

## An Emerging Information Security Minimum Standard of Due Care <sup>1</sup>

by  
Robert Braun, Esq.  
Partner  
Jeffer, Mangels, Butler & Marmaro LLP  
&  
Stan Stahl, Ph.D.  
President  
Citadel Information Group, Inc.

### Abstract

This article examines the emerging body of law surrounding an enterprise's responsibility for securing information, together with the emerging body of information security management principles and practices for doing so. Seven key information security management elements are identified which we believe constitute an *information security minimum standard of due care*. Enterprises failing to implement these seven management elements could face significant legal exposure should they suffer a security breach resulting in damage to a 3<sup>rd</sup>-party.

### Introduction

The microcomputer revolution, and with it the rise of local area networks, wide area networks and the Internet, is more than 20 years old. Interconnecting computers and networks has brought great gains in productivity and opened up exciting new realms of entertainment and information. And it has brought the world closer together. But these virtues are not without unintended, and sometimes undesired, consequences.

The *Federal Trade Commission* estimates that approximately 3,000,000 Americans were the victims of identity theft in 2002, with the majority of these originating in thefts of information from computers or computer systems. At the same time, cyber-vandals write computer viruses which propagate from enterprise to enterprise at the speed with which untrained workers open attachments, causing significant economic loss while systems are being repaired. Electronic inboxes are clogged with Spam. A CyberMafia cruises the internet, looking for easy prey from whom to steal money and other cyberdata of value. Dangerous adults too easily hang around children and teenage *chat rooms*, seeking to take prey on legitimate users, often with tragic consequences. And the *Department of Homeland Security* warns of terrorists taking over large numbers of unsuspecting computer systems to be used in coordination with a large scale terrorist attack.

---

<sup>1</sup> This is a revised version of an article that first appeared in *Information Security Management Handbook, Fifth Edition, Volume 2*, edited by Hal Tipton and Micki Krause, Auerbach, 2005.

Computer crime is a serious challenge. And it's getting worse ... exponentially worse. Every computer crime study over the last 5 years conclusively confirms this. Computer crime is growing exponentially. The speed with which computer viruses spread and the number of security weaknesses in our systems is growing exponentially. Consequently, the total cost to business, in lost productivity, theft, embezzlement, and a host of other categories, is growing exponentially.

Against this backdrop are two legal questions:

- What responsibility does an enterprise have for protecting the information in its computer systems, particularly information that belongs to others?
- What responsibility does an enterprise have to keep its information systems from being used to harm others?

As answers to these two questions emerge, we believe they will define an evolving *information security minimum standard of due care* that will serve to establish, at any point in time, an *adequacy baseline* below which an enterprise will have criminal or civil liability. The specific details of any *information security minimum standard of due care* are likely to vary among the patchwork quilt of federal and state laws, industry specific developments, interpretations by different regulatory agencies, and how the judicial system addresses these issues.

There are three coevolving forces that, we believe, will serve to define any evolving *information security minimum standard of due care*.

- The evolving legislative and regulatory landscape regarding the duty of information holders to protect nonpublic information about others in their computer systems
- The evolving interpretation of contract and tort law as it pertains to the securing of information and information assets
- The evolving recommended *effective security practices* of the professional information security community

We begin, therefore, in Section 1, with an exposition of the privacy & safety issues addressed by the legislation and subsequent regulations. In Section 2 we explore the implications of contract and tort law on information security. In Section 3 we explicate several current *Information Security Management Practice Models* which serve to define "effective security practices" in use by the information security profession. These are brought together in Section 4, in the context of a *Battle of the Expert Witnesses*, in which we identify what we believe is an *information security minimum standard of due care*. Then in Section 5, we discuss how this standard is likely to evolve over the next few years.

## **Section 1. Laws And Regulations Effecting Privacy In Computer Transactions**

### ***Gramm-Leach-Bliley (GLB)***

*It is the policy of the Congress that each 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.*

*In furtherance of the policy ... each agency or authority ... shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards*

- (1) to insure the security and confidentiality of customer records and information;*
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and*
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer*

### *15USC6801, Gramm-Leach-Bliley Act*

With these words, Congress in 1999 passed the Gramm-Leach-Bliley (GLB) Act. The GLB act regulates the use and disclosure of nonpublic personal information about individuals who obtain financial products or services from financial institutions.

GLB, on its face, applies only to financial institutions. However, the broad definitions in GLB 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 transactions. 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. The Federal Trade Commission has even held that GLB applies to lawyers that provide tax and financial planning services,<sup>2</sup> although that position has, predictably, been contested.

From the standpoint of maintaining the privacy of customer information, GLB 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

---

<sup>2</sup> In a letter the American Bar Association, dated April 8, 2002, J. Howard Beales, Director of the Federal Trade Commission Bureau of Consumer Protection states that attorneys are not exempt from the application of GLB's privacy rule.

