PRIVACY & DATA SECURITY LAW JOURNAL

VOLUME 1 NUMBER 4 MARCH 2006

An Emerging Information Security Minimum Standard of Due Care

ROBERT BRAUN AND STAN STAHL

A variety of statutes, regulations, regulatory action, court cases, and industry practices adopted over the past years have begun to define a standard regarding the proper use and protection of information. This article summarizes some of these developments and discusses how they have impacted the development of a minimum standard of due care for information security.

The explosion of information technology, and the increasing ease with which personal and business information can be collected, retained and used, has made significant changes in virtually all businesses. While these changes are often most observable in e-commerce and Internet related businesses, they affect almost every entity, including traditional brick and mortar enterprises. The result is that nearly every entity is now forced to address how it collects, maintains, uses, and protects that information.

The information can come from a number of sources and can be used for a number of purposes; it may be names, addresses, and billing information provided by customers to make purchases. It may be login information, including names, email and physical addresses, and other identifying information to customize the buying process. It can be employee information, including health and financial data. It can be the entity's financial data or any other internally generated information describing a company's vital corporate and business interests.

The transformation in the technology of information, as impacted by statutory, regulatory, and other legal developments, makes it essential

Robert Braun is a partner with Jeffer, Mangels, Butler & Marmaro LLP. Stan Stahl, Ph.D., is president of Citadel Information Group, Inc.

for enterprises to have meaningful standards to follow which can both facilitate the proper use of information, but meet obligations to protect that same information. A variety of statutes, regulations, regulatory action, court cases, and industry practices adopted over the past years have begun to define such a standard. This article summarizes some of these developments and discusses how they have impacted the development of a minimum standard of due care for information security.

FEDERAL LAWS AND REGULATIONS

For over a decade now, Congress has addressed minimum security requirements applicable to a wide variety of regulated entities, including health care providers, financial services, and entities targeting their services to children. Probably the most far-reaching of these efforts, and the one with the broadest impact, has been the adoption of the Gramm-Leach-Bliley Financial Institutions Improvements Act of 1999 (the GLB Act).[1]

The GLB Act

The GLB Act was adopted primarily to modernize financial services by ending most of the regulations inhibiting the merger of banks, stock brokerage companies, and insurance companies.[2] By removing these regulations, however, Congress raised significant risks that these new financial institutions would have significantly greater access to personal information, because the new institutions would have greater ability to consolidate, analyze, and sell the personal details of their customers' lives.[3] Because of these risks, the GLB Act incorporated three basic requirements to protect the personal data of individuals: First, banks, brokerage companies, and insurance companies must securely store personal financial information. Second, they must advise customers of their policies on sharing of personal financial information. Third, they must give consumers the option to opt-out of some sharing of personal financial information.[4]

The GLB Act, on its face, applies only to financial institutions.[5] However, the broad definitions in the GLB Act mean that it applies not only to banks and other traditional financial institutions but also to a wide variety of firms and individuals that assist in effecting financial transac-

tions. These include not only banks, credit unions, broker dealers, registered investment advisors and other "obvious" financial institutions, but also mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors.[6] Until very recently, portions of the GLB Act applied to lawyers that provide tax and financial planning services.[7] Consequently, the GLB Act has a broad impact on not only traditional financial institutions, but also companies that are only tangentially involved in the delivery of financial services.

The GLB Act generally prohibits a financial institution from disclosing non-personal public information to a non-affiliated third party, either directly, or through an affiliate, unless the institution has disclosed to the customer, in a clear and conspicuous manner, that the information may be disclosed to a third party; has given the consumer an opportunity to direct that the information not be disclosed; and described the manner in which the consumer can exercise the nondisclosure option.[8]

Under the GLB Act financial institutions must also prepare and make public privacy statements which describe the institution's policies with regard to disclosing non-public personal information to affiliates and non-affiliated third parties; disclosing non-public personal information of persons who have ceased to be customers of the institution; and the categories of non-public personal information the institution collects. The institution is required to disclose clearly and conspicuously those policies and practices at the time that it establishes a customer relationship and not less than annually during the continuation of the customer relationship. This has resulted in an avalanche of paper from banks, brokerage houses, accountants and others who provide financial services.

