The State of Information Security Law

A Focus on the Key Legal Trends

By Thomas J. Smedinghoff[1]

Information security is rapidly emerging as one of the most critical legal and public relations issues facing companies today. As the series of highly-publicized security breaches over the past few years has demonstrated, it is in many respects a time bomb waiting to explode.

The problem stems from 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. Most business entities are, quite literally, fully dependent upon information technology and an interconnected information infrastructure. This has, of course, provided companies with tremendous economic benefits, including significantly reduced costs and increased productivity. But the resulting dependence on electronic records and a networked computer infrastructure also creates significant potential vulnerabilities that can result in major harm to the business and its stakeholders.[2] Creating, communicating, and storing corporate information in electronic form greatly enhances the potential for unauthorized access, use, disclosure, and alteration, as well as the risk of accidental loss or destruction.

Concerns regarding corporate governance, individual privacy, accountability for financial information, the authenticity and integrity of transaction data, and the security of sensitive business data are driving the enactment of new laws and regulations designed to ensure that businesses adequately address the security of their own data. These legislative and regulatory initiatives are imposing obligations on all businesses to implement information security measures to protect their own data and to disclose breaches of security that do occur.

---

[1] Thomas J. Smedinghoff is a partner in the Privacy, Data Security, and Information Law Practice at the law firm of Wildman Harrold, in Chicago. Mr. Smedinghoff is a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), where he participated in the negotiation of the *United Nations Convention on the Use of Electronic Communications in International Contracts*. He is also the chair of the International Policy Coordinating Committee of the American Bar Association section of Science & Technology Law. He was also an American Bar Association representative to the Drafting Committee for the *Uniform Electronic Transactions Act* (UETA), and chair of the Illinois Commission on Electronic Commerce and Crime (1996-1998) that wrote the *Illinois Electronic Commerce Security Act* (5 Ill. Comp. Stat. 175). He can be reached at smedinghoff@wildman.com.

[2] "As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security." OECD Guidelines for the Security of Information Systems and Networks, July 25, 2002, at p. 7, available at www.oecd.org/dataoecd/16/22/15582260.pdf.

Four legal trends in the U.S. are rapidly shaping the information security landscape for most companies. And increasingly, these trends are having a significant impact on the development of international law as well. They are:

- A continuing expansion of the duty to provide security;
- An emergence of a legal standard for compliance;
- A focus on security obligations regarding specific data elements and controls; and
- The imposition of a duty to warn.

While 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. This paper will examine new developments as they relate to these three major trends.

A. The Expanding Duty to Provide Security

1. Where Does It Come From?

There is no single law, statute, or regulation that governs a company's obligations to provide security for its information. Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement actions, as well as common law duties and other express and implied obligations to provide "reasonable" or "appropriate" security for corporate data.

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. And in other cases, governmental regulatory interests, or evidentiary requirements are at stake. Many of the requirements are industry-specific (e.g., focused on the financial industry or the healthcare industry) or data-specific (e.g., focused on personal information or financial data). Others focus only on public companies.

When viewed as a group, however, they provide ever-expanding coverage of most corporate activity. The most common sources of obligations to provide security include the following:[3]

Statutes and Regulations. Numerous statutes and regulations impose obligations to provide security. Sometimes they are readily recognized by their use of terms such as "security" or "safeguards,"[4] but in many cases the fact that they impose security obligations is evident only by their use of terms relating to the attributes of security, such as "authenticate," "integrity," "confidentiality," "availability of data," and the like.[5]

---

[3] See Appendix for a compilation of some of the key laws and regulations governing information security.

[4] *See, e.g.*, EU Data Protection Directive and HIPAA, cited in Appendix

[5] *See, e.g.,* E-SIGN, UETA, and UN Convention cited in Appendix.

Some of the most common sources of statutes and regulations with such requirements include:

- Privacy laws and regulations that require companies to implement information security measures to protect certain personal data they maintain about individuals;
- E-transaction laws designed to ensure the enforceability and compliance of electronic documents generally;
- Corporate governance legislation and regulations designed to protect public companies and their shareholders, investors, and business partners;
- Unfair business practice laws and related government enforcement actions; and
- Sector-specific regulations imposing security obligations with respect to specific data**.**

A list of some of the more common statutes and regulations governing the security of personal data is set forth in the Appendix

Common Law Obligations. For years, commentators have argued that there exists a common law duty to provide appropriate security for corporate data, the breach of which constitutes a tort.[6] Courts are now beginning to accept that view, and recent decisions have recognized that there may be a common law duty to provide security, the breach of which constitutes a tort.[7] See cases cited in Appendix.

Rules of Evidence. Recent decisions, at least at the federal level, suggest that security will increasingly be a requirement for the admissibility of digital records.[8]

Industry Standards. In some cases, companies become obligated to comply with the requirements of certain technical security standards. Examples include the Payment Card Industry Data Security Standards ("PCI Standards")[9] that merchants must agree to

---

[6] *See, e.g.*, Kimberly Kiefer and Randy V. Sabett, *Openness of Internet Creates Potential for Corporate Information Security Liability*, BNA Privacy & Security Law Report, Vol. 1, No. 25 at 788 (June 24, 2002); Alan Charles Raul, Frank R. Volpe, and Gabriel S. Meyer, *Liability for Computer Glitches and Online Security Lapses*, BNA Electronic Commerce Law Report, Vol. 6, No. 31 at 849 (August 8, 2001); Erin Kenneally, *The Byte Stops Here: Duty and Liability for Negligent Internet Security*, Computer Security Journal, Vol. XVI, No. 2, 2000.

[7] *See, e.g.*, Wolfe v. MBNA America Bank, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007); Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 (D. Minn. Feb. 7, 2006); and Bell v. Michigan Council, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005) (all affirming a negligence cause of action). See also, In Re TJX Companies Retail Security Breach Litigation, 2007 U.S. Dist. Lexis 77236 (D. Mass. October 12, 2007) (rejecting a negligence claim due to the economic loss doctrine, but allowing a negligent misrepresentation claim to proceed).

[8] *See, e.g.*, American Express v. Vinhnee, 2005 Bankr. Lexis 2602 (9th Cir. Bk. App. Panel, 2005); Lorraine v. Markel, 2007 U.S. Dist. Lexis 33020 (D. MD. May 4, 2007).

[9] Available at www.pcisecuritystandards.org.

as a condition of accepting credit cards, the EV SSL Guidelines[10] that certification authorities must agree to in order to issue EV SSL certificates, and the international ISO/IEC 27001 Standard[11] often imposed upon businesses by contract with trading partners. In each of these cases, the standard has no legal authority by itself, but becomes binding typically through a contractual agreement. In some cases, however, such as in Japan, compliance with a particular standard (in that case, ISO/IEC 27001) may be required by regulation.

System Rules. In some cases, companies may be subject to certain system rules that will impose additional privacy and security obligations on it. These generally arise, for example, in connection with use of various electronic payment systems (such as the ACH payment system) or federated identity systems that require agreement to system rules as a condition of participation (such as Extended Validation SSL Certificates).

Contractual Obligations. As businesses increasingly become aware of the need to protect the security of their own data, they frequently try to satisfy their obligation (at least in part) by contract in those situations where third parties will have possession of, or access to, their business data. This is particularly common, for example, in outsourcing agreements where a company's data will be processed by a third party. In such cases, for example, both the EU Data Privacy Law and U.S. GLB Safeguard Rules mandate that the customer impose appropriate security obligations on the outsource provider. In addition, in any situation where the business may have access to someone else's data, it is quite common for the other party to impose both confidentiality and security obligations with respect to that data.

Self-Imposed Obligations. In many cases, security obligations are self-imposed. Through statements in privacy policies, on websites, or in advertising materials, for example, companies often make representations regarding the level of security they provide for their data (particularly the personal data they collect from the persons to whom the statements are made). By making such statements, companies impose on themselves an obligation to comply with the standard they have represented to the public that they meet. If those statements are not true, or if they are misleading, such statements may become, in effect, deceptive trade practices under Section 5 of the FTC Act, or under equivalent state laws. Through a series of enforcement actions and consent decrees, both the FTC and several state attorneys general have used those deceptive business practice statutes to bring enforcement actions against the offending companies.

The bottom line is that a company's duty to provide security may come from several different sources and several different jurisdictions – each perhaps regulating a different aspect of corporate information – but the net result (and certainly the trend) is a general obligation to provide security for all corporate data and information systems. In

[10] Available at www.cabforum.org

[11] ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements (Oct. 2005) (hereinafter "ISO/IEC 27001"), available at www.27000.org.

other words, information security is no longer just good business practice. It is becoming a legal obligation.

2. Who Does It Apply To?

In Europe, the legal duty to provide security generally applies to all companies that posses personal information. In fact, the obligation to provide security for the protection of personal information is one of the key principles set forth in the EU Data Protection Directive.[12] The Directive establishes omnibus protection for the privacy of all personal information of EU residents, and applies to all companies established in the EU, that make use of equipment within the EU, or that are in another jurisdiction where an EU member country's law applies by virtue of private international law.

Subsequent EU country implementations of the Directive also impose such a requirement for security on all companies.[13] Numerous other country privacy laws (which also tend to take on omnibus approach to privacy, like the EU) also impose a general duty on all companies to protect the security of personal information. Examples include Canada, Japan, Argentina, South Korea, Hong Kong, and Australia.[14]

In the U.S., obligations to provide security were initially applied on a sector-specific basis. The first substantive corporate obligations to provide security for personal information appeared in the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[15] which regulated the healthcare sector. This was followed in 1999 by the Gramm-Leach-Bliley Act (GLB),[16] which regulated the financial sector. Detailed security regulations implementing the security provision of GLB were released in 2001[17]

---

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "EU Data Protection Directive").

[13] See statutes listed in Appendix.

[14] See statutes listed in Appendix.

[15] Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4, (providing that "each person . . . who maintains or transmits *health* information shall maintain reasonable and appropriate administrative, technical, and physical safeguards: (A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated: (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person." at 42 U.S.C. 1320d-2(d)(2).

[16] Gramm-Leach-Bliley Financial Services Modernization Act ("GLB"), Pub. L. No. 106-102, 113 Stat. 1338 (November 12, 1999), at §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, providing that "[E]ach financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

[17] See, Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 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) and 16 C.F.R. Part 314 (FTC).

and security regulations implementing the security provision under HIPAA were released in 2003.[18]

Since then, however, the sector-specific approach to imposing security obligations to protect personal information has significantly shifted. Today, U.S. law is rapidly expanding to impose security requirements on all companies (regardless of sector), thereby matching the EU approach, at least with regard to the security of personal information.[19] This is occurring in three ways:

First, through a series of enforcement actions and consent decrees beginning in 2002, both the FTC and several state attorneys general have, in effect, extended security obligations regarding personal information to non-regulated industries by virtue of Section 5 of the FTC Act and similar state laws. Initially, cases were based on the alleged failure of companies to provide adequate information security contrary to representations they made to customers.[20] In other words, these were claims of deceptive trade practices. But beginning in June 2005, the FTC significantly broadened the scope of its enforcement actions by asserting that a failure to provide appropriate information security for consumer personal information was itself, an unfair trade practice – even in the absence of any false representations by the defendant as to the state of its security.[21]

Second, several states have enacted laws imposing a general obligation on all companies to ensure the security of personal information. The first was California, which enacted legislation in 2004 requiring all businesses to "implement and maintain reasonable security procedures and practices" to protect personal information about California residents from unauthorized access, destruction, use, modification, or disclosure. Other states have recently followed suit, including Arkansas, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.[22]

---

[18] Final HIPAA Security Regulations, 45 C.F.R. Part 164.

[19] There have also been efforts in the U.S. to pursue comprehensive federal privacy similar to the approach taken by many other countries. See e.g., Microsoft position paper at www.microsoft.com/presspass/download/features/2005/PrivacyLegislationCallWP.doc. While it remains to be seen whether that approach will ultimately be adopted, it is clear that the combination of U.S. state and federal has, in effect, imposed a comprehensive obligation of security with respect to all personal information held by all companies.

[20] *See, e.g.,* FTC enforcement actions regarding In the Matter of Sunbelt Lending Services, Inc.; In the Matter of Petco Animal Supplies, Inc.; In the Matter of MTS, Inc., d/b/a Tower records/Books/Video; In the matter of Guess?, Inc.; FTC V. Microsoft; and In the Matter of Eli Lilly and Company cited in the Appendix.

[21] *See, e.g.,* FTC enforcement actions regarding In the Matter of CardSystems Solutions, Inc.; United States v. ChoicePoint, Inc.; In the Matter of DSW Inc.; and In the Matter of BJ's Wholesale Club, Inc. cited in the Appendix.