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.

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.

In addition to regulating how financial institutions may intentionally share information, GLB 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 having GLB jurisdiction have written separate information security safeguard regulations.<sup>3</sup> While no two are identical, all have a similar flavor:

- Executive management involvement
- Risk- and vulnerability-driven, based on regular assessments
- Written information security policies
- Employee training
- Control of 3<sup>rd</sup>-parties

There has also been a spill-over effect from regulation under the GLB Act. The key regulator under the GLB Act is the Federal Trade Commission, and its experience has spurred it to explore areas not directly implicated under the GLB Act.<sup>4</sup> Additionally, many of the industries which are directly impacted by the GLB Act, such as the banking and insurance industries, are beginning to apply the standards imposed on them to their clients. For example, insurance companies are beginning to review privacy statements and policies of their insureds, and banks are beginning to consider these issues in their underwriting decisions.

### ***Health Care and Insurance Portability and Accountability Act (HIPAA)***

One of the first significant attempts to adopt a standard of care for electronic transactions in the field of health care is the *Health Care and Insurance Portability and Accountability Act* of 1996 (HIPAA). While much of HIPAA addresses the rights of patients under the health care insurance plans, HIPAA also includes key provisions relating to the privacy rights of patients in response

---

<sup>3</sup> 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), 16CFR 314 (Federal Trade Commission); 17CFR 248 (Securities and Exchange Commission).

<sup>4</sup> See discussion of FTC Safeguards Rule, below.

to the concerns that this information was not being adequately protected. Insurance companies, doctors, hospitals, laboratories and employers who maintain employee health plans are subject to HIPAA provisions.

The *Department of Health and Human Services* (DHHS) has issued *Privacy Rule* regulations providing for the protection of the privacy of “individually identifiable health information” created, received or otherwise in the possession of entities covered by HIPAA.<sup>5</sup>

HIPAA information security regulations require covered entities to do the following to protect “individually identifiable health information.”<sup>6</sup>

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or otherwise required
- Ensure compliance by its workforce.

HIPAA is a broad ranging act and has spawned significant regulation. Importantly, because it affects so many different entities, we can expect that the standards required by HIPAA will have a significant meaningful impact on non-health care related industries.

### ***Sarbanes Oxley (SOX)***

The Sarbanes-Oxley Law of 2002 (“SOX”) has been called the most significant new securities law since the Securities and Exchange Commission was created in 1934. SOX places substantial additional responsibilities on officers and directors of public companies, and imposes very significant criminal penalties on CEOs, CFOs and others who violate various provisions of SOX.

While the corporate scandals at HealthSouth, Adelphia, Qwest, Tyco and of course, Enron, the mother of SOX, made headline news, the new requirements under SOX promise to transform the way that all public companies are managed from top to bottom. Even corporations that are not public today, but hope to become publicly owned or to be sold to a public company in the future, need to be aware of the basic requirements for operating a company in compliance with certain requirements of SOX, particularly the requirements for establishing and following detailed internal controls and disclosure of these controls and procedures. These requirements will obligate all public companies to address their information security procedures and practices in a very public way.

---

<sup>5</sup> 45CFR 160, 162, 164

<sup>6</sup> 45CFR 162, Federal Register Vol. 68, No. 34, 8377.

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.

The most significant new responsibility faced by the CEO and CFO of every public company is the required personal certification of their company's annual and quarterly reports. The SEC has specified the exact form of personal certification that must be made, without modification, in every annual and quarterly report, including a certification that the CEO and CFO have evaluated the company's internal controls and disclosure controls within the last 90 days and disclosed to the audit committee and outside auditor any deficiencies in such controls. In order to meet the certification requirements regarding the internal controls and disclosure controls, the SEC recommends that every company establish a disclosure committee consisting of the CFO, controller, heads of divisions and other persons having significant responsibility for the company's principal operating divisions. The disclosure committee should review the company's existing internal controls and disclosure controls and procedures, document them, evaluate their adequacy, correct any material weaknesses and create monitoring and testing procedures that will be used every quarter to continuously evaluate the company's internal controls and disclosure controls and procedures.

It will be critical for every company to involve its auditors in the design and implementation of the internal controls and disclosure controls and procedures, because beginning in July 2003, the SEC requires a public company's outside auditor to audit and report on the company's internal controls and procedures. The big four accounting firms have issued public advice that they will not be able to audit a company's internal controls without some documentation of the design and procedures, including the monitoring and testing procedures used by the company. This means that a company will need to establish detailed records, as well as reporting, testing and monitoring procedures that must be reviewed by the company's outside auditors. If a company's outside auditor finds that there are significant deficiencies or material weaknesses in the company's internal controls, the auditor will be required to disclose its findings in its audit report on the company's financial statements. The company will then be forced to correct the deficiencies or its CEO and CFO will be unable to issue their personal certifications that the internal controls are adequate.