The GLB Act also regulates what steps a business must take to prevent the unintentional sharing of nonpublic personal information in its computer systems. Each of the different federal and state agencies with jurisdiction to enforce the GLB Act has adopted written information security safeguard regulations. While no two are identical, all have a similar flavor:

- *Executive management involvement* — the need for senior management of the institution to be involved in and responsible for the development and implementation of privacy and security policies and procedures.
- *Risk- and vulnerability-driven, based on regular assessments* — Rather than a "one-size fits all" concept, the GLB Act, as implemented, contemplates that subject institutions will analyze their specific weaknesses and liabilities in order to develop effective security and privacy programs.
- *Written information security policies* — all security policies must be in writing and adopted by the institution.
- *Employee training* — hands-on training in the rationale and requirements of security policies, the goals of the policies and their implementation is an essential factor in complying with the GLB Act.
- *Control of third-parties* — to the extent that an institution relies on third parties for privacy-sensitive functions, ranging from outsourcing data processing, maintaining data in offsite locations, hiring independent contractors, entering into joint ventures and strategic alliances and the like, the GLB Act requires that a covered institution identify and control the risks imposed by that relationship.

The rules and their impact are described in greater detail below.

HIPAA

The Health Care and Insurance Portability and Accountability Act of 1996 (HIPAA)[9] was adopted, in part, to address perceived weaknesses in the treatment of some of the most sensitive information available — health care information. As with the GLB Act, HIPAA has a broad impact in its definition of health records and who can be deemed to be responsible for the maintenance of the privacy of those records. As with the GLB Act, not only are the obvious entities — physicians, hospitals, health insurers — responsible for compliance with HIPAA, but also employers, schools, pension plans and others with access to the information. The Department of Health and Human Services has, under HIPAA, adopted the "Privacy

Rule" to implement and enforce HIPAA.[10] The Privacy Rule covers key elements of privacy, which it defines as ensuring the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits; protecting against any reasonably anticipated threats or hazards to the security or integrity of such information; and ensuring compliance by its workforce.

While not as detailed as the rules adopted under the GLB Act, the Privacy Rule addresses the same key elements, focusing on individual analysis of risks and development of meaningful steps for compliance.

Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002[11] (SOX) is often cited as the single most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s. In line with federal securities regulation generally, SOX, which was adopted in reaction to perceived corporate abuses, focuses on ensuring meaningful, timel, and complete disclosure of corporate events and conditions as means of protecting the public. While SOX does not explicitly address information security, experts contend that compliance with SOX is incomplete without an adequate information-security program.[12] Because of the broad impact of SOX over virtually all public companies, as well as investors, lenders, insurers and others, SOX has had, in its short history, a profound impact on security policies.

Section 302 of SOX requires that the principal executive officer and principal financial officer of a public company certify the accuracy and fairness of the company's periodic reports, and moreover, that these officers certify that they are responsible for establishing and maintaining internal controls, and that any significant deficiencies in the design and operation of the internal controls have been disclosed to their auditors and audit committees. They must also disclose in required periodic reports any significant changes in internal controls that might affect those controls after they are evaluated.

Section 404 of Sarbanes-Oxley requires the management of a public company to assess the effectiveness of the company's internal control over financial reporting. Section 404 also requires management to

include in the company's annual report to shareholders, management's conclusion as a result of that assessment about whether the company's internal control is effective. While there are a variety of steps companies must take to comply with SOX, it is Section 404 that has the most relevance to information security with its requirement that management develop, document, test and monitor its internal controls and its disclosure controls and procedures.

While SOX was adopted in response to perceived inadequacies and misconduct by corporate officers and directors, its focus on systems, and certification of the adequacy of reporting schemes, is likely to have a broad effect on the establishment of corporate controls and standards. A variety of consultants, including accounting firms, software developers and others, have developed and are actively marketing automated systems to assist in establishing a reporting regimen for corporations, allowing certifying officers and boards of directors to establish compliance with the requirements imposed by SOX and ensuring that corporate controls are followed. These changes, moreover, do not exist in a vacuum; principles of corporate governance which first applied to public corporations have often been extended to private companies, sometimes through application of state law and regulation applied to non-public companies, other times through market forces, such as auditors and insurance carriers who adopt similar standards for public and non-public companies. Observers, including the American Society of Certified Public Accountants, have suggested that the reforms imposed by SOX could be viewed as best practices and result in new regulations by federal and state agencies affecting nonpublic companies.