[22] See list in Appendix.

Third, some recent case law also recognizes that there may be a common law duty to provide security for personal information, the breach of which constitutes a tort.[23] In *Bell v. Michigan Council*, for example, the court held that "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."[24] In *Guin v. Brazos Education*, the court acknowledged that in some negligence cases, a duty of care may be established by statute (in that case, the GLB Act).[25] And in *Wolfe v. MBNA America Bank*, the court found that where the injury is foreseeable and preventable, the "defendant has a duty to verify the authenticity and accuracy of a credit account application."[26]

Most recently, in the case of *In Re TJX Companies Retail Security Breach Litigation*,[27] the court allowed plaintiffs to proceed on a "negligent misrepresentation" claim based on the theory that TJX and its acquiring bank made implied representations to the issuing banks that they took the security measures required by industry practice to safeguard personal and financial information. According to the court, the theory is that "TJX and [its acquiring bank] knew that the issuing banks were part of a financial network that relies on members taking appropriate security measures."[28]

3. What Is Covered?

The ultimate concern is electronic corporate information. But protecting electronic information also requires addressing the means by which such information is created, stored, and communicated. Thus, statutes and regulations governing information security typically focus on the protection of both *information systems*[29] – i.e., computer systems, networks, and software – as well as the *data, messages, and information* that is typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems.

---

[23] *See, e.g.*, Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 (D. Minn. Feb. 7, 2006) and Bell v. Michigan Council, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005).

[24] 205 Mich. App. Lexis 353 at *16 (Mich. App. 2005).

[25] 2006 U.S. Dist. Lexis 4846 at *9 (D. Minn. 2006).

[26] Wolfe v. MBNA America Bank, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007).

[27] In Re TJX Companies Retail Security Breach Litigation, 2007 U.S. Dist. Lexis 77236 (D. Mass. October 12, 2007), at pp. 28-29.

[28] Id.

[29] The Homeland Security Act of 2002 defines the term "information system" to mean "any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes – (A) computers and computer networks; (B) ancillary equipment; (C) software, firmware, and related procedures; (D) services, including support services; and (E) related resources." Homeland Security Act of 2002, Pub. L. 107-296, at Section 1001(b), amending 44 U.S.C. § 3532(b)(4).

When addressing corporate information, it is also important to remember that all types of information need be considered, including financial information, personal information, tax-related records, employee information, transaction information, and trade secret and other confidential information. Moreover, the information can be in any form, including databases, e-mails, text documents, spreadsheets, voicemail messages, pictures, video, sound recordings, etc.

(a) Personal Data

The obligation to provide adequate security for personal data collected, used, and/or maintained by a business is a critical component of all privacy laws. Thus, most statements of basic privacy principles include security as a key component.[30] The privacy of a person's data is illusory at best if there is no security for the data.

In Europe, the legal duty to provide security for the protection of personal information is one of the key principles set forth in the EU Data Protection Directive.[31] It recognizes that the protection of the rights of data subjects with respect to the processing of their personal data require the implementation of appropriate security measures.[32] Accordingly, the Directive required that EU Member states enact legislation obligating the controllers of personal data to "implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[33]

Subsequent EU country implementations of the Directive generally impose such a requirement for security.[34] Numerous other country privacy laws (which also tend to take on omnibus approach to privacy, like the EU) also impose a general duty on all companies to protect the security of personal information. Examples include Canada, Japan, Argentina, South Korea, Hong Kong, and Australia.[35]

---

[30] *See, e.g.*, Australia, Information Privacy Principles under the Privacy Act 1988, Principle No. 4, available at www.privacy.gov.au/publications/ipps.html; AICPA and the Canadian Institute of Chartered Accountants (CICA), Generally Accepted Privacy principles, Principle No. 8, available at http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles; APEC, Privacy principles, Principle No. 7, available at http://austlii.edu.au/~graham/APEC/APECv10.doc; US-EU Safe Harbor Privacy Principles, available at www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm; Direct Marketing Association, Online Marketing Guidelines, available at www.the-dma.org/guidelines/onlineguidelines.shtml.

[31] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "EU Data Protection Directive").

[32] EU Data Protection Directive, Preamble at Para. 46.

[33] EU Data Protection Directive, Article 17(1).

[34] See statutes listed in Appendix.

[35] See statutes listed in Appendix.

Likewise, in the U.S. protecting personal information is the focus of numerous federal and state laws. These include sector-specific privacy laws such as GLB (financial sector), HIPAA (healthcare sector), and the Privacy Act of 1974 (federal government), as well as numerous more general state laws as outline din the Appendix.

(b) Most Other Corporate Data

Although security obligations in the EU are focused on personal data, in the U.S. such obligations are expanding to cover most other types of corporate data. This include, for example:

- Corporate Financial Data: Corporate governance legislation and caselaw designed to protect the company and its shareholders, investors, and business partners, such as Sarbanes-Oxley and implementing regulations, require public companies to ensure that they have implemented appropriate information security controls with respect to their financial information.[36] Similarly, several SEC regulations impose a variety of requirements for internal controls over information systems.

- Transaction Records: E-transaction laws designed to ensure the enforceability and compliance of electronic documents generally – Both the federal and state electronic transaction statutes (E-SIGN and UETA) require all companies to provide security for storage of electronic records relating to online transactions.

- Tax Records: IRS regulations require companies to implement information security to protect electronic tax records, and as a condition to engaging in certain electronic transactions.

- E-Mail: SEC regulations address security in a variety of contexts, and FDA regulations require security for certain records

(c) All Digital Evidence?

Providing appropriate security as necessary to ensure the integrity of electronic records (and, where necessary, the identity of the creator, sender, or signer of the record) will likely be critical to securing the admission of the electronic record in evidence in a future dispute. This conclusion is supported both by recent case law as well as provisions relating to the form requirement for an "original" in electronic transaction legislation.

[36] See generally, Bruce H. Nearon, Jon Stanley, Steven W. Teppler, and Joseph Burton, Life after Sarbanes-Oxley: The Merger of Information Security and Accountability, 45 Jurimetrics Journal 379-412 (2005)..

The Ninth Circuit decision in the case of *American Express v. Vinhnee*[37] suggests that appropriate security is a condition for the admissibility in evidence of electronic records. In that case, the court refused to admit electronic records into evidence because American Express did not adequately establish that they were "authentic."

According to the court, the primary authenticity issue for admissibility is establishing "what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial." And to do this, the court said, "one must demonstrate that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file. Fed. R. Evid. 901(a)."[38]

In other words, it requires a showing that appropriate security was in place to ensure the integrity of the electronic records from the time they were created until the time that they were introduced in court. As the court pointed out:

> The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.[39]

Thus, the court required a showing that "the business has developed a procedure for inserting data into the computer," and "the procedure must have built-in safeguards to ensure accuracy and identify errors." Those safeguards, the court noted, "subsume details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records."[40]

Because American Express provided "no information regarding [its] computer policy and system control procedures, including control of access to the pertinent databases, control of access to the pertinent programs, recording and logging of changes to the data, backup practices, and audit procedures utilized to assure the continuing integrity of the records" the court concluded that a refusal to admit the electronic records was appropriate.[41]

---

[37] American Express v. Vinhnee, 336 B.R. 437; 2005 Bankr. Lexis 2602 (9th Cir. December 16, 2006).

[38] Id. at p. 444.

[39] Id. at p. 445.

[40] Id. at pp. 446-447.

[41] Id. at p. 449.

It remains to be seen whether, or to what extent, other courts will adopt this approach to admissibility of electronic evidence. Given the growing awareness of the ability to manipulate electronic data, however, it seems likely that this trend will only continue.

The bottom line is that, quite simply, the admissibility of all types of electronic data will depend, in many situations, on the level of information security provided in order to ensure that the integrity and availability of the information remains intact.

4. Who Is Responsible?

Protecting the security of corporate information and computer systems was once just a technical issue to be addressed by the IT department. Today, however, as information security has evolved into a legal obligation, responsibility for compliance has been put directly on the shoulders of senior management, and in many cases the board of directors. It is, in many respects, a corporate governance issue.[42]

Under the Sarbanes-Oxley Act, for example, responsibility lies with the CEO and the CFO.[43] In the financial industry, the Gramm-Leach-Bliley ("GLB") security regulations place responsibility for security directly with the Board of Directors.[44] In the healthcare industry, the HIPAA security regulations require an identified security official to be responsibility for compliance.[45] Several FTC consent decrees involving companies in a variety of non-regulated industries do likewise.[46] And federal law places the responsibility for information security within each government agency on the head of such agency.[47]

Evolving case law also suggests that, by virtue of their fiduciary obligations to the company, corporate directors will find that their duty of care includes responsibility for the security of the company's information systems. In particular, it may "extend from safeguarding corporate financial data accuracy to safeguarding the integrity of all stored data."[48] In the *Caremark International Inc. Derivative Litigation,* for example, the Delaware court noted that "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate

---

[42] See, e.g., national Association of Corporate Directors, Information Security Oversight (2007).

[43] Sarbanes-Oxley Act, Section 302.

[44] *See, e.g.*, GLB Security Regulations (Federal Reserve) 12 C.F.R. 208, Appendix D-2.III(A).

[45] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(2).

[46] *See, FTC Decisions and Consent Decrees* listed in Appendix, including Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance, Para. 27(a), p. 7; Eli Lilly Decision at II.A.

[47] FISMA, 44 U.S.C. 3544(a).

[48] E. Michael Power and Roland L. Trope, *Sailing in Dangerous Waters: A Director's Guide to Data Governance*, American Bar Association (2005), p. 13; Roland L. Trope, "Directors' Digital Fiduciary Duties," IEEE Security & Privacy, January/February 2005 at p. 78.

to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility."[49] And in *Bell v. Michigan Council*, liability was imposed where the Board was aware of the risk, but failed to take action.[50]

The private sector is also beginning to recognize that the responsibility for security lies with upper management and the board of directors. The Business Roundtable, for example, has noted both that "[i]nformation security requires CEO attention" and that "[b]oards of directors should consider information security as an essential element of corporate governance and a top priority for board review."[51] The Corporate Governance Task Force Report has taken a similar position, noting that:

> The board of directors/trustees or similar governance entity should provide strategic oversight regarding information security, including:
>
> - Understanding the criticality of information and information security to the organization.
> - Reviewing investment in information security for alignment with the organization strategy and risk profile.
> - Endorsing the development and implementation of a comprehensive information security program.
> - Requiring regular reports from management on the program's adequacy and effectiveness.[52]

The scope of that responsibility can also be significant. The GLB security regulations, for example, require the Board of Directors to approve the written security program, to oversee the development, implementation, and maintenance of the program, and to require regular reports (e.g., at least annually) regarding the overall status of the

---

[49] Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

[50] Bell v. Michigan Council, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005), at pp. 11-13 (noting that harm was foreseeable, but Board took no action).

[51] Securing Cyberspace: Business Roundtable's Framework for the Future, Business Roundtable, May 19, 2004 at pp. 1, 2; available at www.businessroundtable.org/pdf//20040518000CyberSecurityPrinciples.pdf. The Business Roundtable is an association of chief executive officers of leading U.S. corporations with a combined workforce of more than 10 million employees in the United States. See www.businessroundtable.org.

[52] Information Security Governance: A Call to Action, Corporate Governance Task Force Report, National Cyber Security Partnership, April 2004, pp. 12-13, available at www.cyberpartnership.org/InfoSecGov4_04.pdf. The National Cyber Security Partnership (NCSP) is led by the Business Software Alliance (BSA), the Information Technology Association of America (ITAA), TechNet and the U.S. Chamber of Commerce in voluntary partnership with academicians, CEOs, federal government agencies and industry experts. Following the release of the 2003 White House National Strategy to Secure Cyberspace and the National Cyber Security Summit, this public-private partnership was established to develop shared strategies and programs to better secure and enhance America's critical information infrastructure. Further information is available at www.cyberpartnership.org.

security program, the company's compliance with regulations, and material matters relating to the security program.[53]

Similarly, under the Federal Information Security Management Act ("FISMA"), the head of each agency is responsible for providing information security protections, complying with the requirements of the statute, and ensuring that information security management processes are integrated within agency strategic and operational planning processes. The head of each agency is also required to appropriately delegate implementation tasks to the CIO and others. The HIPAA security regulations require that an identified security official be responsible for developing and implementing the required policies and procedures.