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. According to the *American Society of Certified Public Accountants*, “Many of the reforms could be viewed as best practices and result in new regulations by federal and state agencies [affecting nonpublic companies].”<sup>7</sup>

### ***Children's Online Privacy Protection Act (COPPA)***

The Children's Online Privacy Protection Act ("COPPA") became effective April 21, 2000, and applies to any online operator that collects personal information from children under 13. The rules adopted under COPPA spell out what a web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect the children's privacy and safety online. Unlike HIPAA and GLB, COPPA is designed to address a class of individuals – minors -- and not a regulated business. It thus has a scope that is in many ways broader, although in some ways less inclusive, than prior existing laws. In addition to creating challenges for the design of web sites—for example, many web operators have redesigned their web sites to make them less appealing to children under 13—COPPA and the rules adopted implementing COPPA impose requirements on privacy notices and creates specific procedures which must be followed before an operator may obtain information from children. COPPA has caused many businesses (and should spur all businesses) to consider their privacy policies, both in form and substance, and develop practice guidelines.

### ***FTC Safeguards Rule***

As noted above, the Federal Trade Commission has been at the forefront of privacy regulations. In that role, the FTC has adopted a "safeguards rule" 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.”*<sup>8</sup>

The FTC regulation is a step which is likely to take us beyond existing laws. Under its authority to protect consumers, 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 Rule.

---

<sup>7</sup> Website of Hood & Strong at <http://www.hoodstrong.com/InStep/2002/NFP%20YREND02%20Articles.html>.

<sup>8</sup> 16CFR 314

### ***FTC Unfair & Deceptive Practice***

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 online privacy practices. 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. 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.<sup>9</sup>

In enforcing this power, the FTC has brought and settled charges relating to online privacy with Eli Lilly and Company (relating to sensitive information collected on its Prozac website); Microsoft Corp. (regarding the privacy and security of personal information collected from consumers through its "Passport" web services); and Guess, Incorporated (relating to potential disclosure of credit card and other information).

### ***State Actions***

California has been at the forefront of protecting the privacy of online and electronic information. California has attempted to address these matters through laws regarding identity theft, privacy obligations of online merchants and remedies for disclosure. As with the FTC approach toward enforcement of the Safeguards Rule and claims of deceptive practices, these efforts are directed toward all businesses; in other words, all businesses are directly impacted by California developments, since they typically impact any entity that does business in California.

### ***California Civil Code 1798.84 (SB1386)***

California Senate Bill 1386 became effective July 1, 2003. It is designed to give prompt notice when personal information has been released, and impacts all businesses which do business in California, as well as governmental and nonprofit agencies. Its application to a business does not require an office or significant presence in California; a single employee, a customer or vendor located in California is enough to trigger the obligations under the law. The law requires these entities to notify their customers anytime they become aware of a breach of their security which involves the disclosure of unencrypted personal information.

---

<sup>9</sup> FTC Website at <http://www.ftc.gov/privacy/privacyinitiatives/promises.html>.

The statute defines "personal information" as a person's first name or first initial and last name in combination with any one or more of the following elements whether either the name or the elements are nonencrypted: (a) social securities number; (b) driver's license or identification card number; or (c) account number, credit or debit card number together with a code which permits access to a financial account. Thus, records with an attached name to any typical identifier can be considered personal information. It is important to know at the same time that the law does not define a financial account or access code, adding to the uncertainty of the law. Because of this, one cannot assume that the law applies to obvious targets, like credit cards and bank accounts. Electronic data interchange accounts, recordkeeping accounts (even if they do not provide for financial transactions) and other data bases are likely to be targets.

It should be noted that this law does not exist in a vacuum. The law is a reaction to the failure by the State of California's Teale Data Center to promptly notify an estimated 265,000 state employees whose personal data was exposed during a hacking incident in April of 2002. The problem has not gone away—as recently as March 13, 2004, the Los Angeles Times reported that a malfunctioning web site may have allowed the social security numbers, addresses and other personal information of more than 2,000 University of California applicants to be viewed by other students during the application process. The data displayed may have included names, phone numbers, birth dates, test scores, and e-mail addresses in addition to social security numbers.

### ***Senate Bill 27***

In 2003, California adopted Senate Bill 27, which becomes operative on January 1, 2005. SB 27 allows consumers to discover how companies disseminate personal information for direct marketing purposes. It obligates companies to designate a mailing address, an e-mail address or toll free number or facsimile number at which it will receive requests. It also requires companies to train agents and employees to implement a web site privacy policy and make information readily available to customers. It opens the possibility that companies could avoid reporting by adopting an "opt-in" policy for third party disclosures, at the price of restricting the company's ability to engage in cross-marketing and similar opportunities.

It should be noted that, like the other California laws discussed here, this is a broad ranging law. It covers all businesses, and makes specific disclosure requirements. It also incorporates the opt-in concept, which has become a prevalent means by which regulators and legislators seek to allow consumers to control access to their personal and financial information.

