

April 15, 2003

Terrorist threat demands urgent action

Security survey demonstrates widespread complacency, need for focus on workplace protection

Engaged in two wars—the continuing battle against terrorism and now the military campaign in Iraq—the United States of America faces an unprecedented threat to its homeland. A heightened anxiety pervades U.S. society as Americans worry about further terrorist attacks in reprisal for the invasion of Iraq. This unease further exacerbates the chronic nervousness that has accompanied the downturn of the U.S. economy. Despite these mounting pressures, the majority of American businesses have taken relatively little action to strengthen their defenses. In fact, many organizations have responded only to fears for the bottom line, reducing security even below pre-September 11 levels in some cases.

This issue of The Lipman Report examines the results of a survey taken last month to assess Americans' attitudes toward safety and security against the backdrop of current world events. Commissioned by Guardsmark, LLC, and conducted by Penn, Schoen & Berland Associates, the study incorporates the input of 203 security professionals and 601 members of the general public who shared their perspectives on security both at home and in the workplace. The survey confirms that businesses throughout the United States have become complacent and remain unprepared to manage an assault of the magnitude experienced on September 11, 2001.

While recognizing that no security program can provide total immunity to either internal or external threats, this newsletter offers a wide range of security recommendations that can help organizations of any size protect themselves to the greatest extent possible.

Ongoing complacency

Conducted two weeks before the war with Iraq, the survey found that a majority of the American public and security professionals agreed that the companies they work for have become complacent about the importance of workplace security. Fifty-eight percent of security professionals and 66 percent of the general public indicate that workplace security has become too loose and relaxed, primarily because the United States has not experienced a recent terrorist attack.

The perceived consequences of this complacency are reflected in the finding that both the general public and security professionals overwhelmingly feel safer at home than in the workplace. In fact,

security professionals expressed greater confidence in their home safety by a margin of 8 to 1.

Although Americans believe the nation faces a significant risk of terrorist attack, few—just under one third—take very seriously a change in the government security warning system. A similarly low percentage believes that the color system is effective in communicating the current threat level. Not surprisingly, 69 percent of security professionals and 63 percent of the general public indicate that a change in the national security warning does not affect security policies and actions at their companies.

In fact, more than half of the general public report that their companies have taken no action to prepare for potential attacks over the next several weeks. These findings come at a time when 96 percent of the respondents agree that the nation faces a serious threat from terrorism, with 84 percent of security professionals sharing the view that the war with Iraq further increases this danger.

First Responders Task Force

Recognizing the need for immediate action, the Council on Foreign Relations recently announced the creation of a task force that will identify the most urgent steps required to improve first responders' capabilities in key U.S. cities. The First Responders Task Force will work with local officials and first responder professional associations to raise consciousness in Congress and around the country of the challenges faced by first responders. Other aspects of the team's mission include securing and distributing funds to local governments and assisting local and federal government agencies with general planning and organization.

The task force's goals include the following:

- Create a reliable three-year budget plan for first responders with counsel from experts and city government officials.
- Speed up distribution of funds to first responders by working with Congressional legislators.

(continued on next page)

Terrorist threat demands urgent action

Security survey demonstrates widespread complacency, need for focus on workplace protection

(continued from preceding page)

- Identify methods of expediting delivery of funds and equipment to first responders in the nation's primary target cities and seaports.
- Educate state and local governments and citizens on the urgency of the homeland security threat and the necessity for immediate remediation.

The task force will help address weaknesses in the public sector, but swift action is also required in the private sector.

Commitment from the top

To combat this complacency in the business community, chief executive officers, chief operating officers and other C-level executives need to take an active role in ensuring that their company's security needs are met. By taking the following steps, they will demonstrate the urgency of the security mission throughout the company:

- **Assess facility vulnerabilities.** Top management needs to ask what conditions currently exist that would contribute to a successful, devastating attack against the facility. This analysis should include not only clinical identification of weaknesses, but also a realistic assessment of risks. Every organization has a responsibility both to employees and to shareholders to minimize those vulnerabilities that present a viable threat.
- **Create an environment of cooperation and understanding.** Employees at every level in the company need to learn basic facts about war, terrorism threats and the overall security mission. This objective can be accomplished through internal seminars on safety and security. Such an initiative will communicate the importance of security and encourage employees to participate in the security effort, enabling them to recognize and report any suspicious objects or activities they may observe.
- **Evaluate the state of the security program.** To gain a thorough understanding of the company's commitment to security, a senior executive

should meet with the security director and discuss measures to enhance the security program. This frank discussion should examine recommendations that were made but rejected in previous years and determine their current relevance in light of the heightened threats now facing the nation.

- **Identify obstacles to the security mission.** Often, the authority to make security-related decisions rests not with senior management or the security department, but with other entities that may not consider the many factors involved in developing a sound program. Sometimes turf wars and emotional considerations may interfere with the implementation of security measures; in other cases, the individuals who purchase the security services may not be the ones held accountable for the program's effectiveness. The chief security officer must have access to senior management in case he or she encounters a serious problem that compromises the facility's safety and security.

Above all, those men and women responsible for managing an organization need to make a personal investment in the safety and security program. By making their interest known, senior executives influence departments and individual employees throughout the company to make security a priority, which can contribute not only to a safer workplace, but also to higher morale and productivity.

Elements of a successful program

No precautions can ensure complete protection from a terrorist attack or other catastrophic incident, but there are many actions that firms can take to minimize the impact of such an event.