A key problem, however, is that the nature of the legal obligation to address security is often poorly understood by those levels in management charged with the responsibility, by the technical experts who must implement it, and by the lawyers who must ensure compliance. Yet, it is perhaps one of the most critical issues companies will face.

B. The Emergence of a Legal Obligation for Compliance

The general obligation to provide security for data is often simply stated in the law as an obligation to provide "reasonable" or "appropriate" security designed to achieve certain objectives. In some cases, statutes and regulations define those objectives in terms of positive results to be achieved, such as ensuring the *availability* of systems and information, controlling *access* to systems and information, and ensuring the *confidentiality, integrity, authenticity* of information[54] In other cases, they define those objectives in terms of the harms to be avoided – e.g., to protect systems and information against unauthorized access, use, disclosure or transfer, modification or alteration, processing, and accidental loss or destruction.[55] And in some cases, no objectives are stated.

Regardless of approach, achieving these objectives involves implementing security measures designed to protect systems and information from the various threats they face. What those threats are, where they come from, what is at risk, and how serious the consequences are, will of course, vary greatly from case to case. But responding to

---

[53] GLB Security Regulations (OCC), 12 C.F.R. Part 30, Appendix B, Part III.A and Part III.F.

[54] *See, e.g.*, Homeland Security Act of 2002 (Federal Information Security Management Act of 2002) 44 U.S.C. Section 3542(b)(1); GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.B; HIPAA Security Regulations, 45 C.F.R. Section 164.306(a)(1); Microsoft Consent Decree at II, p. 4.

[55] *See, e.g.*, 44 USC 3532(b)(1), emphasis added. See also FISMA, 44 U.S.C. Section 3542(b)(1). Most of the foreign privacy laws also focus their security requirements from this perspective. This includes, for example, the EU Privacy Directive, Finland's Privacy Law, Italy's Privacy Law, and the UK Privacy Law. Also in this category is the Canadian Privacy Law.

the threats a company faces with appropriate physical, technical, and organizational security measures is the focus of the duty to provide security.

The key questions for companies that must comply, however, is determining the scope of its obligation. Just what exactly is the business obligated to do? Unfortunately, laws and regulations rarely specify what specific security measures a business should implement to satisfy those legal obligations.[56] Most laws simply obligate the company to establish and maintain internal security "procedures," "controls," "safeguards," or "measures"[57] directed toward achieving the goals or objectives identified above, but often without any further direction or guidance.

1. General Recognition that Security Is Relative

Defining the scope of a company's security obligations begins with understanding that the law views security as a relative concept. Thus, the standard for compliance, if one is stated, often requires simply that the security be "reasonable"[58] or "appropriate."[59] Other expressions of the standard that appear in some regulations include "suitable," "necessary," and "adequate." But there is typically little or no guidance on what kind of security measures are required, or on the subject of how much security is enough.

In Europe, for example, the Data Protection Directive requires the controllers of personal data to:

> implement *appropriate* technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[60]

---

[56] Although they often focus on categories of security measures to address. *See, e.g*., HIPAA Security Regulations, 45 C.F.R. Part 164. They also address some specific issues, such as _____. See __ below.

[57] *See, e.g*., FDA regulations at 21 C.F.R. Part 11 (procedures and controls); SEC regulations at 17 C.F.R. 257.1(e)(3) (procedures); SEC regulations at 17 C.F.R. 240.17a-4 (controls); GLB regulations (FTC) 16 C.F.R. Part 314 (safeguards); Canada, Personal Information Protection and Electronic Documents Act, Schedule I, Section 4.7 (safeguards); EU Data Privacy Directive, Article 17(1) (measures) available at http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[58] *See, e.g.,* HIPAA 42 U.S.C. 1302d-2, and HIPAA Security regulations, 45 CFR 164.306; COPPA, 15 U.S.C. 6502(b)(1)(D), and COPPA regulations 16 C.F.R. 312.8; IRS Rev. Proc. 97-22, sec. 4.01(2); SEC regulations 17 C.F.R. 257. See also UCC Article 4A, Section 202 ("commercially reasonable" security procedure), and Microsoft Consent Decree.

[59] "Appropriate" security required by: HIPAA 42 U.S.C. 1302d-2, and HIPAA Security regulations, 45 CFR 164.306; EU Data Protection Directive, Article 17(1).

[60] EU Data Protection Directive, Article 17(1) (emphasis added)

Thus, country implementations of the EU Data Protection Directive generally require the use of security measures that are *appropriate* to protect the personal data[61] or that are *necessary* to protect the personal data.[62]

In the U.S., the Privacy Protection Act of 1974 [63] requires government agencies that maintain a system of records about an individual to:

> establish *appropriate* administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;[64]

Similarly, HIPAA requires "reasonable and appropriate" security,[65] the GLB security regulations require covered financial institutions to "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards *appropriate* to the size and complexity of the bank and the nature and scope of its activities,"[66] and state personal information security laws, such as in California, generally require "reasonable security procedures and practices."[67]

---

[61] *See, e.g.,* Belgium – Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as modified by the law of 11 December 1998 Implementing Directive 95/46/EC, and the law of 26 February 2003, Chapter IV, Article 16(4); Denmark – Act on Processing of Personal Data,; *Act No. 429 of 31 May 2000,* (unofficial English translation), Title IV, Part 11, Section 41(3); Estonia -- Personal Data Protection Act; Passed 12 February 2003 (RT[1] I 2003, 26, 158), entered into force 1 October 2003, Chapter 3, Sections 19(2); Greece – Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000 and 2915/2001); Article 10(3); Ireland – Data Protection (Amendment) Act 2003; Section 2.-(1)(d) and First Schedule Article 7; Lithuania – Law on Legal Protection of Personal Data, 21 January 2003, No. IX-1296, Official translation, with amendments 13 April 2004, Article 24(1); Netherlands – 25 892 - Rules for the protection of personal data (Personal Data Protection Act) (Unofficial translation); Article 13; Portugal – Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), Article 14(1); Slovakia – Act No 428 of 3 July 2002 on personal data protection; Section 15(1); Sweden – Personal Data Act (1998:204); issued 29 April 1998, Section 31; and UK – Data Protection Act 1998, Schedule 1, Part I, Seventh Principle

[62] *See, e.g.,* Finland – The Finnish Personal Data Act (523/1999), given on 22.4.1999, Section 32(1); Germany – Federal Data Protection Act as of 1 January 2003, Section 9; Hungary – Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest, Article 10(1); Italy – Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003, Sections 31 and 33; Spain – Organic Law 15/1999 of 13 December on the Protection of Personal Data, Article 9

[63] 5 USC Sec. 552a.

[64] 5 U.S.C. § 552a (d)(10) (emphasis added).

[65] 42 U.S.C. 1320d-2(d)(2).

[66] See, Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 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) and 16 C.F.R. Part 314 (FTC) (emphasis added).

[67] Cal. Civil Code § 1798.81.5(b).

In other words, and the choice of security measures and technology can vary depending on the situation. Thus, in most laws there are no specific requirements regarding whether or not a particular security measure must be implemented, and there are generally no safe harbors.

The most recent international legal effort, the 2005 UN Convention on the Use of Electronic Communications in International Contracts, also expressly adopts the view that security is a relative concept. In addressing requirements for electronic signatures, the Convention requires that the method used to authenticate the identity of a party singing a contract and to indicate the party's intent must either be "as reliable as appropriate for the purpose" or "proven in fact." In addressing the requirements for originality of electronic records, the Convention requires only that there exist "a reliable assurance as to the integrity of the information." And it makes clear that "the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances." The UN Convention does not in any way require the use of any specific security measures or technologies.[68]

Finally, it is important to note that the new international information security standard released in October 2005, known as ISO/IEC 27001, also recognizes both that security is a relative concept, and that the process-oriented approach to security is the most appropriate response.[69]

2. Developing Legal Definition of "Reasonable Security"

Although consistent with the view that security is relative, laws requiring only that companies implement "reasonable" or "appropriate" security leave businesses with little or no guidance as to what is required for legal compliance, and without any safe harbor to ensure that they have satisfied their legal obligation. Legal developments over the past few years, however, suggest that a legal standard for "reasonable" security is clearly emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, PKI, or the like), and instead adopts a fact-specific approach to corporate security obligations that requires a "process" applied to the unique facts of each case.

Thus, rather than telling companies what specific security measures they must implement, the legal trend is to require 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. The decision regarding the specific security measures is left up to the company.

---

[68] *See* UN Convention at Article 9(3), 9(4), and 9(5).

[69] ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements (Oct. 2005). See text at footnotes 157-169, *infra*.

As a consequence, the presence or absence of specific security measures says little about the status of a company's legal compliance with its information security obligations. Because armed guards at a the front of a building don't protect against hackers accessing information through the Internet, and because firewalls designed to stop hackers don't protect against dishonest employees with authorized access, the law puts its focus on implementing those security measures that respond to the specific threats a business faces. It recognizes that there are a variety of different appropriate security measures responsive to specific threats, and recognizes that threats (and appropriate responsive security measures) are constantly changing.

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

- Identify its information assets
- 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, including obtaining regular independent audits and reporting where appropriate
- Oversee third party service provider arrangements.

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

This "process oriented" legal standard for corporate information security was first set forth in a series of financial industry security regulations required under the Gramm-Leach-Bliley Act (GLBA) titled *Guidelines Establishing Standards for Safeguarding Consumer Information.* They were issued by the Federal Reserve, the OCC, FDIC, and the Office of Thrift Supervision, on February 1, 2001,[70] and later adopted by the FTC in its GLBA *Safeguards Rule* on May 23, 2002.[71] The same approach was also incorporated in the Federal Information Security Management Act of 2002 ("FISMA"),[72] and in the HIPAA *Security Standards* issued by the Department of Health and Human Services on February 20. 2003.[73]

---

[70] 66 Fed. Reg. 8616, February 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).

[71] 67 Fed. Reg. 36484, May 23, 2002; 16 C.F.R. Part 314.

[72] 44 U.S.C. Section 3544(b).

[73] 45 C.F.R. Parts 164.

The FTC has since adopted the view that the "process oriented" approach to information security outlined in these regulations sets forth a general "best practice" for legal compliance that should apply to all businesses in all industries.[74] Thus, it has, in effect, implemented this "process oriented" approach in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security.[75] The National Association of Insurance Commissioners has also recommended the same approach, and to date, several state insurance regulators have adopted it.[76] Several state Attorneys General have also adopted this approach in their actions against perceived offenders.[77] And now we are starting to see some cases take the same approach.[78]

In *Guin v. Brazos Education*, for example, the court rejected the view that the law requires specific security measures (in that case, encryption). Instead, it focused on the fact that the defendant had followed the proper "process" – i.e., had put in place written security policies, had done current risk assessments, and had implemented proper safeguards as required by the GLB Act. And because the defendant had properly followed such a process, the court held there was no liability for a breach that did occur.[79] Conversely, in *Bell v. Michigan Council*, the court imposed liability where the defendant was aware of the security risk, but did nothing to address it.[80]

The New Jersey Advisory Committee on Professional Ethics also briefly addressed this issue of reasonable security in the context of a 2006 opinion on attorney use of technology to store client information for remote access. Noting the ethical obligation of the attorney to "exercise reasonable care" against the possibility of unauthorized access to client information, the Committee noted that "reasonable care,"

---

[74] See, Prepared Statement of the Federal Trade Commission on Identity Theft: Innovative Solutions For An Evolving Problem, Presented by Lydia Parnes, Director, Bureau of Consumer Protection, Before the Subcommittee On Terrorism, Technology and Homeland Security of the Senate Committee on the Judiciary, United States Senate**,** March 21, 2007 at p. 7 (noting that "the FTC Safeguards Rule promulgated under the GLB Act serves as a good model" for satisfying the obligation to maintain reasonable and appropriate security); available at www.ftc.gov/os/testimony/P065409identitytheftsenate03212007.pdf. See also, Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, U.S. House of Representatives on "Protecting Our Nation's Cyberspace," April 21, 2004, at p. 5 (noting that "security is an ongoing process of using reasonable and appropriate measures in light of the circumstances"), available at www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

[75] *See, e.g.,* FTC Decisions and Consent Decrees listed in the Appendix.

[76] *See, e.g.,* National Association of Insurance Commissioners "Standards for Safeguarding Customer Information Model Regulation" IV-673-1 available at www.naic.org (adopted in at least 9 states so far)

[77] See, e.g., State Attorneys General Consent Decrees listed in the Appendix

[78] *See, e.g.*, Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 (D. Minn. Feb. 7, 2006) and Bell v. Michigan Council, 2005 Mich. App. LEXIS 353 (Mich. App. February 15, 2005).

