

August 15, 2002

## Complacency compounds vulnerability to terrorism

Companies must balance financial concerns with protection, continuity

*In the aftermath of the September 11 terrorist attacks, many security directors believed that the tragedy would lend new urgency to their repeated requests to strengthen security operations. They believed the magnitude of the assaults would force organizations to reevaluate their commitment to protecting their employees and their facilities, and senior management would finally approve the proposals for increased funding, improved technology and additional security personnel.*

*As expected, many companies immediately expanded their uniformed security coverage and reviewed existing policies concerning such issues as personnel employment, crisis management and threat response. The heightened interest, however, proved short-lived with the passage of time. Despite a steady stream of public alerts, additional terror attacks failed to materialize, and a large number of organizations have once again adopted a "business-as-usual" approach to security, rationalizing that the chances of terrorists targeting their firm or their city were infinitesimally small. Sadly, many of the occupants of the World Trade Center or the Pentagon would have made the same claim on September 10, 2001.*

*Participants at a security conference last month asked a well-regarded terrorism expert whether he believed that the United States had inflicted sufficient damage to the al Qaeda network to prevent future attacks on domestic soil. Absolutely not, he replied. Studying the pattern of previous assaults—including the blasts at the U.S. embassies in Africa, the suicide bombing of the U.S.S. Cole and last fall's attacks involving four hijacked airliners—reveals that al Qaeda typically executes major acts of terror 10 to 14 months apart. In other words, the United States could be a looming target for another terrorist event. Unfortunately, as indicated by numerous media reports, the nation has made limited progress over the last 11 months in improving its defenses against another attack of September 11 magnitude.*

### Bottom line: Top concern

History has demonstrated on countless occasions that security awareness rises to fever pitch following a breach, only to return to its previous position as an unnecessary expense when memories of the incident fade. The April 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City and the shootings at the U.S. Capitol in July 1998 offer but two recent, high-profile examples.

To many people, the extent of the losses sustained on September 11 should have ensured that security would remain a paramount concern for years to come. The continued slowdown of the U.S. economy, however, has proven otherwise.

In spite of continued concern about a future terrorist attack, many companies have returned their focus to the bottom line. Some organizations are outsourcing their security departments to realize cost savings, but may sacrifice quality by overemphasizing price in the decision process. In other cases, those responsible for the security function rationalize that they have no need to upgrade their security program. After all, the chances of their facility being targeted by terrorists are slim. This "it-won't-happen-to-me" attitude ignores the fact that many businesses largely came to a standstill in the days following September 11 as the nation, reeling from shock, attempted to piece together how and why the tragedy occurred. The shutdown of air travel and some overnight delivery services—in addition to the emotional and psychological effects on American workers from coast to coast—negatively impacted countless businesses, regardless of their geographic proximity to the attacks. Even now, corporate America continues to suffer financially from the impact of that day as insurance premiums skyrocket, forcing companies everywhere to help the insurance industry recoup the astronomical losses incurred from the strikes.

Nevertheless, a surprisingly large number of organizations continue to ignore the need to strengthen their security programs. Six weeks into last fall's anthrax attacks, an international trade association surveyed its members to learn how their firms were responding to the anthrax problem. Of 42 companies surveyed, only 29 had changed the screening process for incoming mail and packages since learning of the anthrax attacks. Thirty-six conducted training for mail handling personnel, while four added extra equipment and one considered restricting mail operations to a single location to minimize potential employee exposure.

(continued on next page)

---

## Complacency compounds vulnerability to terrorism

Companies must balance financial concerns with protection, continuity

(continued from preceding page)

Thirty-eight firms revealed that they planned to address the anthrax threat, primarily through communication. During this time—the height of the anthrax contamination—only 27 organizations made gloves available to mailroom personnel as an option. Even though American businesses were under biological siege, approximately one-third of the organizations surveyed had failed to upgrade their security measures. In the post-September 11 world, such inaction is unwarranted.

