DEFENDING THE SECURITY OF THE ACCOUNTING SYSTEM

*By **Michael S. Luehlfing, Cynthia M. Daily, Thomas J. Phillips, Jr., and L. Murphy Smith***

UNINTENTIONAL ERRORS AND OMISSIONS CAUSE the great majority of computer security problems. Errors and omissions are particularly prevalent where there is sloppy design, implementation, and operation.

System security measures should be a primary focus in developing a new accounting information system (AIS). The viability of security measures depends upon informed and constant monitoring of the system; unfortunately, it is often neglected. Key components of systems security include passwords, firewalls, data encryption, employee participation, and protection from computer viruses.

Security Philosophy

Generally speaking, systems security involves risk assessments and countermeasure implementations to ensure that such systems will operate, function correctly, and be safe from attack by internal and external adversaries. Central to proper systems security is that all stakeholders must understand the general need for security and the specific potential threats faced by the organization.

In January 2000, the AICPA published its annual list of top 10 technology issues. The systems security topics of information security and controls, disaster recovery, and high availability and resiliency of systems all made the top five.

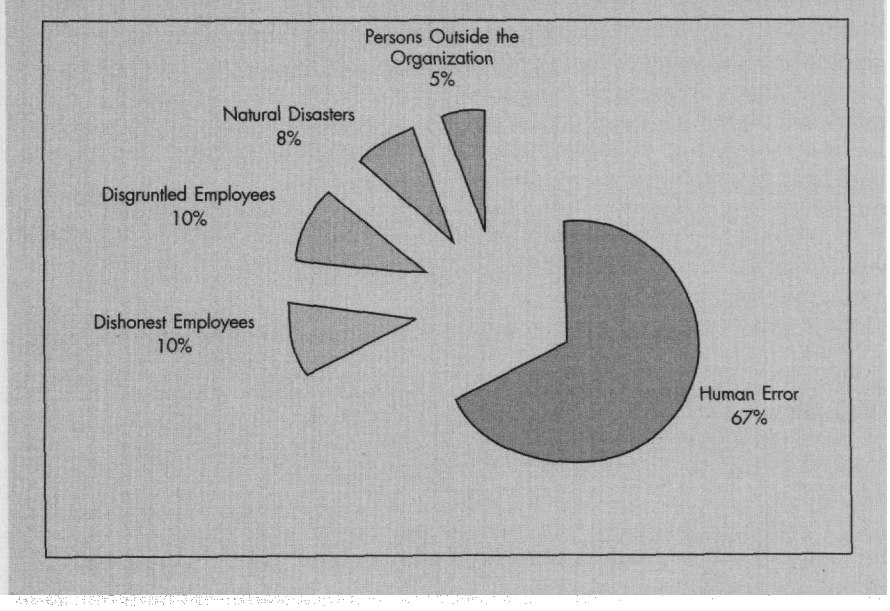
Barriers to developing systems security are both financial and philosophical. Systems security is often viewed in a manner similar to physical security: Buy it once and use it forever. Unfortunately, like physical security, obsolete policies, procedures, and technologies leave systems extremely vulnerable to external and internal attacks. Most stakeholders find it difficult to accept the need for constant spending on systems security when it is difficult to quantify the benefits. Even when benefits can be quantified, unenlightened stakeholders may still question the need for continuous spending in the systems security area. In many cases, education can overcome this philosophical barrier. Unfortunately, often only severe losses from a security breakdown will prompt appropriate, albeit late, action.

Calculation of security benefits. The benefits of systems security can be calculated from a loss exposure perspective. The following process is generally undertaken to quantify loss exposure: First, each system must be identified. Second, each system must be prioritized in terms of sustaining daily operations. Finally, a dollar amount must be calculated for the upper cost limits to the company if a particular system were compromised or even destroyed. Once this is done, the cost of the security system program or upgrade must be compared to the upper cost limits of system failure. Before undertaking such a task, the system's vulnerabilities in terms of passwords, firewalls, data encryption, and employees must be understood.

