

July 15, 1998

Criminals Target Corporate Networks

Computer crime proliferates despite billions spent on network security

In February 1998, an international group of teenagers breached U.S. Department of Defense computer networks, including a network related to the global positioning satellite (GPS) system. The attack represents one of many successful attacks launched by hackers against the federal government in the last two years. Other victims include the Central Intelligence Agency, the U.S. Department of Justice, the National Aeronautics and Space Administration and the U.S. Air Force. In response to the growing threat in cyberspace, the Federal Bureau Of Investigation (FBI) created the National Infrastructure Protection Center (NIPC) on February 26 to detect and deter acts that threaten or target the nation's eight critical infrastructures (The Lipman Report, February 1998): telecommunications, banking and finance, transportation, electrical energy, gas and oil supply, water supply, emergency services and government operations.

The U.S. government is not the only target, nor is technological conquest the only aim. According to a 1998 study performed in cooperation with the FBI, more than six out of every 10 businesses, government offices and universities reported computer security breaches during 1997. Losses ranged from \$25 million worth of research stolen from one corporation to \$50 in repairs. As Corporate America rushes to embrace the productivity gains afforded by increased connectivity, it should also consider the inherent security risks in linking its private networks with the very public Internet.

Recent issues of The Lipman Report have addressed various aspects of computer security, ranging from laptop computer theft and cyberterrorism to employee sabotage. This report examines ways in which security directors and information systems managers can safeguard their organization's networks from both internal and external attacks.

The Villains—External and Internal

While the Information Age offers a myriad of ways for organizations to enhance efficiency and profitability, it also provides the criminal element with novel ways to reap illicit gains. Drug cartels, for instance, take advantage of international banking systems to launder millions of dollars in illegal profits faster than law enforcement agencies can track the funds.

In addition, many of the technical whizzes known as hackers are changing from pranksters to profiteers. Traditionally, hackers have invaded computer networks for the sheer technical challenge of the feat. As more and more organizations use networked computers to transfer money and to store sensitive proprietary information, however, an increasing number of hackers have made the transition to “crackers”—computer criminals. Each year, crackers attack the information systems of large corporations and government agencies, producing losses of \$100 billion in commercial espionage in the United States alone.

Although these malicious outsiders pose a significant menace, the greatest threat of all comes from within. Insiders often do not need to break into a computer system; instead, they simply use—or abuse—their legitimate access. According to the FBI, many of the reported computer violations are traced back to either an employee or a trusted outsider, such as a consultant or a temporary employee, who has exceeded his or her access, often in retribution for a perceived wrong.

Security directors armed with the tools to recognize these threats to their organization's information systems can respond with knowledge, technology and preparedness.

Security: Don't Log on Without It

By now, most organizations have recognized the need for computer security. In fact, cybersecurity has become big business. Companies worldwide spent approximately \$6.3 billion on computer network security in 1997, and that figure is expected to reach nearly \$13 billion by 2000. A relatively new market, intrusion detection tools have already grown to a \$65 million industry and are projected to grow as large as the firewall market, which reached approximately \$255 million in 1997. The furor over computer crime has even prompted the creation of security assurance services, which

(continued on next page)

Criminals Target Corporate Networks

Computer crime proliferates despite billions spent on network security

(continued from preceding page)

offer an initial vulnerability assessment and a continuous security improvement process—starting at just \$40,000 per year.

The figures add up to one simple fact: network security is costly, but critical. By some estimates, hackers penetrate a different computer on the Internet every 20 seconds, and the FBI believes that fewer than one of every eight hacker attacks is reported to law enforcement authorities. Organizations that believe they cannot afford security, in reality, cannot afford to lack it. In 1995, hackers infiltrated the network of a small network management company, installing a program that allowed them to record passwords and access the entire network. The hackers used these stolen privileges to gather sensitive information on the company and its customers, then launched similar attacks on those organizations. The chief executive of the network management firm said she knew the risks involved but didn't want to pay the \$20,000 for the technology that might have prevented the attack.

Organizations need to realize, however, that simply buying the appropriate tools is not enough. Despite the billions spent on security in 1996, American corporations lost an estimated \$10 billion from information systems attacks. Even worse, the latter figure undoubtedly represents only a fraction of the actual loss since many organizations elected to withhold the magnitude of their losses. Improper system configuration most likely accounts for this disturbing figure. A 1998 study by a global computer security organization, for instance, revealed that 93% of the organizations surveyed had security flaws that left them vulnerable to even rudimentary attacks—despite the fact that most had firewalls in place at their network perimeter. This illustrates a basic premise of security: Security technologies are only as good as the policies behind them.

Establishing a Security Policy

In the eyes of a former FBI official who was responsible for protecting that organization's information assets, "having a well planned, well defined policy that has the backing of executive management and is well understood and enforced" constitutes the most important element of computer security. "Technology alone, if not properly employed, will not secure a computer network," he said. "Likewise, an alert employee who is paying attention is more to notice something that is out of the ordinary. Aberrations will show up much more readily if the vast majority of employees are using the systems and security practices as intended."

To succeed, a computer security policy must have the support of top management, working in conjunction with the information systems department and the security director. At the same time, the policy should include input from the employee level. Incorporating user feedback will assist policy developers in balancing the degree of security with ease of operations, while providing employees with a measure of "ownership" in the policy. To some individuals, restrictions imply distrust by management. Allowing employees to participate in the the process will help them become a part of the solution, not part of the problem.

