Trends in the Law of Information Security

By Thomas J. Smedinghoff

Three legal trends are rapidly shaping the information security landscape for most companies. They are:

1. An increasing recognition that providing information security is a corporate legal obligation;

2. The emergence of a legal standard against which compliance with that obligation will be measured; and

3. A new emphasis on a duty to disclose breaches of information security.

Although the law is still in developing, and is often applied only in selective areas, these three trends are posing significant new challenges for most businesses.

Duty to Provide Information Security

For many companies, information security is no longer just good business practice. It is becoming a legal obligation.

Key to this developing trend is the fact that, in today's business environment, virtually all of a company's daily transactions, and all of its key records, are created, used, communicated, and stored in electronic form using networked computer technology. Electronic communications have become the preferred way of doing business, and electronic records have become the primary way of creating and storing information. As a consequence, most business entities are now "fully dependent upon information technology and the information infrastructure."[1]

This has provided companies with tremendous economic benefits, including significantly reduced costs and increased productivity. But the resulting dependence on information technology also creates significant potential vulnerabilities that are increasingly being exploited by a stream of new threats, such as viruses, worms, hackers, phishing attacks, and rogue employees.

Lawmakers are beginning to take notice of this problem. Concerns include ensuring the viability of business operations, protecting individual privacy and avoiding identity theft, safeguarding sensitive business data, ensuring accountability for corporate financial information, and preserving the authenticity and integrity of transaction data. Issues like these are driving the enactment of laws and regulations, both in the United States and globally, that are imposing new obligations on businesses to implement information security measures to protect their own data.

Thomas J. Smedinghoff, Of Counsel in the Chicago office of Baker & McKenzie, may be reached at *smedinghoff@bakernet.com.*

Corporate Legal Obligations

In the United States, corporate legal obligations to implement security measures are set forth in an expanding patchwork of federal and state laws, regulations, and government enforcement actions, as well as common law fiduciary duties and other implied obligations to provide "reasonable care."[2] Some laws seek to protect the company and its shareholders, investors, and business partners. Others focus on the interests of individual employees, customers, and prospects. In other cases, governmental regulatory interests or evidentiary requirements are at stake.

These laws regulate information security from a variety of perspectives. In some cases they are focused on the industry in which a company operates, particularly in the case of critical infrastructure industries. Thus, for example, the operation of IT systems and the security of data are heavily regulated in the financial and health care industries. In fact, in the financial industry alone there are more than 200 laws, regulations, and government bulletins, alerts, and other guidance documents addressing the information security obligations of financial institutions.[3]

In different situations regulatory requirements focus on the type of corporate records involved, targeting categories of records such as those containing personal data, financial records, tax records, and the like. Privacy laws and regulations, for example, require companies to implement information security measures to protect certain personal data that they maintain about employees, customers, or prospects in a variety of cases.[4] Corporate governance legislation, such as the Sarbanes-Oxley Act, requires public companies to ensure that they have implemented appropriate information security controls with respect to their financial information.[5]

Tax-related records are governed by Internal Revenue Service (IRS) regulations, which require companies to implement appropriate information secu-

rity measures to protect those records.[6] Likewise, other regulatory agencies, such as the Securities and Exchange Commission (SEC), Federal Reserve, Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), Food and Drug Administration (FDA), and Health and Human Services (HHS), have adopted a variety of regulations designed to address information security issues of importance to the types of records they regulate.

Electronic Signatures

Information security regulation also focuses on the nature of the electronic activity a company undertakes. Thus, for example, under some laws, electronic signatures are enforceable in certain cases only if appropriate security is used. The proposed Convention on the Use of Electronic Communications in International Contracts that is being finalized by the United Nations, for example, would condition the enforceability of electronic signatures on an assessment of their level of reliability or trustworthiness.[7] Other laws in the United States, such as the Uniform Electronic Transactions Act (enacted in 46 states) and the Uniform Commercial Code Article 4A (enacted in all states), recognize the role of information security as a basis for allocating risk of loss and liability.

