Overview of Public Policy Relating to Information Assurance Practices

Information Assurance and Public Policy

Information Assurance (IA) professionals are faced daily with issues that increasingly demand adequate awareness of the effect of public policy on an organization's data processing workflows. Public policy impacts how enterprise information is collected, protected, and shared. From the way an organization adopts information collection practices in response to accounting and record-keeping requirements, to the means by which these assets are leveraged, even business continuity planning, will all depend on a proper understanding of the legal framework that ultimately constrains how the enterprise produces services and organizes its resources.

In this new environment of distributed systems, social networks and networked knowledge silos, public policy has tended to place new requirements on IA professionals, beyond those of merely protecting and controlling access to the enterprise network boundary. Compromises between consumer protection and enterprise systems defense requirements have been achieved in public policy in the United States, for example; yet, the approach has resulted in a patchwork of federal and state laws that can be guaranteed to result in increased burdens on disclosure, retention, and disposal practices in the avoidance of charges of negligence.

Methods

This document details an analysis of public policy as it relates to IA practice, with particular concern towards structuring evidence collection and sharing methods. Our team analyzed the literature on the legal outcome of data breach and accidental disclosure cases, laws impacting information assurance and cybersecurity practices, and IA information seeking and sharing trends. Our efforts resulted in a map that details the rise of laws in response to policy breach incidents of severe impact, and the cultural concerns of IA professionals who inevitably will influence lobbying efforts that affect the final structure of trade laws—see an abbreviation of this map in Appendix 1 below.

Our goal herein is not merely to take note of regulatory concerns, but to provide a framework baseline by which IA professionals can achieve an understanding of the regulatory policy impacting their domain; and, perhaps, to suggest means by which proper safeguards and controls can be developed and maintained in consideration of the operating constraints imposed by regulations.

Public Policy

The spectrum of interest in public policy for an IA professional extends from the laws of the land where the enterprise operates to the set of operating policies in effect within the organization that control the way data is stored, used and shared as reflected, for example, in the terms of use for services provided—the outward perception of the organization.

The capacity of the organization to continue as a going concern depends first on its adherence to trade regulations, but more importantly on its relations with the consumers of its products. The public position the enterprise takes on the privacy and data protection needs of their consumers is essential to its survivability.

Public policy is the body of principles that underpin the operation of legal systems in each state. Laws under public policy regulate behavior either to reinforce existing social expectations or to encourage constructive change. Information security public policies are written by the Federal Government, for example, to protect information and the systems which store and process the information. These written policy documents provide a high-level description of the various controls the organization will use to protect information.

Depending on the states and nature of work in organizations, these public policies are enacted through agreements, controls and safeguards within an organization. Written information security policy documents are a formal declaration of an organization's intent to protect information, and are required for compliance with a complex set of security and privacy regulations. Organizations that require audits of their internal systems for compliance with various regulations will often use information security policies as the reference for the audit. This is where the IA officer plays a critical role in establishing proper network controls as a means towards regulatory compliance.

Operating successfully on the web requires a sincere engagement with the user. The focus on self-support user tools demands open agreements that enhance collaborative interactions. Yet, this opens the door to the possibility of a systems policy breach; and, invokes the need for continued information assurance awareness on the part of all stakeholders in the domain of concern.

An organization's evolving position on public policy therefore should strive to ensure stakeholder understanding of the impact of regulation, both in the public and the enterprise domains. As much as it is important to understand how to serve the customer within the boundaries of the law, it is more critical to ensure that agents understand how their actions could affect the reputation or continuity of the enterprise as a result of policy vulnerabilities. Moreover, the organization's managers need to anticipate the impact of mandates on breach evidence documentation, and the potential ramifications of making such evidence public.

Regulations

Federal

Much of federal law under consideration today is being based on an industry recommendation sponsored by Microsoft in 2005 that establishes a Baseline Privacy Standard[1]. The guidelines suggest consideration for control over personal information, central oversight of the laws, transparency of information collected, control over the use of personal info, information security standards, and explicit consent to the owners of the information—the consumers of the services.