### ***Assembly Bill 68—Online Privacy Protection Act.***

Effective July 1, 2004, all operators of web sites and other online services are required to implement privacy policies with specific provisions. Each privacy policy must:

- Identify the categories of personally identifiable information that the operator collects and the categories of third parties with whom the operator might share that information;

- Describe the process by which an individual consumer may review and request changes to his or her information;
- Describe the process by which the operator notifies consumers who use or visit its commercial web site or online service of material changes to the operator's privacy policy; and
- Identify the effective date of the policy.

The law includes specific requirements regarding the location and prominence of the privacy policy, and businesses should be aware that by adopting a privacy policy, as required by Assembly Bill 68, they are making themselves subject to FTC regulation on this very matter!

### *Other State Actions*

There have been several cases in which a company victimized by cyber criminals has faced liability under a state's consumer protection statutes.

#### *Victoria's Secret*

On October 21, 2003, New York State Attorney General Eliot Spitzer announced an agreement with Victoria's Secret to protect the privacy of its customers.<sup>10</sup>

The agreement follows the discovery that personal information of Victoria's Secret customers was available through the company web site, contrary to the company's published privacy policy.

Under the terms of the settlement, Victoria's Secret is to provide refunds or credits to all affected New York consumers, and is to pay \$50,000 to the State of New York as costs and penalties.

Also under the terms of the settlement, Victoria's Secret is required to:

- Establish and maintain an information security program to protect personal information
- Establish management oversight and employee training programs
- Hire an external auditor to annually monitor compliance with the security program

In announcing the agreement, Mr. Spitzer said: "A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information security and privacy practices."

#### *Ziff-Davis Media, Inc.*

---

<sup>10</sup> Office of New York State Attorney General Eliot Spitzer, *Victoria's Secret Settles Privacy Case*, October 21, 2003.

In November 2001, Ziff-Davis, a New York-based multimedia content company, ran a promotion on its web site, receiving approximately 12,000 orders for one of its magazines. According to legal briefs, inadequate security controls left these orders—including credit card numbers and other personal information—exposed to anyone surfing the internet with the result that at least five consumers experienced credit card fraud.

Ziff-Davis, in its online security policy made several representations concerning the privacy and security of information it collected from consumers, including the following:

*We use reasonable precautions to keep the personal information you disclose ... secure and to only release this information to third parties we believe share our commitment to privacy.*

The Attorney Generals of California, New York and Vermont brought suit against Ziff-Davis, arguing that, in light of the above experience, this representation constituted an unfair or deceptive act. In an agreement reached between the parties, Ziff-Davis agreed to

- Identify risks relating to the privacy, security and integrity of consumer data
- Address risks by means that include management oversight and training of personnel
- Monitor computer systems
- Establish procedures to prevent and respond to attack, intrusion, unauthorized access, and other system failures<sup>11</sup>

## **Section 2. Contract and Tort Law**

### ***Specific Contractual Obligations Regarding Financial Transactions***

The *National Automated Clearing House Association (NACHA)*, along with both *Visa* and *MasterCard*, contractually impose information security requirements on their members.<sup>12 13</sup>

Visa's Cardholder Information Security Program (CISP) contractually imposes the following 12 basic security requirements with which all Visa payment system constituents need to comply:

1. Install and maintain a working firewall to protect data
2. Keep security patches up-to-date
3. Protect stored data
4. Encrypt data sent across public networks

---

<sup>11</sup> Assurance of Discontinuance between Ziff-Davis and the Attorney Generals of California, New York and Vermont, August 28, 2002, [http://www.oag.state.ny.us/press/2002/aug/aug28a\\_02\\_attach.pdf](http://www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf).

<sup>12</sup> NACHA, Risk Management for the New Generation of ACH Payments 111, 2001.

<sup>13</sup> Visa, Cardholder Information Security Program (CISP), 1999.  
[http://www.usa.visa.com/business/merchants/cisp\\_index.html](http://www.usa.visa.com/business/merchants/cisp_index.html).

5. Use and regularly update anti-virus software
6. Restrict access by "need to know"
7. Assign a unique ID to each person with computer access
8. Don't use vendor-supplied defaults for passwords and security parameters
9. Track all access to data by unique ID
10. Regularly test security systems and processes
11. Implement and maintain an information security policy
12. Restrict physical access to data

### ***Breach of Contract***

While there is, as yet, little case law in the area, it is possible, if not likely, that those harmed by a disclosure of sensitive information will seek redress through a breach of contract claim. An example would be a purchaser of technology or technology services, claiming an explicit or implicit warranty from security defects in the technology.

A second example concerns the unauthorized disclosure of information which could generate a contractual liability if it occurs contrary to a non-disclosure or confidentiality agreement.

