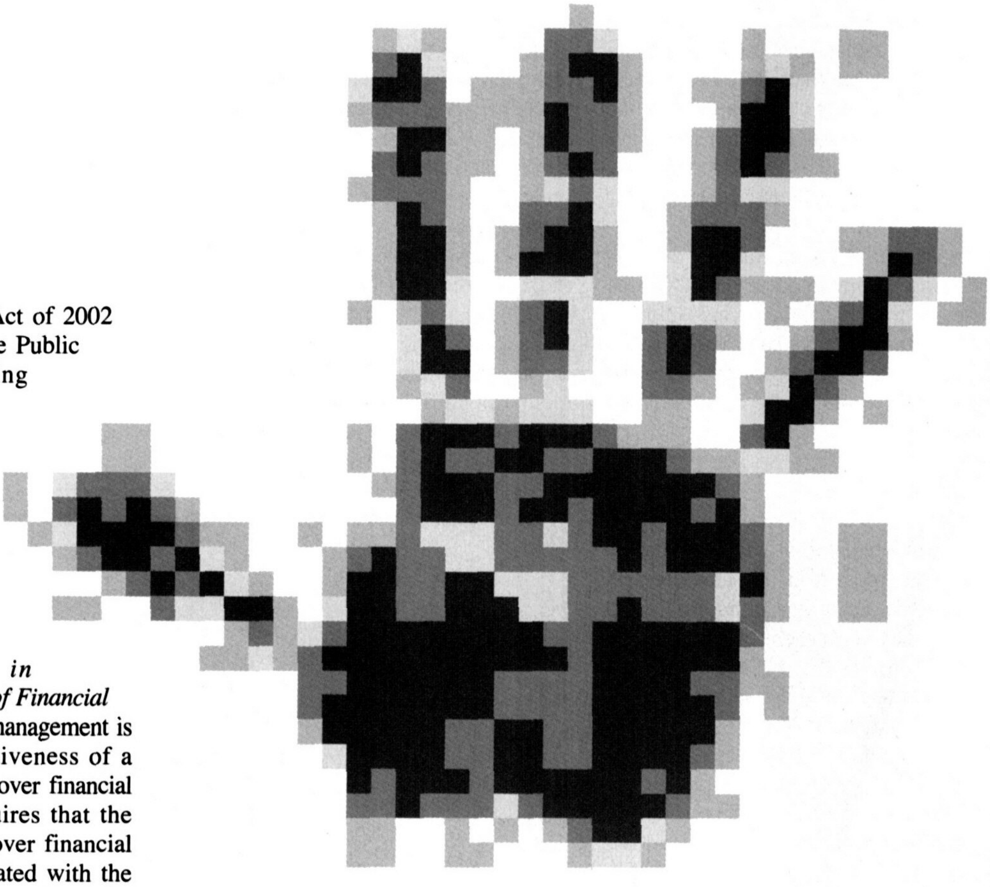
System Security Threats and Controls

By P. Paul Lin



The Sarbanes-Oxley Act of 2002 (SOX) authorized the Public Company Accounting Oversight Board (PCAOB) to establish auditing and related practice standards to be used by public accounting firms. PCAOB Auditing Standard 2 (AS 2; *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*) mandates that management is responsible for the effectiveness of a company's internal control over financial reporting. AS 2 also requires that the audit of internal controls over financial reporting should be integrated with the audit of the financial statements. The 2005 CSI/FBI Computer Crime and Security Survey (i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf) indicated that SOX has had an impact on information security in several industries.

ComAir's system crash on December 24, 2004, was just one example showing that the availability of data and system operations is essential to ensure business continuity. Due to resource constraints, organizations cannot implement unlimited controls to protect their systems. Instead, they should understand the major threats, and implement effective controls accordingly. An effective internal control structure cannot be implemented overnight, and internal control over financial reporting must be a continuing process.

