

Security Breach Notification Laws: Views from Chief Security Officers

*A Study Conducted for the Samuelson Law, Technology & Public Policy Clinic,
University of California-Berkeley School of Law[†]*

December 2007

[†] We wish to thank Olive Huang (JD-MPP 2007) for her assistance in researching and reviewing this paper. This pilot study compliments work by Professors Deirdre K. Mulligan and Kenneth A. Bamberger of UC-Berkeley Law, who are studying the factors that contribute to decision-making by chief privacy officers. It was supervised by Chris Jay Hoofnagle of the Samuelson Law, Technology & Public Policy Clinic. It is part of a comprehensive research initiative regarding Chief Security Officers now underway at the Samuelson Clinic led by Aaron J. Burstein and Professor Mulligan. The work of the Samuelson Clinic is supported by the Institute for Information Infrastructure Protection (I3P), the California Consumer Protection Foundation, NSF Science and Technology Center Team for Research in Ubiquitous Secure Technologies (NSF CCF-0424422), and the Rose Foundation Privacy Rights Fund. The views contained herein are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied, of the US government or any of its agencies.

EXECUTIVE SUMMARY.....	3
METHODS	6
SECURITY BREACH NOTIFICATION LAWS AND ENHANCED SECURITY MEASURES	7
LAWS REQUIRING NOTIFICATION OF SECURITY BREACHES	8
WHAT DO THE BREACHES FOR WHICH NOTIFICATION HAS BEEN PROVIDED TELL US ABOUT SECURITY BREACHES? 10	
<i>Who is disclosing security breaches?</i>	10
<i>What causes the types of security breaches being disclosed?</i>	11
<i>How much are breaches and notification costing organizations that suffer them?</i>	12
WHAT EFFECT HAVE THE NOTIFICATION REQUIREMENTS HAD ON THE SECURITY OF PERSONAL INFORMATION?	13
<i>Effects Within Organizations</i>	13
<i>Effects Across Organizations</i>	22
<i>Effects on Consumers</i>	23
WHAT DOES NOTIFICATION ADD TO THE OTHER FORMS OF REGULATORY AND INDUSTRY PRESSURE?.....	27
HOW CAN NOTIFICATION REQUIREMENTS BE IMPROVED?.....	30
THE NEED FOR A UNIFORM STANDARD FOR ALL SECURITY BREACHES.....	30
REQUIRE NOTIFICATION TO A CENTRALIZED ORGANIZATION IN ADDITION TO CONSUMERS.....	31
CLARIFY DEFINITIONS OF FORMS OF DATA STORAGE EXEMPT FROM NOTIFICATION STANDARDS	31
TIMELINE REQUIRED FOR NOTIFICATION	32
PROVIDE CONSUMER-TARGETED GUIDELINES ON THE CONTENT OF NOTIFICATIONS.....	33
GATHER MORE INFORMATION ON THE APPROPRIATE NOTIFICATION "TRIGGER"	34
CONCLUSIONS AND DIRECTIONS FOR FURTHER RESEARCH.....	35
APPENDIX A: FEDERAL AND STATE REGULATIONS REGARDING BREACH NOTIFICATIONS... 37	
FEDERAL AND INDUSTRY REGULATIONS AND STANDARDS.....	37
<i>Gramm-Leach-Bliley Act (GLB Act) and Enacting Interagency Guidelines</i>	37
<i>Sarbanes-Oxley internal controls requirement (§ 404)</i>	38
<i>Health Insurance Portability and Accountability Act (HIPAA)</i>	39
<i>Payment Card Industry Data Security Standard (PCI)</i>	39
<i>Federal Trade Commission enforcement actions</i>	40
STATE BREACH NOTIFICATION LAWS.....	40
<i>California sets the precedent – S.B. 1386</i>	40
<i>Other states follow</i>	42
APPENDIX B: EXAMPLE OF A BREACH NOTIFICATION LETTER—LEXISNEXIS.....	47
APPENDIX C: SECURITY BREACH NOTIFICATION IMPACT STUDY INTERVIEW QUESTIONS	49

EXECUTIVE SUMMARY

At least 36 states have enacted legislation requiring organizations that possess sensitive personal information to warn individuals of security breaches. California led the way in the creation of these laws, driven by concerns about identity theft and lax information security. In following California's lead, other states have expanded upon the requirements of the California statute by, for example, requiring that organizations report breaches to a state regulatory agency.

Much still needs to be learned about information security practices, security breaches, and the link between these breaches and fraud. However, the proliferation of state laws has driven many businesses to call for federal security breach legislation that overrides state law. Data holders have begun to question whether consumers pay attention to security breaches, and whether most security breaches result in identity theft.

In the midst of calls for federal legislation, survey data collected on identity theft reveals that the crime is becoming more complex and difficult to track. Security breaches no doubt contribute to some identity theft, but it is unclear how much. Also, while some federal proposals require different notification policies based on the size of the security breach, since stealing identities is labor intensive, a small breach may be just as risky as a very large one.

Organizations have not yet formulated notices that communicate security breaches effectively to consumers. The idea that consumers will become inured to notices and ignore warnings is a familiar refrain, but even if some customers ignore notices, apathy among some does not justify abrogating the rights of all to receive notices of security breaches. Furthermore, this problem suggests a remedy of creating better notices, rather than providing none at all.

This study surveys the literature on changes in the information security world and significantly expands upon it with qualitative data from seven in-depth discussions with information security officers. These interviews focused on the most important factors driving security investment at their organizations and how security breach notification laws fit into that list. Often missing from the debate is that, regardless of the risk of identity theft and alleged consumer apathy towards notices, the simple fact of having to publicly notify causes organizations to implement stronger security standards that protect personal information.

The interviews showed that security breaches drive information exchange among security professionals, causing them to engage in discussions about information security issues that may arise at their and others' organizations. For example, we found that some CSOs summarize news

reports from breaches at other organizations and circulate them to staff with "lessons learned" from each incident. In some cases, organizations have a "that could have been us" moment, and patch systems with similar vulnerabilities to the entity that had a breach.

Breach notification laws have significantly contributed to heightened awareness of the importance of information security throughout all levels of a business organization and to development of a level of cooperation among different departments within an organization that resulted from the need to monitor data access for the purposes of detecting, investigating, and reporting breaches. CSOs reported that breach notification duties empowered them to implement new access controls, auditing measures, and encryption. Aside from the organization's own efforts at complying with notification laws, reports of breaches at other organizations help information officers maintain that sense of awareness.

Though security breach notification laws rarely top the list of security professionals' priorities, organizations keenly understand that reputational harm may result from a breach. This has profound consequences in the enterprise. Security breach notification duties lead to more awareness and attention across different levels of management and, in some cases, they have led to specific security measures taken in response to this threat. All the organizations interviewed noted concerns that a public notification of a breach would damage their organization's reputation and the trust behind their name. Almost all the information officers interviewed have at least implemented an incident response plan that formalized the procedures departments would follow to detect and investigate a security breach. In addition, some organizations took specific steps to assess the risk of a security breach, and respond accordingly. Others were satisfied that their security standards were strong enough, and therefore took no further steps.