Analogously, a statement in an organization's privacy policy could give rise to a contractual liability if it is not effectively enforced, as a potential plaintiff may seek to recast terms of use and privacy statements as a binding contract. As such, plaintiffs will analyze the sometimes "soft" statements made in privacy policies, and may bring breach of contract claims for failure to follow strictly the policy.

If a web site operator, for example, states that it uses its "best efforts" to protect the identity of users, it may be brought to task for not taking every possible step to prevent disclosure, even if it uses reasonable efforts to do so. Consequently, every privacy statement and terms of use must be analyzed carefully and tailored to its exact circumstances lest it inadvertently subject a business to a contractually higher standard of care than is intended.

### ***Tort Law***

Numerous legal models are emerging arguing that tort law may be used to establish liability in information security situations. We investigate two of these:

- Negligence Claims
- Shareholder Actions

## *Negligence Claims*

Negligence is defined as the “failure to use such care as a reasonable prudent and careful person would use under similar circumstances.”<sup>14</sup>

For a victim of a security breach to prevail in a negligence claim, the victim must establish four elements:

- *Duty of Care*: The defendant must have a legal duty of care to prevent security breaches;
- *Breach of Duty*: The defendant must have violated that duty by a failure to act “reasonably;”
- *Damage*: The plaintiff must have suffered actual harm; and
- *Proximate Cause*: The breach of duty must be related to the harm closely enough to be either the direct cause of the harm or, if an indirect cause, then it must be (i) a substantial causative factor in the harm and (ii) occur in an unbroken sequence linking to the harm.<sup>15</sup>

Beyond the obvious need to establish proximate cause, there are three challenges to a successful negligence claim:

*Duty of Care*. At the present time there is uncertainty over whether or not a legal duty exists in the case of an information security breach, except in those circumstances where a clear legal obligation or contractual relationship exists that requires the securing of information. Thus, financial institutions and health care providers have a clear duty of care, as do businesses possessing nonpublic personal information about California residents. However, as more and more businesses adopt privacy policies or are required to do so (under federal or state law or FTC prodding), a more generalized duty of care may emerge. Thus, even in those circumstances where there is no statutory duty of care, analogous duty of care situations suggest a duty of care may also exist for the securing of information assets.

In the case of *Kline v. 1500 Massachusetts Avenue Apartment Corp.*, for example, the *U.S. Court of Appeals for the District of Columbia Circuit* ruled that a landlord has an obligation to take protective measures to ensure that his or her tenants are protected from foreseeable criminal acts in areas “peculiarly under the landlord's control.” The plaintiff in this case had sought damages for injuries she sustained when an intruder attacked her in a common hallway of her apartment building. The Court held that the landlord was in the best position to prevent crimes committed by third parties on his property. In remanding the case for a determination of damages, the court stated,

*“[I]n the fight against crime the police are not expected to do it all; every segment of society has obligation to aid in law enforcement and minimize the opportunities for crime.”<sup>16</sup>*

---

<sup>14</sup> *Black's Law Dictionary*, 6<sup>th</sup> ed., 1032

<sup>15</sup> *Black's Law Dictionary*, 6<sup>th</sup> ed., 1225

<sup>16</sup> *Kline v. 1500 Massachusetts Avenue Apartment Corp.*, 439 F.2d 477, 482 (D.C. Cir. 1970); see also *Morton v. Kirkland*, 558 A.2d 693, 694 (D.C. 1989).

A similar argument would suggest that a business is in the best position to prevent cyber crimes against its own computer systems, as these are “peculiarly under the business’ control.”

To the extent that the claim that business is in the best position to prevent cyber crimes can be substantiated, it would raise the question of whether they legally ‘should’ take the actions necessary to prevent such a crime. The issue is whether the cost of avoidance is small enough relative to the cost of an incident to warrant imposing a duty on the business to take steps to secure its information assets. This cost-benefit analysis follows from Judge Learned Hand’s equation “ $B < PL$ ” articulated in *United States v. Carroll Towing Co.*, in which Hand wrote that a party is negligent if the cost (B) of taking adequate measures to prevent harm is less than the monetary loss (L) multiplied by the probability (P) of its occurring.<sup>17</sup> As Moore’s Law continues to drive down the cost of basic protection and as cybercrime statistics continue to show exponential growth, Hand’s equation is certain to be valid: the cost of protection is often 2 or more orders of magnitude less than the expected loss.

*Breach of Duty.* Equally uncertain, at the present time, is what constitutes “reasonable care.” On the one hand, “reasonable care” is hard to pin down precisely as the security needs and responsibilities of organizations differ widely.

