

October 15, 2002

Misplaced priorities

Economic pressures impede continued need for heightened security

More than a year has passed since last fall's terror attacks against America, and the Bush administration remains resolute in its war against terrorism. Daily news coverage continues to examine the nation's state of readiness in the event of future assaults. What steps have been taken? What more can the country do? How can private entities and individuals contribute to the effort to increase homeland security?

While it is true that a veritable industry dedicated to homeland security has emerged, most U.S. businesses and private citizens have successfully convinced themselves that the tragic events of September 11, 2001, were a one-time calamity; they rest assured that the federal government is now aware of the danger and is doing everything in its considerable power to protect them from future strikes. Many people believe that, if another event does occur, it will happen "somewhere else." In other words, complacency has indeed returned with full force to settle upon most of the nation—despite the newfound awareness.

Most security directors, however, remain gravely concerned about the possibility of terrorist assaults, recognizing areas that represent greater vulnerabilities given the new global climate. In recent months, other, more traditional concerns, such as workplace violence, have also started to re-emerge as priorities, largely because the continuing slide of the economy has prompted widespread downsizing. Unfortunately, many companies have reduced their security budgets across the board, believing the current economic pressures to be more important than their survival.

This issue of The Lipman Report examines the evolution of corporate security since last fall's attacks and offers recommendations on how to balance the continued need for heightened vigilance with the pressures of a still-turbulent economy.

A changed world

In the immediate aftermath of the September 11 attacks, security directors practically received carte blanche from their organizations to enhance their security programs. The United States was under attack, and no one knew where or when the next strike would occur. Once the initial shock subsided, however, many American busi-

nesses—primarily in the central portion of the country—began to turn their attention to other issues, dismissing the danger as a regional threat limited to the nation's most prominent metropolitan centers: New York, Washington, Los Angeles.

As the individuals directly responsible for safeguarding their companies' facilities and employees against a future strike, security directors and managers have remained focused on the increased threat, expanding the scope of their vigilance. For instance, the energy and transportation sectors now receive more attention because of their importance to the U.S. infrastructure and thus their attractiveness as terrorist targets. Geopolitical developments also hold more interest for American businesses because of the potential risk to U.S. citizens traveling and living abroad.

The continued decline of the American economy, unfortunately, has compounded these concerns. First, the recession has forced many organizations to eliminate a significant number of jobs. This rampant downsizing not only brings the increased threat of workplace violence, but also internal theft and sabotage as worried and disgruntled employees retaliate against perceived injustice. Second, history has demonstrated a trend for crime to increase as the economy declines, making security a greater concern than ever. Ironically, the security budgets are often the first to experience cuts during times of recession, and the current period of economic turmoil has followed suit, further frustrating security directors in their efforts to prevent possible future terror attacks at their facilities.

Attractive targets

Since September 11, 2001, the energy and transportation sectors have emerged as primary targets. Intelligence agencies know that economic devastation remains as much a terrorist goal as significant loss of life.

(continued on next page)

Misplaced priorities

Economic pressures impede continued need for heightened security

(continued from preceding page)

Energy plants, particularly those providing nuclear power, have started to fortify their defenses on their own, even though no national unified plan exists to govern such action. These measures to date have included the installation of additional barricades and the increasing of the security force. During times of heightened alert, such as last summer's Independence Day, the federal government has banned flights near the nation's nuclear reactors. A study conducted by the Nuclear Energy Institute indicates that U.S. reactors can withstand a direct hit by a Boeing 767 at 300 miles per hour; critics, however, point out that the analysis does not examine the consequences of a collision at 500 miles per hour—the speed at which jetliners crashed into the World Trade Center. The Nuclear Regulatory Commission wants to raise the security standards but requires approval from a deeply divided Congress.

The transportation industry has similarly entered the spotlight because of its potential as a terrorist target. Naturally, airport security has received the greatest attention because of the failings that enabled al Qaeda operatives to hijack four commercial airliners in a single morning. Meanwhile, experts worry about the vulnerabilities that exist throughout the rail and shipping systems. Passengers and baggage do not undergo the same thorough screening as conducted at the airports. Sheer volume prohibits thorough screening of cargo containers, enabling the potential smuggling of explosives or even terrorist agents. Despite these weaknesses, little attention has been given to these critical sectors. Even with the top priority accorded to airport security, only limited progress has been made during the last 13 months.

The global community

The ongoing war on terror has made many organizations keenly aware of events in other parts of the world, particularly those with operations and

business alliances overseas. Executive protection and travel security have gained prominence during the last year as more companies monitor world events to assess the potential impact on their employees and strategic interests.

Additionally, those U.S.-based firms that are identified as American icons have become especially sensitive to the heightened risk of attack on foreign soil. As private businesses, these companies do not receive the same increased protection as U.S. embassies, yet face greater danger because of their symbolic value and the often-easy accessibility, as many of them are commercial establishments that serve the public. The widespread awareness currently found throughout the United States makes an attack within the nation's borders significantly more difficult today than before September 11. This fact has the secondary effect of making American targets abroad more desirable.

Economic pressures

Several experts have reported the same disturbing trend in corporate America: Now that more than a year has passed without any major terrorist incidents, senior management no longer views security as a top priority. In many cases, security costs have regained the former perception as a drain on the bottom line, rather than a risk management necessity, and security directors from coast to coast are worrying about the impact of budget reductions on their facilities' defenses. "Many of them detect a certain amount of apathy, and along with that goes a certain amount of reluctance to spend funds on first-class security," said one authority.