Security of personal data still is not a marketable characteristic for companies that sell directly to consumers, because consumers are unable to adequately gauge security methods when considering the importance of other product features. However, security is slowly gaining ground as a vital business feature for businesses that interact with and handle the sensitive data of other organizations. Organizations that are strengthening their own security mechanisms are increasingly requiring the same of third party vendors. This pressure strips away the reputation shelter from third party data collectors that lack direct interactions with the general public, and pushes towards a more uniform set of security practices. For instance, a data selling company interviewed for this study now allows external entities to audit its systems.

Based on the benefits described above, this study proposes establishing a uniform set of notification requirements to maximize information exchange about security breaches:

- Establish a uniform standard that requires public notice of all security breaches – to help security professionals track and adapt to incidents at other organizations and to ensure that all affected consumers are being provided with breach notices.
- Establish a uniform reporting standard and require notification to a centralized organization in addition to consumers – to make information on breaches publicly available and allow industry professionals to reference breach reports for information on security vulnerabilities.
- Clarify and broaden technology safe harbor provisions beyond encryption – to give better guidance to organizations on what types of security mechanisms are sufficient to prevent lost data from being accessible for the purposes of misuse and to incubate research into and adoption of other technologies that effectively render personal information useless if accessed without authorization.
- Create a safe harbor period for notifications – to compromise between giving clear instructions on how quickly notifications must be given and providing enough flexibility for organizations to investigate and remedy security breaches.
- Collect more information on the type of notification trigger language that should be used.

Methods

The interview data reported here were gathered over a one-month period through seven separate interviews with information security professionals that possessed responsibilities similar to chief information security officers at their organizations. Interview subjects were selected to cover a broad range of industries. All were employed by organizations that do business in states with security breach notification duties. Interview questions were designed as open-ended, qualitative information gathering instruments. The main topics covered by the interview questions involved internal organizational structure around security investment decisions, regulatory and market factors that affect investment decisions, the organizations' responses to the enactment of security breach notification laws, market effects of security breaches, and industry best practices.

All interview questions and procedures were reviewed and approved for exemption by the University of California Berkeley Institutional Review Board and Office for the Protection of Human Subjects before they commenced. In accordance with the security protocols required by the Office for the Protection of Human Subjects, responses of the interview subjects have been de-identified. All interview responses have been kept confidential and anonymous. Individual respondents have been assigned a unique identifier (A1 through A7), which will be used to refer to their responses. Table 1 lists the main characteristics of the interview subjects' industries, organization, and whether the organization has suffered a security breach requiring public notification.

Table 1: Interview Subjects By Industry, Category, and Other Characteristics

Identifier	Industry Category	Ownership Status	Customer Status (Business to Business and/or Business to Consumer)	Has the organization experienced a breach?
A1	Internet Retail	Public	B2C	No
A2	Software	Public	B2C & B2B	No
A3	Data Collector	Public	B2B	Yes
A4	Telecommunications	Public	B2C & B2B	Yes
A5	Insurance / Financial	Public	B2C & B2B	No
A6	Healthcare	Non-profit	B2C	No
A7	Software	Public	B2C & B2B	No

Security Breach Notification Laws and Enhanced Security Measures

Security breach notification laws are well-positioned to provide incentives for companies to enhance security measures for personal information. An analogy can be drawn here to environmental regulation, where companies that store toxic chemicals are required to register their presence, and report to the public when these chemicals are spilled.¹ Such reporting has reduced the prevalence of toxic releases, and caused chemical companies to internalize the costs of spills. In a similar way, security breach notification statutes cause data collectors to internalize more costs associated with data loss.² To avoid seeming like an irresponsible gatherer of data, organizations will seek to prevent unauthorized information disclosure by enhancing security investments aimed at minimizing risks of losing personal information.

There are, however, some key differences between the toxic release reporting regime and the security breach notification requirements. First, many fewer businesses are subject to the toxic chemical release reporting than security breach notification laws, meaning that the toxic release reporting requirement is more easily monitored and enforced by governing agencies. For security breach notification laws, it is nearly impossible for a government agency to track every security breach that occurs at various organizations to ensure that they are being reported.

Second, the pattern of disclosure that would actually warrant public reprimand in the two areas is markedly different. Toxic release information can be easily compared for similar organizations. Businesses releasing chemical waste are punished when either the amount released is different from what is expected of them or when the amount released is excessive as compared to peers.³ When businesses seek to reduce the amount of toxins being released, their progress can be monitored through the released information. By contrast, data security breaches defy measurement with simple statistics. Consumers only know when a company suffers a breach, a data point that may be a reflection of serious problems, or a simple accident in an organization with otherwise good practices. While notification of a breach may comment on the

¹ See *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Technology and Homeland Security of the Sen. Comm. On the Judiciary*, 110th Cong. (2007) (statement of Deirdre K. Mulligan, Clinical Professor of Law, and Chris Jay Hoofnagle, Senior Staff Attorney, Boalt Hall School of Law), available at <http://judiciary.senate.gov/pdf/3-21-07HoofnagleTestimony.pdf>.

² *Id.*

³ See Madhu Khanna, Wilma Rose H. Quimio & Dora Bojilova, *Toxics Release Information: A Policy Tool for Environmental Protection*, 36 *J. of Environmental Econ. & Management* 243 (1998).

organization's security practices at that point in time, the lack of consistent centralized reporting prevents consumers and regulators from tracking security over time.

Despite the differences, security breach notification laws ultimately do bring to light incidents of security breaches that had remained hidden from public view for years. Furthermore, the initial hit that an organization suffers by having to disclose any security breach, regardless of its magnitude, may encourage organizations to protect more carefully the personal information under their control. This section distills whether such effects exist by reviewing the different regulatory requirements that govern information security, analyzing how security breach notification laws supplement such requirements, and using in-depth discussions with security professionals and industry surveys to evaluate whether and how security breach notification laws have caused them to change their security practices. Furthermore, this section evaluates what other benefits may have arisen from the provision of security breach information.

Laws requiring notification of security breaches

Growing concerns about identity theft and a particularly well-publicized data breach at the Stephen P. Teale Data Center that leaked the personal information of 265,000 California state employees prompted the California legislature to enact the country's first state-level security breach notification law, effective July 1, 2003.⁴ Known as the Security Breach Information Act, AB 700, or Senate Bill 1386 (SB-1386), the statute requires any agency, person, or business that conducts business in California, and "that owns or licenses computerized data that includes personal information" to notify affected residents of California of any security breach in the resident's personal information was, or is reasonably believed to have been accessed by an

⁴ SB-1386 was originally introduced as a way of clarifying that personally identifiable information that was collected by a state agency pursuant to a privacy policy was not subject to public records disclosure requirements. See SB-1386 as introduced, February 12, 2002; Senate Judiciary Committee Analysis, April 2, 2002; Senate Floor Analysis, April 4, 2002; Senate Floor Analysis, April 11, 2002, available at http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=0102&house=B&site=sen. The data breach incident at the Stephen P. Teale Data Center was characterized by a delay of over a month between the breach and discovery, and a delay of another two weeks before employees were notified, during which time unauthorized persons had attempted to access the accounts of several employees whose data was compromised in the breach. The controversy surrounding this breach motivated the original supporter of the bill to modify the bill to require active public notification in cases where personal information was acquired by unauthorized persons. See Analysis of the Assembly Committee on Judiciary, S.B. 1386, June 18, 2002, available at http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=0102&house=B&site=sen.

unauthorized person.⁵ Under the statute, personal information means "an individual's first name or first initial and last name in combination with any one or more of"

- a social security number, driver's license or California Identification Card number, or
- account, credit, or debit card number in combination with any security or access code or password that would allow access to said account.⁶

Notification must be made whenever personal information "was, or is reasonably believed to have been, acquired by an unauthorized person," and must be made without unreasonable delay (unless delay is necessary to comply with a law enforcement investigation). Notice must be provided in writing. If the notifying person or business can demonstrate that notification will cost more than \$250,000 or affect more than 500,000 people, then substitute notice in the form of a website posting and notification to major statewide media can be used. The statute exempts from notification any unauthorized acquisition where the personal information has been encrypted.