Threats to Computer Security

Based on movies and television shows, it might appear that the greatest threat to computer security is intentional sabotage or unauthorized access to data or equipment. For most organizations this is simply not true. There are five basic threats to security: natural disasters,

EXHIBIT 1
THREATS TO COMPUTER SECURITY



dishonest employees, disgruntled employees, persons outside of the organization, and unintentional errors and omissions. The extent to which each of these threats is actually realized is shown in *Exhibit 1*.

As shown in the exhibit, unintentional errors and omissions cause the great majority of computer security problems. Errors and omissions are particularly prevalent where there is sloppy design, implementation, and operation; if the systems development process is done properly, errors and omissions will be minimized. An effective internal control structure is an integral part of any reliable information system.

A primary motive for a well-designed set of internal controls is to support the fiscal management capabilities of the firm's officers and employees. Inadequate internal controls can severely hinder fiscal management and unduly tempt officers and employees to become engaged in questionable activities and accounting practices. Chaotic accounting and fiscal management conditions resulting from inadequate controls create unnecessary conditions of stress, which can impair officers' and employees' mental well-being and task effectiveness. Strong controls guard honest officers and employees from suspicion and false accusations.

INADEQUATE INTERNAL CONTROLS can severely hinder fiscal management and unduly tempt officers and employees. Strong controls guard honest officers and employees from suspicion and false accusations.

Passwords

User authentication is especially important as applications are tied into operating systems and linked around the world. In this regard, inappropriate use of passwords, internally or externally, is a primary risk that systems face.

Password control is essential. Employees should be admonished to safeguard passwords. For example, they should not tape passwords inside desk drawers or under keyboards and they should not use obvious terms such as the name of a spouse, child, or home address. Furthermore, simple things like randomly putting a number within a password will enhance security.

With respect to the overall organization, access to passwords should be strictly controlled. While organizations typically allow their information technology (IT) personnel access to all employee passwords, this creates an unnecessary opportunity for unauthorized access using another person's name. Similarly, employees should only have access to areas that are essential to their particular functions. For example, staff accountants do not need access to high-level administrative files. Accordingly, security levels must be articulated for each user or group of users.

Password maintenance requires constant diligence on the part of both the IT and human resources departments. For example, the passwords of employees leaving the organization should be immediately canceled upon notice or before termination, as applicable. Given the sensitivity of certain termination situations, coordination between IT and human resources is critical to successful password maintenance.

Just like industrial spies, hackers can also pose as employees to obtain sensitive information such as passwords. Typically, they make an authentic-looking ID and walk into an office under the guise of service contractor or government inspector. Hackers then install a "sniffer" (a device plugged into a network jack) that collects passwords as well as user names. Hackers can also acquire passwords by nontechnical means. They often begin by socializing with employees to obtain employee names, departments, or personal information and then name drop to get user names to support front-end attacks. Armed with this information, a hacker can easily enter most systems.

Firewalls

While the appropriate use and safeguarding of passwords is often associated with the prevention of front-end attacks, firewalls are typically deployed to