The laws have arisen as a patchwork of regulation that is segmented by industry. More power is being sought for federal agencies in the declaration and enforcement of 'reasonable' systems and data protection standards. A summary of federal laws and guidelines regulating disclosure, disposal and notification appear in Table 1, below.

Executive Branch

The *President's Identify Theft Task Force (PITTF)* recommends that congress allow regulatory agencies to set and regulate organizations based on evolving standards. One of the recommendations of the task force is the adoption of FISMA[2].

FISMA. Federal Information Security Management Act. FISMA replaced an expired set of rules under the Government Information Security Reform Act (GISRA). It is a comprehensive framework for securing the federal government's information technology. The act proposes a set of specific guidelines to federal agencies on how to plan for, budget, implement, and maintain secure systems:

- *Categorize the information and information systems.*
- *Select the appropriate minimum or baseline security controls.*
- *Refine the security controls using a risk assessment.*
- *Document the security controls in the system security plan.*
- *Implement the security controls in the information system.*
- *Assess the effectiveness of the security controls.*
- *Determine agency-level risk to the mission of business case.*
- *Authorize the information system for processing.*
- *Monitor the security controls on a continuous basis.*

[1] Microsoft Data Privacy Recommendation: http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx

[2] FISMA Compliance Guide: http://www.bly.com/newsite/Pages/WP_FISMACompliance_062206.pdf

Table 1. Summary of Federal Laws Impacting Information Security Practices

Title	Reference	Domain	Concerns	Mandates
Sarbanes-Oxley (SOX)	The Sarbanes-Oxley Act, Pub. L. No.1 07 - 204	Federal	disclosure of material events arises from fallout of Enron collapse	requires all publicly traded companies to adopt financial reporting integrity controls requires disclosure of material events (actual and anticipated), including data security breaches
Gramm-Leach-Bliley (GLBA)	The Gramm-Leach-Bliley Act, 15 U.S.c. §§ 6801-6809	Federal	arises from fallout of Long-term Capital Management, LTCM	allows investment firms to provide bank services
Health Information Portability and Accountability Act (HIPAA)	The Health Insurance Portability and Accountability Act, 42 U.S.C. § 1306	Federal	intended to protect *Personal Health Information (PHI)*	requires "reasonable and appropriate controls" • ensure the CIA of all health data • protect from prohibited disclosures • privacy rule was amended in 2000 • ensure compliance (with internal and external info sec policies)
Fair Credit Reporting (FCRA)	The Fair Credit Reporting Act, 15 U.S.c. §§ 1681-1681x	Federal	addresses consumer credit and identity theft	Establishes a *Disposal* rule
Federal Trade Commission (FTC)	The Federal Trade Commission Act, 15 U.S.c. § 45	Guidelines	establishes a *Reasonable Safeguards* rule	requires organizations to have a data security plan in place • technology safeguards • physical safeguards • administrative safeguards
Federal Communications Commission (FCC)	Federal Communications Act, 47 U.S.C. § 222	Guidelines	establishes *Disclosure* guidelines	Disclosure should only occur (1) as required by law; (2) with the consent of the consumer; or, (3) to facilitate communications services

State Regulations

In the absence of federal leadership in establishing clear regulations, most states have now taken steps to enact laws that compel organizations with sensitive data to protect personal identifiable information (PII), enhance consumer protection against identity theft and fraud; and, more recently, establish penalty schedules to promote adoption of safeguards.

State laws tend to fall into one of four general categories: State Information Safeguard Statutes, State Social Security Number Protection Laws, State Disposal Laws, and State Data Breach Notification Laws. We found the American Bar Association's *Data Security Handbook* (2008) a very useful compendium that helped structure our research.

Although well intended, these mandates tend to arise as a reaction to a severe breach events, which sometimes results in the imposition of operational burdens to organizations, with direct consequences to the existing business model. Some companies have even gone out of business as a result of changes in public policy that were not properly assessed.

California

Because of the number of enterprises in defense and information technology based in California, and the state's unique market size and diversity, the state has traditionally been a pioneer in efforts to establish identity theft and consumer protection laws.

A few years ago[3], California took the lead in introducing new laws to create incentives for data protection, compel disclosure in case of a security breach incident, and to increase limits on the use of personal information surrendered to financial institutions.