In addition, government enforcement agencies such as the Federal Trade Commission (FTC) have actively pursued companies for "deceptive" trade practices whenever the information security representations that they voluntarily make to the public don't match their actual security practices. This may occur, for example, on Web sites, in privacy policies, or in documents where companies seek to assure potential customers that the company's products, the customer information that they collect, or the electronic transaction processes that they use are safe, adequately protected, and free from unauthorized alteration or disclosure. Companies such as Eli Lilly, Microsoft, Guess?, Tower Records, and Barnes & Noble have all been the target of enforcement actions based on FTC allegations that they were not living up to their representations regarding information security. Even more significant, however, the FTC has recently hinted that it is prepared to expand its enforcement actions to pursue companies that do not provide adequate information security, even in the absence of any voluntarily representations, on the ground that such failure constitutes an unfair trade practice.

Information on a company's computer system is not the only target. As companies move to outsource an ever-increasing array of business processes, government regulators are focusing their efforts on requirements that ensure the security of the corporate information that will be under the control of the outsource provider. In many cases, laws and regulations imposing information security obligations expressly cover the use of third-party outsource providers. This is particularly true in the financial sector and under the various EU data protection laws. Thus, laws are recognizing that it is absolutely essential that any outsourcing agreement impose information security obligations on the outsource provider in a manner designed to ensure that the data will be protected in a manner that satisfies the legal obligations.

Finally, it is important to recognize that information security is no longer just a technical issue for the IT department. New laws and regulations are making clear that it is a legal and corporate governance issue for upper management. In many cases, these laws, as well as government enforcement actions, put the responsibility directly on the CEO and the board of directors.

The Developing Legal Standard for Information Security

A legal obligation to address information security raises key questions for companies that must comply. Just what exactly is a business obligated to do? What is the scope of its legal obligations to implement information security measures?

The FTC has acknowledged that the mere fact that a breach of security occurs does not necessarily mean that there has been a violation of a company's legal obligations. But it has also noted that an organization can fail to meet its security obligations, even in the absence of a breach of that security.[8] Thus, the key issue (from a legal perspective) is defining the scope and extent of a company's "legal" obligation to implement information security measures.

Until recently, most laws addressing information security focused simply on establishing a requirement to provide security procedures, controls, safeguards, or measures, often without any further direction. If they specified a standard, it was only a general one, such as requiring "reasonable" security or "appropriate" security. Other expressions of the standard that appear in some regulations include "suitable," "necessary," and "adequate."

Yet recently enacted US statutes and regulations, as well as a series of government enforcement actions, suggest that we are witnessing the development of a legal standard for information security that is likely to be applied to most organizations whenever an obligation to provide security arises. The trend in US law adopts a relatively sophisticated approach to corporate information security obligations and recognizes that legal compliance with security obligations requires a "process" applied to the unique facts of each case.

Security Measures

Thus, rather than telling companies what specific security measures they must implement, developing law requires companies to engage in an ongoing and repetitive process that is designed to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments. In most cases, it does not require use of any specific security measures, instead leaving the decision up to the company.

Key to the new legal standard is a requirement that security be responsive to a company's fact-specific risk assessment. In other words, merely implementing seemingly strong security measures is not sufficient. They must be responsive to the particular threats a business faces and must address its vulnerabilities. Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat that the company faces is unauthorized remote access to its data via the Internet, that particular security measure is of little value. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers, but if a company's major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords, then even those sophisticated security measures, while important, will not adequately address the problem.

"Comprehensive Information Security Program"

As a consequence, newer US statutory and regulatory requirements (and government enforcement actions) are beginning to require the development of what is often referred to as a "comprehensive information security program." Rather than require implementation of specific security measures, they take a process-oriented approach, requiring each entity to do a risk assessment and then develop and implement a security plan appropriate to its specific business and the specific threats it faces. Thereafter, continual monitoring, review, reassessment, and revision of the plan are also required.