At last count, 36 other states have enacted similar data breach notification laws since California's statute went into effect.⁷ While most of these states follow California's examples in many ways, there are some key differences among the statutes.⁸ All of the states have defined "personal information" at least as expansively as California's statute, and many states have expanded the definition to include other forms of personal information, such as email address, alien registration number, passport number, medical records.⁹ Some statutes require notification whenever there is unauthorized access of personal information, while others do not require notification if an organization reasonably determines that harm is not likely to result from the breach.¹⁰

Most notably, New York's statute requires that companies must notify the Attorney General, the Consumer Protection Board, and the State Officer of Cyber Security and Critical

⁵ S.B. 1386, codified at Cal. Civil Code, §§ 1798.29, 1798.82-1798.84.

⁶ *Id.*

⁷ See THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, 32 (2007) [hereinafter COMBATING IDENTITY THEFT]. See also NATIONAL CONFERENCE OF STATE LEGISLATORS, BREACH OF INFORMATION, Apr. 7, 2007, available at <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>.

⁸ For additional detail on the variations in state statutes, see Appendix A.

⁹ See CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, APPROACHES TO SECURITY BREACH NOTIFICATION: A WHITE PAPER, 11-14 (2007) [hereinafter CIPPIC WHITE PAPER], available at http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-print.pdf.

¹⁰ Alabama, Arkansas, Connecticut, Delaware, Florida, Louisiana, New Jersey, North Carolina, Pennsylvania, Rhode Island. CIPPIC WHITE PAPER at 16.

Infrastructure Coordination, and that this agency notification must contain information about the number of individuals affected, and the timing and distribution of the notice.¹¹

What do the breaches for which notification has been provided tell us about security breaches?¹²

Many organizations have analyzed publicly announced security breaches to determine what types of breaches are occurring, what types of information are compromised as a result of these breaches, which sectors tend to experience breaches more often than others, and whether the breaches disclosed are likely to result in identity theft. Trends are difficult to measure from publicly available information alone. Most state notification statutes do not require widespread or formal public acknowledgement of the breach, so many small breaches are silently mailed to the affected consumers without ever being reported publicly to a central authority. Many breach reports also do not contain reliable information on the number of individual records affected. Furthermore, since California's statute was enacted, many other states have copycatted the law. Therefore, depending on the time period of analysis, an increase in the number of incidents may simply mean an increase in the number of organizations that are required to notify. Also, some data sources, while comprehensive, are user-generated and contain security breach data that cannot be confirmed.¹³ Nonetheless, certain findings are consistent throughout most of the studies and are summarized here.

Who is disclosing security breaches?

Over a one- to two-year time period, mostly covering 2005 and 2006, and using publicly available information on data breach announcements, the studies show roughly 200 to 250 breaches. Educational institutions and government agencies reported the greatest number of

¹¹ CIPPIC WHITE PAPER at 18. New Jersey and North Carolina also require reporting to a government agency. New Hampshire's Department of Justice publishes security breach notices online at <http://doj.nh.gov/consumer/breaches.html>.

¹² Note that this paper only discusses trends in security breaches that have been analyzed to date. The Samuelson Clinic is currently conducting an in-depth analysis of security breach letters, and these observations may change depending on the results of that analysis.

¹³ Hasan and Yurcik's study combines databases from Privacyrights.org and Attrition.org, the latter of which contains both confirmed and unconfirmed reports of data breaches. Ragib Hasan and William Yurcik, *Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work* (unpublished working paper) (on file with author).

breaches.¹⁴ However, corporations—particularly financial services companies—have larger breaches, with more identities being exposed per breach.¹⁵

These trends do not necessarily indicate that educational institutions and government agencies are more likely to suffer security breaches than private businesses. Observation here suffers from both underinclusion and overinclusion, because not all government entities are required to notify of security breaches, and because not all entities comply with notification laws. In a survey conducted by CIO Magazine, 11% of the security professional respondents who indicated that they need to be in compliance with SB-1386 also answered that they are not actually in compliance.¹⁶ While this response could reflect that security professionals do not feel that they have instituted the necessary precautionary measures to protect personal information, it could also indicate a large number of companies that have suffered security breaches but have failed to disclose the breach and notify affected consumers.

What causes the types of security breaches being disclosed?

The security breaches divulged thus far indicate that the majority of incidents and personal accounts compromised resulted from intentional unauthorized access – hackers and physical theft.¹⁷ It stands to reason that these forms of data loss are more likely to result in misuse than accidental data loss (such as a missing laptop or accidental disposal) because the people who have gained unauthorized access targeted the information in the first place. Accidental data loss may still result in misuse, when the perpetrator discovers the value of the

¹⁴ Analyzing publicly disclosed security breaches from January 1, 2005 through May 26, 2006, the AARP Public Policy Institute found that educational institutions and government agencies were the most common sources of security breach notifications, together comprising almost 60 percent of all publicly reported security breaches during this period of time, and around 42 percent of the total number of personal accounts compromised. AARP PUBLIC POLICY INSTITUTE, INTO THE BREACH: SECURITY BREACHES AND IDENTITY THEFT (2006) [hereinafter AARP Study], available at http://www.aarp.org/research/frauds-scams/fraud/dd142_security_breach.html. Note, however, that if one takes out the CardSystems breach of June 2005, which alone accounts for over 40 million records compromised, the number of records compromised by educational institutions and government agencies accounts for 76 percent of all personal records lost. Of course, since the number of accounts affected was not disclosed for 35 of the breaches during this time period, these percentages may not be accurate.

¹⁵ Hasan and Yurcik (businesses = 35% of breached identities); IDANALYTICS, NATIONAL DATA BREACH ANALYSIS (2006) (majority of breached identities, even excluding Cardsystems, occurred in the financial services sector) [hereinafter IDANALYTICS DATA BREACH ANALYSIS], available from <http://www.idanalytics.com/>.

¹⁶ CIO MAGAZINE, THE GLOBAL STATE OF INFORMATION SECURITY (2005) [hereinafter GLOBAL STATE OF INFORMATION SECURITY], available at http://www.cio.com/article/11691/The_Global_State_of_Information_Security_.

¹⁷ The AARP study says 62% of incidents and 84% of identities were intentional access. AARP STUDY at 3. idAnalytics says that the majority of incidents were intentional breaches, as opposed to accidental or incidental. IDANALYTICS DATA BREACH ANALYSIS at 3.

data.¹⁸ Lastly, many of the security breaches result from the theft, loss or misplacement of portable storage devices, such as laptops, hard drives, and thumb drives,¹⁹ which emphasizes the fact that technological solutions without employee diligence may not actually help to secure personal information.

How much are breaches and notification costing organizations that suffer them?