Senate Bill No. 1386 ("SB 1386"), is a breach notification law; and, Senate Bill No. 1 ("SB 1") places limits on financial institutions in sharing personal details— such as disclosed in credit applications.

What's particularly troubling about SB 1386, and which could easily expose a company to negligent liability, is its requirement that disclosure be made even if the company "reasonably believes" that a breach occurred. This only seems like a bargain for tort litigation lawyers. Imagine how an unsuspecting CISO could get trapped in litigation based on a case that hinges on a theory of "reasonable belief". Consider how easily such a case might be supported by structuring an email thread in such a way as to prove cause.

[3] California Raises The Bar On Data Security And Privacy, http://library.findlaw.com/2003/Sep/30/133060.html

Massachusetts[4]

Whereas most states allow for a degree of ambiguity in how organizations develop controls to comply with the law, Massachusetts' is unique in that it has gone a step further and encoded specific data security requirements.

17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

(1) Secure user authentication protocols including:

> *(a) Control of user IDs and other identifiers;*
>
> *(b) A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;*
>
> *(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;*
>
> *(d) restricting access to active users and active user accounts only; and*
>
> *(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;*

(2) Secure access control measures that:

> *(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and*
>
> *(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;*

(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to- date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

---

[44] Massachusetts Identity Theft Law: www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

Washington[5]

The state of Washington has recently taken a step further to adopt a policy of monetary penalties that could arise as a result of data security incidents from criminal negligence. HB 1149 was signed by the governor on March 22nd, 2010. It modifies the state security breach law to provide "a cause of action for a financial institution if account information is compromised by a lack of reasonable care by a business, processor, or vendor… The law requires that any business or person who owns or licenses computerized data which includes personal information to inform state residents of any security breach of that data. Allows anyone who has experienced an unauthorized expense as a result of the security breach to seek a refund or credit for any loss that was not recovered by the credit card company or appropriate financial institution[6]."

[5] WA Disclosure Law: http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010
[6] Sources: 2009 House Bill 1149, http://washingtonvotes.org/2009-HB-1149; and Bill Information, http://apps.leg.wa.gov/billinfo/summary.aspx?bill=1149&year=2009

International Laws

The scope of our analysis of international laws has been limited. The regulatory framework in Europe differs from that in the United States in that Europe took a lead in establishing privacy rights into their constitution, while the United States has taken a more reactive approach. This is perhaps to be expected given the ideological differences between the continents histories. European laws have trended towards supporting more social objectives, while the United States has focused on promoting free enterprise goals.

The practical implications of these approaches are still being debated. On the one hand, European laws establish privacy rights and data control privileges that result in sometimes onerous responsibilities upon business but are increasingly sought in the United States. On the other hand, in the United States, the patchwork of laws described herein have provided a flexible framework that nurtures entrepreneurship. Yet, it has also made it easy for criminals to leverage the internet without significant cost or consequence. What organizations are finding is that the lack of standards and collaboration inherent in information security practice has resulted in a misguided attempt to protect consumers while imposing requirements that can only partially be met by poorly designed solutions; and, ultimately, benefits only the legal professional class.

Europe Slams Facebook Privacy Settings (AFP 2010)

[http://news.yahoo.com/s/afp/20100513/tc_afp/useutechnologyinternet]

Google's Inadvertent Capture of Wi-Fi Data (WSJOnline 2010)

[http://online.wsj.com/article/BT-CO-20100526-716064.html]

Google Antitrust Concerns in Europe (L.A. Times 2007)

[http://articles.latimes.com/2007/dec/18/business/fi-google18]

Microsoft Loses Anti-trust Appeal (BBC News2007)

[http://news.bbc.co.uk/2/hi/business/6998272.stm]

Culture: Focus on Information Assurance Professionals

Focus of Information Security Professionals. IA professionals are typically concerned with business continuity and asset protection issues. Information on systems availability is of particular concern. Secondarily, but just as importantly, is that the systems are not compromised by either internal or external agents in the commission of a crime.