The term "system security threats" refers to the acts or incidents that can and will affect the integrity of business systems, which in turn will affect the reliability and privacy of business data. Most organizations are dependent on computer systems to function, and thus must deal with systems security threats. Small firms, however, are often understaffed for basic information technology (IT) functions as well as system security skills. Nonetheless, to protect a company's systems and ensure business continuity, all organizations must designate an individual or a group with the responsibilities for system security. Outsourcing system security functions may be a less expensive alternative for small organizations.

Top System Security Threats and Controls

The 2005 CSI/FBI Computer Crime and Security Survey of 700 computer security practitioners revealed that the frequency of system security breaches has been steadily decreasing since 1999 in almost all threats except the abuse of wireless networks (*Exhibit 1*). *Exhibit 2* shows the financial losses resulting from the threats individually. Note, however, that the survey report pointed that the implicit losses (e.g., lost sales) are difficult to measure and might not have been included by survey participants.

Viruses

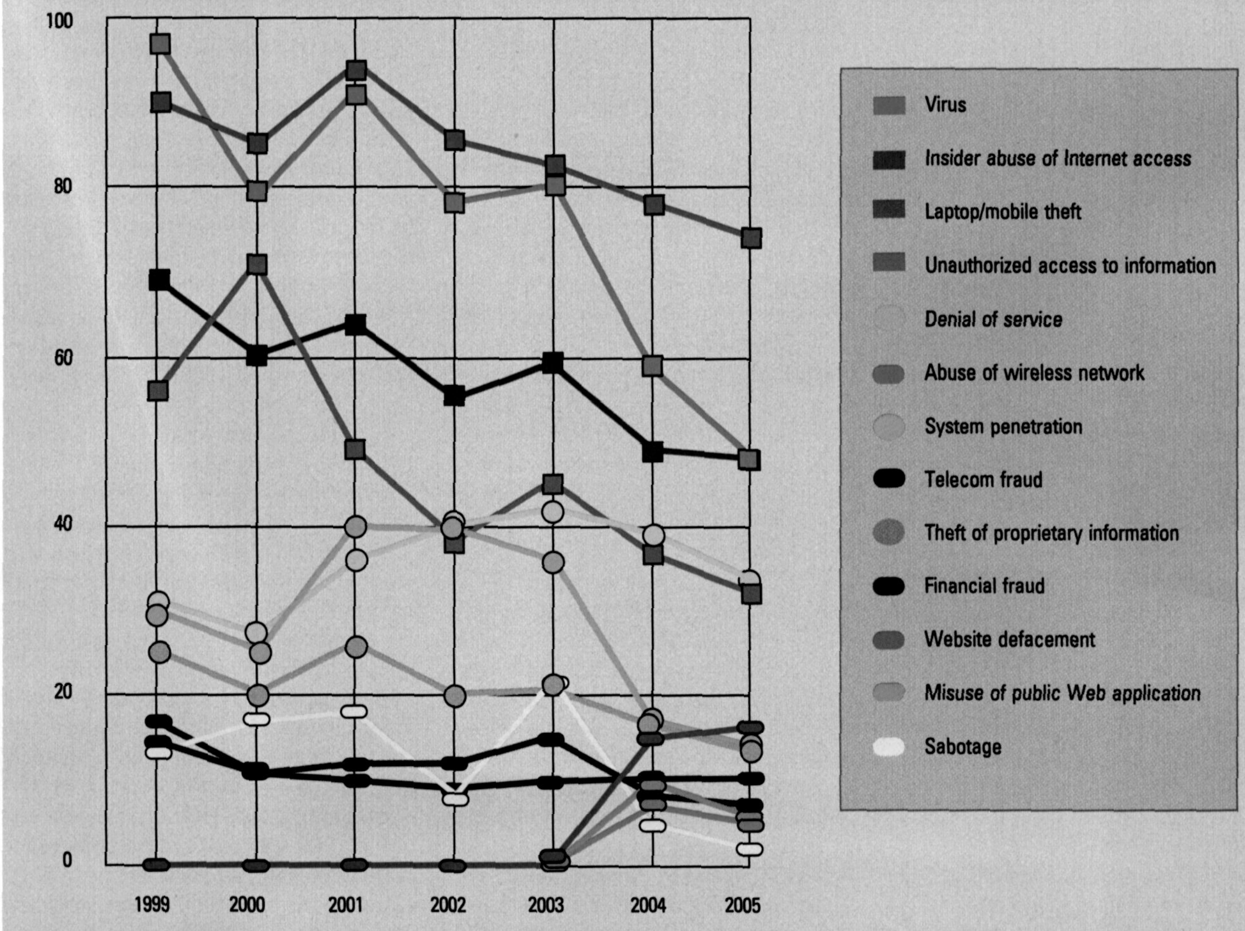
A computer virus is a software code that can multiply and propagate itself. A virus can spread into another computer via e-mail, downloading files from the Internet, or opening a contaminated file. It is almost impossible to completely protect a network computer from virus attacks; the CSI/FBI survey indicated that virus attacks were the most widespread attack for six straight years since 2000.

