

November 15, 1999

## The Menace of Information Warfare

Computer crime threatens valuable information assets as reliance on technology grows

*Last month, the Federal Bureau of Investigation (FBI) revealed that hackers apparently operating from Russia have systematically raided U.S. government computers for more than a year. The cyber-thieves have plundered vast amounts of non-classified, but sensitive information from the U.S. Department of Defense, the U.S. Department of Energy's nuclear weapon and research labs, the National Aeronautics and Space Administration (NASA), and several university research facilities and defense contractors. Despite a concentrated, multi-agency inquiry led by the FBI, investigators still cannot identify the perpetrators or confirm espionage as the motive behind the attacks. The extent of the attack and the hackers' ability to elude law enforcement serve as chilling reminders that information warfare—no longer a frightening possibility, but a harsh reality—presents a challenge that the technologically advanced nations of the world are not prepared to face.*

*Even worse, susceptibility to information warfare escalates each day. The harsh competition of a global market forces companies to seek the increased productivity gains that only technology can offer, but many organizations take this step without committing the necessary resources and attention to security. Such carelessness jeopardizes business operations just as surely as if the companies had ignored the need for computerization altogether. Not only can these technological marvels exponentially increase a firm's productivity and efficiency, but they can also enable a technically savvy competitor or insider to single-handedly bring an organization to a halt.*

### The Growing Danger

According to a 1999 study conducted with cooperation from the FBI, computer crime continues to pose an increasing threat to organizations in the private and public sectors. The survey, which includes responses from 521 security practitioners representing U.S. corporations, government agencies, financial institutions and universities, confirms trends established during the first three years of its existence. For the third consecutive year, unauthorized system access has increased, with 30 percent of respondents reporting outside system penetration and 55 percent reporting internal system breaches. Furthermore, the financial losses caused by computer security violations continue to

mount. The 163 organizations that could quantify losses report losing almost \$124,000,000 during 1998; this number excludes the 20 percent of respondents who acknowledged experiencing losses but could not provide a dollar figure.

Although laptop theft and virus attacks represent the two most common incidents resulting in financial loss, theft of proprietary information and financial fraud result in the greatest monetary loss, totaling more than \$74 million combined last year. Even though reported incidence of proprietary information theft has not increased over the years, the resultant loss from each instance rises steeply, reflecting a growing perception of its value. The \$42.5 million in financial losses reported from information theft in 1999 signifies a 112 percent increase over 1997, with the number of incidents remaining steady. Thus, the financial stake for organizations continues to climb even when the frequency of attacks maintains a constant level.

Financial fraud and trade-secret theft certainly rank among the most devastating computer crimes in terms of loss per incident, but even smaller, unsophisticated acts can produce significant consequences. Last year, a former U.S. Coast Guard employee received a five-month prison sentence for intentionally erasing critical data from the service's personnel database after she resigned, which caused the computer system to crash. Recovering and re-entering the lost data required 115 Coast Guard personnel and more than 1,800 hours, at a cost exceeding \$40,000. In another case, an employee dismissed from a publishing powerhouse secretly copied a co-worker's account and password information, which enabled him to crash over half of the company's computer network servers and delete all of the data on the affected systems. This act of sabotage cost his former employer more than \$100,000. As organizations grow progressively more reliant on their information systems and the general population becomes more and more techno-savvy, the frequency and financial impact of such attacks will only increase.

(continued on next page)

---

## The Menace of Information Warfare

Computer crime threatens valuable information assets as reliance on technology grows

(continued from preceding page)

### Security as a Secondary Concern

Fierce competition forces companies to consider each budget dollar to maximize their bottom line. Although technology upgrades often receive top priority due to the quantifiable benefits of greater productivity, management tends to view the security measures to protect that investment as an unnecessary profit drain. One study reveals that, in 1998, 43 percent of the Fortune 1,000 companies surveyed spent less money on their network security programs than their annual budgets for break-room refreshments.