FTC Safeguards Rule

The GLB Act has been implemented by inter-agency regulations among all of the chief banking regulators — the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Office of the Comptroller of the Currency — as well as the Federal Trade Commission.[13] The FTC has, in fact, been at the forefront of privacy regulations. In that role, the FTC has adopted a "safeguards rule" under the GLB Act, which

requires each financial institution to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."[14]

Depending upon one's point-of-view, the FTC Safeguards Rule is either a logical regulation implementing existing privacy and security laws or a regulatory leap taking privacy and security regulation far beyond existing laws. Nevertheless, under its authority to protect consumers and its mandate under the GLB Act, the FTC is in a position to adopt regulations which cross the boundaries of all industries. Significantly, it also requires each business to make determinations that are consistent with the size and complexity of its business and activities, as well as a sensitivity of customer information at issue. It does not provide specific rules; but it does require that businesses regulate themselves. Companies are thus forced to analyze their operations, needs, and vulnerabilities in order to comply with the Safeguards Rule.

FTC Regulation of Unfair and Deceptive Practice

In addition to the Safeguards Rule, the FTC has been active in the regulation of privacy and security through its authority to regulate unfair and deceptive trade practices. One of the key tools used by the FTC to address privacy violations has been the application of the FTC's policy toward unfair and deceptive practices to privacy practices, both online and physical.[15] Under the FTC Act, the FTC is directed, among other things, to prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce.[16] The FTC has highlighted its intention to regulate online privacy as part of its privacy initiative. A key part of the Commission's privacy program is making sure companies keep the promises they make to consumers about privacy and, in particular, the precautions they take to secure consumers' personal information. To respond to consumers' concerns about privacy, many Web sites post privacy policies that describe how consumers' personal information is collected, used, shared, and secured. Indeed, almost all the top 100

commercial sites now post privacy policies. Using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information.

The FTC's actions under the GLB Act and the Safeguards Rule, and under its authority to ferret out and eliminate unfair and deceptive practices, are particularly important in developing a standard of care. Several recent cases are good examples of the similarity of the FTC's approach under each regulation:

Superior Mortgage Corporation, Docket C-4153, December 14, 2005.[17] This recent case was brought by the FTC against Superior Mortgage Corporation, a residential mortgage lender with forty offices in ten states, as well as six separate Web sites. The FTC found that Superior failed to assess risks to its customer information until more than a year after the Safeguards Rule's effective date; institute appropriate password policies to control access to company systems and documents containing sensitive customer information; and encrypt or otherwise protect sensitive customer information mailed by respondent and its service providers using networks outside of respondent's computer network.

DSW, Inc., File No. 052-3096, Settled December 1, 2005.[18] DSW is a shoe discounter operating approximately 190 stores in 32 states. It generated $961 million in net sales in 2004 and sold approximately 23.7 million pairs of shoes. It 2005 it discovered that approximately 1.4 million credit and debit cards and 96,000 checking accounts had been compromised. DSW uses computer networks to obtain authorization for credit card, debit card and check purchases and to track inventory. DSW collects personal information, including the name, card number and expiration date from magnetic stripes. The FTC charged that, in violation of the prohibition against unfair and deceptive trade practices, DSW created unnecessary risks to sensitive information by storing it in multiple files when it no longer had a business need to keep the information; failed to use readily available security measures to limit access to its computer networks through wireless access points

on the networks; stored the information in unencrypted files that could easily be accessed using a commonly known user ID and password; failed to limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and failed to employ sufficient measures to detect unauthorized access. DSW's settlement with the FTC requires DSW to establish and maintain a comprehensive information security program that includes administrative, technical and physical standards, obtain every two years for the next 20 years an audit from a qualified, independent, third-party professional to assure that its program meets the standards of the order; maintain record keeping and reporting provisions to allow the FTC to monitor compliance.