Viruses are just one of several programmed threats or malicious codes (malware) in today's interconnected system environment. Programmed threats are computer programs that can create a nuisance, alter or damage data, steal information, or cripple system functions. Programmed threats include, computer viruses, Trojan horses, logic bombs, worms, spam, spyware, and adware.

According to a recent study by the University of Maryland, more than 75% of participants received e-mail spam every day. There are two problems with spam: Employees waste time reading and deleting spam, and it increases the system overhead to deliver and store junk data. The average daily spam is 18.5 messages, and the average time spent deleting them all is 2.8 minutes.

Spyware is a computer program that secretly gathers users' personal information and relays it to third parties, such as advertisers. Common functionalities of spyware include monitoring keystrokes, scanning files, snooping on other applications such as chat programs or word processors, installing other spyware programs, reading cookies, changing the default

EXHIBIT 1
The Trend of Top System Security Breaches



Source: CSI/FBI 2005 Computer Crime and Security Survey homepage on the Web browser, and consistently relaying information to the spyware home base. Unknowing users often install spyware as the result of visiting a website, clicking on a disguised pop-up window, or downloading a file from the Internet.

> As a preventive control, **every company should** have a written policy **regarding the use of** corporate computing **facilities.**

Adware is a program that can display advertisements such as pop-up windows or advertising banners on webpages. A growing number of software developers offer free trials for their software until users pay to register. Free-trial users view sponsored advertisements while the software is being used. Some adware does more than just present advertisements, however; it can report users' habits, preferences, or even personal information to advertisers or other third parties, similar to spyware.

To protect computer systems against viruses and other programmed threats, companies must have effective access controls and install and regularly update quarantine software. With effective protection against unauthorized access and by encouraging staff to become defensive computer users, virus threats can be reduced. Some viruses can infect a computer through operating system vulnerabilities. It is critical to install system security patches as soon as they are available. Furthermore, effective security policies can be implemented with server operating systems such as Microsoft Windows XP and Windows Server 2003. Other kinds of software (e.g., Deep Freeze) can protect and preserve original computer configurations. Each system restart eradicates all changes, including virus infections, and resets the computer to its original state. The software eliminates the need for IT professionals to perform time-consuming and counterproductive rebuilding, re-imaging, or troubleshooting when a computer becomes infected.

Fighting against programmed threats is an ongoing and ever-changing battle. Many organizations, especially small ones, are understaffed and underfunded for system security. Organizations can use one of a number of effective security suites (e.g., Norton Internet Security 2005, ZoneAlarm Security Suite 5.5, McAfee VirusScan) that offer firewall, anti-virus, anti-spam, anti-spyware, and parental controls (for home offices) at the desktop level. Firewalls and routers should also be installed at the network level to eliminate threats before they reach the desktop. Anti-adware and anti-spyware software are signature-based, and companies are advised to install more than one to ensure effective protection. Installing anti-spam software on the server is important because increasing spam results in productivity loss and a waste of computing resources. Important considerations for selecting anti-spam software include a system's effectiveness, impact on mail delivery, ease of use, maintenance, and cost. Many Internet service providers conveniently reduce spam on their servers before it reaches subscribers. Additionally, companies must maintain in-house and off-site backup copies of corporate data and software so that data and software can be quickly restored in the case of a system failure.