The essence of the comprehensive process-oriented approach to security compliance is implementation of a program that requires companies to:

- Conduct periodic risk assessments to identify the specific threats and vulnerabilities the company faces;
- Develop and implement a security program to manage and control the risks identified;
- Monitor and test the program to ensure that it is effective;
- Continually review and adjust the program in light of ongoing changes;
- Obtain regular independent audits and reporting;
- Oversee third-party service provider arrangements; and
- Make upper management (*e.g.*, the CEO and board of directors) responsible for the security program.

A key aspect of this process is recognition that it is never completed. It is ongoing and continually reviewed, revised, and updated.

This comprehensive and process-oriented approach to corporate security compliance was first set forth in a series of GLBA security *Guidelines Establishing Standards for Safeguarding Consumer Information* issued by the Federal Reserve, the OCC, FDIC, and the Office of Thrift Supervision, on February 1, 2001,[9] and later adopted by the FTC in its GLBA *Safeguards Rule* on May 23, 2002.[10] The same approach was also incorporated in the Federal Information Security Management Act of 2002 (FISMA)[11] and in the HIPAA *Security Standards* issued by the Department of Health and Human Services on February 20. 2003.[12]

The FTC has also adopted the view that this approach to information security sets forth a general best-practice approach to legal security compliance and has, in effect, implemented this approach in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security.[13] The National Association of Insurance Commissioners has also recommended the same approach, and to date, several state insurance regulators have adopted it.[14] Several state Attorneys General have also adopted this approach in their actions against perceived offenders.[15]

The Security Process

Although this remains an unsettled area, the bottom line is that developing law seems to be recognizing what security consultants have been saying for some time: "security is a process, not a product."[16] Consequently, legal compliance with security obligations involves a "process" applied to the facts of each case in order to achieve an objective (*i.e.*, to identify and implement the security measures appropriate for that situation) rather than the implementation of standard specific security measures in all cases. Thus, there will likely be no hard-and-fast rules. Instead, the legal obligation regarding security seems to focus on what is reasonable under the circumstances to achieve the desired security objectives. Consequently, the legal trend

focuses on requiring businesses to develop comprehensive information security programs but leaves the details to the facts and circumstances of each case.

Duty to Disclose Security Breaches

Finally, we are also witnessing a series of new and proposed laws and regulations focused not on imposing an obligation to *implement* security measures but rather on imposing an obligation to *disclose* security breaches. These are also beginning to have a significant impact.

Designed in many cases as a way to help protect persons who might be adversely affected by a security breach, this approach seeks to impose on companies an obligation similar to the common law duty to warn of dangers. Such a duty is often based on the view that a party who has a superior knowledge of a danger of injury or damage to another that is posed by a specific hazard must warn those who lack such knowledge.

The most widely publicized law requiring disclosure of security breaches is the California Security Breach Information Act (S.B. 1386), which became effective on July 1, 2003.[17] That law requires all companies doing business in California to disclose any breach of security that results in an unauthorized person's acquiring certain types of personally identifiable information about a California resident. Disclosure must be made to all persons whose personal information was compromised and anyone who is injured by a company's failure to do so can sue to recover damages. But notwithstanding all the publicity it has received, S.B. 1386 appears to be just one of a growing list of security disclosure requirements imposed on companies.

IRS regulations also impose a disclosure requirement on taxpayers whose electronic records were the subject of a security breach. In a Revenue Procedure that sets forth its basic rules for maintaining tax-related records in electronic form, the IRS requires taxpayers to "promptly notify" the IRS District Director if any electronic records "are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed . . ., or are found to be incomplete or materially inaccurate."[18] Likewise, the OCC requires banks to report cases where they are the victim of a phishing attack.[19]

Perhaps the most expansive cybersecurity disclosure requirements to date appear in proposed rules released for comment last year by several federal financial regulatory agencies.[20] These proposed regulations require financial institutions to develop a response program to protect against and address breaches of the security of customer information maintained by the financial institution or its service provider. Such program must include procedures for notifying customers, as well as regulatory and law enforcement agencies, about incidents of unauthorized access to customer information that could result in substantial harm or inconvenience to the customer. The rules would also require the financial institution to offer assistance to customers whose information was the subject of the incident (*e.g.*, inform customers of their rights, recommend actions that they should take, assist them in the process, etc.).