This case, brought under the regulation of unfair and deceptive trade practices, is significantly similar to, if not identical to, claims brought under the Safeguards Act.

BJ's Wholesale Club, Inc., Docket C-4148, September 20, 2005.[19] BJ's operates approximately 150 warehouse clubs in 16 eastern states. BJ's uses computer networks to obtain authorization for credit card, debit card and check purchases and to track inventory. BJ's collects personal information, including the name, card number and expiration date from magnetic stripes. The FTC alleged in its complaint that BJ's did not employ reasonable and appropriate measures to secure personal information collected at its stores. Among other things, BJ's did not encrypt information while in transit or when stored on in-store computer networks; stored information in fields that could be accessed anonymously, using a commonly known default user id and password; did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules.

Again, the action brought against BJ's, like the DSW action, show a merging of the State Laws and Regulations

OTHER PRIVACY LAW INITIATIVES

California Civil Code 1798.84

In 2002, the California legislature adopted a statute requiring consumers be notified when there was a breach of the security of the system and the consumers' unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person. The law has raised a number of issues — what is adequate encryption, when is it reasonable to assume that information has been compromised, what if information is generally available, and other definitional and procedural issues. Despite these concerns, at least 20 other states have adopted privacy legislation that includes mandatory notice in the event of a breach. Most have followed the California model.

Federal Initiatives

Regulators initially adopted regulations based on GLBA and the Safeguards Rule. Congress has also taken up mandatory notification; more than a dozen bills have been introduced in the House and Senate addressing, to some degree, mandatory notification.[20]

COURT CLAIMS

Court actions in this area are in their infancy; however, at least one class action has been brought in California, *Eric Parke et al v. CardSystems Solutions, Inc.,* et al.[21] The case revolves around the theft of account information relating to approximately 40 million Visa and MasterCard accounts from CardSystems Solutions, Inc., a third-party payment processor. The information included names, account numbers and security codes but not Social Security numbers or home addresses. MasterCard publicly disclosed the breach on Jun 17, 2005, approximately 25 days after learning of the breach.

The action alleges that the defendants failed to comply by providing affected customers with notice of the breach within the time required by the law. It should be noted that there is no specific time frame; only that the notice should be given "in the most expedient time possible and without unreasonable delay."

Another case, *Bell v. Michigan Council 25 of the AFSCME, AFL-CIO Local 1023*[22] also gives guidance as to the direction of court cases alleging violation of security obligations. In this case, a union's treasurer brought home documents containing the names and social security numbers of union members, and that information was then stolen by the treasurer's daughter. The court addressed whether there was a special duty between the treasurer, and therefore the union, and the members which created liability for negligence on the part of the treasurer. The court found that there was such a duty, and noted, in particular, that the union could have reasonably foreseen that allowing one of its officers this degree of access; in fact, the union board members and addressed the issue and had not taken action; effectively, the union had taken the duty upon itself. Additionally, the court noted that the severity of the risk was high, particularly where entities holding personal information are required to be "vigilant" in regard to identity theft and that there was a direct causal connection between the lack of safeguards and procedures and the access by unauthorized persons. Finally, in an important statement, the court held that a Michigan law addressing the disclosure of confidential information actually strengthened the position that there was a special relationship: underlying the adoption of such a law is the assumption that a special relationship exists between those who hold private, non-public information and those who provide the information. This concept can be cited in any of the states which have addressed privacy issues.

A third case, *Weigh Systems South, Inc. v Mark's Scales & Equipment, Inc.*,[23] addresses a different aspect of security. In that case, Weigh Systems South failed in a claim that former employees had misappropriated trade secrets because, among other things, the plaintiff failed to show that it had taken effective measures to protect the information it claimed as trade secrets. Among the factors cited by the court was that computer software was not uniformly or effectively password protected, that Weigh Systems employees regularly gave customers a password allowing them to access Weigh Systems' computer system, and that Weigh Systems otherwise made it easy to access and duplicate the information. Other factors, including the

nature of the trade secrets themselves, also impacted the decision; however, the case makes clear another impact of failing to take effective information security measures.