To date, the only in-depth study of the costs associated with security breach notifications has been that conducted by the Ponemon Institute. Their 2005 survey found that estimated direct costs, i.e. direct cash outlays, associated with a security breach from detection to notification to ex-post response varied widely among the fourteen companies surveyed. Estimates of direct costs ranged from \$161,600 to over \$23 million.²⁰ The size of the breach, which ranged from 1,600 to 900,000 records, is highly correlated with total direct costs.²¹ However, per notification costs show great variability and are only loosely and negatively correlated with the size of the breach. Direct costs totaled nearly \$70 million, or \$50 per lost record.

Adding indirect costs (time, effort, other organizational resources expended and lost productivity) but not the estimates of the cost of lost customers results in a total of over \$88 million for the 14 entities, or roughly \$64 per lost record.²² Of these total direct and indirect costs, the least costly aspect of breach notification (comprising about 16% of total costs) seems to be detection and escalation, that is, detecting the breach, investigating its source, and determining its scope.²³ While the actual act of notification makes up another 29%, the majority of costs associated with a breach notification have to do with the aftermath of the notification – setting up call centers, engaging in legal counseling and defense services, and compensating victims through payments or discounts on related services.²⁴

¹⁸ COMBATING IDENTITY THEFT at 17.

¹⁹ See, CALIFORNIA OFFICE OF PRIVACY PROTECTION. RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION, 6 (2007) [hereinafter OPP RECOMMENDED PRACTICES], available at <http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf> (stating that 53% of the Office of Privacy Protection's sample set of notice letters were issued as a result of a lost or stolen portable storage device).

²⁰ Larry Ponemon, *What Do Data Breaches Cost Companies? Beyond Dollars, Customers Are Lost*, 4 PRIVACY AND SECURITY LAW REPORT 1310 (2005) [hereinafter PONEMON NOTIFICATION COSTS SURVEY 2005].

²¹ *Id.*

²² However, given the variation in per notification direct costs (indicative of variation in how companies approach their responses) across breaches of different sizes, these per notification estimates are inaccurate estimates of how much a security breach notification *would* cost breaches of similar size.

²³ *Id.*

²⁴ *Id.*

The pervasiveness of notification laws across the country likely causes these costs to increase as more and more consumers fall under breach laws' protection. The follow-on Ponemon survey in 2006 found that these costs increased to \$54 per lost record in direct costs, and an additional \$30 per lost record in indirect costs.²⁵ The study attributed the cost increase to the increase in the number of state laws that required notification.²⁶ Ultimately, however, these estimates provide only rough estimates of notification costs, since a host of factors, many of which may be specific to the organization suffering the breach and its attitude towards customer accountability, play a role in determining the scope of the services provided after the breach.

Another cost that organizations suffer as a result of security breach notifications is lowered stock value. Acquisti et al, analyzed the effect of data breaches on the stock market prices of firms that had publicly announced data breaches. They found that data breaches have a transient, but statistically significant, negative impact on the breaching company's stock price.²⁷ Furthermore, stock market participants appear to react more negatively to announcements by retail firms, intentional or malicious hacking or attempts to access data, and very large data breaches.²⁸

What effect have the notification requirements had on the security of personal information?

Effects Within Organizations

Although organizations have a significant incentive to protect proprietary information such as trade secrets, their incentives to protect sensitive consumer information are less direct. Consumer information is collected by these organizations as part of their business process for a variety of purposes, such a fulfilling orders and marketing. So long as they have that information and it provides them with value in their business process, it is less important to an organization how many other businesses have the same information. Even in the case of data brokers, which license databases that they compile from public records, there are no illusions that their data is

²⁵ *Survey Finds Breach Costs on the Rise in 2006; Productivity, Customer Turnover Affected*, 5 PRIVACY AND SECURITY LAW REPORT 1500 (2006) [hereinafter PONEMON NOTIFICATION COSTS SURVEY 2006]. However, the number of companies in Ponemon's 2006 survey also doubled.

²⁶ PONEMON NOTIFICATION COSTS SURVEY 2006.

²⁷ Alessandro Acquisti, Allan Friedman and Rahul Telang, *Is There a Cost to Privacy Breaches? An Event Study*, Workshop on the Economics of Information Security, 13-15 (2006), <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf>.

²⁸ *Id.*

unique from that obtained by other organizations. Their specific combination might be unique or presented in a more useful format, but the information on each individual account they have collected has already been disseminated.

Many organizations that hold sensitive information do not bear the full cost of identity theft resulting from data loss. Most of those financial costs are borne by consumers and financial institutions. This disconnect between protection and costs is termed a data security externality by Schwartz and Janger.²⁹ Reputation and technological cost concerns aside, these organizations therefore do not have an incentive to keep illicit users from accessing the consumer information they have on file. Furthermore, if the organization never discloses that it suffered a breach, consumers generally would not be able to trace identity theft resulting from a breach back to the originating organization. If other companies are not disclosing data breaches, those that do may become the culprit for an identity theft incident that was not actually a result of their data breach. Without disclosure, then, organizations are not liable for identity thefts, and therefore do not internalize the cost of these thefts into their risk analysis when making resource allocations.³⁰

Interviewees reported that fear of reputation damage, in addition to the notification requirement itself, drives organizations to take steps to at least evaluate, if not correct and enhance, security mechanisms currently in place to protect personal information

Requiring organizations to give notice of breaches exposes them to potential liability, which in turn may encourage them to translate this risk into heightened data protection. Since the sensitive information in their hands is best controlled by them, it makes sense to allocate some of the risk to them to control.³¹ Because of the reputation sanctions that come from the public acknowledgement that security mechanisms have failed or, worse yet, were deficient to begin with, organizations will guard against these costs by increasing security.³² Companies are aware that reporting a data breach or other security event could result in negative publicity. In fact, negative publicity was cited as a reason for not reporting a computer security breach to law

²⁹ Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 928 (2007).

³⁰ *Id.*

³¹ See Ross Anderson and Tyler Moore. *The Economics of Information Security: A Survey and Open Questions*, 314 SCIENCE 610 (2006)("Legal theorists have long known that liability should be assigned to the party that can best manage the risk.").

³² Schwartz and Janger.

enforcement by 48 percent of respondents to the most recent CSI/FBI survey.³³ In addition, over three-quarters of marketing professionals surveyed believe that security breaches have negatively impacted the reputations of companies.³⁴ Nearly three-quarters of the information security professionals that participated in Ernst & Young's survey listed consumer privacy and personal data security issues as the area in which they are being most proactive, because of the negative attention from security breaches.³⁵ These forces and the impact of security breach notification laws on security investment decisions have been confirmed through the interviews conducted for this study.

Among the interview subjects, security breach notifications did not top the list of drivers behind security investment decisions, but neither were they completely ignored. Most of the information officers noted that the notification laws do not have much "bite." After all, the notification laws do not require that specific security measures be implemented. Furthermore, enforcement actions in the form of either consumer lawsuits or regulatory fines were only a remote possibility. Most information officers interviewed were more concerned about the regulatory scrutiny of other agencies such as the Securities Exchange Commission (Sarbanes-Oxley), the Department of Health and Human Services (HIPAA), or one of the financial agencies (Gramm-Leach-Bliley). Even those who acknowledged the possibility of notification fines considered the penalties to be fine amounts fairly small compared to the revenue of the organization.