In the current economic climate, more and more security managers are finding it increasingly difficult to get budget approvals. These men and women must determine how they can reduce the size of their department, even while they grapple with the growing concern that another American target will fall prey to a terror strike. Although

security directors overwhelmingly recognize the need to upgrade their programs, they realize the futility of arguing for such enhancements. Too many purchasing departments regard security as simply another line item, giving it equal rank with janitorial or food and beverage services.

Consequently, those individuals responsible for safeguarding corporate America may find themselves in the same difficult predicament that federal law enforcement agencies faced on September 11. For years, repeated requests for additional funding for anti-terror programs were declined by Congress, yet these organizations were ultimately held accountable for the catastrophic attacks of that day.

A balancing act

Private industry cannot ignore the ongoing presence of the terrorist threat or idly expect the federal government to protect the nation from future attacks. Businesses and individuals must participate in the effort to enhance homeland security, at the same time reducing the risk of more common problems such as workplace violence and theft.

- **Increased awareness.** As the passing months continue to distance much of the nation from the horrors of September 11, 2001, many organizations have adopted the attitude that “it won’t happen here.” Some view the terrorist attacks as an isolated event, while others view the threat as limited to major metropolitan areas. This complacency compounds the threat due to the increased vulnerabilities resulting from inadequate security and the lack of proactive measures. Corporate security directors must get assistance from senior management in a campaign for heightened awareness on the importance of comprehensive security programs, particularly in the face of an unsteady economy.
- **Security surveys.** A thorough security assessment can not only identify an organization’s

security vulnerabilities, but also provide a cost-effective means of determining the most appropriate security procedures to implement. Companies in high-risk industries or those with facilities in the vicinity of potential targets should evaluate the level of the existing threat and plan accordingly. Security audits conducted by professionals skilled in analyzing a facility, identifying vulnerabilities and developing solutions can provide a blueprint for an organization’s security program and for business continuity or even survival. Once potential problems and viable solutions have been identified, companies need to implement the solutions without compromising quality. Organizations should regularly re-evaluate their security programs to ensure that the procedures in place evolve with their needs and the threat level.

- **Physical security measures.** Increased security measures and heightened vigilance on the part of the private sector can aid in preventing acts of terrorism, violence or theft. Effective perimeter security, rigorous access control and sophisticated security technology—combined with alert, educated security personnel—can reduce a company’s risk of falling prey to terrorists or other criminals. Investing in sophisticated security technology, such as biometric access control systems and infrared intrusion monitors, can provide additional assistance when used to supplement, rather than replace, security teams. When used effectively, such devices can reduce the number of security officers required for coverage and enable security personnel to make more productive use of their time.

High-risk facilities such as energy plants and medical facilities must take precautions to safeguard dual-use chemicals and equipment that can be used as weapons of terror. Companies that manufacture or use such substances or devices need to communicate with federal, state

(continued on next page)

Misplaced priorities

Economic pressures impede continued need for heightened security

(continued from preceding page)

and local authorities to alert them of suspicious activities that could represent a terrorist threat and to develop a response plan in the event of a security breach. To prevent these dangerous resources from falling into the wrong hands, organizations must employ a trusted security team to implement stringent physical security, access control procedures and 24-hour electronic surveillance of the site.

- **Travel precautions.** Companies with global interests should take steps to help traveling employees recognize and avoid the threat of terrorist attacks or kidnappings. Organizations need to conduct security awareness briefing sessions to inform employees of existing threats and to recommend ways in which employees can protect themselves. The U.S. Department of State's website, www.state.gov, provides information about the culture and social customs of various countries and offers practical guidelines for Americans overseas, in addition to bulletins warning of destinations dangerous to American travelers.

High-profile executives must exercise extra precautions while traveling in foreign countries. Experts recommend establishing contact with the U.S. embassy or consulate in the destination country and maintaining a low profile by dressing inconspicuously. Other tips for foreign travel include paying close attention to surroundings and activities and avoiding predictability by varying travel routes.

Although homeland security remains a priority for the federal government, the private sector cannot wait for legislative resolutions and economic recovery to produce a safer nation. Business entities and individuals should continue to emphasize the issue by lobbying government representatives to take action. At the same time, corporate America must take action to enhance the security of its facilities and prevent potential attacks.

Once again, the cycle of security has repeated itself: Immediately after a major event, organizations go on heightened alert and dust off security initiatives that had been shelved for lack of funding, only to return to their previous state of complacency with the uneventful passage of time. The United States witnessed this phenomenon in 1993, after the initial attack on the World Trade Center in New York, and again in 1995, in the aftermath of the Oklahoma City bombing. In September 2001, experts warned that the nation would fall into the same irresponsible pattern, even as outraged Americans denied that they could ever forget such evil deeds. Yet, one year later, many of the purse holders in corporate America have turned a blind eye to those tragic assaults, and the pressures of a troubled economy have convinced them to gamble that any future strikes will occur somewhere else.

Security directors must have the tools to defend their budgets and to upgrade existing programs. The stakes have never been higher, as demonstrated by last fall's attacks. The present economic climate demands that every department in an organization re-evaluate its needs and reorganize for maximum efficiency, and security is no exception. By drawing upon available resources, such as security consultants, professional associations and other peer networks, this challenging responsibility can be managed in an effective way that can reduce the potential for compromising an organization's security. Such responsible planning can also have the added benefit of convincing senior management of the need for essential program enhancements.

The imminent nature of the threat to national security, coupled with the bottom-line concerns of a recession, requires a very delicate balance on the part of security professionals, but it's one they cannot afford to tip.



The Lipman Report Editors