

A Primer on Information Security: Part 2

Part 1 of this article examined some of the overall issues regarding cybersecurity, privacy, basics on security protection, and security policies. Part 2 discusses some of the specific legislative and regulatory initiatives involving security and strategies that businesses should consider in securing information and systems. Finally, Part 2 looks at identity theft, one of the fastest growing problems facing individuals and businesses.

New Rules Regarding Security

While there have been a number of legislative initiatives at both the state and federal levels dealing with information security, the three that have received the most attention involve the Health Insurance Portability and Accountability Act (HIPAA),¹ the Gramm-Leach-Bliley Financial Institutions Modernization Act (GLB),² and the Patriot Act of 2001.³

HIPAA

HIPAA is generally known for the rules that deal with coverage of pre-existing conditions and the privacy of health information. The statute also mandated, however, that health care providers, employers, and any other entity with access to personally identifiable health information must also take actions that fall within the purview of information security.

While a number of rules and regulations have been announced and made effective over time, the statute also provides for certain obligations that are immediately effective. Foremost among these is the obligation of the health care provider to ensure the integrity of data. This essentially requires that any person maintaining systems for personally identifiable health care information have systems in place that ensure that the data cannot be tampered with and is otherwise free from corruption. Systems should have access

limited to those authorized to view and change the data, and are required to have reasonable protocols to prevent data corruption.

The second phase of HIPAA implementation, the privacy rules, became effective on April 14, 2003. While the majority of the new regulations deal with privacy disclosures for health care providers, providers are also required to ensure that access to patient files and information is limited to those people who have the authority to view and use the information.

Finally, the HIPAA security rules were released in final form in March 2003. The essential elements of the security rules fall into four categories:

- **Administrative safeguards:** These deal with safeguards such as passwords.
- **Physical safeguards:** These deal with securing the physical site where data is kept. How are devices and computers protected? Who has access?
- **Technical safeguards:** These deal with access and audit controls, data integrity issues, and individual authentication processes.
- **Risk management and analysis:** Organizations privy to HIPAA data must look at cost-effective security measures. Security requirements are scalable based upon the kind of information used and the organization using the information.

One of the items not mandated in the final HIPAA security rules was a requirement regarding data encryption. Initial discussions had involved the potential use of specific levels of data encryption, but these were left out of the final rules. As encryption technology matures, however, it will not be a surprise to see encryption requirements in the future.

Gramm-Leach-Bliley

GLB also has several privacy and

security components. The privacy requirements are responsible for all of the confusing and often poorly-written inserts to our bank, insurance, and brokerage account statements. GLB also addressed requirements for the security of financial transactions, similar to the requirements of HIPAA.

U.S.A. Patriot Act

The enactment of the U.S.A. Patriot Act and some of the discussions regarding Patriot II actually address the ability of governmental authorities and other entities involved in the flow of information to compromise the security of data. Under the Patriot Act, the government now has the ability to conduct electronic surveillance of anyone it suspects of being involved in terrorist activity. One of the significant provisions of the act allows Internet service providers (ISPs), universities, network administrators, and other people involved in the administration of computer networks to conduct surveillance of "trespassers" without a court order.

If requested by the FBI, Internet providers and telephone companies are actually required to turn over customer information, including phone logs, without a court order if the FBI claims that the records are related to a terrorism investigation. The ISP or telephone company is actually prohibited from disclosing to its customer that it has received this request from the FBI or that it has turned over any information.

While effective tools for governmental investigations are necessary to protect us from terrorism, there are many concerns that the Patriot Act will not only compromise privacy but potentially compromise security. This is an issue that people involved in information security should follow closely.

Disclosure of Security Breaches

California now requires ISPs and other organizations that collect personal information to notify citizens if their personal data is compromised.

Most companies have long avoided a public admission of embarrassing security lapses, but there is speculation that similar legislation may get floated at the federal level.

Many security breaches are never reported to the authorities, and people or companies that have had private data stolen may never know until it is too late. However, there are obligations that do exist.

For taxpayers that maintain electronic records, the Internal Revenue Service (IRS) requires taxpayers to notify the IRS if electronic tax records are "lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed . . . or are found to be incomplete or materially inaccurate."

Proposed regulations and recently introduced legislation may be adding additional obligations in the financial services arena and could impose obligations similar to California on a national basis, especially for public companies.

Business Responsibilities

Businesses have multifaceted responsibilities regarding information security. The basic obligation to ensure business continuity rests on the officers and directors of the company, but the businesses also have responsibilities to employees, customers, and others.