However, all the organizations interviewed noted concerns that a public notification of a breach would damage their organizations' reputation and the trust behind their name. This was true even though two of the interview subjects who had not suffered a breach thought that the first breach would at least be forgiven, while a second would not. The respondents varied in terms of who the target audience they would be most concerned about was, and these concerns

³³ LAWRENCE A. GORDON, MARTIN P. LOEB, WILLIAM LUCYSHYN AND ROBERT RICHARDSON, COMPUTER SECURITY INSTITUTE, CSI/FBI COMPUTER CRIME AND SECURITY SURVEY, 19-22 (2006) [hereinafter CSI/FBI SURVEY]. Note that, since the survey covers negative security events beyond those that are covered by security notification laws, it is not surprising that so many security events were not reported.

³⁴ CMO COUNCIL, SECURE THE TRUST OF YOUR BRAND: HOW SECURITY AND IT INTEGRITY INFLUENCE CORPORATE REPUTATION, 7 (2006) [hereinafter SECURE THE TRUST: CORPORATE], available at http://www.cmocouncil.org/programs/current/secure_trust.asp.

³⁵ ERNST & YOUNG, ACHIEVING SUCCESS IN A GLOBALIZED WORLD: IS YOUR WAY SECURE? 24 (2006) [hereinafter ERNST & YOUNG SURVEY], available at http://www.ey.com/global/content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2006.

generally tracked specific characteristics of how the organizations generate value. All the interview subjects stated, almost verbatim, that no one wants to have their organization on the front page of the newspaper. A6, an information officer from a non-profit, was concerned that the organization would take a reputation hit among the individuals who fund the organization. A1 and A5 both operate in businesses reliant on consumer trust, and voiced concern that a security breach would harm their reputation among consumers. A2, A3 and A4, while worried about the general public's perception of their organization, were additionally interested in how a security breach affects their reputation among businesses with which they interact, and among others in their industries.

Other surveys reflect this concern about reputation and brand damage. Of those security professionals surveyed in CSO Magazine's latest E-Crime survey, 23% of security professionals who have experienced negative security events cited harm to the organization's reputation as a loss resulting from an electronic crime suffered by the organization.³⁶ This figure represents a significant increase from the 12% who noted reputation harm in 2004.³⁷ Also, the Ernst & Young survey report noted, "While privacy and personal data protection has been in the public limelight for years, the driver behind the issue achieving such a high ranking in this year's survey is the notoriety corporations and government agencies have received from well-publicized lapses in consumer data security..."³⁸

The notification statutes have focused these reputation concerns on the organizations interviewed in such a way that most took some action at the time that the statute was enacted to assess the risks of a security breach and to respond to these risks. Almost all the information officers interviewed have at least implemented an incident response plan that formalized the procedures departments would follow to detect and investigate a security breach. Response plans were seen as a minimum requirement for complying with the notification statutes. These response plans, in turn, have fostered inter-departmental cooperation.

In addition to the response plans, some organizations took specific steps to assess the risk that a security breach would occur, and responded accordingly to lower that risk. Others were

³⁶ CSO MAGAZINE, 2005 E-CRIME WATCH SURVEY (2005), available at <http://www.cert.org/archive/pdf/ecrimesummary05.pdf> [hereinafter 2005 E-Crime Watch Survey]; CSO MAGAZINE, 2006 E-CRIME WATCH SURVEY (2006), available at <http://www.cert.org/archive/pdf/ecrimesurvey06.pdf>.

³⁷ *Id.*

³⁸ ERNST & YOUNG SURVEY at 24.

satisfied that their security standards were strong enough, and therefore did nothing.³⁹ A2 mentioned that the security breach notification laws gave his department the authority to affect information databases being maintained by other departments, and for one particular member of his department to begin locking down these databases through audits, access control, encryption, and secure authentication methods. Furthermore, the reporting and notification requirements mean that his department is involved in making sure that all new databases being created are secure.

A5 noted significant changes to their security policies in addition to the incident response plan. They began with a risk assessment of their information security practices to determine which areas contained the most sensitive information or were at greatest risk for breach. They then implemented data classification standards in the areas that contained the most personal information. In addition, they encrypted back-up tapes, and enacted stringent employee policies on the transport of laptops and portable drives.

A6 also developed new security measures beyond an incident response plan. First, they not only developed the response plan at their own organization, but also audited their information suppliers to make sure that each supplier would execute the plan if it ever suffered a breach of their information. At the time the statute was enacted, the organization did not have a round-the-clock breach alert system. In response, they implemented system mitigation software so that they would be alerted if someone tried to hack into their firewall or virtual private network. For some systems, they purchased data encryption software so that loss of encrypted data would be exempt from the notification requirement. They also established a differentiated badge system such that employees and healthcare providers had different levels of access to different levels of sensitive information.

Encryption has been on the rise at organizations overall because of breach notification laws. One lawyer who concentrates in information privacy has stated that, with the advent of security breach notification laws, encryption is now cost-effective for some organizations, and she is more likely now to advise clients to invest in encryption, especially for portable devices.⁴⁰ Even though encryption is costly, per record costs of encryption might be low if an organization

³⁹ A1, for example, stated that he did not know whether his organization implemented any additional security measures at the time of enactment because he was not yet employed there, but that his organization had begun encrypting databases of personal information in 1999.

⁴⁰ Donald G. Aplin, *Panelists Advise Companies on Navigating the Notification, FTC 'Maze' After the Breach*, 5 PRIVACY AND SECURITY LAW REPORT 481 (2006) [quoting Lisa Sotto of Hunton & Williams].

possess a large store of sensitive information, and might be justified by the high cost of notification itself.⁴¹ A survey of security professionals released in 2005 showed that security breach notification laws were the most influential regulation in the decision to use encryption.⁴² In addition, 55% of security professionals surveyed chose to use encryption in order to prevent data breaches, and another 40% to avoid the reputation harm and notification consequences that would follow from such a breach.⁴³ An updated survey confirms these trends and concerns about security breaches as a driving factor in undertaking encryption, and additionally emphasizes that enterprises are taking more strategy-based approaches to encryption rather than ad-hoc fixes.⁴⁴

Organizations that did not necessarily change any security practices at the time the statute was enacted strengthened their security after experiencing a breach. The individuals responsible for security from A3 and A4, which had suffered data security breaches, noted dramatic changes in security programs undertaken in direct response to those breaches and in the attitude of executive management towards the importance of information security protocols. Therefore, actual breach incidents, and the publicity following from these incidents, have caused organizations to revisit and strengthen their data retention policies and security initiatives.

Notification laws have raised the level of awareness of the importance of information security throughout all levels of a business organization, and have fostered cooperation between information security departments and other departments in an organization

Prevention requires more than adopting heightened technological standards. Many security breaches result from negligence of employees, insider fraud, and poor business processes relating to information security.⁴⁵ Security professionals consider employee negligence and broken business processes much more acute threats to the security of confidential

⁴¹ See, e.g., AVIVAH LITAN, DATA PROTECTION IS MUCH LESS COSTLY THAN DATA BREACHES, Testimony Before the Committee on Veterans' Affairs (2006) [hereinafter LITAN TESTIMONY]. ("For large processing systems, Gartner has seen estimates of \$200,000 for encryption appliances and an equal amount for professional services. Additional fees for process and procedure development and other ancillary concerns would increase the costs to about 20 percent to 25 percent. Gartner estimates that an expenditure of \$500,000 would be feasible for protecting large (100,000 or more customer records) processing systems. This level of protection would cost about \$5 per customer account in the first year, with approximately \$1 per account per year in recurring costs.")