Insider Abuse of Internet Access

Annual U.S. productivity growth was 2.5% during the second half of the 1990s, as compared to 1.5% from 1973 to 1995, a jump that has been attributed to the use of IT (Stephen D. Oliner and Daniel E. Sichel, "Information Technology and Productivity: Where Are We Now and Where Are We Going?," *Reserve Bank of Atlanta Economic Review*, Third Quarter 2002). Unfortunately, IT tools can be abused. For example, e-mail and Internet connections are available in almost all offices to improve productivity, but employees may use them for personal reasons, such as online shopping, playing games, and sending instant messages to friends during work hours.

The 2005 Electronic Monitoring and Surveillance Survey (www.amanet.org/research/pdfs/EMS_summary05.pdf) conducted by the American Management Association (AMA) and the ePolicy Institute revealed that 76% of employers monitor employees' web connections, while 50% of employers monitor and store employee computer files. The survey also revealed that 26% of participating employers have fired workers for workplace offenses related to the Internet; 25% have fired employees for misuse of e-mail; and 65% of those surveyed used software to block employee access to inappropriate websites. Most U.S. companies allow reasonable use of computers for personal reasons, but many never define "reasonable." As a preventive control, every company should have a written policy regarding the use of corporate computing facilities. In addition, companies should update their monitoring policies periodically, because IT evolves rapidly.

If an Internet monitoring policy is clearly stated, companies need not worry about employee privacy concerns; the Electronic Communications Privacy Act does give companies the right to monitor electronic communications in the ordinary course of business.

Laptop or Mobile Theft

Because they are relatively expensive, laptops and PDAs have become the targets of thieves. Although the percentage has declined steadily since 1999, about half of network executives indicated that their corporate laptops or PDAs were stolen in 2005 (*Network World Technology Executive Newsletter*, 02/21/05). Besides being expensive, they often contain proprietary corporate data, access codes to company networks, and sensitive information.

The following suggestions can help minimize the chance of theft when outside the office:

- Never leave a notebook or PDA unattended, including in a car or hotel room.
- Install a physical protection device such as a lock and cable or an alarm.
- Put the notebook in a nondescript bag or case.
- Install stealth-tracking software.
- If notebooks are stolen, automatic logins make it easy for a thief to access sensitive information. Password protection does not deter a theft, but it does make it more difficult for thieves to use the stored information. Biometric security, such as the fingerprint readers included in some new ThinkPad models, is even better.
- Back up data regularly, or install a desktop/notebook/PDA sync program.

Denial of Service

A denial of service (DoS) attack is specifically designed to interrupt normal system functions and affect legitimate users' access to the system. Hostile users send a flood of fake requests to a server, overwhelming it and making a connection between the server and legitimate clients difficult or impossible to establish. The distributed denial of service (DDoS) allows the hacker to launch a massive, coordinated attack from thousands of hijacked (zombie) computers remotely controlled by the hacker. A massive DDoS attack can paralyze a network system and bring down giant websites. For example, the 2000 DDoS attacks brought down websites such as Yahoo! and eBay for hours. Unfortunately, any computer system can be a hacker's target as long as it is connected to the Internet.

DoS attacks can result in significant server downtime and financial loss for many companies, but the controls to mitigate the risk are very technical. Companies should evaluate their potential exposure to DoS attacks and determine the extent of control or protection they can afford.

Unauthorized Access to Information

To control unauthorized access to information, access controls, including passwords and a controlled environment, are necessary. Computers installed in a public area, such as a conference room or reception area, can create serious threats and should be avoided if possible. Any computer in a public area must be equipped with a physical protection device to control access when there is no business need. The LAN should be in a controlled environment accessed by authorized employees only. Employees should be allowed to access only the data necessary for them to perform their jobs.