Consistently high on their list of concerns is the need to acquire and share knowledge on systems vulnerabilities, and ensuring that their systems are protected against such. Their response to this information is intended to respond to two priorities: safeguarding against adverse conditions (malware, root kits, phishing, unauthorized entry, etc.) and providing safeguards against disruptions to systems availability (denial of service, corrupted data, untested software, etc.)

Beyond the need to continuously learn about how to monitor and analyze patterns and behavioral signals in their system detection programs, IA professionals are particularly concerned with the nature of information security crimes such as the theft of intellectual property, the destruction of property (corruption), the theft of physical goods (or digital assets), fraud and identity theft.

They need constant update of the state of systems technical defenses. For this, they reach out to known sites and literature, they attend symposiums and meet-ups, and participate in academic and industry conferences. Moreover, they nurture open relations with their collaborators and partners in industry, so that the results from recent breaches of policy can be easily shared without compromising individual interests in the market.

This doesn't really leave much time to stay on top of the latest regulatory changes. Most large corporations, such as Microsoft or Amazon, organize product teams to include legal associates that shadow strategic planning and development projects to ensure compliance with laws. Smaller partnerships would do well to mimic this distribution of tasks by having a preferred on-board legal advisor that understands the business model and ready to respond quickly as project needs arise.

Information assurance professionals will insist on anonymity and the highest degree of discretion in cases of systems policy breach. This is one of the issues that will need to be surmounted as information sharing of network defense methods is structured into adaptive models and frameworks in the coming years that can promote collaborative industry prevention compacts. How does one inject more awareness of information assurance into the enterprise without losing anonymity or constraining productivity? How can one convert that capability into an organizational asset? How does it change the behavior of the market, when defense systems logs are shared to select members of a protection alliance.

The concerns that arise are overwhelming and problematic, to say the least; but, comfort cannot be found in ignoring how to leverage systems in the process of complying and influencing the law, among the daily chaos that is systems management in practice. The answers will require a formulaic approach focused on public policy awareness that will be realized as consideration is given for how law and operational practice play roles in the design of systems and processes.

User Agreements as Public Policy

User agreements (UAs) are at the core of an organization's public representation of its goods and services to its consumers. These are generally concerned with establishing use and content rights, the limits of service, the methods by which notification will be provided, and consumer protection rights built into the features of the application. Generally, the purpose of user agreements is to set expectations with users as compelled by regulations on the limits of collection of data, its uses, disclosure to regulators and consumers, and commitments to dispose of unnecessary information.

Information Assurance Business Practices as Public Policy

Operational policies, guidelines and working frameworks add up to a form of public policy within the perimeter of an organization. Managers of information system operations groups should promote ownership of information assurance practices throughout all layers of the enterprise, whether by documented or verbal means. Particular investment should be devoted to the education of stakeholders on the extent of laws requiring compliance of the organization. These and other practices compose the legal position of the enterprise as it develops revenue generating programs, while protecting itself from negligible liability.

Protections against the loss to access to production data—regardless of group priority, against the intentional or unintentional corruption of critical information, and in favor of systems availability to support the continuity of its mission, should include considerations on: prevention controls, monitoring and detection methods, safeguards, countermeasures, business continuity plans, enterprise recovery strategies, compliance mechanisms, insurance, and even lobbying.

Business Associate Agreements as Public Policy

Business associate agreements are the means by which IA policies are enforced beyond the firewall. The effective compliance of service providers to an organization, as it relates to its information assurance policies, must include dispositions in the compact, at the very minimum, that include incentives (and penalties) to ensure data protection, requirements for the disposal of data beyond its useful lifecycle, and establish expectations for resource sharing in the event of a breach that threatens the relationship and responsibilities bound in the agreement.

It is important to understand the risks inherent in these business agreements. A prudent CISO should anticipate the likely causes that could result in a breach of the contract, and understand how the data exchanged could be compromised. Terms should be included into any business agreement to establish rights and procedures to control under what circumstances and to what extent data is to be disclosed.

CISO LAW Survival Toolkit

Given these considerations, and finding ourselves incapable of providing a modest view of the complexity of the collision of IA practice as influenced by public policy, and vice versa, we decided we could at least try to consolidate our findings into a practical set of guidelines that today's IA professionals can use to develop a public policy awareness capability.