EXHIBIT 2
CPA WEBTRUST SEAL

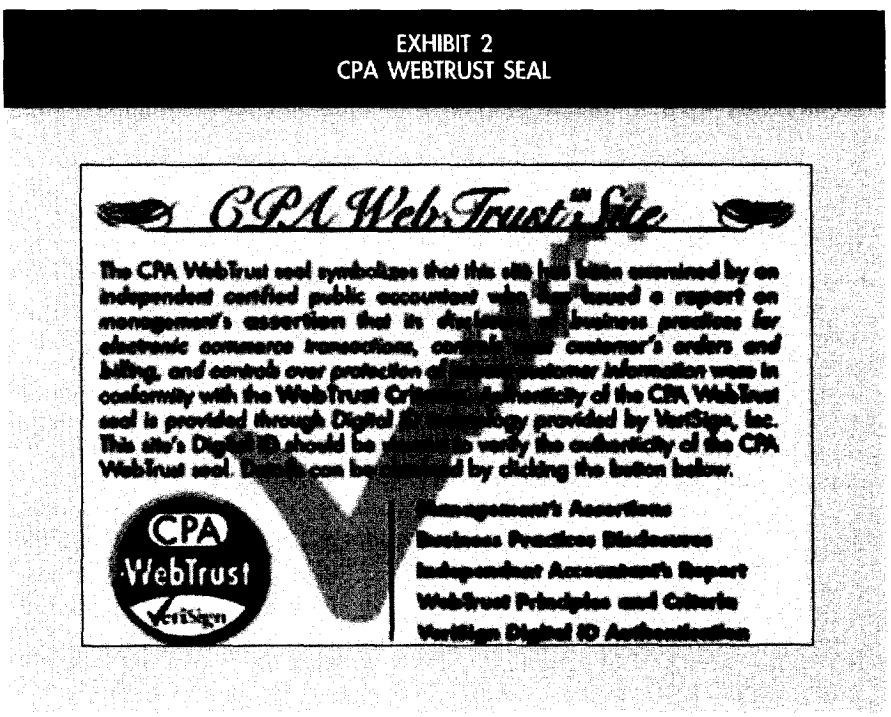


EXHIBIT 3
SAFE USER PROCEDURES FOR DEFENDING AGAINST COMPUTER VIRUSES

- Make backup copies of both programs and data files.
- Use public domain software such as freeware and shareware with extreme care.
- Test all software, both retail and public domain.
- Create meaningful volume labels on all hard disks and diskettes, and routinely check them for changes.
- Take notice of unusual system activities such as less available system memory than normal or activity in a system device that should be idle.
- Be wary of opening e-mail containing attachments of executable files (e.g., .exe, .com, .vbs).

impede back-end attacks. Generally speaking, a firewall is a combination of hardware and software that controls access between systems. Firewalls are especially critical when linkages exist between the Internet and internal systems. Firewalls are typically designed to allow users connected to internal systems to download information from the Internet, but not vice versa.

A firewall is only as good as its weakest link. In order to exploit holes in a security system, hackers often employ repetitive lurking schemes such as war dialers, which automatically dial a block of phone extensions thought to be connecting an internal network to the Internet. Developing countermeasures for such techniques is a continual process, because hackers are constantly developing new techniques. For example, if hackers find a way to penetrate through a weakness in an application, the vendor will likely write a patch to fix the problem, forcing hackers to find a new way to attack the application.

Because patching is a continuous process, monitoring a firewall is as important as implementing it. In this regard, current firewall systems should be grounded in real-time monitoring and response capabilities. Similarly, automated detection systems must be in place in order to alert IT personnel that a security breach is in progress.

Data Encryption

Encryption techniques should be employed by any company involved in e-commerce or electronic payment and collection activities. Encryption protects data as it moves between systems by scrambling it in transit. The current minimum encryption level is 128-bit encryption, but it will soon be 256-bit; lower levels (e.g., 64-bit) of encryption can be easily deciphered by today's computers. Accordingly, encryption complexity must evolve with the computer technology used to crack it.

Employees

For all of the fear pertaining to external attacks, internal users are a more likely threat. Although the need for external security measures goes without saying, internal policies and procedures (including monitoring) are at the heart of systems security. Identifying user profiles and understanding user tendencies will often identify unusual situations. Background checks of potential and current employees may also provide insight into unusual situations.

Employee security breaches may be categorized as rather innocent, seemingly reckless, or outright criminal, depending upon the circumstances. Unfortunately, there are no foolproof means for preventing the inappropriate use of a system or its contents by an employee. The existence of good internal control policies and procedures is the best defense.