CALIFORNIA — STATEMENT OF PRIVACY STANDARDS

The California Office of Privacy Protection, a division of the California Department of consumer Affairs, has actively issued papers identifying recommended practices in the privacy protection area, including "Recommended Practices on Notification of Security Breach Involving Personal Information" (October 10, 2003) and "Recommended Practices for Protecting the Confidentiality of Social Security Numbers" (January 2003).[24] Two more recent publications deserve particular attention:

Recommended Practices on California Information-Sharing Disclosures and Privacy Policy Statements — November 22, 2004[25]

This initiative addresses best practices in responding to requests for information under California law, adopted in Assembly Bill 68 in 2004. While the Office's recommendations are not surprising, they do reinforce the importance of evaluating the impact of California's privacy laws in light of the exact parameters of business operations. Among other things, the policy statement emphasizes that:

- Disclosure under AB 68 should be specific and comprehensive. The OPP recommends that in order to buttress the disclosure of all categories of customer personal information disclosed during the past calendar year to other companies for their direct marketing purposes, as required by the statute, the company give specific examples of the types of information provided.
- Privacy statements and other compliance statements should be clear and understandable.
- Companies should make sure that when customers give their preference of allowing the business to communicate with others, or preventing it, that the communication create a record.
- The reason for marketing to others should be included and explained.

- Companies should use plain, straight-forward language, as well as titles and headers to identify key parts of the notice.
- Privacy statements should be readily accessible and conspicuous.

A California Business Privacy Handbook — September 2005[26]

This recently published handbook deals more specifically with the affirmative obligation of California businesses to protect personal non-public information. The Handbook recommends, among other things, that businesses control access to information, including limiting employees' access to personal information to just what is necessary for them to perform their duties; requiring employees to use passwords for access to databases containing personal information; maintaining an "audit trail" to track any abuses that may occur; adopting a "clean desk policy" of keeping records containing sensitive personal information that are not being used in locked drawers or cabinets; training employees in their responsibilities for protecting personal information from unauthorized access; and using other generally accepted security practices to protect sensitive personal information.

The Policy statement also requires that if personal information is collected or retained — including sensitive information such as Social Security number, driver's license number, state ID card number, credit card or other financial account number, or medical information of California residents, the company should use reasonable security measures to protect the personal information from unauthorized access, use, disclosure, modification or destruction; make sure that contracts with service providers and others with whom the company shares personal information require those companies to protect the personal information with reasonable security measures; adopt a written information security policy and make sure employees know what is expected of them. Under the policy, security measures include administrative, physical, and technological safeguards. These three categories of safeguards, identical to those found in the GLB Act and HIPAA, reflect best practices among information security practitioners.

Administrative safeguards include assigning senior management responsibility, implementing information security policies, screening

employees, training of all personnel, implementing business continuity and disaster recovery plans, managing third-parties with whom information is shared.

Physical safeguards include door locks and surveillance cameras, environmental (fire and flood) controls, guards, use of locked file cabinets for storing paper records containing sensitive personal information, use of shredders for secure records disposal.

Technological safeguards include secure network design, proper use of firewalls, identification and authentication mechanisms to control access, anti-virus and anti-spyware software to protect computers and networks, patch management systems to update software, data encryption (both at rest and in transit), intrusion detection and protection systems.

CONTRACTUAL OBLIGATIONS

Companies are also bound by contractual obligations to maintain the security of sensitive information. Credit agencies, in particular, have been active in establishing security standards.

National Automated Clearing House Association (NACHA)

The National Automated Clearing House Association (NACHA), along with both Visa and MasterCard, contractually impose information security requirements on their members. Visa and MasterCard have jointly published the Payment Card Industry Data Security Standard which contractually imposes twelve basic security requirements upon all Visa and MasterCard payment system constituents[27] addressing building and maintaining a secure network; protecting cardholder data; maintaining a vulnerability management program; implementing strong access control measures; regularly monitoring and testing networks; and maintaining an information security policy. Given the dependence of retail systems on credit cards issued under the Visa and MasterCard names, adhering to these policies is virtually a universal requirement for conducting business. Moreover, these standards are often required to be adopted and adhered to by service providers who may have access to information or are otherwise part of the payment systems.

