

July 15, 2000

‘Culture of indifference’ endangers security

Breakdowns at government agencies should alert corporations to their own risk

Recent security lapses at government agencies have raised concern.

- *An undercover team flashing fake badges penetrated security at 19 federal buildings, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).*
- *A laptop computer containing highly classified information disappeared from the U.S. Department of State. Last year, an electronic listening device was found in a conference room.*
- *At Los Alamos National Laboratory in New Mexico, computer hard drives containing highly sensitive nuclear weapons data disappeared from a vault. After several weeks, the drives were found behind a copying machine near the vault. An investigation continues.*
- *Also at Los Alamos, a former scientist is awaiting trial on charges of transferring secret material to an unsecured computer and portable tapes, some of which are missing.*
- *A former CIA director kept government secrets on an unsecured home computer connected to the Internet.*
- *The problem extends to Great Britain, where two government laptops with secret information were stolen recently.*

Officials promise to crack down on security. Already, the Department of Energy has announced its decision to strip the University of California of its security responsibilities at Los Alamos and Lawrence Livermore National Laboratories because of the security lapses. Still, a disturbing question remains: If governmental agencies are vulnerable, what about corporate America? Corporations face some of the same security problems. Even a single incident of the magnitude cited above can destroy the confidence of customers and shareholders alike. Security directors need to scrutinize their existing programs carefully to reduce the likelihood of such a disaster.

Fake badges and credentials

The story made headlines in May. Posing as plainclothes law enforcement officers, a General Accounting Office (GAO) undercover team gained entrance to 19 federal buildings, including the FBI, the U.S. Department of Justice, the State Department, the Pentagon and the CIA. The agents used credentials made with widely avail-

able computer programs and badges purchased over the Internet or at police supply stores. Though they declared they were armed and were carrying briefcases, the undercover agents were never searched. In some cases, they were allowed to walk about unescorted. They were able to enter the private suites of Cabinet officers or department heads. They parked and walked away from a rental van in the courtyard at the Justice Department without being inspected.

Reasons for the breakdown

What is causing these breakdowns in governmental security? A former director of the CIA blames three factors. First, there has been a post-Cold War relaxation; protecting secrets from foreign enemies doesn't seem as important. Second, technology has made it faster and easier to steal large amounts of data; a single computer disk can hold a trove of secrets. Finally, there appears to be a lack of concern about security at the highest levels.

Many members of the U.S. Senate are very concerned about the widespread incidence of security lapses at the nation's most sensitive facilities. One significant problem cited, particularly in the case of the breaches at Los Alamos, is a "culture of indifference" about security among some laboratory scientists. Experts, however, warn against "overclassification" or stamping everything top-secret. That blurs the line between the trivial and the important. Security should be concentrated on highly-sensitive material, such as the hard drives that temporarily disappeared.

Government representatives also blame a "cultural failing" at Los Alamos, indicating that the cavalier attitude toward security has been made worse by poor management. For instance, a former Secretary of Energy banned color-coded identification badges because they "divided" employees. The different colors had allowed security officers to see at a glance who had the highest security clearance.

(continued on next page)

‘Culture of indifference’ endangers security

Breakdowns at government agencies should alert corporations to their own risk

(continued from preceding page)

Similarly, the private sector contends with numerous forces that can ultimately undermine security. Budgetary pressures, for instance, often have a negative impact as companies cut security funding to control costs. But such narrow thinking ignores the cost of lost inventory or stolen secrets or violent episodes. Successful management takes a broader view. Spending on security is an investment that pays off in higher productivity.

While some companies demand high levels of security, others—especially those that deal with the public—will sometimes limit security levels to promote accessibility. No company wants to harass customers or visitors. When security becomes a burden, the tendency will be to circumvent it. A well-planned security program, however, can be both effective and low-profile.

Corporations, like the government, have human, material, and intellectual assets to protect. Corporations, like the government, can fall victim to espionage or violence or theft. When it comes to security, a relaxed attitude can be costly.

Consequences of inadequate security

The cost of industrial espionage is staggering. In a recent survey, nearly 50 percent of the Fortune 1000 and the 300 Fastest Growing companies who responded reported suspected intellectual property losses but were unable to document them. Potential losses from intellectual property theft for U.S.-based companies may exceed \$250 billion annually. In 1999, within the Fortune 1000 alone, losses from proprietary information theft totaled \$45 billion, according to another study.

Targeted information includes customer lists, sales figures, research and development information, and manufacturing and marketing plans, anything a competitor could use to gain an advantage. According to the survey, the highest risk groups include former employees, temporary staff, current employees, suppliers and con-

sultants. High-technology companies are most frequently targeted, followed by manufacturing and service industries.

Only 63 percent of the Fortune 1000 and 300 Fastest Growing companies surveyed have formal programs to safeguard proprietary information. Of that group, only 51 percent think the security programs have been uniformly implemented throughout the company.

Economic espionage also presents a significant threat as many foreign countries try to acquire critical technologies for military and commercial application. The United States is a tempting target because it leads in many cutting-edge technical and scientific fields and has an open society where much information is legally available. Foreign intelligence services are expanding their focus from military secrets to collecting economic intelligence.

Researchers under contract to the FBI developed a way to assess loss from theft of intellectual property. In one case, a foreign competitor stole secrets from a U.S. corporation and, as a result, captured the market. The researchers calculated \$600 million in lost sales, plus the loss of 2,600 jobs.

In addition to the loss of intellectual assets, the theft of physical property or inventory continues to plague companies. According to the U.S. Chamber of Commerce, employee theft costs employers \$40 billion a year, and theft causes one-third of all business bankruptcies.

