—The perpetrator has a personal relationship with the victim.

Dealing with the problem

After talking with security directors, one security expert said he was surprised to learn that many companies, particularly smaller ones, do not have a written policy on workplace violence.

Based on U.S. Occupational Safety and Health Administration guidelines and the recommendations of security experts, companies can combat workplace violence in the following ways.

Top-down commitment. A violence-prevention expert noted that a successful program often requires a change in corporate culture. That is unlikely to happen without leadership. Top management should budget for effective, ongoing security instead of applying temporary bandages during a crisis, then lapsing into complacency. The security director should report to senior executives to assure a high level of communication and coordination of a consistent and focused plan. Leading by example, top executives should wear badges and have visitors escorted. Once procedures and safeguards are in place, according to a security manager at a large manufacturer, they must be monitored for compliance. Signs, written reminders and education can create a security-conscious workplace.

Zero tolerance for threats. Violence often follows threats or intimidation. All employees should understand that anyone who threatens a co-worker can expect appropriate discipline up to and including dismissal. A security manager noted that sometimes a pattern of aggressiveness is accepted and explained away: “Oh, that’s old George; he’s just like that.” A zero-tolerance policy avoids acceptance of risky behavior.

Deal with complaints. Each complaint about an employee’s behavior must be handled fairly and with finality, so that it doesn’t escalate into more serious problems. A security manager noted that fair, decisive action can satisfy both the complainant and the person accused. The company should encourage workers to come forward.

Risk factors. In tutorials, supervisors should learn the signs that indicate a potential for violence. In an article published earlier this year, the Society for Human Resource Management noted the phenomenon of “desk rage,” fueled by stress and aimed at co-workers. According to a leading criminologist, red flags include a history of failure, the need to blame others, social and psychological isolation, and a fascination with guns. Most often, the “workplace avenger” is a middle-aged, white male whose self-worth is tied to his job. The criminologist cautioned that screening for red flags must be done with discretion. Supervisors should intervene early, offering help and counsel.

Get employees involved. They must share some responsibility. For instance, if a person has a restraining order against an abusive spouse or significant other, he or she should inform the company. Then, the offender would not be admitted at the workplace.

Handle terminations carefully. Several security directors complained about a lack of coordination. Human resources terminates and security finds out later, as one manager put it. Notice of termination must be communicated to security and posted at all security posts. It does no good

to revoke an access card for the front entrance if an ex-employee can walk through a service entrance. Coordination is especially important with large-scale layoffs. HR and Legal must meet with security and plan what, where and when the announcement will be and who will attend. By asking questions first, security can avoid trouble later.

Infatuation on the job

Several companies were interested in the problem of on-the-job infatuation, where one employee gives unwanted attention to another. Without early, decisive action, the behavior can escalate into stalking, where the pursuer follows the pursued or parks outside his or her home. Lawsuits or police involvement may result.

One risk management executive was herself being stalked and asked what she could have done to head off the problem. A security veteran explained that, just as workplace violence starts with angry words and builds toward an explosion, office infatuation follows a pattern of escalation. At first, the pursuer drops by the object's desk again and again. Next come flattering e-mails, perhaps an invitation to a business lunch. Finally, the pursuer offers a gift, often a trivial one. If the object of the attention accepts the gift, the pursuer sees it as personal acceptance and may continue the pursuit outside work.

A direct, final rejection during the drop-by phase usually halts the behavior. Employees must know that if they report an infatuation problem they will pay no penalty.

International work or travel

With globalization of business comes a globalization of security concerns. Security directors reported that they were increasingly called on to provide overseas intelligence and planning.

Security directors discussed a hypothetical question: What if an executive must fly to Bogotá, Colombia, South America, at the last minute? An

atmosphere of open, ongoing communication between senior executives and the security director fosters confidence, minimizes surprises, and facilitates security preparations. According to an expert in executive protection, the first critical factor for trip planning is sound intelligence. This is available through networking with colleagues and foreign sources and on the Internet; data on potential destinations should be kept up-to-date. Second, contingency planning should include the use of a security escort with a standing evacuation plan that can be quickly adapted to a new locale.

Here are some sources a company might consider for intelligence on foreign countries:

- U.S. Department of State (www.state.gov) offers travel warnings and crime and security information.
- Foreign and Commonwealth Office (www.fco.gov.uk) provides information and alerts from the British government.
- Overseas Security Advisory Council (www.ds-osac.org) fosters the exchange of information between the U.S. government and companies operating overseas.
- www.365news.com—Links to hundreds of overseas newspapers.
- www.stratfor.com provides in-depth reports and strategic forecasting on world politics, economics, security and flash points.
- TransSecur, founded by a counter-terrorism expert from the U.S. Department of Defense, analyzes foreign security issues via an on-line subscription service.

Using such sources as well as contacts in foreign governments and at embassies, the director of security for a global company monitors developments in China, Indonesia, the Middle East, Europe, Africa and South America. The concern may center on political instability or a repressive

(continued on next page)

Critical issues for security directors

Professionals discuss workplace violence, overseas travel, cost-effective security

(continued from preceding page)

government, on political terrorism or street crime, on environmental protesters or kidnaping for ransom. The security chief distills this information and shares it with employees worldwide through a daily briefing.

Some companies instruct American employees overseas to avoid flag-waving, be sensitive to the feelings of their hosts, and stay out of political discussions. For instance, when North Atlantic Treaty Organization (NATO) planes mistakenly bombed the Chinese Embassy in Belgrade in 1999, one company kept employees based in China off the streets and took down the U.S. flag at its facility to avoid provocations.

The security director for a firm that operates in South America factors street crime into his planning. He noted a wave of carjackings in which victims were forced to withdraw cash from an ATM. In some countries, if an American hails a cab, he or she could be robbed and dumped outside town. Guerrillas may target employees of American companies.

Companies should offer tutorials on overseas risks. Employees must learn to recognize dangers and extricate themselves from trouble, to avoid certain practices or locales. Travelers should not be predictable in coming and going and should avoid displays of wealth.

Reliance on technology

Many security directors were concerned about a growing reliance on technology at the expense of personnel, due to budget constraints. Some facilities have no security except a card-reader for access and closed-circuit television. But the monitoring of these systems may be incomplete or sporadic. If the front door has the card reader, according to a security expert, "Smokers taking a break will use another door and prop it open, so they can get back in. They may forget to close it again, so the front door is protected but the back door exposed." If a card-reader database is not

updated regularly, a former employee can use his or her badge to get in. Or an employee can use a badge to let others piggyback in.

A technical security expert pointed out that a pro-active monitoring system combines technology with the human element. When an alarm goes off at a remote site, for instance, a camera can verify the problem and then security officers can respond.

The quest for a cost-effective, high-technology solution can go too far. Technology is invaluable as a supplement to physical security but cannot carry all the load. A combination of humans at busy checkpoints with electronic security at little-used areas works best.

Security directors have a large responsibility; they are on the line trying to maintain effective security and still contain costs. Senior management has a responsibility to support security directors with resources and a commitment to a secure workplace. A focus on security is especially important during an economic slowdown.

Sharing concerns with other professionals can lead to fresh ideas. Some managers noted the prime importance of the security provider. A technically proficient security company can assess a company's needs and recommend the best blend of physical and electronic security, allowing a company to reduce costs without compromising safety. Whether dealing with the threat of workplace violence, the risks of international travel or the best way to use technology, a security-conscious company will employ all the resources at its disposal. These include solid intelligence, a cost-effective security provider and a security director with authority.



The Lipman Report Editors