PRIVACY CODES AND STANDARDS

Along with statutes and governmental regulation, trade groups have adopted standards for information security and management. Trade groups are a particularly important authority because of their ability to provide *de facto* regulation of their members and are often a gateway to conducting business in the effected fields.

International Organization for Standardization (ISO)

ISO is the world's largest developer of standards, establishing accepted standards for engineers, manufacturers and others to address basic problems in production and distribution and promote universally accepted codes of operation and conduct.[28] As a result, ISO has a significant economic and societal impact. Standards adopted by ISO, like uniform laws, are intended to reflect generally accepted practices.

ISO 17799,[29] the code of practice for information security management, identifies ten specific vital information security management practices. According to ISO, an organization's information can be considered "secure" only to the extent that these ten practices are being systematically managed. Weaknesses in any single practice can often negate the combined strength in the other nine. The 10 information security management practices are: Security Policy; Organizational Security; Asset Classification and Control; Personnel Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Systems Development and Maintenance; Business Continuity Management; and Compliance. The ISO's stated goal in this policy is to serve as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

Generally Accepted Information Security Principles (GAISP), Version 3.0[30]

GAISP is an ongoing project to collect and document information security principles that have been proven in practice and accepted by practi-

tioners. GAISP draws upon established security guidance and standards to create comprehensive, objective guidance for information security professionals, organizations, governments, and users. The use of existing, accepted documents and standards will ensure a high level of acceptance for the final GAISP product, and will enable a number of benefits to be achieved.

The GAISP:

- Promotes good information security practices at all levels of organizations;
- Creates an increase in management confidence that information security is being assured in a consistent, measurable, and cost-efficient manner;
- Is an authoritative source for opinions, practices, and principles for information owners, security practitioners, technology products, and IT systems;
- Encourages broad awareness of information security requirements and precepts;
- Enables organizations to seek improved cost structures and program management through use of proven practices and global principles rather than varied, local, or product-specific guidelines;
- Is written hierarchically to allow application to any appropriate level of the organization or IT infrastructure, from the Corporate Board to the technical staff working "in the trenches."

GAISP is organized around three levels of guiding principles that are applicable at varying levels of the organization: "Pervasive Principles," which target organizational governance and executive management; "Broad Functional Principles," which serve as guidelines to planning and execution of security tasks and to establishment of a solid security architecture; and "Detailed Principles," written for information security professionals and which highlight specific activities to be addressed in day-to-day risk management.

Pervasive Principles

The Pervasive Principles outline high-level recommendations to help organizations solidify an effective information security strategy, and

include conceptual goals relating to accountability, ethics, integration, and assessment.

- *Accountability Principle*: Information security accountability and responsibility must be clearly defined and acknowledged.
- *Assessment Principle*: The risks to information and information systems should be assessed periodically.
- *Awareness Principle*: All parties, including but not limited to information owners and information security practitioners, with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information.
- *Equity Principle*: Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.
- *Ethics Principle*: Information should be used, and the administration of information security should be executed, in an ethical manner.
- *Integration Principle*: Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.
- *Multidisciplinary Principle*: Principles, standards, conventions, and mechanisms for the security of information and information systems should address the considerations and viewpoints of all interested parties.
- *Proportionality Principle*: Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information.
- *Timeliness Principle*: All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems.

Broad Functional Principles

Broad Functional Principles are designed to be the building blocks of the Pervasive Principles and which more precisely define recommended tactics from a management perspective. These Principles are designed as guidelines to planning and execution of security tasks and to establishment of a solid security architecture.