The policy provides the foundation for network security; all of the technological components will support the principles established within. In formulating the policy, management should consider the following issues: access control, both internal and external; physical and data vulnerability; information classification; and user guidelines. Perhaps most importantly, the policy should include specific, enforceable consequences for violators—up to, and including, criminal prosecution, if necessary. Only a small fraction—perhaps 15%—of detected computer attacks are ever reported to law-enforcement agencies because

companies fear negative publicity—a fact that has not escaped the notice of computer criminals.

Turning Paper into Procedure

Once the security policy has been formulated and disseminated throughout the organization, the following steps will help support and enforce the guidelines therein:

Prioritize information. Classify all information according to its value. Prioritization of information assets facilitates the security concept of defense in depth,” in which higher levels of security protect increasingly sensitive data. For instance, the U.S. military classifies information according to the following system: confidential, secret and top secret. Information classification allows an organization to focus its security efforts on the most critical data, while providing a basis for employee access levels. An individual with secret clearance, for example, can access any files except those with a top-secret rating. For additional protection, security may be granted on a limited basis, with employees receiving only the level of access required to perform their duties.

Implement appropriate technological defenses.

Companies sometimes make the mistake of relying upon a single, off-the-shelf security solution, such as a firewall. This practice may account for the high vulnerability found in the 1998 study cited above. Using standard equipment means leaving the standard security holes that have already been published on hacker sites across the Internet. Instead, organizations should put together a combination of security products that work together, customizing the individual components to meet their needs.

- **Firewalls.** These devices can use both hardware and software resources to erect an isolation barrier between networks. Unfortunately, firewalls often fail to deter hackers because they are either improperly configured or not activated. To remedy these common problems, companies need to make certain that in house network administrators have the necessary

technical skills to install and configure these electronic barriers; otherwise, they should employ outside experts to do the job. In choosing the latter route, however, organizations need to screen their service provider very carefully. Outsourcing presents a potential threat to internal network security since outsiders have no loyalty to the organization.

- **Encryption.** Encryption programs convert plain text into gibberish, using a mathematical formula. To decrypt the data, users must supply the appropriate “key,” usually in the form of a password or passphrase. Encryption adds another layer of security by rendering data unreadable to users who do not have the appropriate key, making it an essential tool in protecting information assets. Even if an intruder manages to penetrate the firewall, he or she will be unable to read encrypted documents.
- **Virus protection.** With six viruses created every day, virus scanning remains an essential aspect of information security. Viruses primarily enter networks in attachments to e-mail messages, which means that organizations should scan for viruses at network entry points, such as firewalls and mail gateways. Because viruses spread in a variety of ways, security directors and information systems managers should make special efforts to become aware of new security threats by visiting web sites where these are discussed. One such site is www.cert.org, maintained by the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University.

Selecting and configuring the appropriate network security components represents only the beginning of security administration. For firewalls and virus protection software, companies must constantly watch for patches and upgrades that fix discovered security problems and neutralize new viruses. In addition, organizations should periodically

(continued on next page)

Criminals Target Corporate Networks

Computer crime proliferates despite billions spent on network security

(continued from preceding page)

cally conduct scans and penetration tests against their firewalls and related systems to simulate an Internet-based network attack. While many novice hackers use commercially available software to infiltrate networks, experienced network administrators can utilize these same programs to detect and patch security holes.

Enforce strong passwords. To ensure authentication and confirm that employees are indeed who they electronically claim to be, organizations need to enforce a strict password policy. Users frequently select passwords that are easy to remember—and consequently easy to guess. The following should never be used as passwords: real words in any language, spelled either forward or backwards; proper names; and plain numbers. If possible, network administrators should configure the networks to require that passwords: 1) consist of a combination of letters and numbers or symbols, 2) have minimum lengths, 3) change frequently, and 4) do not repeat within a specified period of time. In addition, the security policy should forbid the transmission of passwords via e-mail or telephone, including strict consequences for violators.

Continuously monitor the security program. In addition to keeping up with the latest software updates, companies need to assess the effectiveness of the network security program to ensure that it continues to meet their needs. Security directors and information systems managers should interview users regularly to find out how they use the network and with what types of information. The process will reveal how employees follow security policies in their everyday operations, whether the policies are strictly enforced, and where policies should be updated. Conducting such an assessment on at least an annual basis will enable the security policy to grow with the organization. Management should also review security logs frequently to ensure their integrity and to identify any suspicious behavior.

Develop a disaster recovery contingency plan.

Computers have become such an integral part of business today that companies can ill-afford to operate without their networks for a significant period of time. For this reason, organizations need to develop a business recovery plan to implement in the event of a disaster. This plan should require frequent system backups and provide for storage of backup data in a secure, off-site facility. In addition, disaster recovery plans should clearly specify procedures to be followed in case of data loss, whether stemming from sabotage, employee accident or a natural disaster.

Technology continues to evolve at a breakneck pace—much faster, in fact, than the measures required to secure it. As a result, those who seek to exploit technology for personal gain enjoy a significant advantage over those who strive to protect it. (After all, a hacker only needs to find one way in, whereas a security director or information systems manager needs to find and close countless access points. Organizations must recognize this fact and commit the necessary resources to secure their networks from prying eyes without and within.

The May failure of the Galaxy IV satellite gave the American population a taste of its dependence upon computerized telecommunications. And on June 24, CIA Director George Tenet warned a Senate subcommittee that the United States needs to fortify its key computer networks against both domestic and foreign attacks, citing knowledge of at least one active targeting effort. Unless organizations act now to protect their information assets, the term “cyber Pearl Harbor” will become more than a warning—it will explode into a devastating reality.



The Lipman Report Editors