Conclusion

Taken as a group, these existing and proposed rules seem to suggest a possible new direction for the law on corporate information security obligations, one that does not necessarily require a company to protect itself as much as to warn those who might be adversely impacted by a failure of, or lack of, its security. Implicit in such an approach is recognition of the wide-ranging impact of a company's electronic activities and the fact that corporate security vulnerabilities can have a significant adverse impact on others outside of the company.

In all cases, however, what we are seeing is an increasing recognition that information security is critical, and that addressing it is a legal obligation.

Notes

1. "U.S. National Strategy to Secure Cyberspace," Feb. 14, 2003, at p.6, available at *www.whitehouse.gov/pcipb.*
2. For a compilation of laws governing information security, *see www.bakernet.com/ecommerce.*
3. For the list of these laws, regulations, and government bulletins, alerts, and other guidance documents, *see www.ffiec.gov/ffiecinfobase/resources/re_01.html.*
4. *See, e.g.*, Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801, 6805, and implementing regulations; Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §§ 1320d-2 and 1320d-4, and implementing regulations; and Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501, *et seq.*, and implementing regulations. *See also*, European Union Directive 95/46/EC of February 20, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Data Protection Directive), Article 17.
5. *See* Sarbanes-Oxley Act, Pub. L. 107-204, §§ 302 and 404.
6. *See* IRS Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.
7. *See* Draft Convention on the Use of Electronic Communications in International Contracts, Article 9, (May 18, 2004), available at *http://daccess-ods.un.org/access.nsf/Get?Open&JN=V0454106.*
8. *See* Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, US House of Representatives on "Protecting Our Nation's Cyberspace," Apr. 21, 2004, at pp.5-6, available at *www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.*

9. 66 Fed. Reg. 8616, Feb. 1, 2001; 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision).
10. 67 Fed. Reg. 36484, May 23, 2002; 16 C.F.R. Part 314.
11. 44 U.S.C. § 3544(b).
12. 45 C.F.R. Part 164.
13. *See, e.g.*, In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (FTC File No. 032-3209, Apr. 21, 2004), available at *www.ftc.gov/os/caselist/0323209/ 040421agree 0323209.pdf;* In the matter of Guess?, Inc. (FTC File No. 022 3260, June 18, 2003), available at *www.ftc.gov/os/2003/06/ guessagree.htm*; FTC v. Microsoft, Consent Decree (FTC, Aug. 7, 2002); *available at www.ftc.gov/os/2002/08/microsoftagree.pdf*; and In the Matter of Eli Lilly and Company, Decision and Order (FTC Docket No. C-4047, May 8, 2002); available at *www.ftc.gov/os/2002/05/elilillydo.htm.*
14. *See, e.g.*, National Association of Insurance Commissioners "Standards for Safeguarding Customer Information" (adopted in nine states).
15. *See, e.g.*, In the Matter of Barnes & Noble.com, LLC (Attorney General of New York, Assurance of Discontinuance, April 20, 2004); available at *www.bakerinfo.com/ecommerce/barnes-noble.pdf*; In the Matter of Ziff Davis Media Inc. (Attorneys General of California, New York, and Vermont), Assurance of Discontinuance, Aug. 28, 2002; available at *www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf.*
16. Bruce Schneier, Secrets & Lies: Digital Security in a Networked World (John Wiley & Sons, 2000) at p.XII.
17. Cal. Civil Code § 1798.82. A copy is available at *www.leginfo.ca.gov/calaw.html.*
18. Rev. Proc. 98-25, § 8.01.
19. *See* OCC Alert 2003-11 (Sept. 12, 2003).
20. *See* proposed "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," 68 Federal Register 155, at page 47954, August 12, 2003, jointly released by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.