Such policies and procedures are necessary in view of the typical defense of untrustworthy employees (i.e., nobody told me it was wrong). Most programmers or web designers are too busy worrying about functionality and design to worry about system security. As a countermeasure, companies need to obtain assurances from external security specialists. Addressing some aspects of system security is a relatively new service available from CPAs called WebTrust.

The AICPA and the Canadian Institute of Chartered Accountants (CICA) jointly introduced CPA WebTrust in September 1997. Websites bearing the WebTrust seal have been deemed trustworthy and reliable by a CPA. Clicking on the seal on a particular website provides access to information about the firm's business practices, management assurances, and the independent auditors' report.

Exhibit 2 shows the WebTrust seal. Organizations that bear the seal are listed online at www.cpawebtrust.org. Some WebTrust-certified firms prominently display the seal on their homepage (e.g., www.alpinebank.com), while others display it under the security section or on some other page. Some firms use more than one type of assurance service (such as the Better Business Bureau Online and TrustE certifications). For a further discussion of WebTrust and its perception by consumers, see the feature article on page 46.

Another employee-related issue is inappropriate use of the Internet and e-mail systems. For example, downloading or e-mailing pornography or other insensitive materials should be expressly forbidden. Pornography is a major concern under the hostile environment definition of sexual harassment. Employers that care about their employees will want to protect them from pornographic materials. The use of e-mail to transmit insensitive materials is also a problem. Sooner or later the organization can and will be held responsible and accountable for such transmission.

Computer Viruses

Numerous news stories have left many computer users confused about the nature of viruses and the damage they can cause. A virus is a computer program that piggybacks or attaches itself to application programs or other executable system software. There are many different ways that viruses can be transmitted and executed. When a virus is activated, the results also vary: Sometimes it erases files, sometimes it just leaves harmless messages. Antiviral techniques include safe user procedures and antivirus software (see *Exhibit 3*).

Getting Started

The following five steps provide a starting point for developing systems security:

Don't wait. Appropriate systems security should be developed as early as possible. First, all information systems user departments should develop their own security and response capabilities in preparation for possible disruptions.

Involve users. Ralph Waldo Emerson once said, "Nothing great was ever achieved without enthusiasm." People are the most important component of any systems security process. The goal of preventing security breakdowns must be explained to all system users. Top management must support the process with clear policy statements and directives. After a security breakdown occurs, a thorough after-the-fact analysis must be conducted in order to facilitate the development of solutions to prevent such incidents from happening in the future. The focus must be on solving problems, not placing blame.

Friends and enemies. When a system breakdown occurs, it is essential to determine whether it was a software or hardware failure or an intentional disruption by an adversary. This distinction is critical in order to develop appropriate countermeasures. Often an organization can benefit from the assistance of consultants specializing in security measures.

Be prepared. To catch a thief think like a thief. Organizations can stay alert by identifying potential weaknesses in the accounting system and implementing appropriate countermeasures.

Beware of canned software. Default settings in vendor-supplied software are generally set to "accept" all requests. Security-related settings should be changed to a "deny all" mode and later methodically reset to accept only what is essential. As with all system components, any changes should be carefully documented to assist with future investigations.

A Continuous Process

Systems security may be viewed as a necessary evil, but the key word is "necessary." Identifying vulnerabilities and taking measures to eliminate them can save an organization from severe losses. As technology changes, so do potential weaknesses. Keeping up with protective measures and how they can be used to eliminate weaknesses is crucial. Websites such as www.securitywatch.com and www.securityfocus.com provide information regarding available products, explanations of various security-related terms, and trends in computer security. ❑

***Michael S. Luehlfing, PhD, CPA, CMA**, is an associate professor of accounting, **Cynthia M. Daily, MBA, CPA**, a doctoral candidate, and **Thomas J. Phillips, Jr., PhD, CPA**, a professor, all at Louisiana Tech University, Ruston. **L. Murphy Smith, DBA, CPA**, is a professor of accounting at Texas A&M University, College Station.*