

A Primer on Information Security: Part 1

Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society, the federal government, state and local governments, the private sector, and the American people.

—White House home page for The National Strategy to Secure Cyberspace¹

These attacks (viruses) did not occur because the extremely innovative engineers creating the underlying codes disregarded security. They occurred because equally innovative criminal hackers worked day after day to find, create and exploit vulnerabilities in the software or in human nature that gave them new ways to trespass on your computers, steal your data and shut down your networks.

—Howard Schmidt, former U.S. Cybersecurity Chief⁹

Security is everyone's responsibility.

—James E. Gordon, Vice President, Pinkerton Consulting & Investigations

Recent world events have overshadowed the move toward improving information security among governments, businesses, and individuals; but security issues have been on the agenda for years. This article reviews some of the key concepts related to information security. The next installment will discuss areas of potential exposure and liability that clients face.

National Cybersecurity Priorities

The federal government's policies and efforts toward securing cyberspace have been the subject of much debate and controversy. This spring, the second cybersecurity chief appointed this year resigned. Most reports attribute his resignation to

the lack of priority the government is giving to this issue. At the time of this writing, the national cybersecurity chief's position was reported to be undergoing an effective demotion in prominence and priority.

Meanwhile, the International Information Systems Security Certification Consortium (also known as (ISC)²), a nonprofit organization dedicated to training and certifying information security professionals worldwide, announced in late May that 13 senior-level U.S. civilian agency and national security managers have been named charter members of the (ISC)² Government Advisory Board for Cyber Security. The volunteer advisory board is to provide insight and advice to the (ISC)² executive management team on information security policies and trends and make recommendations regarding certifications for government sector cybersecurity professionals.

Despite mixed signals and some changing priorities, the administration's policies provide an important road map for this discussion. From the start, the administration suggested a number of efforts for individuals, businesses, and government:

- implement procedures to authenticate users
- plan enterprise architecture and deployment with security in mind
- train all employees on the need to maintain security
- create a regular process to assess and correct network vulnerability
- continuously assess threats and vulnerabilities and their risks to government agencies

Security Versus Privacy

At the outset, it is important to remember that there is a distinction between security and privacy. The privacy initiatives (including those mandated by the government) are

very different from the security issues.

The essence of the privacy initiatives is *disclosure, collection, and use*. The security issues, on the other hand, primarily deal with *access, identification, and integrity*. A financial institution, health care provider, employer, or Internet service provider may be subject to a number of rules on privacy that simply affect disclosures to users, customers, or patrons about what information may be collected and how that information may be used.

Business Continuity

An important aspect of the corporate responsibility of officers and directors is to ensure the continuity of the business. For information systems, this typically means ensuring that backups of data are maintained in a secure environment or that disaster recovery plans are in place to facilitate continuity in the event of an exceptional event. Increasing reliance on information technology coupled with the exposure to the systems from hackers (intruders who either wish to engage in economic espionage or for malicious reasons) has required companies to take another look at their security and procedures to ensure business continuity.

While special rules have recently come into effect regarding information security, it is important to remember that officers and directors are always under an obligation to address these important issues. The obligations of officers and directors to ensure the operation of the company in a prudent manner require that mission-critical information systems be kept secure, that backups be maintained, and that alternatives be available in the event of a disaster. Similarly, it is the responsibility of the officers to ensure that the books and records of the company be maintained in a method that is both retrievable and auditable.

What Is Information Security?

At its core, effective information security seeks to prevent unautho-

rized access to its systems and data and to ensure that a business can rely on its information systems. These policies and activities take many forms, and a few are discussed below in more detail.

Physical Security. Companies who are looking for high-tech solutions to their security problems often forget the basic, low-tech activities. It is just as important to ensure that the security threat does not walk through your company's front door as it is to ensure that a surreptitious threat does not hack in through the back door. As part of this analysis, you need to ask your client whether it

- restricts unauthorized access to the business premises;
- sets up its information systems so that only authorized users can access important applications, data, or other systems;
- has a coherent and effective process for information storage and backup; and
- establishes and enforces employment policies that deal with securing the company's systems and preventing unauthorized access.

It does no good for a company to spend thousands or millions of dollars on various security methodologies if physical security is ignored and an intruder can walk into the office of an executive and rummage through confidential files. If a personal computer is left on and logged in, the intruder can access, copy, or tamper with data for the company's mission-critical applications.

Authentication. Now that your client has ensured that the intruder is stopped at the front desk and cannot freely access the computer systems, the next step is to ensure that anyone who attempts to access the information systems is, in fact, the person who is purporting to access your system. In other words, *who* is accessing the information system?

