

December 15, 1998

Cybercrime Threatens Billions of Assets

Federal agencies bring much needed focus to escalating problem

Corporate America is spending an estimated \$6 billion annually on technology to protect information systems against hackers, crackers and employees who sabotage computers and steal proprietary information.

Despite the expense, companies continue to lose millions of dollars worth of technology, data and proprietary information to unauthorized computer users. A recent survey of more than 4,000 information technology managers showed computer intrusions were up sixfold from the previous year affecting 38 percent of respondents.

Experts say the real problem isn't hardware or software. Hackers, industrial spies and dishonest employees will raid any company computer system where technological protections are not part of a realistic security plan.

Past issues of The Lipman Report on computer security have discussed laptop theft, employee sabotage, hacker intrusions and national security problems. This issue suggests basic ways to defend the company computer network.

An Expensive Proposition

According to the FBI official who serves as the head of the National Infrastructure Protection Center, computer attacks have reached epidemic proportions. The figures bear out his alarm. The Computer Emergency Response Team (CERT) at Carnegie Mellon University, which has an internationally renowned engineering and computer science program, reports 2,490 incidents in the three-quarters of 1998, compared to 2,134 in all 1997. Developed in 1988 with funds from the Defense Advanced Research Projects Agency, CERT has responded to more than 14,000 security breaches at 200,000 sites at the Department of Defense, other federal agencies and the private sector. An annual survey of businesses conducted in cooperation with the FBI put reported losses from intrusion at \$136.8 million.

Experts conclude the cost is much higher. A Massachusetts research firm recently estimated the damage a computer intruder could do if \$1,000 was stolen from each of 1,000 bank accounts. The firm concluded that in addition to the \$1 million lost, a bank would incur a total of \$105.1 million in related expenses. These expenses

ranged from \$96 million spent on various aspects of increased computer security, lost information and network down time to \$1 million for an emergency audit of 250,000 accounts in search of more discrepancies.

Considering what is at stake, most companies should be employing strong security measures. Yet reports show many firms fail to practice information security fundamentals. For example, a San Francisco-based association of information security professionals claims that a walk around a typical office after hours would reveal 90 to 95 percent non-compliance with basic computer security. Furthermore, a recent survey by a national computer magazine found only 55 percent of U.S. companies responding in 1998 even monitor for security threats.

Such a reaction to the problem could be construed as ignoring the problem in hopes it will go away. However, a former FBI agent charged with protecting the bureau's information systems said he senses that businesses have misunderstood how to reduce their exposure to intrusion. Some companies believe that, if they can't afford highly technological equipment, they are doomed to be attacked. A more accurate assessment is that taking basic precautions can protect information assets against all but the most sophisticated intruder, he said.

Back to Basics

Some risk of intrusion is inherent in the open architectural design of computer networking and Internet connectivity. However, security managers can help assess the risk of computer breaches by identifying vulnerable areas and implementing basic security measures.

The top computer security issues—which account for 40 percent of network failures—include: inadequate implementation of technology; poor or non-existent company computer policies; internal data destruction; physical security breaches; and poor physical access controls.

(continued on next page)

Cybercrime Threatens Billions of Assets

Federal agencies bring much needed focus to escalating problem

(continued from preceding page)

Experts agree that a necessary first step in addressing these issues is an information protection plan that incorporates sound security practices and technology. Such a plan should be part of the company's security policy, fit into company business objectives, and include a cost/risk analysis. Balancing the risks and cost of intrusion against the expense of protection is a basic consideration. One major computer corporation recently decided maximum cyberspace security was more expensive than the risk of proprietary information theft. This corporation valued the freedom to communicate electronically more than a high level of security and credits this decision with helping cut its product development cycle in half.

In drawing up the overall plan, senior management and security managers must take visible leadership roles. Managers overseeing the computer policy should meet quarterly to review computer use. This meeting should provide managers with a list of those who are no longer associated with the firm. Companies should routinely deactivate all accounts and passwords used by these individuals. One expert estimated that 30 percent of company files are for people or firms no longer associated with the company. Once a worker is gone, an information system manager should also check for any trap doors left open by former contractors or workers.

Another part of the quarterly meeting should include reviewing the use of company computers by subcontractors and vendors. Experts agree that outside service providers should be monitored and required to follow the company computer security policy.

A valuable element in any computer security plan is the involvement of employees through an effective awareness and education program. For example, any employee who notices something dramatically different in a file or in the performance of the system should report it to the security manager or system administrator. Any radical

change in the network can alert an employee to an intrusion. Employees can also be the first to notice if an unauthorized user asks for passwords or access to files.

Employees must participate in physical security aspects of a company wide plan. At least one computer security expert advises giving employees step-by-step advice in awareness training. He suggests implementing a "clean desk" policy that prevents employees from leaving passwords and other computer related information on top of their desks or in unlocked drawers. As part of company policy, desk keys should be left in a secure area. Security personnel should routinely check for desk keys that are left in the open or in the reception area. A former FBI official said the "clean desk" policy should include asking employees to close down their computers when they take a break.

Computer security experts assert that a consistently executed security plan involving employees make it easier to track down an intruder, while deterring all but the most determined hacker.

Protection

A computer security program as an integrated part of the overall security plan of a company should incorporate provisions to protect the network physically and in cyberspace, detect any unauthorized user or attempted breach of the system, and react to any effort to tamper with the system.