[79] Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 (D. Minn. Feb. 7, 2006).

[80] Bell v. Michigan Council, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005).

"does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access." Moreover, the Committee rejected requirements for specific technical solutions. Instead, it noted that the touchstone of reasonable care is that "use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data."[81]

In the EU, the process-oriented approach noted above is also specifically referenced in a few statutes.[82] In addition, several statutes incorporate the various elements of the process, including conducting periodic risk assessments,[83] developing and implementing a responsive security program[84] including employee training and education,[85] monitoring and testing the program,[86] continually reviewing and adjusting the program,[87] and overseeing third party service provider arrangements.[88]

Thus, although this remains an unsettled area, the trend is to recognize what security consultants have been saying for some time: "security is a process, not a product."[89] 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.

---

[81] New Jersey Advisory Committee on Professional Ethics, Opinion 701 (2006) available at http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf.

[82] *See, e.g.*, Italy – Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003, Annex B, § 19.3; Slovakia Act No 428 of 3 July 2002 on personal data protection, § 16(5).

[83] From Appendix, see Italy Act, Annex B, Section 19.3; Slovak Republic Act, Section 16(5)

[84] From Appendix, see Argentina Act, Article 9(1); Estonia Act, Section 19(1); Belgium Act, Art. 16(4); Denmark Act, Section 41(3); Estonia Act, Section 19(1) ("IT"); Finland Act, Section 32(1); German Act, Section 9; Greece Act, Article 10(3); Hungary Act, Article 10(1); Lithuania Act, Article 24(1); Netherlands Act, Article 13; Portugal Act, Article 14(1); Slovak Republic Act, Section 15(1); Spain Act, Article 9; Sweden Act, Section 31; UK Act, Schedule 1, Part I, Seventh Principle; Swiss Act, Article 7.

[85] From Appendix, see Australia Act, Schedule 2, Section 3.1(b); Belgium Act, Art 16(2)(3); Canada Act, Schedule 1, 4.7 Principle 7, Clause 4.7.4; Estonia Act, Section 20(3); Ireland Act, Section 2C(2); Italy Act, Annex B, Sections 4 and 19.6; Slovak Republic Act, Sections 17 and 19(3).

[86] From Appendix, see German Act, Section 9a (audit); Poland Ordinance, Attachment A (Basic Security Measures) § VII (monitor); Slovak Republic Act, Section 16(6)(d); Spain Royal Decree 994/1999 – Medium (audit).

[87] From Appendix, see Spain Royal Decree 994/1999 – Basic.

[88] From Appendix, see Australia Act, Section 14, Principle 4; Austria Act, Article 15(2); Belgium Act, Article 16; Denmark Act, Sections 41 and 42; Estonia Act, Section 20; Finland Act, Section 32(2); Ireland Act, Section 2C-(3); Italy Act, Annex B, Sections 4 and 19.6; Slovak Republic Act, Sections 17 and 19(3).

[89] Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons, 2000) at page XII.

The legally-mandated process for reasonable security may be summarized as follows:

(a) Asset Assessment

When addressing information security, the first step is to define the scope of the effort. What information, communications, and processes are to be protected? What information systems are involved? Where are they located. What laws potentially apply to them? As is often the case, little known but sensitive data files are found in a variety of places within the company.

(b) Periodic Risk Assessment

Implementing a comprehensive security program to protect these assets requires a thorough assessment of the potential risks to the organization's information systems and data.[90] This involves identifying all reasonably foreseeable internal and external threats to the information assets to be protected.[91] Threats should be considered in each area of relevant operation, including information systems, network and software design, information processing, storage and disposal, prevention, detection, and response to attacks, intrusions, and other system failures, as well as employee training and management.[92]

For each identified threat, the organization should then evaluate the risk posed by the threat by:

- Assessing the likelihood that the threat will materialize;
- Evaluating the potential damage that will result if it materializes; and
- Assessing the sufficiency of the policies, procedures, and safeguards in place to guard against the threat.[93]

Such risk should be evaluated in light of the nature of the organization, its transactional capabilities, the sensitivity and value of the stored information to the organization and its trading partners, and the size and volume of its transactions.[94]

---

[90] *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(A).

[91] *See, e.g.*, Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance, Para. 25(b), p. 5; Eli Lilly Decision at II.B; GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(1)

[92] *See, e.g.*, Microsoft Consent Decree at II, p. 4; Eli Lilly Decision at II.B.

[93] *See, e.g.*, FISMA, 44 U.S.C. Sections 3544(a)(2)(A) and 3544(b)(1); GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(2)

[94] *See, e.g.*, Authentication In An Electronic Banking Environment, July 30, 2001, Federal Financial Institutions Examination Council, page 2; available at www.occ.treas.gov/ftp/advisory/2001-8a.pdf.

This process will be the baseline against which security measures can be selected, implemented, measured, and validated. The goal is to understand the risks the business faces, and determine what level of risk is acceptable, in order to identify appropriate and cost-effective safeguards to combat that risk.

(c) Develop Security Program to Manage and Control Risk

Based on the results of the risk assessment, a business should design and implement a security program consisting of reasonable physical, technical, and administrative security measures to manage and control the risks identified during the risk assessment.[95] The security program should be in writing,[96] and should be coordinated among all parts of the organization.[97] It should be designed to provide reasonable safeguards to control the identified risks[98] (i.e., to protect against any anticipated threats or hazards to the security or integrity of the information and systems to be protected[99]). The goal is to reduce the risks and vulnerabilities to a reasonable and appropriate level.[100]

In other words, it is not enough merely to implement impressive-sounding security measures. They must be responsive to the particular threats a business faces, and must address its specific vulnerabilities. Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat 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 and protect sensitive databases, but if a company's major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated technical security measures, while important, will not adequately address the problem.

---

[95] *See, e.g.*, Microsoft Consent Decree at II, p. 4; GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.A; Eli Lilly Decision at II.B; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(i); Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3544(b).

[96] *See, e.g.*, Microsoft Consent Decree at II, p. 4; GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A; HIPAA Security Regulations, 45 C.F.R. Section 164.316(b)(1); Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3544(b).

[97] *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A; Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Section 3544(b).

[98] *See, e.g.*, Microsoft Consent Decree at II, p. 4; GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.B

[99] *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.B(2); HIPAA Security Regulations, 45 C.F.R. Section 164.306(a)(2).

[100] *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(B)

(1) Relevant Factors to Consider

In determining what security measures should be implemented within a particular organization, virtually all of the existing precedent recognizes that there is no "one size fits all" approach. Which security measures are appropriate for a particular organization will vary, depending upon a variety of factors.

Traditional negligence law suggests that the relevant factors are (1) the probability of the identified harm occurring (i.e., the likelihood that a foreseeable threat will materialize), (2) the gravity of the resulting injury if the threat does materialize, and (3) the burden of implementing adequate precautions.[101] In other words, the standard of care to be exercised in any particular case depends upon the circumstances of that case and on the extent of foreseeable danger.[102]

Security regulations take a similar approach, and indicate that the following factors are relevant in determining what security measures should be implemented in a given case:

- The probability and criticality of potential risks
- The company's size, complexity, and capabilities
- The nature and scope of the business activities
- The nature and sensitivity of the information to be protected
- The company's technical infrastructure, hardware, and software security capabilities
- The state of the art re technology and security
- The costs of the security measures[103]

Interestingly, cost was the one factor mentioned most often, and certainly implies recognition that companies are not required to do everything theoretically possible.

(2) Categories of Security Measures that Must Be Addressed

Specifying a process still leaves many businesses wondering, "What specific security measures should I implement?" In other words, in developing a security plan, what security measures or safeguards should be included?

Generally, developing law in the U.S. does not require companies to implement specific security measures or use a particular technology. As expressly stated in the

---

[101] *See, e.g., United States v. Carroll Towing,* 159 F.2d 169, 173 (2d Cir. 1947).

[102] *See, e.g.*, *DCR Inc. v. Peak Alarm Co.,* 663 P.2d 433, 435 (Utah 1983); *see also Glatt v. Feist,* 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with facts and circumstances of each case).

[103] *See, e.g.,* HIPAA Security Regulations, 45 C.F.R. Section 164.306(b)(2); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A and Part II.C; FISMA, 44 U.S.C. Sections 3544(a)(2) and 3544(b)(2)(B); Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance.

HIPAA security regulations, for example, companies "may use any security measures" reasonably designed to achieve the objectives specified in the regulations.[104]

This focus on flexibility means that, like the obligation to use "reasonable care" under tort law, determining compliance may ultimately become more difficult, as there are unlikely to be any safe-harbors for security. As one commentator has pointed out with respect to the HIPAA security regulations: "The new security rules offer no safe harbor to covered entities, business associates, or the people who make security decisions for them. Rather, whether security countermeasures are good enough to 'ensure' the confidentiality, integrity, and availability of [protected health information], and protect it from 'any' hazard one could reasonably anticipate, is likely to be judged retroactively."[105]

Nonetheless, developing law seems to consistently require that companies consider certain *categories* of security measures, even if the way in which each category is addressed is not specified. At a high level, for example, most recent security rules require covered organizations to implement physical, technical, and administrative security measures.[106]

In addition, there are several more specific categories of security measures that regulations often require companies to consider. They include the following:

- **Physical Facility and Device Security Controls** – procedures to safeguard the facility,[107] measures to protect against destruction, loss, or damage of information due to potential environmental hazards, such as fire and water damage or technological failures,[108] procedures that govern the receipt and removal of hardware and electronic media into and out of a facility,[109] and procedures that govern the use and security of physical workstations.[110]

- **Physical Access Controls** – access restrictions at buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.[111]

---

[104] HIPAA Security Regulations, 45 CFR Section 164.306(b)(1).

[105] Richard D. Marks and Paul T. Smith, *Analysis and Comments on HHS's Just-released HIPAA Security Rules,* Bulletin of Law / Science & Technology, ABA Section of Science & Technology Law, No. 124 April 2003, at p. 2, available at http://www.abanet.org/scitech/DWTSecurityRules021703.pdf.

[106] *See, e.g.*, HIPAA regulations 45 C.F.R. Sections 164.308, 164.310, and 164.312; GLB Regulations, 12 C.F.R. 208, Appendix D-2.II(A) and 12 C.F.R. Part 30, Appendix B, Part II; Microsoft Consent Decree, at p. 4.

[107] HIPAA Security Regulations, 45 C.F.R. Section 164.310(a)(2)(ii)

[108] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.

[109] HIPAA Security Regulations, 45 C.F.R. Section 164.310(d)

[110] HIPAA Security Regulations, 45 C.F.R. Sections 164.310(b) and (c)

[111] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; HIPAA Security Regulations, 45 C.F.R. Section 164.310(a)

- **Technical Access Controls** – policies and procedures to ensure that authorized persons who need access to the system have appropriate access, and that those who should not have access are prevented from obtaining access,[112] including procedures to determine access authorization,[113] procedures for granting and controlling access,[114] authentication procedures to verify that a person or entity seeking access is the one claimed,[115] and procedures for terminating access.[116]

- **Intrusion Detection Procedures** – procedures to monitor log-in attempts and report discrepancies;[117] system monitoring and intrusion detection systems and procedures to detect actual and attempted attacks on or intrusions into company information systems;[118] and procedures for preventing, detecting, and reporting malicious software (e.g., virus software, Trojan horses, etc.);[119]

- **Employee Procedures** – job control procedures, segregation of duties, and background checks for employees with responsibility for or access to information to be protected,[120] and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means;[121]

- **System Modification Procedures** – procedures designed to ensure that system modifications are consistent with the company's security program[122]

- **Data Integrity, Confidentiality, and Storage** – procedures to protect information from unauthorized access, alteration, disclosure, or destruction

---

[112] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(3)

[113] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(3)(ii); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C

[114] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(4) and 164.312(a); Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

[115] HIPAA Security Regulations, 45 C.F.R. Section 164.312(d)

[116] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(3)(ii)(C)

[117] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(5)(ii)(C)

[118] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 24(d), p. 5 and Para. 25, p. 6

[119] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(5)(ii)(B)

[120] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.

[121] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C.