These tools and guidelines reflect the findings from our analysis of information assurance professionals' information seeking-behavior, as described above in the Culture section of this document. The guidelines herein are intended to address the primary concerns of protection, availability and compliance. The recommendations are provided as a baseline for the development of a proprietary process and set of policies that enhance the public policy awareness position of the organization, in relation to its information assurance preparedness process.

Law Reference Tools

Understanding the scope of laws that impact the operational ability of the organization is the first step in developing a sound legal strategy that ensures the organization is compliant while maximizing the ability of the organization to generate revenues. Once the set of regulations affecting the enterprise has been settled, the next step is to understand the degree of risk of non-compliance that the organization is exposed to, and the potential ramifications (both in terms of recovery costs and penalties) that could arise if the company is hit by a breach event. The following resources encapsulate the scope of law and the outcomes of litigation that should be taken into consideration as the information assurance legal strategy is formulated.

Literature

1. Johnson's (2005) "Cybersecurity, Identity Theft, and the Limits of Tort Liability"[7]
2. Lazzarottii's (2008) "The Emergence of State Data Privacy and Security Laws Affecting Employers"
3. Scott's (2007) State Data Breach Notification Laws Matrix[8]
4. State Law Primer. "Notice of Security Breach Laws."[9]
5. Crowell Moring's "State Laws Governing Security Breach Notification"[10]

Law Web Resources

1. Electronic Frontier Foundation on Fair Use. www.eff.org/issues/intellectual-property
2. Electronic Privacy Information Center. epic.org/privacy/
3. Identity Theft Resource Center. www.idtheftcenter.org. *State and Local Resources.*
4. JSTOR - Law Archive. www.jstor.org/stable/27645745[11]
5. National Conference of State Legislatures. www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws
6. E-commerce Law Blog (www.ecommercelaw.typepad.com)
7. Internet Business Law Services (http://www.ibls.com/internet_law_news_portal.aspx)

---

[7] 57 S. C. L. Rev. 255 (2005-2006) http://heinonline.org.offcampus.lib.washington.edu/HOL/Page?collection=journals&handle=hein.journals/sclr57&page=255

[8] State Regulations Matrix: http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf

[9] *Consumers Union*, http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf. (7 pp)

[10] Table. Cites to bills and codes. Covers exemptions. Includes forty states and Puerto Rico. Current as of July 2008. www.crowell.com/pdf/SecurityBreachTable.pdf (1 p)

[11] Fienberg (2006) on Privacy and Confidentiality: http://www.jstor.org/pss/27645745

People/Community

Success depends on people; machines and processes alone cannot do the job! Every organization needs to have a policy in place to distribute the ownership of evidence sharing responsibilities after a breach response, one which is based on legal requirements, legal precedent, and the organization's resources in response to a breach event. Clear lines of control are very important when organizing a response to the event.

Information Seeking Behavior of Engineers and Lawyers. Information assurance professionals are typically focused on making decisions. Uncertainty reduction is a key process in decision making (Leckie and Pettigrew, 1996; Kuhlthau, 1993; and Wilson, 1999). It is thus critical in this process, and in particular during high severity (Sev 1) events, that IA professionals can draw from their strategic partnerships, both business as much as technical. Nurturing those relationships demands time; yet, the investment will pay back handsomely when the organization is faced with an unknown type of breach event. Public policy stakeholders that play various, sometimes critical, roles include politicians, law enforcement agents, the Public, lobbyists and private data processing services organizations**.** Below, we present a list of collaborations to consider structuring into an event response strategy.

1. Lawyers. Legal specialists should understand the risk profile of the enterprise and be ready to provide legal advice during a breach event.
2. Law enforcement. IA managers should be well informed of the process, requirements and demands of working with law enforcement.
3. Politicians. Relations with politicians can be useful when laws are being drafted.
4. Competition. Industry players can play a role as partners in information security.
5. Symposiums. Meet-ups with other regional professionals is critical to establish personal trust.
6. Internal response teams. Specialists (network, process, systems, and legal)are indispensible during an event response.
7. Functional owners. Escalation managers or functional owners should be identified as part of an advance response strategy, providing the ability to divide activities during a response event.