⁴² Larry Ponemon, *National Encryption Survey*, 4 PRIVACY AND SECURITY LAW REPORT 1521, 1522 (2005) [hereinafter PONEMON 2005 ENCRYPTION SURVEY].

⁴³ PONEMON 2005 ENCRYPTION SURVEY at 1522.

⁴⁴ PONEMON INSTITUTE, LLC. 2007 ANNUAL STUDY: U.S. ENTERPRISE ENCRYPTION TRENDS (2007), available at http://download.pgp.com/pdfs/whitepapers/Ponemon_US-EntEncryTrends_Full_070202_F.pdf.

⁴⁵ See Alexei Alexis, *Data Security Breaches Rampant Among Business, Survey Shows*, 6 PRIVACY AND SECURITY LAW REPORT 811 (2007) (reporting that a Ponemon Institute survey revealed the largest threat of security breaches come from lost or stolen data storage equipment, and the second largest threat came from negligent employees, temporary employees, and contractors).

data than hackers.⁴⁶ Two of the most highly publicized breaches, Choicepoint and the U.S. Department of Veterans Affairs (VA), were not the result of a lack of technological protections so much as they were a result of poor business practices. Choicepoint failed to extend information security into customer validation processes, and the VA allowed an employee to take home a laptop containing millions of personally identified records.⁴⁷ As data storage becomes more and more mobile, large amounts of confidential information become more easily accessible. Surveyed security professionals, in fact, acknowledge that it is very likely that PDAs, mobile devices, and laptops all contain unprotected sensitive or confidential information, and that is also likely that they would never be able to determine what actual sensitive data was stored on these devices in the event they were lost or stolen.⁴⁸ What is even more disconcerting is that over 80 percent of these same respondents stated that their organization had suffered a loss or theft of one of these types of storage devices.⁴⁹

The success of information security initiatives, therefore, depends just as much on the awareness of the employees, contractors, and executives implementing them as the design of the initiatives themselves. Most organizations emphasize the importance of using policies, procedures, and close supervision of personnel who have access to sensitive information as a form of reducing the likelihood of a breach.⁵⁰ Surveys of corporate executives and marketing professionals indicate that information security is slowly becoming a business-wide concern, rather than one confined to the information technology department. The trend is true for both executive-level staff as well as workers who carry out day-to-day operations. In a recent survey, over 70% of corporate executives respondents believe that there is a higher degree of concern regarding security issues.⁵¹ Furthermore, almost all corporate executives surveyed were aware of the status of their organization's breach containment action plan.⁵² Another survey shows that increased awareness of the importance of information security has not only helped information security risk become more integrated with overall risk assessment practices at various types of

⁴⁶ PONEMON INSTITUTE, LLC, U.S. SURVEY: CONFIDENTIAL DATA AT RISK, 16 (2006) [hereinafter PONEMON CONFIDENTIAL DATA SURVEY], available at http://www.vontu.com/uploadedFiles/global/Ponemon-Vontu_US_Survey-Data_at-Risk.pdf.

⁴⁷ LITAN TESTIMONY.

⁴⁸ PONEMON CONFIDENTIAL DATA SURVEY at 6.

⁴⁹ PONEMON CONFIDENTIAL DATA SURVEY at 17.

⁵⁰ PONEMON INSTITUTE, LLC, NATIONAL SURVEY ON THE DETECTION AND PREVENTION OF DATA BREACHES, 4 (2006) [hereinafter PONEMON DATA BREACH SURVEY].

⁵¹ SECURE THE TRUST: CORPORATE at 10.

⁵² *Id.*

companies, but has also fostered cooperative effort between different departments in an organization to address information security issues.⁵³

The interviews conducted for this study confirm these trends, and suggest that breach notification laws have significantly contributed to heightening awareness of the importance of information security throughout all levels of a business organization. Almost all of the interview subjects named at least three other departments (most often, legal, human resources, marketing, product development) that worked with the information security department in either developing or implementing security initiatives. For one information officer, cooperation meant working together to develop initiatives, but also delegating responsibility for the protection of whatever sensitive information existed in each department to the head of that department. For another, cooperation meant putting specially trained privacy and security personnel into each department. Three other information officers stated that departments that wanted to access or use sensitive customer information databases had to get clearance and specific security-related instructions from their department before doing so. While some of this cooperation came together as a result of active regulatory compliance with information security standards (such as those required under Sarbanes-Oxley and Gramm-Leach-Bliley), much of it is a direct result of implementing incident response plans, and the need to monitor data access to detect, investigate, and report breaches.

Disseminating information about data security breaches within an organization can help information security professionals obtain more resources to implement higher security standards. Almost all of the interviewed security professionals said that they used the publicity surrounding breaches at other organizations as an awareness tool, as well as using the reported effects as other organizations as a way of tuning management and executive staff into the importance of privacy and security. A7 noted that, although security breach notification laws most directly affect breach responses, raising enough awareness on the response side can then force attention onto breach prevention. Four other interview subjects mentioned the use of media reports and the importance of preventing security breaches as leverage for getting funding for information security. A1 mentioned that media reports of breaches can sometimes be used to justify implementing a new security protocol, or to defend one that has already been implemented. As

⁵³ ERNST & YOUNG SURVEY at 6.

details of security breaches help security officers bring awareness and justification to their investments, barriers to improvements in security policy will slowly fall away.

Security breaches at other organizations provide CSOs with information on new and developing forms of threats

Aside from the organization's own efforts at complying with notification laws, reports of breaches at other entities help information officers maintain awareness in their own organizations. Two information officers reported that, every time another story about a security breach is published (special attention is paid to security breaches of those within the same industry, it seems), they email the story to department heads and other employees in possession of sensitive information. These emails usually include not only a summary of the incident, but also "lessons learned" – what the incident says about how not to take sensitive information home on a thumb drive, for example.

Security breaches at other organizations also help security professionals by providing information on new threats and by helping them justify investments. All but one of the information officers stated that the biggest benefit from the notification laws is the fact that reports help them keep track of new and developing trends (and therefore, what to avoid) and help them educate others in their organization about the continuing threat. Therefore, security breach notifications serve as a new public forum for discussing the trends in the field. A1 mentioned that reports of breaches cause them to examine their own security to determine whether a similar threat exists and to remedy it. Three of the information officers noted that the slew of reports about laptop theft have propelled laptop encryption, previously not considered to be an important security mechanism, to the top of their priority lists. This type of information exchange is crucial to maintain security over time, because attack and theft strategies are often used repeatedly, but also evolve over time.⁵⁴

⁵⁴ See Fred Cate, *Information Security Breaches and the threat to Consumers* 6, Sept. 2005 available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf. ("Recent breaches demonstrate an evolution of attack strategies. As one vulnerability in information security systems was identified and patched, attacks evolved to target other weak spots. Moreover, as leading companies enhanced their information security, attacks have clearly increased against less well prepared institutions.")