Of the organizations that have made investments in computer security, an overwhelming majority does not use such tools properly. For instance, 98 percent of the respondents to the FBI-assisted survey claim to use anti-virus software, yet 90 percent report experiencing virus contamination last year. Ninety-one percent of the respondents indicate they have a firewall in place, but the number of successful external attacks continues to grow. Many companies blindly entrust their sensitive information assets to off-the-shelf security solutions, which cannot provide adequate protection against the ever-increasing methods of attack. Each week, for instance, approximately 300 new viruses enter the electronic scene, with some strains capable of not only formatting a hard drive, but also interfering with the system's hardware and rendering it useless. Because of such dangers, organizations must continuously invest in new patches and upgrades for their network security components to ensure the best possible defense against the latest forms of attacks.

In addition, competition drives yet another factor working against companies in their quest for security: in their rush to release new products, software developers often overlook security. Thus, firms that use commercial software packages must compensate for these security holes through their network security programs.

### The Need for Cooperation

Historically, victimized organizations' lack of disclosure to law enforcement has proven a significant hindrance in the battle against computer crime. The survey cited above, however, indicates that more companies are reporting serious information security breaches to law enforcement: 32 percent in 1998, compared to only 17 percent during the previous three years. Despite the improvement, more than two-thirds of computer-crime victims prefer to handle such violations internally.

In many cases, companies fear the negative impact that public disclosure may have on consumer and shareholder confidence; they worry that competitors would use the information to their advantage. Firms of this mindset often believe the legal recourse for computer violations may not compensate for the effects of negative publicity. Some organizations believe that reporting violations will result in burdensome federal regulation that could interfere with their business practices. Other firms fear that an investigation will require disclosure of proprietary business practices, which could threaten their competitive advantage. Yet another obstacle to public disclosure lies in companies' perceptions of law enforcement: many believe that legal authorities cannot help them.

To combat this problem, last year U.S. Attorney General Janet Reno launched the Computer Crime and Intellectual Property Section, a cooperative effort in which attorneys from the U.S. Department of Justice work with government agencies, private companies, universities and foreign governments. In addition, several federal agencies from the FBI to the Defense Department to NASA are expanding their staffs that deal with computer crimes. Still, the incidence of computer crime is growing more rapidly than the law-enforcement teams trained to combat them. The FBI's computer crime caseload has quadrupled from 200 in 1996 to its present level of more than 800, with approximately 200 agents in 10 field offices investigating these incidents. To leverage

---

its ability to respond to cyber-attacks, the FBI has created the National Infrastructure Protection Center (NIPC). The center combines the talents of 107 representatives from relevant federal agencies, including the FBI, the Central Intelligence Agency, the Department of Defense, the U.S. Department of State and the U.S. Secret Service.

The federal cyber-crime investigation effort, however, requires the cooperation of victimized organizations for maximum efficiency. Reluctance to report computer security breaches makes it difficult for law-enforcement officials to learn how to thwart similar attacks, leaving other companies vulnerable to intrusion. Organizations duplicate one another's efforts in learning investigative and prevention techniques, rather than sharing their experiences and fighting computer crime as a united force. Until companies work with law enforcement to allay their concerns and begin a comprehensive cooperative effort, criminals will retain the upper hand in computer security.

### **Safeguarding Computer Networks**

In the absence of this cooperation, firms must exercise extreme vigilance in protecting their information systems. The increasing prevalence of computer crime has spawned a multibillion-dollar computer security industry, which can defend most networks against all but the most sophisticated attacks. Still, successful implementation of these security measures requires the support of a strong security policy. Top management must develop—and enforce—a written policy that includes specific consequences for violations. The policy should address such issues as account creation and deletion, system audits and user behavior; it should also include a disaster-recovery plan. Well-disseminated guidelines can make employees an invaluable asset against computer crime, educating them on what constitutes a system breach and what to do if they encounter suspicious activity.