Likewise, workplace violence exacts a tremendous annual toll on corporate America. According to the U.S. Justice Department’s Bureau of Justice Statistics, employees experience about 2 million violent incidents each year. One out of every six violent crimes occurs in the workplace. In the event of a preventable violent episode, companies must worry about negligence lawsuits. Awards to plaintiffs keep growing. A company that has tried to identify risks and has taken steps to minimize them will be better able to defend itself from security-related lawsuits.

How can corporate America protect itself?

Review security needs. A company that decides to use an outside security provider should choose with care. Insist on a security program tailored to the company's specific needs instead of a "one-size-fits-all" approach. The company should spell out its expectations, and the provider should document how it will meet them. Once security procedures are in place, periodically review and update them. According to a recent survey of 4,900 members of the Society for Human Resource Management, 84 percent of those responding had not conducted a security assessment in more than three years.

Top-down commitment. According to the ex-CIA chief cited above, concern at the top is the most important factor in strong security. According to another former CIA director, who lost his security clearance for drafting highly classified documents on his home computer, "The director of central intelligence is not above the rules."

A company's leaders must practice what they preach. If the boss waves friends through an entry point or fails to wear an ID badge, a signal is sent about what is important. "What is sauce for the goose, must be sauce for the gander," says a former FBI official about consistency. If senior management follows the rules, the message will pass down the ranks. The message should be reinforced with regular reminders.

Change the culture. Some security experts blamed lapses at the State Department on a diplomatic culture that valued openness and access; security took a back seat. Similarly, at Los Alamos, those with access to the vault where the hard drives were stored did not have to sign out when removing materials. "I don't care how skilled you are as a diplomat," Secretary of State Madeleine Albright told colleagues, "if you are not professional about security, you are a failure." This warning could also apply to the corporate world.

Leaders can change the corporate culture, by example and by clear directives. Be pro-active. Change *before* a serious security breach forces the company to change.

Training and awareness. From the moment an employee is hired, a company should stress the importance of security. During orientation, if a company spends 30 seconds on security issues, the perception will be that it is not important. But if simple practices—wearing ID badges, escorting visitors, reporting suspicious activities—are part of the corporate environment, employees understand and participate. Further, there should be ongoing education to remind employees of security procedures and of whom to contact if a violation occurs. In some of the government security breakdowns, unescorted visitors roamed without challenge into sensitive areas; employees accepted their presence because they had cleared the initial checkpoint. But a company that maintains an ongoing commitment to security produces employees who will be alert to possible violations.

In the GAO's undercover operation against federal buildings, the fake badges created a "halo effect" that disarmed the normal security procedures. Badges and suits made the undercover agents the good guys, so there was no need to check further. But a trained officer will not be distracted and will politely but firmly insist on verifying that visitors are who they claim to be. And there must be sanctions when negligence causes security breaches.

Demand loyalty from a security provider. The need for awareness must also extend to this important partner, who should know and understand a company's competitors. The security company must erect a "Chinese Wall" that prevents officers who worked for one client from being assigned to a competitor. Such precautions can protect the confidentiality of customers' trade secrets against both deliberate and accidental information transmission.

(continued on next page)

‘Culture of indifference’ endangers security

Breakdowns at government agencies should alert corporations to their own risk

(continued from preceding page)

Control access. A building should have a minimal number of entry points, each attended by a security officer or receptionist. All employees should be required to present an identification card; many companies require that the ID card be worn at all times. When an employee resigns or is terminated, the ID card must be turned in on the last day. Computer access should be revoked.

Screen visitors. At the reception point, the attendant should verify that each visitor has an appointment or other legitimate reason to be there. Visitors should be issued a temporary ID badge and should be escorted to their destination. In the penetration of federal buildings, visitors were admitted without appointments and sometimes without escorts.

One former FBI official who is now a security executive notes a disturbing trend of allowing delivery people to carry a package to the recipient instead of dropping it off at a reception area. A familiar uniform can cause the security team to let down its guard.

Computer security. The computer revolution has created some new security problems. Last month, *The Lipman Report* discussed how to protect electronic assets. The most sensitive data and equipment should be the focus of security. Essential systems should be in a locked room with limited, card-key access. Sophisticated technology can go beyond simple password protection to prevent unauthorized system access.

Laptop computers are especially vulnerable. Never leave a laptop unattended; where possible, lock it up. Some thieves specialize in airport thefts. At security checkpoints, one thief screens or obstructs the laptop owner, while a partner grabs the laptop when it emerges on the conveyor belt. Business travelers overseas should be especially alert. Foreign intelligence services pay national airline employees or hotel desk clerks to watch for Americans carrying

laptops. Carelessness could cost you your client list, your strategic plans and the benefits of years of research and development.

In the government or in the corporate world, good security is still a matter of following the rules already in place, rather than inventing new ones. A commitment to security requires constant vigilance. Are security procedures in place? Are employees trained in the procedures? Are the procedures enforced?

A former FBI official offers the example of a dent in a car. At first, it stands out. If you don't repair it, however, you soon stop noticing it. Similarly, a company that overlooks security breaches opens the door to trouble.

Organizations must take a proactive approach to security, incorporating preventive measures in the corporate culture. Companies simply cannot afford to experience breaches such as those reported within some of the government's innermost sanctums. Even one publicized incident like the laptop thefts at the State Department could devastate public and shareholders' faith in an organization, raising serious questions regarding the commitment to asset protection.

Now, before an incident occurs, is the time to focus on the security procedures followed throughout an organization—from the most remote location to the corporate headquarters. What vulnerabilities exist? Which policies and practices require updating? Security directors need to dust off and re-examine those recommendations that were deferred or rejected in previous months or years. Any pending suggestions that will eliminate a vulnerability should be implemented. Those responsible for security may not receive the opportunity to make the necessary changes after the breach.



The Lipman Report Editors