Cases

Familiarity with civil and criminal court litigation relating to data security is critical. IA professionals review the causes that led to litigation and the discoveries that arise through evidence. This information can be used to expose vulnerabilities in the organization's legal posture and contract terms. The Data Breach Security Handbook (2008, p.149-150) summarizes a table of cases relating to information assurance concerns, which we have included in Appendix 2 below.

Articles, Blogs and Newsfeeds

Subscribing to feeds of concern is fundamental to staying up to date on the noise about public policy in the network. Here are some starting points we found useful:

1. Scott Berinato's "CSO Disclosure Series | The Dos and Don'ts of Disclosure Letters"[12]
2. Information Systems Security Exchange (http://infosyssec.com/)

Safeguards, Practices and Controls

Updating information assurance practices depends on an awareness of methods across associated groups of concern. Resources to help formulate operational practices in the protection of information resources can be extracted from the contributions of, and in partnership with, some of the following organizations—the emphasis here being on breach evidence collection and sharing:

1. Association for Computing Machinery. "A statistical analysis of disclosed storage security breaches" (http://portal.acm.org/citation.cfm?id=1179559.1179561)
2. Information Sharing and Awareness Council (ISAC) Chapters.
    a. University of Arizona (http://security.arizona.edu/isac)
    b. Greater Los Angeles ISAC (http://isac-greaterla.com/)
3. Multistate Information Sharing and Analysis Center (http://www.msisac.org/)
4. Computer Emergency Readiness Team, CERT (https://portal.us-cert.gov/)
5. Computer Security Resource Center, National Institute of Standards and Technology (http://csrc.nist.gov/)

[12] Disclosure Series:
http://www.csoonline.com/article/217018/CSO_Disclosure_Series_The_Dos_and_Don_ts_of_Disclosure_Letters

Conclusion

Disclosure, disposal and data protection mandates are encoded in the laws. These laws, in one way or another, compel evidence about a breach to be disseminated. Otherwise, organization's can only be compelled to disclose information through a subpoena--civil or criminal, secret (presidential and private) or congressionally mandated.

Information assurance professionals will need to formulate a strategy to stay abreast of the impact of public policy on information protection and systems availability concerns. As systems are opened, distributed, and operated across virtual borders, there is an urgent need for information managers to collaborate with legal professionals and build coalitions to raise awareness on the liability risks that arise from non-compliance with information collection, processing and sharing mandates.

Our analysis of the public policy domain confirms that IA professionals cannot survive the increasing demands for change from regulators without the indispensable tool of cooperation with legal professionals.

Evidence collection and disclosure frameworks have not been mandated, to date; and, we anticipate that the belief that such a framework would constrain development and growth will constrain political attempts to prescribe evidence requirements. Yet, such regulation is likely to arise in the next 20 years, as widely adopted industry evidence-sharing frameworks mature. The growing number of digitized frameworks and tools for handling data breaches suggest that court evidence handling will continue to rapidly evolve in the next 10 years, to include specific instructions on the classifications of information breaches that impact the citizenry.

Meanwhile, preparedness and cooperation will remain key. Implementing reasonable measures to protect information ultimately means that one should control access, plan ahead for breach vulnerabilities, monitor systems use, organize awareness programs—people should be aware of the consequences of negligence, have clear escalation guidelines, and develop business continuity plans—to include succession planning, if the enterprise is to avoid the risk of failure, takeover, or worse, prosecution.

What we find troubling is that, even with a well understood perspective of the scope of the law, a strategy to ensure compliance, and a collaborative response plan in defense against a policy breach, there is no certainty one can avoid negligent liability based on the risks that can arise from any of the patchwork of prevalent regulatory schemes.

We recommend that IA professionals engage regulators actively in the debate over evidence retention mandates, and the potential consequences of these mandates to affect the ability of the organization to remain as a going concern, to safeguard its desire for anonymity, and, the extent of control it has over the combination of safeguards it prefers in defense of its assets.

Sources

American Bar Association. (2008). *Data security handbook*. Chicago, Ill: ABA Section of Antitrust Law.