On the other hand, two classic legal cases suggests that there is a standard of reasonable care applicable to the protection of information assets, even in the circumstances where there is not yet a clear definition of exactly what that standard is. The first of these is the classic doctrine enunciated in *Texas & P.R v Behymer* by Supreme Court Justice Holmes in 1903: “[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it usually is complied with or not.”<sup>18</sup>

In the second case, *T. J. Hooper v. Northern Barge*, two barges towed by two tugboats sank in a storm. The barge owners sued the tugboat owners, claiming negligence noting that the tugboats did not have weather radios aboard. The tugboat owners countered by arguing that weather radios were not the industry norm. Judge Learned Hand found the tugboat owners liable for half the damages even though the use of weather radios had not become standard industry practice, writing:

*Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices ... Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.*<sup>19</sup>

Taken together, particularly in the context of the explosive growth in computer crime, these two statements can be interpreted to suggest that for a business to act “reasonably” it must take

---

<sup>17</sup> *United States v. Carroll Towing Co.*, 159 F.2d 169, 173-74 (2d Cir. 1947).

<sup>18</sup> *Texas & P.R v Behymer*, 189 U.S. 468, 470, 1903.

<sup>19</sup> *T. J. Hooper v. Northern Barge*, 60 F.2d 737 2d Cir., 1932.

meaningful precautions to protect its critical information systems and the information contained in them.

*Economic Loss Doctrine:* Courts have traditionally denied plaintiffs recovery for damages if those damages are purely economic, as opposed to physical harm or damage to property. Since victims of information security breaches typically suffer only economic loss, the *economic loss doctrine* could present a challenge to a successful information security claim.

However, in recent decades, a number of courts have carved out exceptions to the *economic loss doctrine*. For example, the New Jersey Supreme Court in the case of *People Express Airlines v. Consolidated Rail Corp* awarded damages to People Express after the airline suffered economic loss as a result of having to suspend operations due to a chemical spill at the defendant's rail yard. In awarding damages to People Express the Court wrote:

*A defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty.*

*We hold therefore that a defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury, to particular ... plaintiffs comprising an identifiable class with respect to whom defendant knows or has reason to know are likely to suffer such damages from its conduct.*<sup>20</sup>

### *Shareholder Actions*

Shareholders damaged by a drop in the value of a company resulting from the cost of a security breach may seek to sue management for failing to take steps to protect information assets. The nexus of new and developing standards derived from so many new sources – new state laws, federal securities laws, the Patriot Act, requirements of auditors and insurers – will have an impact of allowing potential plaintiffs to establish claims based on failure to comply with accepted standards.

Consider, for example, a public company doing business in California that was the subject of a hacker that obtained sensitive personal and financial information regarding clients. Upon discovery, the corporation was obligated, under California law, to publicize the security breach, thus giving shareholders notice of potential wrongdoing. Not surprisingly, the company's stock price was adversely impacted by the disclosure and subsequent negative publicity about the company. Upon further investigation (or perhaps with little or no investigation), a shareholder engaged a class action lawyer to pursue a claim against the company. The attorney couched the claim on the basis that the company had failed to apply broadly accepted security standards, resulting in damage to the company's shareholders.

---

<sup>20</sup> *People Express Airlines v. Consolidated Rail Corp.*, 495 A.2d. 107 (N. J. 1985).

If the company had, in fact, followed industry standards, it might be able to assert a defense – that it had not been negligent, and that its actions were in full compliance not only with applicable law, but with the standards imposed by regulatory agencies, auditors, insurers and its industry in general. The existence of standards could prove not only to be a sword, but a shield.

### **Section 3. Effective Information Security Practices**

At the same time as the legal risk associated with a failure to protect information assets is increasing, the professional information security community is developing a common body of *Information Security Management Practice Models* for use in effectively managing the security of information.

In this section we review three of these:

- ISO-17799—Code of Practice for Information Security Management <sup>21</sup>
- Generally-Accepted Information Security Principles (GAISP), Version 3.0 <sup>22</sup>
- Information Security Governance: Guidance for Boards of Directors and Executive Management <sup>23</sup>

Each of these three documents deal at an abstract level with the question of standards for the protection of information assets. Their points-of-view are quite different, as is their pedigree. *ISO-17799* originated in Australia and Great Britain before being adopted by the *International Standards Association*. *GAISP* is being developed by an international consortium under the leadership of the *Information Systems Security Association*, with the majority of participants coming from the United States. Both of these practice models were developed by information security practitioners, whereas *Guidance for Boards of Directors and Executive Management* was developed by the *Information Systems Audit and Control Association (ISACA)*.

Our objective in reviewing these three distinctly different practice models, is to *triangulate* around a common set of activities which one could assert would be required for a business to demonstrate that it met a “reasonable” standard of care.

#### **ISO-17799—Code of Practice for Information Security Management**

ISO 17799 is an emerging international standard for managing information security. With roots in Australian information security standards and British Standard 7799, ISO 17799 is the first

---

<sup>21</sup> *Information Technology—Code of Practice for Information Security Management*, International Standards Organization, ISO-17799, 2000

<sup>22</sup> *Generally-Accepted Information Security Principles (GAISP), Version 3.0 (Draft)*, The Information Systems Security Association, 2004.