[122] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

during storage or transmission,[123] including storage of data in a format that cannot be meaningfully interpreted if opened as a flat, plain-text file,[124] or in a location that is inaccessible to unauthorized persons and/or protected by a firewall;[125]

- **Data Destruction and Hardware and Media Disposal** – procedures regarding final disposition of information and/or hardware on which it resides,[126] and procedures for removal from media before re-use of the media;[127]

- **Audit Controls** -- maintenance of records to document repairs and modifications to the physical components to the facility related to security (e.g., walls, doors, locks, etc);[128] and hardware, software, and/or procedural audit control mechanisms that record and examine activity in the systems[129]

- **Contingency Plan** – procedures designed to ensure the ability to continue operations in the event of an emergency, such as a data backup plan, disaster recovery plan, and emergency mode operation plan[130]

- **Incident Response Plan** -- a plan for taking responsive actions in the event the company suspects or detects that a security breach has occurred,[131] including ensuring that appropriate persons within the organization are promptly notified of security breaches, and that prompt action is taken both in terms of responding to the breach (e.g., to stop further information compromised and to work with law enforcement), and in terms of notifying appropriate persons who may be potentially injured by the breach.

(d) Awareness, Training and Education

Training and education for employees is a critical component of any security program. Newer statutes, regulations, and consent decrees in the U.S. clearly recognize that even the very best physical, technical, and administrative security measures are of

---

[123] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C; Ziff Davis Assurance of Discontinuance, Para. 25, p. 6; HIPAA Security Regulations, 45 C.F.R. Sections 164.312(c) and (e)

[124] Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

[125] Ziff Davis Assurance of Discontinuance, Para. 25, p. 6

[126] HIPAA Security Regulations, 45 C.F.R. Section 164.310(d)(2)(i)

[127] HIPAA Security Regulations, 45 C.F.R. Section 164.310(d)(2)(ii)

[128] HIPAA Security Regulations, 45 C.F.R. Section 164.310(a)(2)(iv)

[129] HIPAA Security Regulations, 45 C.F.R. Section 164.312(b)

[130] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(7)

[131] Ziff Davis Assurance of Discontinuance, Paras. 24(d) and 26, pp. 5,6; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(6)(i); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C

little value if employees do not understand their roles and responsibilities with respect to security. For example, installing heavy duty doors with state of the art locks (whether of the physical or virtual variety), will not provide the intended protection if the employees authorized to have access leave the doors open and unlocked for unauthorized persons to pass through.

Security education begins with communication to employees of applicable security policies, procedures, standards, and guidelines. It also includes implementing a security awareness program,[132] periodic security reminders, and developing and maintaining relevant employee training materials,[133] such as user education concerning virus protection, password management, and how to report discrepancies. Applying appropriate sanctions against employees who fail to comply with security policies and procedures is also important.[134]

(e) Monitoring and Testing

Merely implementing security measures is not sufficient. Companies must also ensure that the security measures have been properly put in place and are effective. This includes conducting an assessment of the sufficiency of the security measures in place to control the identified risks,[135] and conducting regular testing or monitoring of the effectiveness of those measures.[136] Existing precedent also suggests that companies must monitor compliance with its security program.[137] To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports[138] is also important.

(f) Review and Adjustment

Perhaps most significantly, the legal standard for information security recognizes that security is a moving target. Businesses must constantly keep up with every changing threats, risks, vulnerabilities, and security measures available to respond to them. It is a never-ending process. As a consequence, businesses must conduct periodic internal reviews to evaluate and adjust the information security program[139] in light of:

---

[132] *See, e.g.*, FISMA, 44 U.S.C. Section 3544(b)(4); HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(5)(i); Ziff Davis Assurance of Discontinuance, Para. 24(d), p. 5

[133] Ziff Davis Assurance of Discontinuance, Para. 27(c), p. 7.

[134] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(C)

[135] Microsoft Consent Decree at II, p. 4

[136] FISMA, 44 U.S.C. Section 3544(b)(5); Eli Lilly Decision at II.C; GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III(c)(3).

[137] Ziff Davis Assurance of Discontinuance, Para. 27(e) and (f), p. 7; Eli Lilly Decision at II.C.

[138] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(D)

[139] Microsoft Consent Decree at II, p. 4; Ziff Davis Assurance of Discontinuance, Para. 27(e) and (f), p. 7; Eli Lilly Decision at II.D, GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.E; HIPAA Security Regulations, 45 C.F.R. Section 164.306(e) and 164.308(a)(8)

- The results of the testing and monitoring
- Any material changes to the business or arrangements
- Any changes in technology
- Any changes in internal or external threats
- Any environmental or operational changes
- Any other circumstances that may have a material impact.[140]

In addition to periodic internal reviews, best practices and the developing legal standard may require that businesses obtain a periodic review and assessment (audit) by qualified independent third-party professionals using procedures and standards generally accepted in the profession to certify that the security program meets or exceeds applicable requirements, and is operating with sufficient effectiveness to provide reasonable assurances that the security, confidentiality, and integrity of information is protected.[141] It should then adjust the security program in light of the findings or recommendations that come from such reviews.[142]

(g) Oversee Third Party Service Provider Arrangements

In today's business environment, companies often rely on third parties, such as outsource providers, to handle much of their data. When corporate data is in the possession and under the control of a third party, this presents special challenges for ensuring security.

Laws and regulations imposing information security obligations on businesses often expressly address requirements with respect to the use of third party outsource providers. And first and foremost, they make clear that regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, "you can outsource the work, but not the responsibility." Thus, third party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.[143]

Accordingly, the developing legal standard for security imposes three basic requirements on businesses that outsource: (1) they must exercise due diligence in selecting service providers,[144] (2) they must contractually require outsource providers to

---

[140] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.E; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(8); Microsoft Consent Decree at II, p. 4; Eli Lilly Decision at II.D

[141] Microsoft Consent Decree at III, p. 5

[142] Ziff Davis Assurance of Discontinuance, Para. 27(h), p. 7

[143] *See, e.g.,* Office of the Comptroller of the Currency, Administrator of National Banks, OCC Bulletin 2001-47 on Third Party Relationships, November 21, 2001 (available at www.OCC.treas.gov/ftp/bulletin/2001-47.doc).

[144] *See, e.g.,* GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(1)

implement appropriate security measures,[145] and (3) they must monitor the performance of the outsource providers.[146]

3. Importance of a Risk Assessment

Key to the legal standard for reasonable security is a requirement that the security measures implemented be responsive to a company's fact-specific risk assessment. In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Those security measures 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 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 latter problem.

A risk assessment focuses on identifying foreseeable threats to corporate information and information systems. And it clearly plays a key role in determining whether a duty will be imposed and liability found. In *Wolfe v. MBNA America Bank*, for example, a federal court held that where injury resulting from negligent issuance of a credit card (to someone who applied using the plaintiff's identity) is foreseeable and preventable, "the defendant has a duty to verify the authenticity and accuracy of a credit account application."[147] In *Bell v. Michigan Council*, the court held that where a harm was foreseeable, and the potential severity of the risk was high, the defendant was liable for failure to provide appropriate security to address the potential harm.[148] On the other hand, in *Guin v. Brazos Education*, the court held that where a proper risk assessment was done, but a particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it.[149]

The importance of a risk assessment, and its role in determining what security controls are required, was also stressed by the Federal Financial Institutions Examinations Counsel (FFIEC)[150] in its FAQ relating to its authentication requirements

---

[145] *See, e.g.,* GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Section 164.308(b)(1) and 164.314(a)(2)

[146] GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(3).

[147] Wolfe v. MBNA America Bank, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007).

[148] *See* Bell v. Michigan Council, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005).

[149] *See* Guin v. Brazos Higher Education Service, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 at *13 (D. Minn. Feb. 7, 2006) (finding that where a proper risk assessment was done, the inability to foresee and deter a specific burglary of a laptop was not a breach of a duty of reasonable care).

[150] The Federal Financial Institutions Examinations Counsel (FFIEC) is a group of U.S. federal regulatory agencies, that include the Board of Governor's of the Federal Reserve System, Federal Deposit Insurance

(discussed below). In response to a question regarding whether a financial institution could forgo a risk assessment and move immediately to implement additional strong authentication controls the FFIEC responded with an emphatic "no." As it pointed out, the security requirements that it imposed for authentication are risk-based, and thus, a risk assessment that sufficiently evaluates the risks and identifies the reasons for choosing a particular control should be completed before implementing any particular controls.[151]

The law does not generally specify what is required for a risk assessment. But the FFIEC has referred financial institutions seeking general information on risk assessments to:[152] (1) the "Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards,"[153] and (2) the "FFIEC IT Examination Handbook, Information Security Booklet."[154] The National Institute of Standards and Technology (NIST) also offers guidance on conducting risk assessments.[155]

4. ISO/IEC 27001 – A Formal Global Standard?

Finally, it is worth making note of the new international information security standard known as ISO/IEC 27001.[156] This standard is an auditable international standard that defines the requirements for an Information Security Management System (ISMS) and provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an IMIS.[157] It was developed jointly by the International Organization for Standardization (ISO)[158] and the International

---

Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

[151] "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8, 2006 at p. 5, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf

[152] "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8, 2006 at p. 5, available at www.ffiec.gov/pdf/authentication_faq.pdf.

[153] Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards, December 14, 2005, available at www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/default.htm.

[154] FFIEC IT Examination Handbook, Information Security Booklet, July 2006, available at www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf.

[155] *See* National Institute of Standards and Technology, "Risk Management Guide for Information Technology Systems," NIST Special Publication No. 800-30; available at

[156] ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements (Oct. 2005) (hereinafter "ISO/IEC 27001").

[157] ISO/IEC 27001 § 0.1.

[158] ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards, and is comprised of a network of the national standards institutes of 155 countries, with one member per country, and a Central Secretariat in Geneva, Switzerland, that coordinates the system. The American National Standards Institute (ANSI), represents the United States. See, www.iso.org/iso/home.htm

Electrotechnical Commission (IEC).[159] Since its formal release in October 2005, ISO/IEC 27001 has been positioned as an international best practice.

While ISO/IEC 27001 is a technical standard, it appears to be based on essentially the same premise as the legal standard outlined above. That is, it "adopts a *process approach* to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's IMIS."[160] And it includes all of the requirements of the legal standard – i.e., compliance with the ISO/IEC 27001 standard requires companies to identify their information assets,[161] conduct risk assessments,[162] select responsive security controls,[163] implement and operate their ISMS,[164] monitor and review their ISMS,[165] maintain and improve their ISMS,[166] and manage security of third parties.[167]

Thus, it can be argued that the adoption of ISO/IEC 27001 by two international standards groups comprised of representatives from most countries, represents at least a tacit endorsement of the legal standard for security at an international level. Moreover, although compliance with the ISO/IEC 27001 standard does not guarantee legal compliance (e.g., it is not a safe harbor),[168] it may offer companies a good starting point on the road to addressing international legal requirements for security.

C. An Increasing Number of Specific Legal Obligations

1. Special Rules for Specific Data Elements

In addition to laws imposing general security obligations with respect to personal information, developing law is also imposing new obligations to protect specific data elements or sub-categories of personal data. That is, laws, regulations, and standards are beginning to focus on specific data elements, and imposing specific obligations with

---

[159] The IEC (International Electrotechnical Commission), also based in Geneva, Switzerland coordinates, designs, and publishes international standards in fields related to electronics, including telecommunications. The electrotechnical standards organizations of each participating country make up its membership, with ANSI representing the United States. See www.iec.ch.

[160] ISO/IEC 27001, § 0.2 (emphasis added).

[161] ISO/IEC 27001, § 4.2.1.

[162] ISO/IEC 27001, § 4.2.1.

[163] ISO/IEC 27001, § 4.2.1.

[164] ISO/IEC 27001, § 4.2.2.

[165] ISO/IEC 27001, §§ 4.2.3 and 6.

[166] ISO/IEC 27001, §§ 4.2.4 and 8.

[167] ISO/IEC 27001, §§ A.10.2.

[168] ISO/IEC 27001 itself specifically states that "Compliance with an International Standard does not in itself confer immunity from legal obligations." p. 1.

respect to such data elements. Prime examples include Social Security numbers, credit card transaction data, and other sensitive data.

(a) Sensitive Data

From its inception, the EU Data Protection Directive has required special treatment for particularly sensitive personal information. Specifically, the Directive prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life," unless certain exceptions apply.[169] Those exceptions include "explicit consent" by the data subject, and carrying out obligations under applicable employment laws.

But even with consent, processing such sensitive data, according to EU interpretation, requires that "special attention" be given to data security aspects to avoid risks of unauthorized disclosure. In particular, "*[a]ccess by unauthorized persons must be virtually impossible and prevented*." [170]

In the U.S. a de facto category of sensitive information has been defined by the various state security breach notification laws (discussed in part D below). These laws require special action (i.e., disclosure) in the event of a breach of security with respect to a subcategory of personal data generally considered to be sensitive because of its potential role in facilitating identity theft.

