

June 15, 2000

Information security requires team-based approach

State-of-the-art information systems demand traditional security measures

The Denial of Service (DoS) attacks that crippled several Internet giants in February delivered a sobering wake-up call to the burgeoning world of electronic commerce. Just as security experts had predicted, hackers developed an attack tool against which no sure-fire defense exists. Technological fears once again became reality last month with the arrival of the "Love Bug" virus, which infected hundreds of thousands of computers worldwide within a matter of hours. Incidents such as these have reinforced the need for technical security measures, such as firewalls and virus protection programs. At the same time, the focus on computer security technology has overshadowed the basic need for physical computer security.

Recent thefts of government laptops have revealed the consequences of ignoring elementary security principles. In March, a British Security Service worker lost a laptop computer at a mass-transit ticket station when he set it down to assist a passer-by. The computer contained sensitive information on Northern Ireland. Two months earlier, a laptop containing files on weapons proliferation disappeared from an intelligence office in the U.S. State Department. A department-wide inventory in May uncovered the absence of at least two additional laptops that did not contain critical files.

When it comes to information security, too many organizations dedicate their resources almost exclusively to technical and logical security measures. Technical security includes uninterruptible power sources (UPS), temperature and humidity controls, and other means of preventing an unwanted system shutdown. Logical techniques, which protect the integrity and security of business functions, include back-up procedures, anti-virus programs and firewalls. These precautions, however, will scarcely prove useful if a person can simply walk in and steal the network server. Companies need to recognize that the confidential information once locked away in file cabinets is now available for perusal at many network terminals. Organizations must consider physical security when developing or reviewing the protection of their information technology (IT) systems.

Costs of computer crime

The world's growing dependence on computers places more and more at stake when disaster strikes, whether in the form of data loss, hacker attacks, industrial espionage or simple theft. Experts

estimate the worldwide damage from the "Love Bug" at up to \$10 billion. The attack demonstrates that the stunning financial losses of the past may only hint at what organizations will experience in the future if they do not dedicate the appropriate resources to their computer security programs.

A West Coast-based organization of information security professionals recently published the results of its fifth-annual "Computer Crime and Security Survey," performed in conjunction with the Federal Bureau of Investigation (FBI). According to the 2000 survey, 90 percent of the 643 respondents detected computer security breaches within the last 12 months, and 74 percent acknowledged financial losses due to computer breaches. Forty-two percent of the respondents quantified their combined financial losses at more than \$265 million in 1999—more than twice the average total losses reported over the last three years of \$120 million. In fact, financial losses in four separate categories exceeded the combined total of the three previous years, reflecting both greater awareness of computer security issues and the increasing profitability of computer crime. Sixty-one respondents in 1999, for instance, quantified losses of \$27 million resulting from sabotage of data or networks, whereas the combined loss from sabotage during the previous years totaled less than \$11 million.

These figures represent a mere *fraction* of the actual losses incurred. Many organizations victimized by computer crime still refuse to discuss such violations with law enforcement, although the situation has improved in recent years. "Most companies who are subject to data theft go to great lengths to avoid publicity about their loss because such information can be viewed as highly damaging to a company's reputation with its shareholders, customers and employees," said one computer expert. This reticence consequently makes it difficult to gain an accurate picture of the true scope of computer crime.

(continued on next page)

Information security requires team-based approach

State-of-the-art information systems demand traditional security measures

(continued from preceding page)

'Incidents of opportunity'

Widespread media coverage of recent computer attacks has succeeded in raising awareness of the need for greater IT security. Yet, in the rush to acquire the latest technologies to thwart hacker and virus attacks, many organizations forget about basic security precautions.

If an employee possesses a highly sensitive report, he or she will usually exercise special care to guard its confidentiality, such as securing it behind a locked door or keeping it upon his or her person. Suppose the report exists in electronic format on the employee's computer. That same individual will think nothing of leaving his or her desk to take a restroom or lunch break without logging off the computer. Suddenly, the information is available to anyone who happens to be in the right place at the right time. This trusting mindset also contributes to the thriving business of laptop larceny; too many notebook computer users treat their \$2,000 to \$5,000 machines as if they were clipboards or calculators. "Most thefts are incidents of opportunity," said one security executive. "Somebody leaves a computer lying around, and someone else will walk by and grab it."

Even before a company begins determining the best technological defenses for its networks, management needs to consider the physical protection of those systems. One small business owner received an abrupt wake-up call last spring when a thief broke into his apartment and stole his home entertainment equipment. Relieved that the burglar had not found his office, which contained more than \$100,000 in computer hardware, he promptly invested in stronger security measures: bars on the windows and a 24-hour security monitoring service. Overlooking physical security within a corporation can render a multimillion-dollar investment in information security completely useless.

To further reduce the opportunities for loss, companies must incorporate employee education

into their security program; otherwise, an organization's personnel can unwittingly aid an intruder in circumventing security measures. Computer criminals, for instance, are quite savvy at social engineering, in which they establish a certain level of trust with an employee to gain necessary information or access. When a company develops security processes, management needs to ensure that all employees receive adequate education regarding those procedures, as well as their roles in reporting any infractions.

Safeguarding electronic assets

The burgeoning arena of computer crime requires close cooperation between the corporate security director and the manager of information systems. Although the security executive may not know the best way to thwart an outside hacker attack, for instance, he or she can protect the company's systems from old-fashioned theft or vandalism.

A basic principle of physical security uses the "concentric circles" model. This model starts with the security of the organization's perimeter, progressing to specific areas or rooms within the buildings, and finally, individual pieces of property. As the circles grow smaller, the security measures should grow stricter, with the tightest security guarding the company's most sensitive assets. When applied to information security, this principle requires a thorough evaluation of the various types of data within an organization. Classification enables an organization to focus its security resources. Data of low sensitivity should be maintained on separate servers from information of high sensitivity, with the latter systems protected by more sophisticated security measures.