Effects Across Organizations

Responsibility for the loss of personal information has resulted in an informal system of industry self-regulation, as organizations are not only strengthening security, but are requiring that other organizations that handle their data meet their standards as well

Industry awareness of information security can have other effects as well. Since organizations are responsible for breaches at third parties, they place pressure on those holding their data to meet their standards. This pressure strips away the reputation shelter that third party data collectors enjoy.⁵⁵ The information officer for the third party data collector interviewed for this report indicated that, as security breach notification laws increase the scrutiny of security measures and raise the reputation stakes, the organization has been feeling more pressure from others to engage in auditing and to enhance security measures. In fact, that organization allows others to conduct external audits on its security systems and authentication processes. The healthcare information officer interviewed confirmed this industry-policing phenomenon from the other side--breaches at two of their subcontractors caused the organization to increase the frequency and scope of the audits that they conduct of those subcontractors' security procedures.

Although organizations respond to reputation concerns among consumers differently, the general increase in awareness among both consumers and businesses means that even businesses that do not interact directly with consumers must increase their security standards. First, because some notification statutes and regulatory guidelines alike require organizations that provide sensitive consumer information to third party organizations, data collectors, or vendors also vouch for the security practices of those organizations, owners of consumer information have taken steps to contractually mandate that third party vendors also establish similar security standards.⁵⁶ The most obvious example of this relationship is the Payment Card Industry Data Security Standard, which established specific guidelines that businesses that accept credit cards must follow. Second, organizations that either have businesses as customers or receive sensitive information from another business often deal with pressure from these businesses to maintain high security standards. A6 affirmed that they conduct security audits of their subcontractors, and that when two of these subcontractors suffered breaches, they increased the frequency and

⁵⁵ Acquisti et al. found that database companies without a traditional business to consumer relationship were far less likely to suffer a reduced stock price following a security breach.

⁵⁶ ERNST & YOUNG SURVEY at 20-22.

scope of these audits. A3 stated that, in order to maintain relationships with its business partners, the organization must have an open-door policy for business partners to come in and conduct audits.

Strong information security, and proof of that strength, is becoming a necessity of doing business with other businesses

The increase in industry awareness has a particularly large impact on B2B servicers, because their customers do have the knowledge and access to information required to shop around. The larger accounts and revenues from B2B customers gives those customers more leverage in demanding higher security standards, particularly when it comes to protecting the business customers' own sensitive information. Even if security does not actually become a competitive advantage for companies that sell to consumers, it is slowly gaining ground as a competitive advantage (or rather, more like a competitive disadvantage if the organization's standards are lax) for companies that sell to businesses. Since many businesses have both consumer and business accounts, the increase in standards resulting simply from heightened awareness therefore benefits consumers as well.

Effects on Consumers

Data breaches have always happened. Security breach notification laws put them in the public's eye. The influx of resulting media reports and the personal experiences that consumers have with identity theft and notification letters have made information security and privacy the hot topic in consumer protection discussions. As a result, more and more consumers are becoming concerned about the security practices at organizations with which they interact. In fact, a 2006 survey showed that about 60% of U.S. respondents indicated that they have become concerned about security recently, and 30% of U.S. respondents indicated that they had always been concerned about security.⁵⁷ In particular, when discussing security, consumers are more concerned about protecting their identity information than financial data.⁵⁸ These concerns seem to be driven by personal experiences with security problems, which in turn have been made more prevalent by the personal notification of security breaches.⁵⁹

⁵⁷ CMO COUNCIL, SECURE THE TRUST OF YOUR BRAND: ASSESSING THE SECURITY MINDSET OF CONSUMERS, 6 (2006) [hereinafter SECURE THE TRUST: CONSUMERS].

⁵⁸ *Id.* at 8.

⁵⁹ *Id.* at 8.

Notification can heighten consumers' awareness of the importance of information security and consumer privacy

Awareness of the importance of information security and privacy can also empower consumers to protect themselves. In a way, notification letters, once a breach actually occurs, shift the responsibility from the organization holding the data onto the shoulders of the consumer. By sending out the letter, the organization has satisfied its legal obligation. Any procedures it chooses to undertake to assist the affected individual in protecting her identity are purely optional, even though the procedures may affect the individual's future perception of the organization.⁶⁰ Many consumers recognize that they hold some responsibility for their own protection against identity theft,⁶¹ particularly because the majority of consumers do not trust that state or federal regulations will protect them from security breaches.⁶² Helping consumers become more aware of the prevalence of identity theft, therefore, not only can help prevent identity thefts resulting directly from the breach, but may also, even if for only a short period of time, make consumers more careful in not falling victim to other sources of identity theft (e.g. phishing).⁶³

Even though information security is not yet a factor on which consumers base their decisions when choosing among different goods and services providers, the influx of media reports about security breaches have at least fostered communication about information security between some consumers and organizations that handle their personal data

Security has a long way to go before it becomes something consumers actually shop for when choosing among competitors. Although most marketing professionals indicate that information security has become a greater concern for customers in the past few years, they have not incorporated information security as a significant theme in their marketing communications.⁶⁴ Security is still not as much of a concern to consumers as the quality of a company's products and services, the way it treats its customers, and the company's honesty and ethics.⁶⁵ Furthermore, different aspects of an industry sector may determine whether or not it is

⁶⁰ PONEMON NOTIFICATION SURVEY at 2.

⁶¹ JAVELIN RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT 5, Jan. 2006.

⁶² PONEMON NOTIFICATION SURVEY.

⁶³ While perhaps invalid as only one data point, and a potentially biased one at that, knowledge and awareness of information security issues and identity theft has certainly made this author more careful about revealing sensitive information.

⁶⁴ SECURE THE TRUST: CORPORATE at 8.

⁶⁵ SECURE THE TRUST: CONSUMERS at 7.

even feasible for consumers to consider security. For example, switching costs may sufficiently high to prevent consumers from switching to another provider of services, even if they disapprove of their current provider's security practices.

Consumers face informational barriers about security investments that make it difficult for them to shop among different companies. While a consumer generally has good information about price, consumers generally have bad information about non-price terms that underlie the price differential.⁶⁶ Even if the full range of security investments were divulged to consumers as part of the marketing process, consumers would have to know whether the organization effectively uses technology and actually implements improved practices. Consumers do not have enough information to judge whether information security is good; they can only tell when something goes wrong that information security is bad.⁶⁷ Furthermore, even when people have sufficient information to make informed choices, they choose to sacrifice long-term privacy for short-term benefits.⁶⁸

Still, 75% of consumers surveyed think that it is very important for corporations to have clear, visible, and comprehensible descriptions of their security practices.⁶⁹ In addition 43% of consumers surveyed in the CMO Council study reported that they have actually stopped a transaction online, on the phone, or in a store due to security questions or concerns.⁷⁰ The message that security is becoming more important to the individual consumer is being conveyed to at least some information officers. The fear that security breaches result in loss of trust seem well-founded. Over 58% of consumers who received a notification announcement indicated that the breach decreased their sense of trust and confidence in the organization sending it.⁷¹ Some industry groups see the possibility of a company's commitment to privacy and security practices becoming an important competitive differentiator.⁷² Furthermore, although most information officers interviewed for this study did not indicate customer churn as a foreseeable consequence of a security breach, about half indicated that security could become a feature that consumers

⁶⁶ Ross Anderson and Tyler Moore. *The Economics of Information Security: A Survey and Open Questions*, 314 SCIENCE 610 (2006).

⁶⁷ *Id.*

⁶⁸ *Id.* (citing Alessandro Acquisti and Jen Grossklags, *Privacy and Rationality: Preliminary Evidence from Pilot Data*, in Third Workshop on the Economics of Information Security (2004)).