Broome, L.L., & Markham, J. W. (2001). *The Gramm-Leach-Bliley Act: An Overview*. Last retrieved May 2010 from http://www.symtrex.com/pdfdocs/glb_paper.pdf.

Broome, L. L., & Markham, J. W. (2000). *Banking and Insurance: Before and After the Gramm-Leach-Bliley Act*. *JOURNAL OF CORPORATION LAW*. 25, 723-786.

Fienberg, S. E. (2006). *Privacy and Confidentiality in an e-Commerce World: Data Mining, Data Warehousing, Matching and Disclosure Limitation*. *STATISTICAL SCIENCE*. 21 (2), 143-154.

Johnson, V. R. (2005). *Cybersecurity, Identity Theft, and the Limits of Tort Liability*.

Kuhlthau, C. C. (1993). A principle of uncertainty for information seeking. *JOURNAL OF DOCUMENTATION*.49 (4), 339.

Lazzarotti, J. (2008). The Emergence of State Data Privacy and Security Laws Affecting Employers.*HOFSTRA LABOR AND EMPLOYMENT LAW JOURNAL*.25 (2), 483-510. Last retrieved May 2010 from: http://heinonline.org.offcampus.lib.washington.edu/HOL/Page?collection=journals&handle=hein.journals/hlelj25&page=483.

Leckie, G., & Pettigrew, K. (1996). Modeling the information seeking of professionals: *Library Quarterly*, *66*(2), 161. Retrieved from Academic Search Complete database.

Lindenmayer, I. (2006). Resort Reports a Data Breach. *American Banker*. 171 (5). *Business Source Complete*. EBSCO. Web. 20 May 2010.

Scott & Scott (2007). State *Data Breach Notification Laws Matrix*. Last Retrieved May 2010 from: http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf

Wolfe, D. (2009). *Breach Settlement*. American Banker. 174 (230).

United States. (2007). *Personal information Data breaches are frequent, but evidence of resulting identity theft is limited; however, the full extent is unknown : report to congressional requesters*. [Washington, D.C.]: U.S. Govt. Accountability Office. http://purl.access.gpo.gov/GPO/LPS84579.

Wilson, T. D. (1999). Models in Information Behavior Research. *Journal of Documentation*. 55 (3), 249-70.

Web Resources

corporate.findlaw.com (Corporate Counsel Center)

www.ftc.gov/infosecurity (Federal Trade Commission Business Guide)

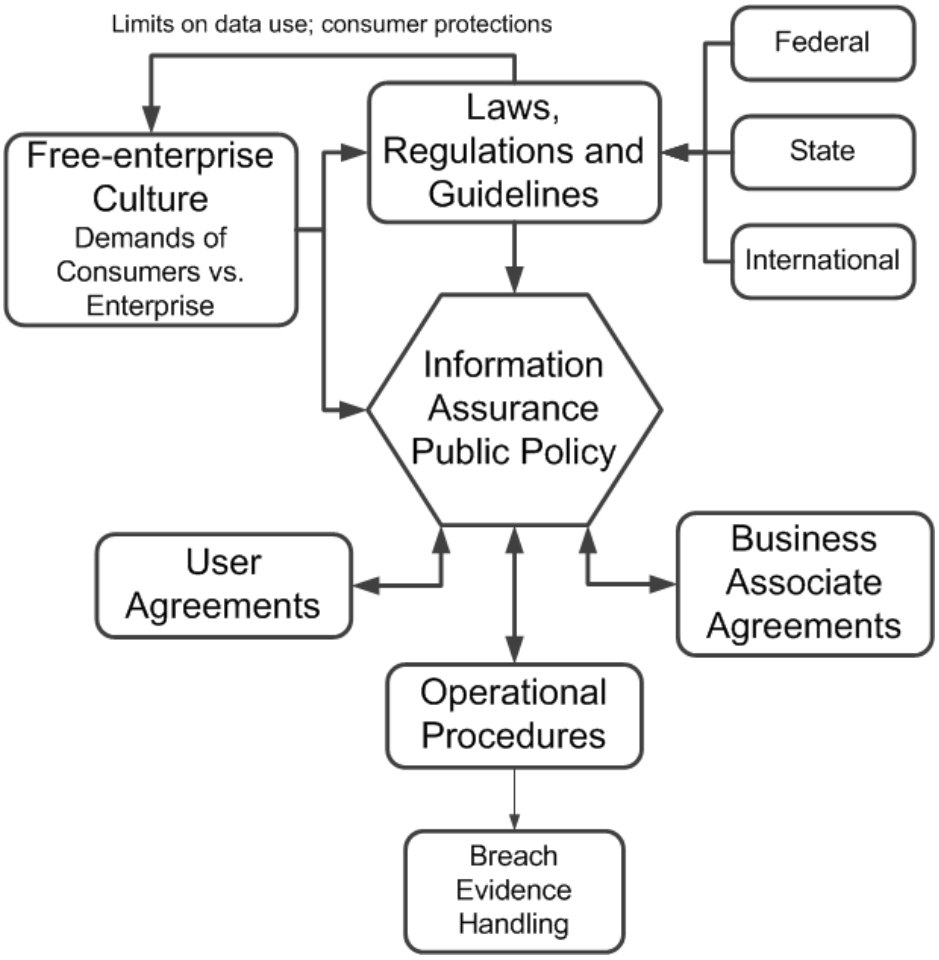
www.sec.gov (or, contracts information found in EDGAR online articles database)