- *Develop and enforce a written policy that addresses the physical security of information systems.* The policy should reflect the views and positions of senior management on information security, backed by unequivocal support. Management's attitude toward the policy will influence the rest of the organization,

determining its effectiveness. The document should state clear directions regarding expectations, protection requirements and enforceable consequences for non-compliance. In addition, the policy should specify different security procedures for workers and computer systems of varying sensitivity levels. Not only will employees not comply with security requirements viewed as overly cumbersome, but treating low-sensitivity data as confidential will also diminish the credibility of the guidelines protecting truly sensitive information.

- *Limit access to network servers and other critical systems.* The location of a network server or mainframe is an important element of an overall information security program. Companies need to isolate these essential systems in a locked room under closed-circuit television surveillance at all times. The room should require card reader access for both entry and exit, and accessibility should be restricted to the network administrator and his or her backup. Organizations can further protect their systems by placing them in a special cabinet that will guard computers against a wide range of dangerous elements, including fire, humidity, magnetic influences, vandalism, theft and illegal access. Such computer “safes” can be equipped with redundant ventilation fans or air conditioning units, and they can be connected to a UPS for added protection.

Organizations with an extensive investment in computer equipment may elect to place their systems in a room-sized protective environment built into the existing building. These special rooms have a microprocessor link to the main building’s environmental services and protection systems. Catastrophic events like fires automatically shut down the computer systems inside the room, preventing information loss.

- *Where warranted, use advanced security technologies to prevent unauthorized system access.* Traditional password protection relies

upon the user for effectiveness. If an employee selects a password that can be easily guessed or posts it on his or her computer as a reminder, the password protection will not provide much of a deterrent. Organizations should consider using more sophisticated technologies to restrict access to sensitive data. Examples of such devices include smart cards, remote identification devices and random number generators. Smart cards contain chips identifying the user and must be inserted into a reader to access the computer. As employees leave their workstations, they should remove the card, which will lock down the computer without losing any of their work. Remote identification devices rely upon proximity. Such tools detect the presence of the user; if the employee walks away from the computer with the device, the workstation will lock until he or she returns. Random number generators reinforce password protection but, unlike smart cards and remote identification devices, do not secure workstations when users leave. These devices generate random numerical passwords, which are used in conjunction with an employee’s personal identification number to access a computer.

As with most other forms of security, however, these access keys are only effective when supported by a sound, enforceable policy. A remote identification device that a user leaves on his or her desk does not offer protection against unauthorized access—neither does a smart card left inside the reader. A random number generator with its secret code printed on it is no security at all and provides an opportunity for theft or loss.

- *Isolate and destroy any discarded data storage media.* Improper disposal of decommissioned servers can pose a significant danger, resulting in the theft of proprietary data. When a company retires a computer system, the IT department should remove the storage media and keep it in a secured location until it is erased and destroyed.

(continued on next page)

Information security requires team-based approach

State-of-the-art information systems demand traditional security measures

(continued from preceding page)

Several techniques exist for safely and effectively disposing of magnetic media. Some companies manufacture devices that produce strong magnetic fields capable of wiping disk drives and tapes. An inexpensive alternative involves physically destroying the storage media. Incineration does not present a viable disposal option due to the carcinogenic chemicals released by the magnetic media.

- *Secure hardware against intrusion and theft.* The high-tech nature of information security sometimes causes organizations to overlook the low-tech security precautions. Sophisticated access control devices like smart cards and remote identification devices can prevent an intruder from using an unattended computer terminal, but they will not stop anyone from removing the hard drive and accessing the information from another computer. Many companies offer inexpensive, effective security devices to thwart the physical theft of hardware, including alarms, locks, tamper-proof screws, anchors and cables.

Laptop computers are especially vulnerable to theft and require special attention whenever left unattended. According to the nation's largest insurer of laptops and other computers, its clients reported 319,000 laptop computer thefts in 1999, representing more than \$800 million in losses. When traveling, laptop users should maintain control of the computer at all times. Business travelers need to either store the computer in the hotel safe or use a locking device to secure it to a stationary object. Users should never leave a laptop unattended in plain view: in the office, secure the computer in a locked cabinet; at home, lock it away beyond the view of the windows; in the car, stow it in the trunk. As an additional protective measure, experts recommend placing company identification information on the computer either with an engraver or with an ultraviolet marking pen.

Information written with the latter is visible only when viewed under an ultraviolet light. Bar codes can provide a subtle method of identification, and organizations can also invest in an identification system that attaches the owner's information to the computer on a metal plate. Removal of the plate leaves an indelible mark on the computer, identifying it as stolen.

Employees must take similar precautions to protect cellular telephones and personal digital assistants (PDAs) and other handheld computers. These tools may contain sensitive information that could present a significant security risk to individuals and organizations alike if allowed to fall into the wrong hands. In addition to exercising vigilance, users of these devices need to use password protection and encryption to safeguard the confidential information programmed within.

Ironically, the rapid rate of technological advancement sometimes obscures the need for elementary security measures. The omission of these basic precautions, however, can cancel out the most sophisticated security tools. For this reason, organizations need to take a team-based approach to information security, coordinating the efforts of the physical security team with those of the IT department through continuous communication and review. This approach will ensure that all aspects of information security are considered, which will reduce the opportunities for mayhem. Addressing only the technical and logical aspects of the security equation provides an illusion of security that leaves a company vulnerable to disaster. With the stakes of computer crime constantly rising, no organization can afford such a risk.



The Lipman Report Editors