EXHIBIT 2
Financial Losses Due to System Security Threats in 2005

Type of System Security Breach	Amount of Losses
Virus	$42,787,767
Unauthorized access to information	31,233,100
Theft of proprietary information	30,933,000
Denial of service	7,310,325
Insider abuse of Internet access	6,856,450
Laptop theft	4,107,300
Financial fraud	2,565,000
Misuse of public Web applications	2,227,500
System penetration	841,400
Abuse of wireless network	544,700
Sabotage	340,600
Telecom fraud	242,000
Website defacement	115,000

Source: 2005 CSI/FBI Computer Crime and Security Survey

Abuse of Wireless Networks

Wireless networks offer the advantage of convenience and flexibility, but system security can be a big issue. Attackers do not need to have physical access to the network. Attackers can take their time cracking the passwords and reading the network data without leaving a trace. One option to prevent an attack is to use one of several encryption standards that can be built into wireless network devices. One example, wired equivalent privacy (WEP) encryption, can be effective at stopping amateur snoopers, but it is not sophisticated enough to foil determined hackers. Consequently, any sensitive information transmitted over wireless networks should be encrypted at the data level as if it were being sent over a public network.

System Penetration

Hackers penetrate systems illegally to steal information, modify data, or harm the system. The following factors are related to system penetration:

- System holes: the design deficiency of operating systems or application systems that allow hijacking, security bypass, data manipulation, privilege escalation, and system access.
- Port scanning: a hacking technique used to check TCP/IP ports to reveal the services that are available and to identify the weaknesses of a computer or network system in order to exploit them.
- Network sniffing: a hardware and software program to collect network (traffic) data in order to decipher passwords with password-cracking software, which may result in unauthorized access to a network system.

- IP spoofing: a technique used to gain unauthorized access to computers, whereby hackers send messages to a computer with a deceived IP address as if it were coming from a trusted host.
- Back door/trap door: a hole in the security of a computer system deliberately left in place by designers or maintainers.
- Tunneling: a method for circumventing a firewall by hiding a message that would be rejected by the firewall inside another, acceptable message.

According to Symantec, unpatched operating system (OS) holes are one of the most common ways to break into a system network; using a worm is also becoming more common. Therefore, the first step to guard against hackers is to download free patches to fix security holes when OS vendors release them. Routinely following this step can dramatically improve network security for many companies. Companies can use patch-management software to automate the distribution of authentic patches from multiple software vendors throughout the entire organization. Not all patches can work flawlessly with existing applications, however, and sometimes the patches may conflict with a few applications, especially the older ones. If possible, patches should first be tested in a simulated environment, and existing systems should be backed up before the patch is installed.

Companies can use software tools or system-penetration testing to scan the system and assess systems' susceptibility and the effectiveness of any countermeasures in place. The testing techniques must be updated regularly to detect ever-changing threats and vulnerabilities. Other controls to mitigate system penetration are as follows:

- Install anti-sniffer software to scan the networks; use encryption to mitigate data-sniffing threats.
- Install all the server patches released by vendors. Servers have incorporated numerous security measures to prevent IP spoofing attacks.
- Install a network firewall so that internal addresses are not revealed externally.
- Establish a good system-development policy to guard against a back door/trap door; remove the back door as soon as the new system development is completed.
- Design security and audit capabilities to cover all user levels.

Telecom Fraud

In the past, telecom fraud involved fraudulent use of telecommunication (telephone) facilities. Intruders often hacked into a company's private branch exchange (PBX) and administration or maintenance port for personal gains, including free long-distance calls, stealing (changing) information in voicemail boxes, diverting calls illegally, wiretapping, and eavesdropping.