### Foreseeability and due diligence

Just as organizations have a financial obligation to their shareholders to increase profitability and to ensure business continuity, they also have an obligation to the shareholders, employees, visitors and vendors to provide a safe working environment. In determining what preventive measures to take, facility managers and security directors must keep in mind the concept of “foreseeability”: What types of risks might an employee reasonably face? Lighting one end of a parking lot and not the other, for example, could constitute negligence if the dangers of inadequate lighting were recognized but not consistently acted upon. Completely ignoring a hazard to avoid penalties for improper prevention could also result in corporate liability. Real estate management firms face an especially challenging situation as they often hold the critical responsibility of protecting tenants, visitors and vendor employees on their properties. Companies in every industry, however, must assess their security needs responsibly, enlisting professional assistance if necessary, and minimize vulnerabilities.

Simply identifying dangers and turning the security function over to a third party does not absolve an organization of the duty to protect individuals on company property. A firm must exercise due diligence in addressing occupational hazards. Once a problem and solution have been identified, the company needs to implement the solution without compromising quality. Safety and security are two areas in which firms can either “pay now”

or “pay later,” and the latter option invariably costs much more as it typically involves expenses such as legal fees, liability damages, increased government regulation or enforcement, public relations bills and, in extreme cases, costs associated with business interruption and grief counseling.

One of the nation’s leading legal minds once observed that “accidents don’t just happen.” There is always evidence that someone cut corners somewhere. When shortcuts are taken in the business world, the results are often disastrous. Occasionally, flawed products are released in the marketplace because companies do not want to invest the necessary expense to correct a problem that only occurs under special conditions. Some firms trust an outside organization to take care of a situation for them without ensuring that the third party takes the necessary steps to fulfill that duty responsibly. Many examples of this type of “buck-passing” can be found in the contract security industry, with the customer learning belatedly of its own culpability when incidents occur.

Client organizations may ultimately be held responsible if a contractor is found negligent. Companies must perform due diligence in ensuring that the firm selected to provide service will do so in a responsible manner. Earlier this year, the Supreme Court of Ohio ruled that a company was “vicariously liable” for an injury to a third party at the hands of a contract security guard. The firm had hired a private security contractor to provide uniformed guard services, and one of the guards shot and killed a man during his shift. Even though the guard company had already settled with the plaintiff, the client was still ruled liable. The fact that some of the guards carried firearms—known to the client, although not specified in the contract—qualified the assignment as “inherently dangerous work.” Consequently, the court found that the employer may delegate the work to a contractor but could not delegate the duty of due care and was therefore responsible in this instance of contractor negligence resulting in a breach of duty. The decision marked a departure from the general

rule that a business owner is not responsible for the negligent acts of an independent contractor.

In many cases, foreseeability and due diligence simply involve common sense. What security risks may a company reasonably expect to face? How can these risks be mitigated? The new realities after September 11, however, demand that organizations exercise more vigilance in responding to these questions than they might have one year earlier. Today, the act of hijacking a commercial airliner and crashing it into a high-rise building constitutes a viable concern in certain metropolitan areas.

### Meeting the challenge

The nation as a whole has become more security conscious during the last 11 months. Ironically, however, those responsible for implementing security initiatives in corporate America face tremendous temptation to cut corners in light of a weak economy and pressure to improve profits. Even without the threat of terrorist attacks, the uncertain economy and trend toward downsizing would be enough to warrant a closer look at increasing security. Factoring in the war on terror, the issue of security rises to an even greater level of urgency.

Organizations cannot afford to bolster their bottom line by allowing their defenses to slip, hoping that the next assault will strike somewhere else. Even discounting the critical nature of business continuity, every firm has an ethical and legal responsibility to assess its risk level and to take appropriate action to safeguard its human resources.

The following elements are critical in meeting the security challenges of today:

- **Increased awareness.** Last fall's terror attacks demonstrated the catastrophic results of American complacency. U.S. businesses cannot assume that they will not become victims of terror based on industry or geographic location. While "trophy" targets are highly desirable, terrorists' primary goal is to inflict the greatest amount of damage possible. Following the strikes on the World Trade Center and the

Pentagon, the nation has increased security around monuments and other culturally significant structures, which has the added, though unintentional, effect of encouraging terrorists to seek easier marks elsewhere. Corporate security departments cannot discount the severity of the terrorist threat without risking potentially significant liability in the event of an attack.