The three key concepts that are important for every business to recognize are (1) confidentiality, (2) integrity, and (3) availability.

Securing the systems to ensure that the confidentiality of proprietary, personal, or trade secret information is a given, but, as was discussed in Part 1 of this article, security systems are sometimes less than adequate.

The integrity of data and the company's systems are necessary for effective business continuity and may also be an element of legislation or regulation. The obligation to secure data, including personal information of employees or customers, requires that the company have controls in place to ensure system

integrity and to be able to audit compliance on system integrity.

Finally, the need for the availability of mission-critical systems is essential for business continuity, and the breach of a system's security is a sure way to compromise availability.

System Protection Strategies

Most companies do employ basic security strategies for their system networks. These include antivirus protections, network firewalls, and company policies to limit security risks. However, in the age of hackers, crackers, and cyberterrorists, more is going to be needed. Each company should consider a planning process to assess the security threats it may face and to make a risk management decision that balances those risks and threats with the costs of protecting its systems. Elaborate security procedures can be very expensive and can result in difficulties in doing business on a day-to-day basis. However, each emergency preparedness and business protection strategy should address these issues.

Among the new tools that are available to information technology professionals are intrusion detection devices. These monitor the network to determine how many times someone attempts to access your network or systems and the manner of that access and attempts to collect information about the intruder. Since most intrusions and network hacks begin with surveillance and information gathering, this is a good way to determine whether you are being targeted.

The industry is also beginning to develop certification procedures for security professionals and standards by which a company can evaluate its systems. All of these will be useful in planning coherent strategies for information in its system security.

Information Security Governance

The dramatic increase in cybersecurity incidents has led to a deluge in the number of reports, recommenda-

tions, and solutions. Until recently, however, no organization had looked at information security governance on a holistic basis.

In a white paper that was published by the Business Software Alliance (BSA), a number of broad policy conclusions, findings, and recommendations were made by a task force with substantial experience in the area.⁴ The white paper discusses four findings of the task force assembled by BSA:

- The government has already established a significant legislative and regulatory regime around ID security, and is considering additional action.
- Information security is often treated solely as a technology issue, when it should also be treated as a governance issue.
- There is already broad consensus on the action necessary to remedy the problem.
- Lack of progress is due in part to the absence of a governance framework.

To promote its recommendation that industry should develop a framework for information security governance, the BSA task force recommends a framework for security governance that recognizes the drivers for both business and governance, the roles and responsibilities of different parts of an organization, and the need for quantifiable metrics. In all cases, those responsible for governance must be able to audit and verify the processes and results.

Efforts such as those of the BSA will improve the quality and consistency of information security in this country.

Identity Theft

One of the fastest growing problems for both businesses and individuals is identity theft. It is estimated that as many as seven million Americans had their identities stolen last year. For individuals, identity theft can mean damaged credit; for businesses,

the financial losses can be staggering. There are efforts on both the criminal and civil fronts to address this problem.

The federal government is attacking identity thieves on three fronts, first by getting the word out. The Federal Trade Commission (FTC), through its ID theft Web site (<http://www.consumer.gov/idtheft/>), is trying to inform the public about the threat of ID theft and how to keep from being a victim. The FTC has also developed a unified ID theft affidavit that consumers can fill out to dispute fraudulent debts across multiple accounts. The FTC has set up an ID theft hotline for consumers at 1-877-IDTHEFT. In addition, the Department of Justice is investigating cases of identity theft and prosecuting alleged identity thieves and Congress is reviewing ID theft legislation.

In the meantime, the best way to protect against identity theft is by vigilantly guarding your personal information.

- Never reveal personal information until you know why it is needed, how it is to be used, and to whom it may be disclosed.
- Guard your mail by placing outgoing mail in U.S. Postal Service deposit boxes and by promptly removing mail from your personal mailbox.
- Use discrete password protection for your credit card, bank, and telephone accounts.
- Protect personal data by shredding or locking up documents that have your Social Security number (SSN) or account information printed on them (even at home).
- If you stop receiving bills or invoices, contact your provider immediately—ID thieves sometimes change your address to cover up the theft.
- Order a copy of your credit report and check it for potential identity theft.

NOTES

1. Pub L No 104-191, 110 Stat 1936 (1996).
2. Pub L No 106-102, 113 Stat 1338 (1999).
3. Pub L No 107-56, 115 Stat 272 (2001).
4. *Information Security Governance: Toward a Framework for Action*, Business Software Alliance, available at www.bsa.org/usa/research (October, 2003).



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.