As analog and digital data communications have converged, some companies have utilized the Voice over

Internet Protocol (VOIP) to lower phone bills. The originating and receiving phone numbers are converted to IP addresses and the PBX is linked to a company's networked computers, and hackers can get into systems through PBX or computerized branch exchange (CBX). In addition, every PBX/CBX system is equipped with a software program that makes it vulnerable to remote-access fraud, and intruders use sophisticated software to find an easy target. Once a PBX is hacked, hackers have the same access to a company's phone system and computer network as do the employees.

Information is a commodity in the e-commerce **era, and there are always buyers for sensitive** information, including customer data, credit **card information, and trade secrets.**

Companies should install software to monitor service usage at various points on the network, including the VOIP gatekeeper, VOIP media controller, and broadcast server. The software can monitor the system packet performance and the router applications on the converged network. The software can also automatically alert the responsible person if any abnormal activities have been detected.

Theft of Proprietary Information

Information is a commodity in the e-commerce era, and there are always buyers for sensitive information, including customer data, credit card information, and trade secrets. Data theft by an insider is common when access controls are not implemented. Outside hackers can also use "Trojan" viruses to steal information from unprotected systems. Beyond installing firewall and anti-virus software to secure systems, a company should encrypt all of its important data.

Access privilege and data encryption are good preventive controls against data theft by unauthorized employees who steal for personal gain. The access controls include the traditional passwords, smart-card security, and more-sophisticated biometric security devices. Companies can implement some appropriate controls, including limiting access to proprietary information to authorized employees, controlling access where proprietary information is available, and conducting background checks on employees who will have access to proprietary information. There will, however, always be some risk that authorized employees will misuse data they have access to in the course of their work. Companies can also work with an experienced intellectual property attorney, and require employees to sign noncompete and nondisclosure agreements.

Financial Fraud

The nature of financial fraud has changed over the years with information technology. System-based financial fraud includes scam e-mails, identity theft, and fraudulent transactions. With spam, con artists can send scam e-mails to thousands of people in hours. Victims of the so-called 419 scam are often promised a lottery winning or a large sum of unclaimed money sitting in an offshore bank account, but they must pay a "fee" first to get their shares. Anyone who gets this kind of e-mail is recommended to forward a copy to the U.S. Secret Service (419.fcd@usss.treas.gov).

Companies should review bank statements as soon as they arrive and report any suspicious or unauthorized electronic transactions. Under the Electronic Fund Transfer Act, if victims notify the bank of an unauthorized transaction within 60 days of the date the statement is delivered, they are not liable for any loss. Otherwise, victims could lose all the money in their account, and the unused portion of the maximum line of credit established for overdrafts.

Phishing is a form of identity theft. Spam is sent claiming to be from an individual's bank or credit union or a reputable e-commerce organization. The e-mail urges the recipient to click on a link to update their personal data. The link takes the victim to a fake website designed to elicit personal or financial information and transmit it to the criminals.

User should never give out credit card numbers, PINs, or any personal information in response to unsolicited e-mail. Instead of clicking a link in a suspicious e-mail, call the office or use a URL that is legitimate to verify an e-mail that claims to be from a bank or financial institution. When submitting sensitive financial and personal information over the Internet, make sure the server uses the Secure Sockets Layer protocol (the URL should be https:// instead of the typical http://).

Misuse of Public Web Applications

The nature of e-commerce—convenience and flexibility—makes Web applications vulnerable and easily abused. Hackers can circumvent traditional network firewalls and intrusion-prevention systems and attack web applications directly. They can inject commands into databases via the web application user interfaces and surreptitiously steal data, such as customer and credit card information.

User authentication is the foundation of Web application security, and inadequate authentication may make applications vulnerable. Companies must install a Web application firewall to ensure that all security policies are closely followed. The following additional controls can mitigate Web application abuses:

- Installing security patches promptly.
- Using a Web application scanner to discover any vulnerability.

- Monitoring the server and applications to identify any potential problems and terminate malicious requests.
- Hiding information that end users do not need to know, including the server machine type and the operating system.