The following recommendations will also help decrease the likelihood of an electronic attack:

- *Senior management needs to take a proactive role in the information security program.* Company leaders must recognize the significant threat that computer sabotage poses to an organization's assets and shareholder interests. They need to possess a thorough understanding of the risks of computerization, as well as the security technologies available to reduce that risk. By staying well-informed, top management can develop a proactive computer security program that continuously evolves to meet the growing threat.
- *Develop a policy on password use and changes.* Companies should require users to select passwords of at least eight characters, using both letters and numerals. Employees should not use obvious passwords, such as anniversaries, birth dates, children's or pet's names, or phone numbers. The passwords need to change at least monthly, with a restriction that limits recycling of old passwords. The use of auxiliary identity confirmation devices, such as dynamic password generators, can offer an added level of security for especially sensitive user accounts.
- *Protect the operating systems of the server.* Network administrators need to disable any unnecessary services, and system administrator passwords must change frequently. Companies should use encryption to protect remote network operations. Administrators should promptly remove terminated employee accounts, as well as audit active accounts to protect against unnecessary or incorrect changes.
- *Enforce a strict e-mail policy.* Today, many of the most insidious computer attacks infiltrate a network through the e-mail system. To prevent such an infection, the firewall should scan all incoming e-mail for viruses using a continuously updated anti-virus program. Any e-mail messages containing executable attachments, perhaps hidden in compressed file formats, should

(continued on next page)

## The Menace of Information Warfare

Computer crime threatens valuable information assets as reliance on technology grows

(continued from preceding page)

be transferred to a quarantined computer system for examination and disposal, if warranted.

- *Restrict access to the network.* By creating day and time restrictions for users who do not need round-the-clock network access, companies can reduce system vulnerability. In addition, organizations should only provide Internet access to employees who require it for their job duties. Ideally, these employees would access the Internet through stand-alone systems, which would protect the corporate network from Internet-based attacks.
- *Scan the Internet for security solutions.* Despite its many risks, the Internet can also serve as an invaluable tool in protecting a company's information assets. Hackers frequently post system-penetration tips on the Internet, as well as specialized software to assist novice hackers with their electronic assaults. The act of publicizing security holes—and, in some cases, ways to fix them—is known in certain hacking circles as “full disclosure,” viewed by traditional hackers as a sort of public service. By visiting such web sites, information technology managers can learn about known security flaws and protect their organization's systems accordingly.
- *Implement comprehensive background screening.* Proper pre-employment screening plays a vital role in preventing a wide variety of crimes, including network sabotage. Important elements of a screening program incorporate the following, at a minimum: verification of work history, educational institutions and degrees earned; confirmation of professional and personal references; and investigation of driving and criminal records, and where applicable, military discharge status. Yet, even companies that follow these requirements for internal employees often accept contract personnel without question, which raises the possibility of third-party

infiltration. The critical nature of information system protection makes background screening of information technology contractors an essential part of network security.

- *Protect network audit logs.* The invisibility of computer attacks presents a special challenge—experts estimate that 85 to 90 percent of all network intrusions are never uncovered. Companies need to capture real-time audit logs from the operating system, applications and database, maintaining them in a secure, centralized location. A strong backup policy, including off-site storage, will protect both data and security logs against accidents and attacks.

*Even though companies and government organizations spend billions of dollars each year on computer security technology, the number of successful attacks and resulting financial losses still climbs annually. Many firms simply fail to make an adequate investment in protecting their information systems; others rely exclusively on the technology without implementing an information security program to ensure its effectiveness. No organization can afford inaction.*

*The world's reliance on computers and technology will only increase in the years to come, further increasing the risk of experiencing a critical network attack. With more criminals working to infiltrate computer systems than law-enforcement agents available to stop them, companies must continuously analyze and update their information security programs to stay ahead of the threat. Public and private entities alike need to recognize the dangers they court with lax computer security, lest they fall among the casualties of information warfare.*



The Lipman Report Editors