(b) Social Security Numbers

Separately, the security of Social Security numbers has also been the focus of numerous state laws enacted during the past few years (see list in Appendix). The scope of these laws range from restrictions on the manner in which social security numbers can be used, to express requirements for security with respect to the communication and/or storage of social security numbers. For example, several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the individual's Social Security number is encrypted.[171] The law in Maryland and Nevada goes further, and prohibits initiating any transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.[172]

---

[169] EU Data Protection Directive, Article 8.

[170] Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, February 15, 2007, at pp. 19-20; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf (emphasis in original).

[171] *See* list of state laws in GAO Report, Social Security Numbers: Federal and State Laws Restrict Use of SSN's, Yet Gaps Remain, September 15, 2005 at Appendix III; available at www.gao.gov/new.items/d051016t.pdf.

[172] Maryland Commercial Code, § 14-3402(a)(4); Nevada Rev. Stat. 597.970.

The bottom line is that if a company wants to continue collecting, maintaining, and transferring data with SSNs, it will have provide special treatment for the protection of that data (at least for the SSN number portion), such as encryption, using secure communications media, controlling access, and adopting special security policies.

(c) Credit Card Data

For businesses that accept credit card transactions, the Payment Card Industry Data Security Standards ("PCI Standards")[173] impose significant security obligations with respect to credit card data captured as part of any credit card transaction. The PCI Standards, jointly created by the major credit card associations, require businesses that accept MasterCard, Visa, American Express, Discover, and Diner's Club cards to comply.

2. Special Rules for Specific Security Controls

(a) Data Destruction

A new trend during the past few years has been for laws and regulations to impose security requirements with respect to the manner in which data is destroyed. These regulations typically do not require the destruction of data, but seek to regulate the manner of destruction when companies decide to do so. These laws also typically apply to the destruction of personal data.

At the Federal level, both the banking regulators and the SEC have adopted regulations regarding security requirements for the destruction of personal data. Similarly, at the State level, at least 19 states have now adopted similar requirements.[174]

Such statutes and regulations generally require companies to property dispose of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. With respect to information in paper form, this typically requires implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot be read or reconstructed. With respect to electronic information, such regulations typically require implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer personal information so that the information cannot practicably be read or reconstructed.[175]

---

[173] Available at www.pcisecuritystandards.org.

[174] See list in Appendix.

[175] See, e.g., 16 CFR Section 682.3.

(b) Online Authentication

Satisfying a company's legal obligations to provide information security will always include an obligation to properly authenticate the identity of persons seeking access to the company's computer systems or data. Such a requirement is expressly addressed, for example, in most U.S. information security laws and regulations, including HIPAA,[176] GLBA,[177] the Homeland Security Act,[178] FDA regulations,[179] and state information security laws.[180] Likewise, in April 2007 the Federal Communications Commission (FCC) issued an Order directed to telephone and wireless carriers to protect personal telephone records from unauthorized disclosure that imposes specific authentication requirements.[181] And in a case involving identity theft, a court found that there was a common law duty to verify the authenticity of a credit card application.[182] In all cases, the key issue is not whether authentication is required, but rather, what form of authentication is legally appropriate.

Historically, the standard approach to authentication of identity has been to use a user ID and password. But based on recent developments, that approach may no longer be *legally* adequate in all cases. In the U.S., regulators in the financial sector were the first to formally state that reliance solely on a user ID and password – so-called single-factor authentication – is considered "to be *inadequate*" at least in the case of high-risk transactions.

This new view of online authentication came in a guidance document issued by the FFIEC in late 2005 titled "Authentication in an Internet Banking Environment" ("FFIEC Guidance").[183] While the FFIEC Guidance applies to the financial sector, it is clearly in line with the developing law of security, and thus may well become legal best

---

[176] Health Insurance Portability and Accountability Act (HIPAA) Security Regulations, 45 C.F.R. § 164.312(d). HIPAA security regulations apply to medical records in the healthcare sector.

[177] Gramm Leach Bliley Act (GLBA) Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C(1)(a). GLBA security regulations apply to customer information in the financial sector.

[178] Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(D), and § 301(b)(1) amending 44 U.S.C. § 3542(b((1) ("'information security' means protecting information and information systems from unauthorized access, ...")

[179] Food and Drug Administration regulations, 21 C.F.R. Part 11.

[180] *See, e.g.*, Cal. Civil Code § 1798.81.5(b).

[181] *See* FCC Order re Pretexting, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 13-25; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf (hereinafter "FCC Pretexting Order")

[182] Wolfe v. MBNA America Bank, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007).

[183] Authentication in an Internet Banking Environment , October 12, 2005 ("FFIEC Guidance"), available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. This was later supplemented by an FAQ titled "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8, 2006, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf.

practice for all companies, especially where access to sensitive personal information is involved. Other countries, such as Singapore, have also adopted similar requirements.[184]

As with other aspects of security, existing U.S. law does *not* usually specify what type or kind of authentication method or technology must be used.[185] Instead, the law requires companies to conduct a risk assessment, and to use the results of that process to identify an appropriate authentication strategy.[186] The FFIEC Guidance document summarizes this requirement (as it relates to authentication obligations), by noting the following four key points:[187]

- When offering Internet-based products and services to customers, companies should use effective methods to authenticate the identity of customers using those products and services.
- The authentication techniques employed should be appropriate to the risks associated with those products and services.
- Companies should conduct a risk assessment to identify the types and levels of risk associated with their Internet applications.
- Where risk assessments indicate that the use of single-factor authentication is inadequate, companies should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Stressing the importance of the risk assessment, the FFIEC Guidance specifically states that:

> The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions.[188]

Then, building on the results of the risk assessment, the FFIEC Guidance states that an effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the company's Internet-based products and services. The level of authentication used in a particular application should be appropriate to the level of risk in that application.[189]

---

[184] Monetary Authority of Singapore, Circular No. SRD TR 02/2005, November 25, 2005.

[185] The FCC Pretexting Order, however, is an exception.

[186] *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(A).

[187] FFIEC Guidance, at p. 6.

[188] *Id*. at p. 3.

[189] *Id* at p. 3.

The bottom line is that the legal appropriateness of any particular authentication method (or any other security measure) is not determined in the abstract. Instead, it must be determined on the basis of a risk assessment specific to the company and its business – i.e., the method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. This means, of course, that the standards for legally appropriate authentication will vary across businesses and applications. It also means that what constitutes legally appropriate authentication may also change over time as new threats arise and better technology is developed to address them. Thus, a single risk assessment in never sufficient. Companies must implement an ongoing process to regularly review threats and authentication technology in order to ensure that appropriate changes are implemented as needed

D. The Legal Obligations to Warn of Security Breaches

In addition to the foregoing legal trend imposing an obligation to *implement* security measures to protect data, we are also witnessing a global trend to enact laws and regulations that impose an obligation to *disclose* security breaches to the persons affected. But unlike laws that impose a duty to provide security, these laws typically require only that companies disclose security breaches to affected persons.[190]

Designed as a way to help protect persons who might be adversely affected by a security breach of their personal information, these laws 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. By requiring notice to persons who may be adversely affected by a security breach (e.g., persons whose compromised personal information may be used to facilitate identity theft), these laws seek to provide such persons with a warning that their personal information has been compromised, and an opportunity to take steps to protect themselves against the consequences of identity theft.[191]

For the most part, laws imposing an obligation to disclose security breaches are a direct reaction to a series of well-publicized security breaches involving sensitive personal information over the past few years,[192] and an effort to address the problem of identity theft. Yet the concept of such laws is not new, nor is it limited to personal

---

[190] Pisciotta v. Old National Bancorp., 2007 U.S. App. Lexis 20068 (7th Cir. August 23, 2007), at p. 13.

[191] *See, e.g.*, Recommended Practices on Notice of Security Breach Involving Personal Information, Office of Privacy Protection, California Department of Consumer Affairs, April, 2006 (hereinafter "California Recommended Practices"), at pp. 5-6 (available at www.privacy.ca.gov/recommendations/secbreach.pdf); Interagency Guidance *supra* note 4 , at p. 15752.

[192] For a chronology of such breaches in the U.S., and a running total of the number of individuals affected, see Privacy Rights Clearinghouse at www.privacyrights.org/ar/ChronDataBreaches.htm.

information. In 1998, for example, the Internal Revenue Service imposed a disclosure requirement on all taxpayers whose electronic tax 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 tax records "are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed …, or are found to be incomplete or materially inaccurate."[193]

With respect to personal information, a total of 39 states in the U.S. have enacted security breach notification laws as of September 2007, all generally based on a 2003 California law.[194] In addition, the federal banking regulatory agencies issued final interagency guidance for financial institutions regarding this duty to disclose breaches (hereinafter "Interagency Guidance").[195]

These laws generally require that any business in possession of computerized sensitive personal information about an individual must disclose a breach of the security of such information to the person affected.[196] Sensitive personal information is typically defined as information consisting of: (1) a person's first name or initial and last name, plus (2) any one of the following: social security number, drivers license or state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account). In some states this list is longer, and may also include medical information, insurance policy numbers, passwords by themselves, biometric information, professional license or permit numbers, telecommunication access codes, mother's maiden name, employer id number, electronic signatures, and descriptions of an individual's personal characteristics.[197] When a triggering event occurs, and the notice requirements themselves, also vary from state-to-state.[198]

---

[193] IRS Rev. Proc. 98-25, § 8.01.

[194] See list of statutes in Appendix.

[195] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), March 29, 2005, Federal Register, Vol. 70, No. 59, March 29, 2005, at p. 15736 (hereinafter "Interagency Guidance").

[196] Except where the business maintains computerized personal information that the business does not own, in which case the laws require the business to notify the owner or licensee of the information, rather than the individuals themselves, of any breach of the security of the system**.**

[197] *See, e.g.*, Ark. Code § 4-110-101 et seq.; La. Rev. Stat. § 51:3071 et seq.; Md. Code, § 14-3501 et. seq.; Neb. Rev Stat 87-801 et. seq.; N.J. Stat. 56:8-163; N.C. Gen. Stat § 75-65; N.D. Cent. Code § 51-30-01 et seq.; Oregon, 2007 S.B. 583. The Federal banking Interagency Guidance also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

[198] *See, e.g.*, Thomas J. Smedinghoff, "Security Breach Notification: Adapting to the Regulatory Framework" Review of Banking & Financial Services, December 2005.

1. **The Basic Obligation**

Taken as a group, the state and federal security breach notification laws generally require that any business in possession of sensitive personal information about a covered individual must disclose any breach of such information to the person affected. The key requirements, which vary from state-to-state, include the following:

- **Type of information** – the statutes generally apply to unencrypted sensitive personally identified information – e.g., information consisting of first name or initial and last name, plus one of the following: social security number, drivers license or other state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account).
- **Definition of breach** – generally the statutes require notice following the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of such personal information. In some states, however, notice is not required unless there is a reasonable basis to believe that the breach will result in substantial harm or inconvenience to the customer.
- **Who must be notified** – notice must be given to any residents of the state whose unencrypted personal information was the subject of the breach.
- **When notice must be provided** – generally, persons must be notified in the most expedient time possible and without unreasonable delay; however, in most states the time for notice may be extended for the following:
  - ✓ Legitimate needs of law enforcement, if notification would impede a criminal investigation
  - ✓ Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system
- **Form of notice** – Notice may be provided in writing (e.g., on paper and sent by mail), in electronic form (e.g., by e-mail, but only provided the provisions of E-SIGN[199] are complied with), or by substitute notice.
- **Substitute notice options** – if the cost of providing individual notice is greater than a certain amount (e.g., $250,000) or if more than a certain number of people would have to be notified (e.g., 500,000), substitute notice may be used, consisting of:
  - ✓ E-mail when the e-mail address is available, and
  - ✓ Conspicuous posting on the company's web site, and
  - ✓ Publishing notice in all major statewide media.

Several of these issues vary from state to state, however, and some have become controversial. The biggest issue revolves around the nature of the triggering event. In

[199] 15 USC Section 7001 *et. seq*. This generally requires that companies comply with the requisite consumer consent provisions of E-SIGN at 15 USC Section 7001(c).