Website Defacement

Website defacement is the sabotage of webpages by hackers inserting or altering information. The altered webpages may mislead unknowing users and represent negative publicity that could affect a company's image and credibility. Web defacement is in essence a system attack, and the attackers often take advantage of undisclosed system vulnerabilities or unpatched systems.

Network firewalls cannot guard against all web vulnerabilities. Companies should install additional Web application security to mitigate the defacement risk. All known vulnerabilities must be patched to prevent unauthorized remote command execution and privilege escalation. It is also important that only a few authorized users are allowed root access to a website's contents. Access to different Web server resources, such as executables, processes, data files, and configuration files, should be monitored. Commercial website monitoring services are also available.

Sabotage

According to the 2005 CSI/FBI survey, system security incidents were committed by insiders about as often as by outsiders. Some of the controls discussed above can provide protection against the sabotages committed by outsiders, but no organization is immune from an employee abusing its trust. For example, Omega Engineering was a thriving defensive manufacturing firm in the 1990s; it used more than 1,000 programs to produce various products with 500,000 different designs for their customers, including NASA and the U.S. Navy. On July 31, 1996, Omega Engineering's server crashed and all of the software programs were lost. To make matters worse, on the same day the backup tape also disappeared. The investigation quickly revealed that it was a deliberate sabotage by the former system administrator, Tim Lloyd, who had been terminated 30 days before the catastrophe. Lloyd designed and planted a time bomb to erase all the programs on the server. The crash resulted in $10 million in lost revenues and led to 80 layoffs.

When it comes to security, companies often pay attention only to the perimeter of the organization, not the inside. Sabotages by insiders is often orchestrated when employees know their termination is coming. In some cases, disgruntled employees are still able to gain access after being terminated. The 2005 insider-threat case study results by CERT/SEI (www.cert.org/archive/pdf/inside cross051105.pdf) help identify, assess, and manage sabotage threats from insiders. Their key findings were as follows:

- A negative work-related event (e.g., firing, downsizing, or promotion pass-over) triggered most insiders' actions.
- Most of the insiders had acted out in the workplace.
- The majority of insiders planned their activities in advance.
- Less than half of all of the insiders had authorized access at the time of the incident.
- Insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, or procedures, but relatively sophisticated attack tools were also employed.
- The majority of insiders compromised computer accounts, created unauthorized back-door accounts, or used shared accounts.
- Remote access was used to carry out the majority of the attacks.
- The majority of the insider attacks were detected only after the damage was already done.
- System logs were the most prevalent means by which the insiders were identified.

As indicated by the CERT/SEI study, the convenience of remote access facilitates the majority of sabotage attacks. Another potential threat of unauthorized use is when employees quit or are terminated but there is no coordination between the personnel department and the computer center. In some cases, employees still have system access and an e-mail account after they have left an organization. It is also not unusual that employees know the user IDs and passwords of their colleagues. Companies can adopt some of the following steps to protect against such threats:

- Disable an employee's system access promptly.
- Enforce a company-wide password change on a regular basis, including the day an employee resigns or is terminated. (This control is not feasible with huge organizations, because people leave every day.)
- Use biometric access control if possible.
- Obtain the password and encryption code to an employee's laptop or encrypted files on the server.
- Maintain a system activity log as a detect control. (The creation of an activity log, however, can increase system overhead, especially for larger organizations.)

When it comes to **security, companies** often pay attention only **to the perimeter of** the organization, not **the inside.**

Company Awareness

Business operations can be disrupted by many factors, including system security breaches. System downtime, system penetrations, theft of computing resources, and lost productivity have quickly become critical system security issues. The financial loss of these security breaches can be significant. In addition, system security breaches often taint a company's image and may compromise a company's compliance with applicable laws and regulations. The key to protecting a company's accounting information system against security breaches is to be well prepared for all possible major threats. A combination of preventive and detective controls can mitigate security threats. ❑

***P. Paul Lin, PhD,** is an associate professor of accounting at the Raj Soin College of Business of Wright State University, Dayton, Ohio.*