The cost of a properly configured system of protection, detection and reaction should be in line with the financial risk a company is to prepared accept if an intruder gains access to the network.

Whatever risk level a company decides to assume, any protection plan should include these elements:

- *Activate built-in system defensive capabilities.* Most computer operating systems can be configured to activate certain precautions. For example, most systems can be set up to access only to those who create or need them.

- *Passwords to deny unauthorized users.* To gain the most effective protection, security managers should see that the overall computer security plan requires users to choose unique passwords, keep them hidden from sight, refuse to divulge them, and change them at least every 30 days.
- *Computer barriers that separate company networks or files from unauthorized users.* One type of barrier is a properly configured and maintained firewall of hardware and software. Another utilizes two separate computer systems: one that allows no communication with the outside world and one that does.
- *Physical barriers.* Security managers should also impose strong physical barriers that deny unauthorized access to the physical plant where computers and system software are located.
- *Encryption software that scrambles messages and data.* Such protection ensures that unauthorized users who breach the firewall cannot understand the information.
- *Scanning.* Software programs are available that scan the computer system for intruders and protect against destructive viruses that can destroy data.

Whatever technological solution companies adopt, one universal principle applies: all technology must be properly installed, maintained and updated to be effective against ever changing intruders. An anti-virus software program installed today will not be effective against the bugs of tomorrow. Experts urge companies to review, update and replace security technology frequently. Technology is not the solution to computer intrusion, but correctly applied, it is a vital tool.

Detection

The benefit of a strong, properly enforced security plan is most evident in detecting an intrusion.

Experts generally agree companies should have some provision for auditing system use. Auditing will reveal when the system is accessed and by whom. Security managers should ask that any aberrations in the audit logs—such as repeated attempts to use the system outside normal work hours—be reported. Often, audit practices and software programs can track the attempted access to its source.

Federal computer security experts suggest looking for signs an intruder has been in the system. For example, frequent changes in particular binaries, files or directories are the signatures of an intruder. A list of these possible signatures, as well as other information on computer intrusion, can be obtained from Federal Computer Incident Response Capability (FedCIRC). FedCIRC, a Washington, D.C.-based partnership of computer incident response, security and law enforcement professionals working under Presidential directive to provide computer security for the Federal government, can be reached via Internet at www.fedcirc.gov.

More information on types of intrusions and ways to detect unauthorized use should be available today. Computer network security is still at a low level of risk management, in part because those charged with protection, detection, reaction and prevention lack statistics and updated information on the types of intrusion now in vogue with hackers, an international computer security expert said.

The dearth of information stems in large measure from a reluctance by businesses to cooperate with law enforcement. The survey of businesses cited above revealed that only a small percentage of break-ins are ever reported. Businesses say they fail to contact the authorities for fear of exposing a computer vulnerability or finding proprietary information compromised by law enforcement.

(continued on next page)

Cybercrime Threatens Billions of Assets

Federal agencies bring much needed focus to escalating problem

(continued from preceding page)

The FBI is particularly concerned about the lack of information on electronic attacks and distrust between private industry and government. The agency began a pilot partnership in 1996 with 35 to 40 Midwestern companies. Ultimately, the agency plans to offer it nationwide. In addition to meeting monthly for security seminars, the partners freely exchange information about intrusions, and the FBI sends electronic warnings on the latest break-in techniques and how to secure computers against them. Such quick information means cooperating companies can address system vulnerabilities before an intruder attacks.

Even with the best protection and detection, a determined hacker can still access the company system. Security managers and system administrators should be prepared to react quickly to unauthorized use.

Reaction

Last fall, one company discovered that pranksters had vandalized its website despite the sophisticated security measures in place. The attack—and the necessary reworking—of the webpage illustrates that computer intrusion can happen to anyone, even those who prepare.

However, the ease with which the company executed its recovery plan demonstrates how an organization that is prepared for disaster can regain its footing quickly. Staff members knew who to call, and everyone responded at once. The staff immediately secured the firm's customer list, which contains e-mail addresses and encrypted credit card numbers. The company then went to work with the FBI to solve the break in. All this was accomplished and most of the information restored within nine hours.

A well-defined business recovery plan, complete with the names of emergency contacts and all necessary phone numbers, will enable employees to understand and implement recovery efforts

immediately. One data expert suggests rehearsing the recovery plans with employees.

However, the most essential ingredient in recovery goes into effect well before any intrusion. Information systems administrators or the security manager should obtain regular back up copies of important data, applications and special instructions on configuration, as well as any hard-to-replace hardware or software. Back-ups should be secured off site for maximum safety.

While it may be impossible to stop attacks, companies will minimize damage and computer down time by developing a quick response, said a researcher for an East Coast network security firm.

Today, companies invest millions of dollars in computer networks to help them produce better products in less time. However, they risk millions more by failing to apply the most basic cyber-security measures. Companies that routinely provide their buildings and employees with physical security appear uncertain about how to protect their information assets.

One of the basic security measures taken by any company is to report a break in to authorities at once. The same principle should be true of a computer breach. For too long companies have hurt themselves by withholding information about computer intrusion-information that could speed the development of technological protection, help apprehend unauthorized users, and alert other companies to the current tactics employed by hackers.

Private industry must become more proactive in protecting against cyber-intruders or face the catastrophic possibility of losing their computer networks and proprietary data.



The Lipman Report Editors