California, for example, notification is required whenever there has been an unauthorized access that compromises the security, confidentiality, or integrity of electronic personal data. In other states, however, unauthorized access does not trigger the notification requirement unless there is a reasonable likelihood of harm to the individuals whose personal information is involved[200] or unless the breach is material.[201]

2. International Adoption

Although the breach notification concept began in the U.S., it is rapidly spreading to the international sector.[202] Japan became the first country outside the U.S. to impose a security breach notification obligation. The obligation is set forth in ministry guidelines to the Act on the Protection of Personal Information, which took effect for the private sector on April 1, 2005.[203]

In September, 2006, the European Commission (EC) released a Communication proposing changes to EU law that would require "electronic communications networks or services" to "notify their customers of any breach of security leading to the loss, modification or destruction of, or unauthorized access to, personal customer data." As the Commission pointed out, "A requirement to notify security breaches would create an incentive for providers to invest in security but without micro-managing their security policies."[204]

Later in the same month, the data protection authorities responsible for steering the implementation of the EU Data Protection Directive (known as the Article 29 Working Party) released an opinion in which it sought to expand the scope of data breach notification. Specifically, the document expressed concerns about the lack of sanctions for telecommunication operators and ISPs if they do not inform customers about data breaches, and included a recommendation that the breach notification obligation should also cover data brokers, banks and other online service providers.[205]

---

[200] Arkansas, Connecticut, Delaware, and Louisiana are examples of states in this category.

[201] Montana and Nevada are examples of states in this category.

[202] *See*, Ethan Preston and Paul Turner, "The Global Rise of a Duty to Disclose Information Security Breaches," 22 J. Marshall Computer & Info. L. 457 (Winter 2004).

[203] *See* Miriam Wugmeister, Saori Horikawa, and Daniel Levison, "What You Need to Know About Japan's New Law Concerning the Protection of Personal Information," BNA Privacy & Security Law Report, Volume 4 Number 19, p. 614, May 9, 2005.

[204] *See* Communication at http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf.

[205] "Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive," September 26, 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf.

In the UK, a July 2007 report by the Select Committee on Science and Technology on the Internet and Personal Safety of the House of Lords also recommended adoption of security breach notification legislation. Specifically, it stated that:

> We further believe that a data security breach notification law would be among the most important advances that the United Kingdom could make in promoting personal Internet security. We recommend that the Government, without waiting for action at European Commission level, accept the principle of such a law, and begin consultation on its scope as a matter of urgency.[206]

In Canada, the Office of the Privacy Commissioner issued voluntary guidelines for responding to data breaches in August 2007. Pointing out that "notification can be an important mitigation strategy" that benefits both the organization and the individuals affected by a breach, the guidelines indicated that "if a privacy breach creates a risk of harm to the individual, those affected should be notified" in order to help them mitigate the damage by taking steps to protect themselves.[207] Shortly thereafter, the Privacy Commissioner in New Zealand released similar guidelines.[208] Although the New Zealand guidelines are voluntary, the Privacy Commissioner noted that "principle 5 of the Privacy Act (governing the way personal information is stored) does require all organizations and individuals that hold personal information to take reasonable steps to protect it. This can include notifying people of significant breaches, where necessary."[209]

The Australian Privacy Commissioner has also recommended that Australia consider amending its privacy legislation to include a mandatory requirement to report security breaches involving personal information. Her February 28, 2007 submission to the Australian Law Reform Commission supported "consideration of the addition of provisions to the Privacy Act to require agencies and organizations to advise affected individuals of a breach to their personal information in certain circumstances."[210] On September 12, 2007, the Australian Law Reform Commission released its *Review of Australian Privacy Law*[211] which proposed numerous changes to Australia's privacy law. Included among the proposals was a new system of data breach notification.[212]

---

[206] Science and Technology Committee, House of Lords, "Personal Internet Security" 5th Report of Session 2006–07, July 24, 2007, at Para. 5.55

[207] Office of the Privacy Commissioner of Canada, Key Steps for Organizations in Responding to Privacy Breaches, August 28, 2007; available at www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp.

[208] See Privacy Breach Guidance Material, Office of the Privacy Commissioner, August 2007, available at www.privacy.org.nz/library/privacy-breach-guidelines.

[209] Privacy Commissioner, Media Release, August 27, 2007, available at www.privacy.org.nz/filestore/docfiles/5001509.doc.

[210] See, Australian Government, Office of the Privacy Commissioner, Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31, February 28, 2007, at paragraphs 127-129; available at www.privacy.gov.au/publications/submissions/alrc/all.pdf.

[211] Available at www.austlii.edu.au/au/other/alrc/publications/dp/72/.

[212] Available at www.austlii.edu.au/au/other/alrc/publications/dp/72/60.pdf

APPENDIX

Key Information Security Law References

A. Federal Statutes

1. **COPPA**: Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 *et seq*.
2. **E-SIGN**: Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001(d).
3. **FISMA**: Federal Information Security Management Act of 2002, 44 U.S.C. Sections 3541-3549.
4. **GLB Act**: Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805.
5. **HIPAA**: Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d-2 and 1320d-4.
6. **Homeland Security Act of 2002**: 44 U.S.C. Section 3532(b)(1).
7. **Privacy Act of 1974:** 5 U.S.C. Section 552a
8. **Sarbanes-Oxley Act**: Pub. L. 107-204, Sections 302 and 404, 15 U.S.C. Sections 7241 and 7262.
9. **Federal Rules of Evidence 901(a):** *see* American Express v. Vinhnee, 2005 Bankr. LEXIS 2602 (9th Cir. Bk. App. Panel, 2005), and *Lorraine v. Markel*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007).

B. State Statutes

1. **UETA**: Uniform Electronic Transaction Act, Section 12 (now enacted in 46 states).
2. **Law Imposing Obligations to Provide Security for Personal Information**:

Arkansas	Ark. Code Ann. § 4-110-104(b)
California	Cal. Civ. Code § 1798.81.5(b)
Maryland	Md. Code, § 14-3503; Md. HB 208 & SB 194
Massachusetts	Mass. Gen. Laws. Ch. 93H, § 2(a); 2007 H.B. 4144
Nevada	Nev. Rev. Stat. 603A, 210
Rhode Island	R.I. Stat. 11-49.2-2(2) and (3)
Oregon	2007 S.B. 583, Section 12
Texas	Tex. Bus. & Com. Code Ann. § 48.102(a)
Utah	Utah Code Ann. § 13-42-201

3. **Data Disposal / Destruction Laws**:

Arkansas	Ark. Code Ann. § 4-110-104(a)
California	Cal. Civil Code § 1798.81.
Georgia	Ga. Stat § 10-15-2
Hawaii	Haw. Stat Section § 487R-2
Illinois	815 ILCS 530/30 (state agencies only)
Indiana	Ind. Code § 24-4-14
Kentucky	Ken. Rev. Stat. § 365.720
Maryland	Md. Code, § 14-3502; Md. HB 208 & SB 194
Massachusetts	Mass. Gen. laws. Ch. 93I
Michigan	MCL § 445.72a
Montana	Mont. Stat. § 30-14-1703
Nevada	Nev. Rev. Stat. 603A, 200
New Jersey	N.J. Stat. 56:8-162
North Carolina	N.C. Gen. Stat § 75-64
Oregon	2007 S.B. 583, Section 12
Texas	Tex. Bus. & Com. Code Ann. § 48.102(b)
Utah	Utah Code Ann. § 13-42-201
Vermont	Vt. Stat. Tit. 9 § 2445 et seq.
Washington	RCWA 19.215.020

4. **Security Breach Notification Laws**

Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code § 1798.82
Colorado	Col. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36A-701(b)
Delaware	De. Code tit. 6, § 12B-101 et seq.
District of Columbia	DC Official Code § 28-3851 *et seq*.
Florida	Fla. Stat. § 817.5681
Georgia	Ga. Code § 10-1-910 et seq. [213]
Hawaii	Hawaii Rev. Stat. § 487N-2
Idaho	Id. Code §§ 28-51-104 to 28-51-107
Illinois	815 Ill. Comp. Stat. 530/1 et seq.
Indiana	Ind. Code § 24-4.9
Kansas	Kansas Stat. 50-7a01, 50-7a02 (2006 S.B. 196, Chapter 149)
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq.
Maryland	Md. Code, §§ 14-3501 thru 14-3508; Md. HB 208 & SB 194
Massachusetts	Mass. Gen. Laws. Ch. 93H; 2007 H.B. 4144
Michigan	MCL 445.63, Sections 12, 12a, & 12b; 2006 S.B. 309
Minnesota	Minn. Stat. § 325E.61, § 609.891

[213] Applies to information brokers only.

Montana	Mont. Code § 30-14-1701 et seq.
Nebraska	Neb. Rev Stat 87-801 et. seq.
Nevada	Nev. Rev. Stat. 603A.010 et seq.
New Hampshire	N.H. RS 359-C:19 et seq.
New Jersey	N.J. Stat. 56:8-163
New York	N.Y. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code § 1349.19, §1347 et seq.
Oklahoma	Okla. Stat. § 74-3113.1 [214]
Oregon	2007 S.B. 583
Pennsylvania	73 Pa. Cons. Stat. § 2303 *(link not available)*
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
Tennessee	Tenn. Code § 47-18-2107
Texas	Tex. Bus. & Com. Code § 48.001 et seq.
Texas (2003)	Tex. Bus. & Com. Code Ann. 35.58
Utah	Utah Code § 13-44-101 et seq.
Vermont	Vt. Stat. Tit. 9 § 2430 et seq.
Washington	Wash. Rev. Code § 19.255.010
Wisconsin	Wis. Stat. § 895.507
Wyoming	Wyo. Stat. §§ 40-12-501 – 40-12-502

5. **State SSN Laws (as of August 2005)**

Arizona (2004)	Ariz. Rev. Stat. § 44-1373
Arkansas (2005)	Ark. Code Ann. § 4-86-107
Arkansas (2005)	Ark. Code Ann. § 6-18-208
California (2001)	Cal. Civ. Code § 1798.85
California (2004)	Cal. Fam. Code § 2024.5
Colorado (2003)	Colo. Rev. Stat. § 23-5-127
Connecticut (2003)	Conn. Gen. Stat. § 42-470
Connecticut (2004)	Conn. Gen. Stat. § 8-64b
Delaware (2004)	Del. Code Ann., tit. 7 § 503
Florida (2005)	Fla. Stat. ch. 97.05851
Georgia (2004)	Ga. Code Ann. § 50-18-72
Hawaii (2005)	Haw. Rev. Stat. § 12-32
Illinois (2004)	815 Ill. Comp. Stat. 505/2QQ3
Indiana (2005)	Ind. Code § 4-1-10-1 et seq.
Indiana (2005)	Ind. Code § 9-24-6-2; § 9-24-9-2;§ 9-24-11-5; § 9-24-16-3
Louisiana (2004)	La. Rev. Stat. Ann. 9:5141; 35:17
Maryland (2005)	Md. Code Ann., Com. Law § 14-3401 et seq.
Michigan (2004)	Mich. Comp. Laws § 445.81 et seq.
Minnesota (2005)	Minn. Stat. § 325E.59
Missouri (2003)	Mo. Rev. Stat. § 407.1355

[214] Applies to state agencies only

Nevada (2005)	Nev. Rev. Stat. Chapter 239; Chapter 239B; Chapter 603
New Jersey (2005)	N.J. Stat. Ann. § 47:1-16
New Mexico (2003)	N.M. Stat. Ann. § 57-12B-1 et seq.
North Dakota (2003)	N.D. Cent. Code § 39-06-14
Oklahoma (2004)	Okla. Stat. tit. 40, § 173.1
Oregon (2007)	2007 S.B. 583, Section 11
Rhode Island (2004)	R.I. Gen. Laws § 6-13-19
South Carolina (2004)	S.C. Code Ann. § 7-5-170
South Dakota (2005)	S.D. Codified Laws § 32-12-17.10; § 32-12-17.13
Texas (2005)	Tex. Bus. & Com. Code Ann. 35.48
Texas (2003)	Tex. Bus. & Com. Code Ann. 35.58
Texas (2003)	Tex. Elec. Code Ann. § 13.004
Utah (2004)	Utah Code Ann. § 31A-21-110
Virginia (2005)	Va. Code Ann. § 59.1-443.2
Wisconsin (2003)	Wis. Stat. § 36.32
West Virginia (2003)	W. Va. Code § 17E-1-11

C. Federal Regulations

1. Regulations Imposing Obligation to Provide Security

(a) **COPPA Regulations**: 16 C.F.R. 312.8.

(b) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 33-36; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

(c) **FDA Regulations:** 21 C.F.R. Part 11.

(d) **FFIEC Guidance:** Authentication in an Internet Banking Environment , October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. See also "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8, 2006 at p. 5, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf.

(e) **GLB Security Regulations**: Interagency Guidelines Establishing Standards for Safeguarding Consumer Information (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 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), and 16 C.F.R. Part 314 (FTC).