Procedures for the authentication of a user are myriad. At its simplest level, authentication can be the logins and password assigned to an

employee, or authorized to a third party through a registration process. However, as we all have experienced, login names and passwords tend to get shared or even left in the open. (Those yellow Post-It notes have made short notes quite easy, but they have provided challenges to those charged with information security.)

When you go beyond the simple login/password process, authentication can improve significantly. In some circumstances, the computer network can limit access to a particular user when that user is logged in to a particular computer. This can prevent the rogue employee who wants to obtain salary information from logging in to the payroll or human resource application based on a surreptitiously copied password.

At the next level, there are a number of authentication methodologies that rely on human unique characteristics. These are known as biometric methodologies and include such methodologies as retinal scans, finger- or hand-print authentication, voice recognition systems, or others that are under continuous development. As the costs of these systems decline (a thumbprint biometric unit is now available for under \$200), the use of these systems may become more common.

Digital Certificates. When you are dealing with someone outside your office, whether across the street or across the world, the means for authentication can sometimes be difficult. This is especially true when there is communication by electronic mail or electronic data interchange. A company can certainly rely on login names and passwords, or the user name in the electronic message, but there is no certainty in either of these systems. One methodology that has been available for a number of years but has had relatively little penetration is the digital certificate.

A certificate is essentially a mathematical formula assigned to a person by a trusted third party known as a certification authority. The person uses the certificate as part of a message or document execution process

and the authentication of the person or the identification of the sender can be established by reference to a publicly available "key" for that person. This methodology is known as a public key infrastructure, or PKI.

While PKI has been available for many years, its use by businesses and individuals has been very limited, primarily because of the issues associated with costs and implementation.

Encryption. Once the issue of authentication is addressed, a company is then ready to deal with the integrity of the data transmission. While the movement of data within a corporate network is not normally an issue, the movement of data over public networks, the Internet, or wireless signals poses security risks. Data that is moved between points in this manner is subject to interception by third parties and may also be subject to alteration.

One method to provide security for data transmission is through the use of encryption. An easy example of encryption can be found on most transactional Web sites. If you are entering information about yourself or using credit card information to make a purchase, you will often be routed to a "secure" Web site. This site will typically use a methodology such as secure socket layer (SSL), which is security software that scrambles the data at the point of transmission using a mathematical algorithm and unscrambles it at the point of receipt. Any third party that intercepts or copies the data transmission will presumably then have a very difficult time making sense of it. This and other types of encryption software have been around for several years (remember PGP—Pretty Good Privacy). As communications and wireless systems improve, encryption of data transmission will become more commonplace as well as more secure.

Where is Security Important?

The use of effective security procedures on mainframes, servers, networks, computers, and workstations

is generally the starting point. If a company uses a transactional Web site, allows employee or third-party access to its networks from outside the facilities, or allows wireless transmission of data, security protocols need to be scaled to address the actual manner in which information is accessed and transmitted. The level of the necessary security will depend on the sensitivity of the data.

One aspect of information security that can be effective but that is often overlooked, is the communication of the company's expectations and policies in a clear manner. Ask yourself the following questions about your own firm or company information systems:

- Are the company's rules and policies scattered among a number of hard copy memos that are not part of an orientation process?
- Is the new employee given two binders of policies but no orientation on what is really expected regarding information and other company security processes?
- When a new employee is given an initial login and password, is the employee required to immediately change the password?
- Are there standards for passwords that are eligible for use, such as requiring both letters and numbers and a certain number of characters or letters?
- Does the network require a user to periodically change his or her password?
- Do the employees responsible for information security monitor network activity or activity at external entrance points to the network?
- At the end of an employment relationship, does the exit interview include a review of the company policies regarding confidential and proprietary information?
- Is the outgoing employee's system login deactivated automatically when the termination is effective?
- If a person has external access to networks, is the external access deactivated on a timely basis?

No process is perfect, but reasonable practices that (1) limit access, (2) provide means for authentication, and (3) protect the integrity and security of data transmission are minimal practices that every company should consider.

Part 2 of this article will address new rules on security and the potential exposure and liability of companies related to information security.

NOTES

1. Available at www.whitehouse.gov/pcipb/ (last visited July 7, 2003).
2. Available at www.energycommerce.house.gov/107/hearings/11152001Hearing420/Schmidt718.htm (Nov 15, 2001).



Michael S. Khoury is a principal with Raymond & Prokop, PC, in Southfield, and practices in the areas of information technology, electronic commerce, and commercial law. In 2003, he was appointed as the team leader for the firm's Technology Industry Group. He is a member of the Business Law Section's council and its director of technology and is a former chair of the Computer Law Section of the State Bar of Michigan.