- *Information Security Policy*: Management shall ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Such guidance must assign responsibility, the level of discretion, and how much risk each individual or organizational entity is authorized to assume.
- *Education and Awareness*: Management shall communicate information security policy to all personnel and ensure that all are appropriately aware. Education shall include standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply.
- *Accountability*: Management shall hold all parties accountable for their access to and use of information, e.g., additions, modifications, copying and deletions, and supporting Information Technology resources. It must be possible to affix the date, time and responsibility, to the level of an individual, for all significant events.
- *Information Asset Management*: Management shall routinely catalog and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned.
- *Environmental Management*: Management shall consider and compensate for the risks inherent to the internal and external physical environment where information assets and supporting Information Technology resources and assets are stored, transmitted or used.
- *Personnel Qualifications*: Management shall establish and verify the qualifications related to integrity, need-to-know, and technical competence of all parties provided access to information assets or supporting Information Technology resources.

- *Incident Management*: Management shall provide the capability to respond to and resolve information security incidents expeditiously and effectively in order to ensure that any business impact is minimized and that the likelihood of experiencing similar incidents is reduced.
- *Information Systems Life Cycle*: Management shall ensure that security is addressed at all stages of the system life cycle.
- *Access Control*: Management shall establish appropriate controls to balance access to information assets and supporting Information Technology resources against the risk.
- *Operational Continuity and Contingency Planning*: Management shall plan for and operate Information Technology in such a way as to preserve the continuity of organizational operations.
- *Information Risk Management*: Management shall ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable.
- *Network and Internet Security*: Management shall consider the potential impact on the shared global infrastructure, e.g., the Internet, public switched networks, and other connected systems when establishing network security measures.
- *Legal, Regulatory and Contractual Requirements of Information Security*: Management shall take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.
- *Ethical Practices*: Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing and enforcing security measures.

Detailed Principles

The third GAISP level consists of Detailed Principles, written for information security professionals and which highlight specific activities to be addressed in day-to-day risk management. The tactics in the Detailed Principles are step-by-step instructions necessary to achieve the appropriate tactical outcome from the Broad Principles and the conceptual goals of the Pervasive Principles.

Information Security Governance: Guidance for Boards of Directors and Executive Management

The Information Systems Audit and Control Association (ISACA) has developed a model for the overall "maturity" of an organization's security management. ISACA's model was built upon a software engineering management maturity framework that had been developed in the mid-to-late 1980's by the Software Engineering Institute, a national technology center at Carnegie Mellon University. The model "measures" — on a scale of 0-5 — the extent to which information security is being formally and proactively managed throughout the organization.

The ISACA model provides an organization with a

- Snapshot-in-time assessment tool, assisting the organization to identify the relative strengths of its information security management practices
- Tool for identifying an appropriate security management maturity level, to which the organization can evolve
- Method for identifying the gaps between an its current security maturity level and its desired level
- Tool for planning and managing an organization-wide Information Security Management Improvement Program for systematically improving the organization's information security management capabilities
- Tool for planning and managing specific information security improvement projects

An essential factor of the ISACA model is that each organization has to determine what maturity level is appropriate for its specific circumstances.

CONCLUSION

The proliferation and accessibility of information, and the growing awareness that the information must be kept secure, has resulted in a need for standards to guide participants in information intense industries. Information security is a very topical subject, and a multitude of legislators, regulators, courts, administrative agencies, industry sources and

others are weighing in on this new area of concern; consequently, guidance is coming from a variety of sources, not all of which are consistent. However, some common management threads to a standard of information security practice have emerged:

- An effective information security management system requires an analysis of the responsibilities the entity has for protecting information, together with an assessment of the risks and vulnerabilities to which information is exposed.
- An effective information security management system requires written information security policies, tailored to meet the needs of the entity. Policies must encompass administrative, technical, and physical controls for protecting sensitive information.
- Information security is a "moving target." Consequently, an entity must periodically assess, review, and update its information security management program, including its information security policies, in accordance with its changing information risks.
- All levels of personnel, from the most senior management to the most junior line employees, must be aware of — and comply with — the entity's information security policies.