<sup>23</sup> *Information Security Governance: Guidance for Boards of Directors and Executive Management*, Information Systems Audit & Control Foundation, ISACA, 2001.

acknowledged world-wide standard to identify a “Code of Practice” for the management of information Security.

ISO 17799 defines *Information Security* as encompassing the following three objectives:

- Confidentiality—Ensuring that information is accessible only to those authorized to have access
- Integrity—Safeguarding the accuracy and completeness of information and processing methods
- Availability—Ensuring that authorized users have access to information and associated assets when required

ISO 17799 identifies 10 specific vital *Information Security Management Practices*. An organization’s information is secure only to the extent that these 10 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:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

### **Generally-Accepted Information Security Principles (GAISP), Version 3.0**

GAISP is an ongoing project to collect and document information security principles that have been proven in practice and accepted by practitioners. 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 guidelines to planning and execution of security tasks and to establishment of a solid security architecture.
- 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*

The second level of the GAISP consists of *Broad Functional Principles*, 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

Note that each organization has to determine what maturity level is appropriate for its specific circumstances.

The following Table provides a brief overview of each of the six “Information Security Management Maturity Level.”

<b><u>Mgmt Maturity</u></b>	<b><u>Description</u></b>
<i>Level 0.....</i>	Security Management is Non-Existent The organization does not manage the security of information assets
<i>Level 1.....</i>	<i>Initial Ad-Hoc Security Management</i> Security management is ad hoc and not organized; management responsibility is fragmented or non-existent
<i>Level 2.....</i>	<i>Repeatable but Intuitive Security Management</i> Basic security countermeasures and processes are implemented; management responsibility, authority and accountability are assigned
<i>Level 3.....</i>	<i>Defined Process</i> Security management flows from organizational strategy and from an organization-wide risk management policy; employees receive regular training and education
<i>Level 4.....</i>	<i>Managed and Measurable</i> Security management is monitored and measured; regular feedback is used to assess and improve management effectiveness
<i>Level 5.....</i>	<i>Security Management is Optimized</i> Information security best practices are followed

## Section 4. Information Security Minimum Standards of Due Care—The Battle of the Expert Witnesses

Let us now consider what Einstein called a *Gedanken Experiment*, a thought experiment. Imagine that company ABC suffers an information security incident resulting in damage to a 3<sup>rd</sup> party, XYZ. Let's stipulate that ABC is not legally bound by the GLB Act, has no printed privacy policy to which it must adhere, doesn't do business with California consumers, etc, and so has no explicit *Duty of Care* to protect. Let's also stipulate that XYZ's losses were not just economic. Finally let's stipulate that ABC has at least 100 employees, 100 workstations and several servers.<sup>24</sup>

In this situation, the case hinges on two points

- A point of law as to whether ABC has an *implicit Duty of Care*
- A point of information security management as to whether the actions ABC took in protecting its information systems were *reasonable*.

Let's now further stipulate that the plaintiff establishes that ABC has, indeed, a *Duty of Care*. The case now hinges on whether the actions ABC took in protecting its information systems were reasonable. Bring on the experts!

*Hypothesis:*

The actions ABC took in protecting its information systems were reasonable if ABC can find an *unimpeachable* expert to testify that ABC's actions were reasonable. Correspondingly, XYZ will prevail if ABC's actions were so egregious that any attempt by ABC to present an expert testifying that ABC's actions were reasonable could be impeached by XYZ's attorneys.

In this context an *unimpeachable* expert is someone with the following qualities:

- Experienced information security professional, respected by colleagues
- Either an information security certification, such as the *CISSP* designation, or some other credentials of expertise
- Active membership in an organization of information professionals, such as the *Information Systems Security Association*
- Expert in information security standards of practice, such as ISO-17799, GAISP, and the ISACA guidelines
- Expert in GLB, HIPAA and other information security standards

---

<sup>24</sup> Duty and reasonableness for a 1-person home office would necessarily be different than for our hypothetical ABC. A software firewall, virus protection, regular patching and the like may be all that a 1-person home office need do.

Imagine now that we have ABC's expert in the witness chair. She's an information security professional with all of the qualities listed above. For this expert to testify that ABC's actions were reasonable she would have to find evidence of the following seven key information security management elements.

**Executive Management Responsibility:** Someone at the top has management responsibility for ABC's information security program, and this program is managed in accordance with its information security policies.

**Information Security Policies:** ABC has *documented* its management approach to security in a way that complies with its responsibilities and duties to protect information.

**User Awareness Training & Education:** Users receive regular training and education in ABC's information security policies and their personal responsibilities for protecting information.

**Computer and Network Security:** ABC's IT staff is securely managing the technology infrastructure in a defined and documented manner that adheres to effective industry practices

**Third-Party Information Security Assurance:** ABC shares information with third parties only when it is assured that the 3<sup>rd</sup>-party protects that information with at least the same standard of care as does ABC.