(f) **GLB Security Regulations (FTC)**: FTC Safeguards Rule (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 16 C.F.R. Part 314 (FTC).

(g) **HIPAA Security Regulations**: Final HIPAA Security Regulations, 45 C.F.R. Part 164.

(h) **IRS Regulations**: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

(i) **IRS Regulations**: IRS Announcement 98-27, 1998-15 I.R.B. 30, and Tax Regs. 26 C.F.R. § 1.1441-1(e)(4)(iv).

(j) **OFHEO Safety and Soundness Regulation**, 12 C.F.R. Part 1720, Appendix C – Policy Guidance; Safety and Soundness Standards for Information, available at www.ofheo.gov/Media/Archive/docs/regs/finalssr.pdf.

(k) **OFHEO Record Retention Regulation**, 12 C.F.R. Part 1732 (at Section 1732.6), available at www.ofheo.gov/media/pdf/RecordRetentionfinalreg102706.pdf.

(l) **SEC Regulations**: 17 C.F.R. 240.17a-4, and 17 C.F.R. 257.1(e)(3).

(m) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).

2. Regulations Imposing Authentication Requirements

(a) **ACH Operating Rules** (2005) Section 2.10.2.2 ("Verification of Receiver's Identity")

(b) Banking Know Your Customer Rules

(c) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 13-25; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

(d) **FFIEC Guidance**: Authentication in an Internet Banking Environment , October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf.

(e) USA PATRIOT Act

i. 31 U.S.C. 5318 – Section 326 – "Verification of Identification"

ii. Know your customer rules

(f) State Credit Freeze laws

3. **Data Disposal / Destruction Regulations**

   (a) **FCRA Data Disposal Rules**: 12 C.F.R. Parts 334, 364

   (b) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).

4. **Security Breach Notification Regulations**

   (a) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at paragraphs 26-32; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

   (b) **GLB Security Breach Notification Rule**: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), available at www.occ.treas.gov/consumer/Customernoticeguidance.pdf.

   (c) **IRS Regulations**: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

D. State Regulations

1. **Insurance – NAIC Model Regulations**: National Association of Insurance Commissioners, Standards for Safeguarding Consumer Information, Model Regulation.
2. **Attorneys** – New Jersey Advisory Committee on Professional Ethics, Opinion 701 (2006) available at http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf

E. Court Decisions

1. *In Re TJX Companies Retail Security Breach Litigation*, 2007 U.S. Dist. Lexis 77236 (D. Mass. October 12, 2007) (rejecting a negligence claim due to the economic loss doctrine, but allowing a negligent misrepresentation claim to proceed).
2. *Wolfe v. MBNA America Bank*, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007)
3. *Lorraine v. Markel*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007)

4. *Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006)
5. *American Express v. Vinhnee*, 336 B.R. 437; 2005 Bankr. LEXIS 2602 (9th Cir. December 16, 2005).
6. *Bell v. Michigan Council 25*, No. 246684, 2005 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005) (Unpublished opinion)
7. *Inquiry Regarding the Entry of Verizon-Maine Into The InterLATA Telephone Market Pursuant To Section 271 of Telecommunication Act of 1996*, Docket No. 2000-849, Maine Public Utilities Commission, 2003 Me. PUC LEXIS 181, April 30, 2003; available at www.maine.gov/mpuc/orders/2000/2000-849o.htm

F. FTC Decisions and Consent Decrees

1. In the Matter of Guidance Software (Agreement Containing Consent Order, FTC File No. 062 3057, November 16, 2006), available at www.ftc.gov/opa/2006/11/guidance.htm
2. In the Matter of CardSystems Solutions, Inc., (Agreement Containing Consent Order, FTC File No. 052 3148, February 23, 2006), *available at* <www.ftc.gov/opa/2006/02/cardsystems_r.htm>
3. United States v. ChoicePoint, Inc. (Stipulated Final Judgment, FTC File No. 052 3069, N.D. Ga. Jan. 26, 2006), *available at* www.ftc.gov/os/caselist/choicepoint/choicepoint.htm
4. In the Matter of DSW Inc., (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), *available at* www.ftc.gov/opa/2005/12/dsw.htm
5. In the Matter of BJ's Wholesale Club, Inc. (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.htm
6. In the Matter of Sunbelt Lending Services, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 16, 2004), *available at* www.ftc.gov/os/caselist/0423153/04231513.htm
7. In the Matter of Petco Animal Supplies, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 7, 2004), *available at* www.ftc.gov/os/caselist/0323221/0323221.htm
8. In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209, Apr. 21, 2004), *available at* www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf
9. In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), *available at* www.ftc.gov/os/2003/06/guessagree.htm
10. FTC V. Microsoft (Consent Decree, Aug. 7, 2002), *available at* www.ftc.gov/os/2002/08/microsoftagree.pdf

11. 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/elililly do.htm

G. State Attorneys General Consent Decrees

1. In the Matter of Providence Health System-Oregon (Attorney General of Oregon, Assurance of Discontinuance), September 26, 2006, *available at* www.doj.state.or.us/media/pdf/finfraud_providence_avc.pdf.
2. In the Matter of Barnes & Noble.com, LLC (Attorney General of New York, Assurance of Discontinuance, Apr. 20, 2004), *available at* www.bakerinfo.com/ecommerce/barnes-noble.pdf
3. 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

H. International

1. UN Convention on the Use of Electronic Communications in International Contracts – Article 9, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html. See also UN Press release at http://www.un.org/News/Press/docs/2005/ga10424.doc.htm.

I. European Union – Directives

See http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

1. **EU Data Protection Directive**: 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 (Data Protection Directive), Article 17, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

2. **EU Data Protection Directive:** European Union Directive 2006/24/EC of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *available at* http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/745.pdf.

J. European Union – Security Provisions in Country Implementations of Data Protection Directive

See http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

1. **Belgium** – Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as modified by the law of 11 December 1998 Implementing Directive 95/46/EC, and the law of 26 February 2003; available at www.law.kuleuven.ac.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf. See Chapter IV, Article 16 (Confidentiality and security of processing**).** See also, 13 February 2001 – Royal Decree Implementing the Act of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data; available at ___.
2. **Czech Republic** – Consolidated version of the Personal Data Protection Act, Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/czech_republic_act_101_en.pdf See Articles 15, 27, 44, and 45.
3. **Cyprus** – Law of 2001, amended 2003; Available at www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/138(I)-2001_en.pdf. See Article 10(3).
4. **Denmark** – Act on Processing of Personal Data,; *Act No. 429 of 31 May 2000,* (unofficial English translation); available at www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1. See Title IV, Part 11, Sections 41 and 42 (Security of processing).
5. **Estonia** – Personal Data Protection Act; Passed 12 February 2003 (RT[1] I 2003, 26, 158), entered into force 1 October 2003; available at www.legaltext.ee/text/en/X70030.htm. See Chapter 3, Sections 18-20 (Personal Data Processing Requirements and Security Measures to Protect Personal Data).
6. **Finland** – The Finnish Personal Data Act (523/1999), given on 22.4.1999; available at www.tietosuoja.fi/uploads/hopxtvf.htm. See Chapter 7, Sections 32-35 (Data security and storage of personal data**).**
7. **France** – ACT 78-17 of January 6th, 1978 on Data Processing, Data Files and Individual Liberties; Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data); available at http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf. See Articles 34 and 35.
8. **Germany** – Federal Data Protection Act as of 1 January 2003; available at www.bfd.bund.de/information/bdsg_eng.pdf. See Section 9 (Technical and □rganizational measures), Section 9a (Data protection audit), and Annex (to the first sentence of Section 9 of this Act).

9. **Greece** – Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/2000 and 2915/2001); available at www.dpa.gr/Documents/Eng/2472engl_all2.doc. See Article 10 (Confidentiality and security of processing).

10. **Hungary** – Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest; available at http://abiweb.obh.hu/dpc/legislation/1992_LXIIIa.htm. See Article 10 (Data Security)**.**

11. **Ireland** – Data Protection Act of 1988; available at www.dataprivacy.ie/6ai.htm; Data Protection (Amendment) Act 2003; available at www.dataprivacy.ie/images/;Act2003.pdf. See Section 2.-(1), Security measures 2C, and First Schedule Article 7 (Data Security).

12. **Italy** – Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003; available at www.garanteprivacy.it/garante/document?ID=311066. See Chapter II (Minimum Security Measures) at Sections 33 (Minimum Security Measures), Section 34 (Processing by Electronic Means), Section 35 (Processing without Electronic Means), Section 36 (Upgrading), and Annex B (Technical Specifications Concerning Minimum Security Measures).

13. **Latvia** – Personal Data Protection Law, amended by Law of 24 October 2002; available at www.dvi.gov.lv/eng/legislation/pdp**.** See Section 26.

14. **Lithuania** – Law on Legal Protection of Personal Data, 21 January 2003, No. IX-1296, Official translation, with amendments 13 April 2004; available at www.ada.lt/en/docs/Official%20translation.doc. See Chapter 4, Article 24 (Security of Data).

15. **Luxembourg** – DPL approved on 2 August 2002 and published in Memorial A 91 of 13 August 2002. [*English version not available*].

16. **Malta** – Data Protection Act of December 14 2001 (Act XXVI of 2001), as amended by Act XXXI of 2002, Full entry into force July 15, 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/malta_en.pdf. See Articles 26 and 27.

17. **Netherlands** – 25 892 – Rules for the protection of personal data (Personal Data Protection Act) (Unofficial translation); available at www.cbpweb.nl/en/structuur/en_pag_wetten.htm. See Articles 13-15.

18. **Poland** –Act of August 29, 1997 on the Protection of Personal Data, amended January 1, 2004, March 1, 2004, May 1, 2004; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/poland_en.pdf. See Articles 7, 31, 36, and 39a. See also, Ordinance of the Minister for Internal Affairs and Administration of 29 April 2004; documentation of processing of personal data and technical and organizational requirements which should be fulfilled by equipment and computer systems used for processing personal data (Journal of Laws of 1 May 2004).

19. **Portugal** – Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data); available at www.cnpd.pt/Leis/lei_6798en.htm. See Chapter II, Section III (Security and confidentiality of processing), at Article 14 (Security of processing), Article 15 (Special security measures), Article 16 (Processing by a processor), and Article 17 (Professional secrecy).

20. **Slovakia** – Act No 428 of 3 July 2002 on personal data protection; available at www.dataprotection.gov.sk/buxus/docs/act_no_428.pdf. See Chapter Two (Security of personal data), at Section 15 (Responsibility for personal data security), Section 16 (The security project), Section 17 (Instruction), Section 18 (Confidentiality obligation), and Section 19 (Personal data protection supervision).

21. **Slovenia** – Personal Data Protection Act, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf. See Chapter 3, Articles 24 (Security of Personal Data), and Article 25 (Duty to Secure).

22. **Spain** – Organic Law 15/1999 of 13 December on the Protection of Personal Data; available at http://europa.eu.int/comm/internal_market/privacy/docs/organic-law-99.pdf. See Article 9 (Data security), Article 10 (Duty of secrecy), and Royal Decree 994/1999, on Security Measures of Automated Databases Containing Personal Data.

23. **Sweden** – Personal Data Act (1998:204); issued 29 April 1998; available at www.datainspektionen.se/pdf/ovrigt/pul-eng.pdf. See Security in processing at Section 30 (Persons who process personal data), Section 31 (Security measures), and Section 32 (The supervisory authority may decide on security measures). See also Personal Data Ordinance (1998:1191); issued 3 September 1998, available at www.sweden.gov.se/content/1/c6/02/56/33/ed5aaf53.pdf.

24. **UK** – Data Protection Act 1998; available at www.hmso.gov.uk/acts/acts1998/19980029.htm. See Article 7 and The seventh principle.

K. Other Countries

1. **Argentina**: Act 25,326, Personal Data Protection Act (October 4, 2000), § 9; Security Measures for the Treatment and Maintenance of the Personal Data Contained in Files, Records, Databanks and Databases, either non state Public and Private (November 2006)

2. **Australia**: Privacy Act 1988, Act No. 119 of 1988 as amended taking into account amendments up to Act No. 86 of 2006, Schedule 3, Clause 4.

3. **Canada**: Personal Information Protection and Electronic Documents Act (2000, c. 5), Schedule 1, § 4.7.
4. **Hong Kong**: Personal Data (Privacy) Ordinance, December 1996, Schedule 1, Principle 4.
5. **Japan**: Act on the Protection of Personal Information, Law No.57, 2003, Articles 20, 21, 22, and 43
6. **South Korea**: The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., Amended by Act No. 7812, December 30, 2005, Articles 28,29