lib.law.washington.edu (Marian Gould Gallagher Law Library, University of Washington)

www.heinonline.org (UW's law librarian's subject compilations of state laws)

Appendix 1: Scope of Analysis

The scope of our Public Policy analysis as it relates to breach evidence sharing included a review of the law, contract litigation, user agreements and business agreements. We then considered how the nature of information assurance concerns and a free enterprise culture of demand for services affects the way laws are enacted and operational policies are structured.



Appendix 2: Data Security/Information Assurance Cases[13]

AmeriFirst Bank v. TJX Co., Civil No. 1:07-cv-l0162 (D. Mass., compl. filed May 9, 2007), 80

Banknorth, N.A. v. BJ's Wholesale Club, 442 F. Supp. 2d 206 (M.D. Pa. 2006),80

Bell v. Acxiom Corp., Civil No. 4:06-CV-00485-WRW, 2006 WL 2850042 (E.D. Ark. 2006), 123

BJ's Wholesale Club, FTC Dkt. No. C-41 48 (Sept. 2005), 130

Cardsystems Solutions, Inc., FTC Dkt. No. C-4168 (Sept. 2006), 131

Cumis Insur. Soc'y v. Merrick Bank Corp., Civil No. BC370409 (Sup 'r. Ct. L.A. Cty., compl. filed May 2, 2007), 80

DSW, Inc., FTC Dkt. No. C-4157 (Mar. 2006), 131

Guess?, Inc., FTC Dkt. No. C-4091 (Aug. 2003), 128

Guidance Software, Inc., FTC Dkt. No. C-4187 (Apr. 2007), 128

Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006), 123

Life is good, Inc., FTC Dkt. No. 072-3046 (Jan. 2008), 129

Mace v. TJX Co., Civil No. 1:07-cv-l0162 (D. Mass., compl, filed Jan. 29,2007), 81

Nations Title Agency, FTC Dkt. No. C-4161 (June 2006), 134, 136

Pa. State Employees Credit Union v. Fifth Third Bank, Civil No. l:CV-04-1554, 2006 U.S. Dist. LEXIS 40066 (M.D. Pa. 2006), 80, 121

Petco Animal Supplies, FTC Dkt. No. C-4133 (Mar. 2005), 128

Sovereign Bank v. BJ's Wholesale Club, 427 F. Supp. 2d 526 (M.D. Pa. 2006),80

Sunbelt Lending Servs., FTC Dkt. No. C-4129 (Jan. 2005), 133

Superior Mortgage Corp., FTC Dkt. No. C-4153 (Dec. 2005), 134

Tower Records, FTC Dkt. No. C-411O (June 2004), 128

United States v. Am. United Mortgage Co., FTC File No. 062 3103 (N.D. Ill. 2007), 134, 135

United States v. ChoicePoint, Inc., FTC File No. 052-3069 (N.D. Ga. 2006), 131

[13] Data Breach Security Handbook (2008), p.149