**Physical & Personnel Security:** ABC provides appropriate physical protection for information, screens candidates for employment, and incorporates security in job responsibilities.

**Periodic Risk Assessment:** ABC conducts an assessment or review of their information security program, preferably by an independent 3<sup>rd</sup>-party, covering both technology and management, at least annually.

These seven management elements form a common core, either explicitly or implicitly, of all three *Information Security Management Practice Models* we examined, as well as the GLB and HIPAA regulatory standards for protecting information. Therefore, we feel confident in asserting that if ABC's unimpeachable expert can testify that ABC is doing these seven things, then ABC's actions are reasonable. We are correspondingly confident that, if the expert is truly an unimpeachable information security professional, then, in the absence of these 6 elements, she would not testify for ABC that its actions were reasonable. Indeed, we think that, in this case, she would line up to testify on behalf of XYZ.

It is these seven key information security management elements, therefore, that we believe form a *Minimum Information Security Standard of Due Care*.

## Section 5. Looking to the Future

As computer crime continues to rise, the legal and regulatory landscape will tilt towards more responsibility, not less.

The *Corporate Governance Task Force* of the *National Cyber Security Partnership*, a public-private partnership working with the *Department of Homeland Security* has recently released a management framework and call to action to industry, non-profits and educational institutions, challenging them to integrate effective information security governance (ISG) programs into their corporate governance processes.<sup>25</sup>

Among the recommendations of the Task Force:

- Organizations should adopt the information security governance framework described in the report and embed cyber security into their corporate governance process
- Organizations should signal their commitment to information security governance by stating on their website that they intend to use the tools developed by the *Corporate Governance Task Force* to assess their performance and report the results to their board of directors
- All organizations represented on the *Corporate Governance Task Force* should signal their commitment to information security governance by voluntarily posting a statement on their website. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their websites.
- The *Department of Homeland Security* should endorse the information security governance framework and core set of principles outlined in this report, and encourage the private sector to make cyber security part of its corporate governance efforts
- The *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance

According to Art Coviello, president and CEO at RSA Security, and co-chair of the Corporate Governance Task Force, “It is the fiduciary responsibility of senior management in organizations to take reasonable steps to secure their information systems. Information security is not just a technology issue, it is also a corporate governance issue.”

Bill Conner, chairman, president and CEO of Entrust, Inc., who co-chaired the Task Force with Coviello, is quoted as saying “We cannot solve our cyber security challenges by delegating them

---

<sup>25</sup> *Information Security Governance: A Call to Action*, Corporate Governance Task Force, National Cyber Security Partnership, April 2004.

to government officials or CIOs. The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs.”<sup>26</sup>

Lest the private sector not step up to its responsibilities, the Federal government is prepared to strengthen laws and regulations requiring the securing of information. As this is being written Senator Dianne Feinstein (CA) has introduced a bill extending California’s “breach disclosure” law to all Americans. Congressman Adam Putnam (FL), chairman of the *House Technology, Information Policy, Intergovernmental Relations and the Census Subcommittee*, has introduced legislation that would require every publicly held corporation in the U.S. to have an information security independent review and include a statement in the annual report that the review established compliance with SEC-mandated information security standards.

Also tilting the landscape towards a greater duty of reasonable care is that businesses, after taking their own security responsibilities seriously, are requiring the same of their trading partners. This will serve to accelerate the adoption of improved information security management which will then, in turn, accelerate the acceptance of the seven key information security management elements as a *Minimum Information Security Standard of Due Care*.

As a result, we feel it safe to say that over the next few years the *Minimum Information Security Standard of Due Care* will, if anything, get tougher, not easier. Thus, while we can expect technology to continue to aid in the battle for security, the need for management at the top, for policies, for training, and for the other key management elements will not go away.

---

<sup>26</sup> Corporate Governance Task Force of the National Cyber Security Partnership Releases Industry Framework, NCSP, Press Release, April 12, 2004.

## Sidebar

### Gramm Leach Bliley Federal Trade Commission Standards for Safeguarding Customer Information <sup>27</sup>

#### Sec. 314.3 Standards for safeguarding customer information.

**(a) Information security program.** You shall 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. Such safeguards shall include the elements set forth in Sec. 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

**(b) Objectives.** The objectives of section 501(b) of the Act, and of this part, are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

#### Sec. 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

- (a)** Designate an employee or employees to coordinate your information security program.
- (b)** Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- (1) Employee training and management;
- (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

---

<sup>27</sup> 16CFR 314.

**(3)** Detecting, preventing and responding to attacks, intrusions, or other systems failures.

**(c)** Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

**(d)** Oversee service providers, by:

**(1)** Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

**(2)** Requiring your service providers by contract to implement and maintain such safeguards.

**(e)** Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.