NOTES

[1] Public Law 106-102, codified in 15 USC 6801 et seq.
[2] Senate Banking Committee, Statement of Managers, Summary of Major Provisions, available at http://banking.senate.gov/conf/somfinal.htm.; 145 Cong. Rec. H11, 544 (daily ed. Nov. 4, 1999)
[3] Electronic Privacy Information Center, The Gramm-Leach-Bliley Act, available at http://www.epic.org/privacy/glba/.
[4] GLB Act Section 502.
[5] GLB Act Section 501(a); Electronic Privacy Information Center, The Gramm-Leach-Bliley Act, available at http://www.epic.org/privacy/glba/.
[6] 65 Fed. Reg 33671, May 24, 2000.
[7] American Bar Association v. Federal Trade Commission, United States Court of Appeals for the District of Columbia Circuit No. 04-5257, Argued May 5, 2005, decided December 6, 2005.
[8] GLB Act Section 502.

[9] Public Law 104-191.
[10] 45 CFR Parts 160 and 164), December 28, 2000 as amended May 31, 2002, August 14, 2002, February 2003, and April 17, 2003.
[11] Public Law 107-204, 116 Stat 745
[12] See, Bruce H. Hearon, Jon Stanely, Steven W. Teppler, and Joseph Burton, Life After Sarbanes-Oxley: The Merger of Information Security and Accountability, 45 Jurimetrics Journal, 379-412 (2005).
[13] See, for example, 66FedReg 8616; 12CFR 30 (Office of the Comptroller of the Currency); 12CFR 208, 211, 225, 263, (Board of Governors of the Federal Reserve System); 12CFR 308, 364 (Federal Deposit Insurance Corporation); 12CFR 568, 570 (Office of Thrift Supervision); 17CFR 248 (Securities and Exchange Commission); 16CFR 314 (Federal Trade Commission)
[14] 16CFR 314 (Federal Trade Commission)
[15] Federal Trade Commission Web site, available at http://www.ftc.gov/privacy/privacyinitiatives/promises.html.
[16] 15 U.S.C. §§ 41-58, as amended.
[17] Available at Federal Trade Commission Web site, http://www.ftc.gov/os/caselist/0523136/051216do0523136.pdf.
[18] Available at Federal Trade Commission Web site, http://www.ftc.gov/os/caselist/0523096/051201agree0523096.pdf
[19] Available at Federal Trade Commission Web site, http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf
[20] See, e.g., Financial Privacy Breach Notification Act of 2005, S. 1216; Personal Data Privacy and Security Act of 2005, S 1789; Financial Privacy Protection Act of 2005, S. 1594; Consumer Data Security and Notification Act of 2005HR 3140; Comprehensive Identity Theft Prevention Act, S. 768; Privacy Act of 2005, S. 116; Identity Theft Protection Act, S. 1408.
[21] No. CGC-05-44264, (S.F. Cty. Super. Ct.). A copy of the First Amended Complaint in that action, filed July 6, 2005, is available at http://www.techfirm.com/cardsystems.pdf.
[22] Wayne Circuit Court, No. 246684, unpublished decision, February 25, 2005.
[23] 347 Ark. 868, 68 S.W. 3d 299; 62 U.S.P.Q. 2d 1589 (2002).
[24] See, http://www.privacy.ca.gov/.
[25] Available at http://www.privacy.ca.gov/recommendations/infosharingdisclos.pdf.

[26] http://www.privacy.ca.gov/business/ca_business_privacy_hb.pdf.
[27] Payment Card Industry Data Security Standard, January 2005, available at https://sdp.mastercardintl.com/documentation/index.shtml.
[28] See, http://www.iso.org/iso/en/ISOOnline.frontpage.
[29] For a summary of ISO 17799, see http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=.
[30] Available at http://www.issa.org/gaisp/_pdfs/v30.pdf.

CHECKLIST

Elements of an Effective Information Security Management System:

- ✔ Conduct an analysis of the responsibilities the entity has for protecting information, together with an assessment of the risks and vulnerabilities to which information is exposed
- ✔ Prepare written information security policies, tailored to meet the needs of the entity, that encompass administrative, technical, and physical controls for protecting sensitive information
- ✔ Periodically assess, review, and update the information security management program, including information security policies, in accordance with its changing information risks
- ✔ Ensure that all levels of personnel, from the most senior management to the most junior line employees, are aware of — and comply with — information security policies