- **Security audits.** Effectively meeting an organization's security needs often requires a professional audit, performed by experts skilled in analyzing a facility, identifying vulnerabilities and developing solutions. When asked to conduct an audit, security directors often consult with a peer, developing a plan based upon an audit prepared for a different organization with different needs. Because each company has unique needs based upon such widely varying factors as industry and culture, firms cannot use a cookie-cutter solution. Instead, security managers must bring in experts who can assist in developing a program specifically tailored to their individual needs. Many security companies are willing to provide basic consulting services at no cost, with more in-depth surveys available on a fee basis. Security directors or facility managers charged with completing a security audit can contact their peers for references of companies or individuals who offer such services. Organizations that do not seek expert advice from security professionals to determine their needs deprive the entire corporation—including shareholders, employees and visitors—of information critical in protecting lives.
- **Diligence in selection.** Never before has screening played a more important role in security. Companies must now contend with the danger of "sleepers"—terrorist agents who establish themselves in society until summoned to action—in addition to traditional employment concerns, such as employee theft and workplace drug abuse. High-turnover positions in organizations with lax employment standards offer

(continued on next page)

## Complacency compounds vulnerability to terrorism

Companies must balance financial concerns with protection, continuity

(continued from preceding page)

excellent opportunities for these agents of terror to embed themselves within a firm while they await their assignment. On a more basic level, foreseeability and due diligence require careful screening to help prevent acts of workplace violence and corporate espionage. The examples of Aldrich Ames in the Central Intelligence Agency and Robert Hanssen of the Federal Bureau of Investigation demonstrate the need for periodic assessments after employment for personnel in especially sensitive positions. Failing to exercise prudence in selecting business partners—such as external auditors, food services, telecommunication providers, security services and building maintenance—can also have disastrous repercussions on a firm if the vendor conducts itself irresponsibly.

- **Open communication.** Companies must integrate security into every facet of their business operations to adequately protect their assets. Open communication is critical in minimizing security lapses. As mentioned above, security should work with the human resources department to ensure that all employees and vendors pass a rigorous background examination, thereby limiting the internal threat. Fostering open communication lines between security and the mailroom and housecleaning services likewise strengthens an organization's defenses, creating an internal intelligence network similar to the federal program currently in the works, whereby employees in a wide range of service sectors can contact the Office of Homeland Security through a direct hotline.
- **Technological efficiency.** The increased security threat of today has convinced many firms to consider investing in sophisticated security technology, such as biometric access control systems and infrared intrusion monitors. Too many companies view these high-tech solutions as a replacement for their security teams, when they actually supplement the human element of security. When used effectively, these

devices can reduce the number of security officers required for coverage; they also free security personnel to make more effective use of their time, fortifying security operations without increasing the size of the workforce.

*Almost one year after the terrorist strikes that toppled the World Trade Center towers, the United States continues to wait, warily, for the next major attack. Security remains a primary concern for most Americans. Oddly enough, fears about safety and security are taking a back seat in many U.S. businesses as they grapple with the pressures of the turbulent economy and meeting shareholder expectations. Many security directors are being pushed out of the operational cycle as companies search for less expensive ways to fulfill their obligations while raising the bottom line. Complacency has settled in, lulled by the apparent inaction of al Qaeda and overshadowed by immediate financial concerns.*

*Regardless of current economic conditions, organizations must continue to ensure the safety and security of their employees and visitors, planning their initiatives while implementing the principles of foreseeability and due diligence. The repercussions of negligence would jar any chief executive or chief operating officer who learned belatedly that a manager in any of a variety of fields—including purchasing, accounting, facility management, human resources, property management and security—jeopardized the future of the corporation for the sake of trimming a few thousand dollars from the budget. The United States remains a prime target for another terrorist assault, and rising crime and workplace violence still pose a grave, immediate threat. Companies must act now to protect their assets—before a catastrophic breach exacts a toll greater than they can bear.*



The Lipman Report Editors