Conduct a thorough risk assessment. Every organization needs to review and analyze the types of risks that employees could face. Potential threats could arise from a wide range of specific factors—including geographic location, industry issues and nature of occupation—as well as from general risks that can occur anywhere, such as crime and

workplace violence. Employing the services of a risk-assessment team will help ensure that the audit provides a full, accurate analysis. At the same time, companies must also implement and install the recommended safety and security measures. Failure to act on identified vulnerabilities can expose a company to legal liability.

Control risk with consistent solutions. Strict access control is critical to prevention. Gates, concrete barriers, and even trees and planters can strengthen perimeter control. Sensitive access points should be protected with trained security professionals. The following recommendations will help regulate access within the facility:

- Install durable locking hardware on all entrances and maintain strict control of keys and pass cards.
- Install closed-circuit television cameras at critical points throughout the facility.
- Maintain a log of all visitors by name, date, time and name of person being visited.
- Require visitors to present photo identification from a local, state or federal agency.
- Escort all visitors at all times.
- Reserve the right to inspect items entering and leaving the premises and post signs advising of this policy.

Special care should be taken to protect those areas that are susceptible to biological or chemical attacks, such as water supplies, food preparation areas, and heating, ventilation and air conditioning (HVAC) systems. The security and maintenance departments should know where to find and how to operate shut-off controls for the HVAC system, and the emergency response plan should designate a specific person to shut down the system in case of a suspected biological or chemical attack.

In addition, all incoming mail and packages need to be processed at a centralized, secure location according to the following guidelines:

- Inspect all incoming mail and packages.
- Never accept unexpected deliveries.
- Positively identify all delivery personnel.
- Develop strict times for receipt of deliveries.
- Document all deliveries by time, date and name of delivery service.
- Isolate any suspicious deliveries immediately.
- Distribute and display U.S. Postal Service information regarding suspicious packages (*e.g.*, foreign substances, excessive postage, poorly written or incorrect addresses, no return address).

Implement emergency preparedness plans. Every business, regardless of its size or nature, needs to develop and practice an emergency response plan that addresses acts of terror, as well as workplace violence and natural disasters. The plan should include detailed evacuation instructions that designate a specific meeting location where personnel gather after leaving the building. Having such a plan is inadequate, however, unless businesses communicate the specifics of the program to employees. These briefings can take place during regularly scheduled safety and security meetings. To ensure the effectiveness of the procedures, companies need to orchestrate frequent drills.

Additional emergency preparedness steps include the following:

- Back up electronic and paper files in a secure, off-site location.
- Assign responsibilities and identify successor personnel for essential tasks, such as evacuation, communication, fire safety and critical business operations.
- Maintain stores of basic supplies in the event that evacuation is not possible; these items can also support a skeleton staff remaining on-site.

(continued on next page)

Terrorist threat demands urgent action

Security survey demonstrates widespread complacency, need for focus on workplace protection

(continued from preceding page)

Screen employees. In many cases, the men and women inside an organization present an even greater threat than external forces because of their unique access. The use of “sleepers”—enemy agents who establish themselves in society until called to action—means that terrorist attacks could come from within. To reduce the internal threat, organizations should conduct a thorough screening of employment candidates that includes verification of:

- Legal work status, as permitted by law,
- Work history,
- Educational institutions and degrees earned,
- Professional accreditation, driving and criminal records,
- Credit history, as permitted by law,
- Personal references, and
- Military discharge status, when applicable.

Companies need to exercise similar precautions in selecting vendors as well, such as outside auditors, food service providers, temporary employees and janitorial services. These individuals often enjoy the same access to proprietary information as employees, but without the same integrity checks.

Maintain open communication. A primary element of a solid safety and security program is effective communication, which facilitates trust and cooperation. To begin, firms should raise employee awareness of potential risks such as workplace violence and terrorism, explaining to them that such dangers are real and convincing them to take security plans and precautions seriously. Companies then need to conduct employee seminars and publish bulletins that describe management’s efforts to counter those threats, while encouraging personnel to create a similar preparedness plan for their families. This last step will help reduce emotional stress in the event of an emergency. Providing a toll-free hot-

line or an electronic message board will allow employees to voice their concerns, express fears and provide information to management. Such communication can assist the security department in addressing vulnerabilities, while enhancing a firm’s ability to stifle rumors that could damage morale and productivity.

The tragic attacks of September 11, 2001, forever altered life in the United States of America, as its citizens learned to live under the specter of the homeland terrorist threat. The war in Iraq has further contributed to the sense of unease that troubles the nation, already compounded by anxieties over the economic recession. While many Americans agree that another attack will indeed occur, they remain equally convinced that terrorists will not strike their home or workplace. Consequently, a large number of U.S. businesses have allowed their security programs to fall behind, buckling to budgetary pressures.

The complacency that has settled upon the nation is not new; in fact, it inevitably appears any time an extended period elapses without a significant security event. But the al-Qaeda assaults of September 11 demonstrate that the stakes have been raised. In light of this dramatic wake-up call, those organizations that contribute to the success of a future attack through inaction will face a potential public backlash.

American businesses have a responsibility to their employees, their shareholders and their customers to protect their assets—human and material—against the modern terrorist threat. Only by embracing the security mission at every level can an organization survive the new war against the United States.



The Lipman Report Editors