⁶⁹ SECURE THE TRUST: CONSUMERS at 13.

⁷⁰ SECURE THE TRUST: CORPORATE at 14.

⁷¹ PONEMON NOTIFICATION COSTS SURVEY at 3.

⁷² ERNST & YOUNG SURVEY at 24.

shop for in the future. At the very least, the lack of reasonable security measures, the type of information that consumers now have easy access to, is becoming more and more of a competitive disadvantage.

Although over 40% of consumers who have experienced security breaches indicate that they might discontinue their relationship with the organization reporting the breach, and another 19% of have reported actually doing so,⁷³ actual customer churn does not seem to be a primary concern of the information officers interviewed. Of the consumers who received notification letters, 33% of them indicated that, although they did not alter their behavior towards the breaching organization, they did not want the incident to happen again.⁷⁴ While some officers indicated that churn was a possibility, all except for one thought that their consumer customers did not evaluate security as part of the organization's services, and others noted that high switching costs and the "sticky" nature of doing business with the organization meant it was unlikely that consumers would leave. Ponemon's estimates of the costs of a security breach show that estimated customer turnover rates vary widely over the 14 security breaches surveyed, anywhere from none at all to 11%, making it difficult to discern whether customer churn is relevant concern.⁷⁵ However, A1 did note that, even if consumers did not leave, a security breach that betrayed consumers' trust might result in a lower volume of transactions.

Security breaches, however, may provide a unique opportunity for companies to communicate with consumers about how they are handling personal information. Notice letters sometimes provide affected consumers with instructions on how to monitor their credit report, as well as print and online resources for more information. In a survey of consumers who had received a breach notice, 12% indicated that their trust in the organization had actually increased because of the manner in which the breach was communicated.⁷⁶ A5 even indicated that, with the advent of breaches at other organizations, he has received correspondence from his consumer customers demanding to know how the organization is protecting their information.

⁷³ PONEMON NOTIFICATION COSTS SURVEY at 3.

⁷⁴ *Id.* at 11.

⁷⁵ *Id.* at Table 1.

⁷⁶ PONEMON NOTIFICATION COSTS SURVEY at 3.

What does notification add to the other forms of regulatory and industry pressure?

All of the organizations interviewed were subject to other forms of regulatory oversight with respect to information security procedures. These regulatory mandates seemed to ride high on the list of priorities faced by the security officers interviewed. Furthermore, the wider population of information security professionals has indicated that regulatory compliance is the top driver of information security practices.⁷⁷

Three of the most frequently mentioned regulations were the Gramm-Leach-Bliley Act and its implementing guidelines, section 404 of Sarbanes-Oxley, and the Health Insurance Portability and Accountability Act (HIPAA). Title V of the Gramm-Leach-Bliley Act authorizes each of the agencies governing financial institutions to establish and enforce guidelines to ensure the security of and protect against unauthorized access to or use of customer data.⁷⁸ These agencies, in turn, have issued two Interagency Guidelines, which, through a combination of standards and regulations, require financial institutions to safeguard personal data by developing reasonable security measures and to develop a formal response plan to deal with data security breaches.⁷⁹ Sarbanes-Oxley compliance efforts are centered around building a sufficient system of internal controls around the personal information gathered from employees, customers, and consumers. Lastly, in implementing HIPAA, the Department of Health and Human Services has issued standards that regulate the manner in which identifiable health information, that is, any information that is created or received by a covered entity and relates to health condition, provision of health care, or payment for provision of health care and that identifies the individual, is protected among covered entities.⁸⁰

Despite the abundance of laws and standards, most of the standards are still fragmented in terms of industries covered, notification requirements, and level of compliance and enforcement. Because the security breach notification requirement of S.B. 1386 is not industry-specific, it covers organizations that may not be subject to any of the other standards. While some entities are covered by statutes like California's A.B. 1950, which mandates that companies

⁷⁷ ERNST & YOUNG SURVEY at 16-19.

⁷⁸ 15 U.S.C. §§ 6801-09.

⁷⁹ Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (2005) [hereinafter Response Guidance]; Interagency Guidance Establishing Information Security Standards, 69 Fed. Reg. 77620 (2004) [hereinafter Security Guidance].

⁸⁰ 45 C.F.R. § 160.103.

maintain reasonable security methods, security breach notification laws provide a public forum for disclosure that a "reasonable standard" does not. Security breach notification laws, in this respect, force companies to realize the costs of security breaches. As a result, these laws might engender a higher level of security standard as well as heighten awareness among all levels of the organization and among consumers themselves.

However, total costs resulting from identity theft have actually been rising slightly, from \$53.3 billion in 2003 to \$56.6 billion in 2006.⁸¹ These figures suggest that identity thieves are becoming more efficient in profiting from stolen identity information before getting caught and having the revenue stream cut off. Identity thieves have changed their methods of using stolen identities in ways that are more difficult to detect and prevent, and may also carry more significant financial and indirect costs.⁸² As one form of attack and misuse becomes easier to detect, and therefore less profitable, fraudsters have not only moved onto more complex and sophisticated forms of identity theft, but have also become more targeted in the entities they steal from and the type of information they seek.⁸³ Law enforcement agencies have also seen increases in the involvement of criminal organizations in identity theft, as well as increases in foreign organized criminals in computer-related identity theft schemes.⁸⁴

The forms of identity fraud are also changing. Results from the Javelin survey show that, while the percentage of the U.S. population experiencing new accounts fraud nearly doubled from 2005 (0.83%) to 2006 (1.52%), existing-accounts fraud declined over this same period by one percentage point.⁸⁵ These trends support the idea that identity thieves are engaging in more complex forms of identity theft that may be more difficult to resolve. Furthermore, research suggests that over 88% of fraudulent accounts are actually opened with synthetic fraud, as opposed to 12% using true-name identity-level data, and that synthetic fraud is accountable for the large majority of financial losses from fraudulent account openings.⁸⁶ Identity thieves are

⁸¹ JAVELIN RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT, 1, Jan. 2006. Significant debate exists concerning the number of incidents and severity of identity theft that occurs, and measurement tools for the crime are both uninclusive in some respects and overinclusive in others. *See Identity Theft: Making the Unknown Known*, 21 Harv. J. of L. & Tech ____ (forthcoming 2007), available at <http://ssrn.com/abstract=969441>.

⁸² *See, e.g.*, SYMANTEC, SYMANTEC INTERNET SECURITY THREAT REPORT. TRENDS FOR JULY--DECEMBER 06 (2007), available at <http://www.symantec.com/business/theme.jsp?themeid=threatreport>.

⁸³ CATE at 6.

⁸⁴ COMBATING IDENTITY THEFT at 13.

⁸⁵ JAVELIN RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT, 12, Jan. 2006.

⁸⁶ Mike Cook, *The LowDown on Fraud Rings*, 10 Collections & Credit Risk 2 (2005).

already highly unlikely to get caught,⁸⁷ and these trends indicate that identity theft will be more difficult to detect, and even more difficult to rectify than before.

Because data thieves are notoriously difficult to track, the large majority of identity theft victims do not know the identity of the person who is misusing their information.⁸⁸ This lack of knowledge makes it all the more difficult for consumers to anticipate identity theft threats and change their behavior either in anticipation of potential identity theft or in response to past identity theft. While consumer diligence is no doubt an important factor in catching, responding to, and mitigating the effects of identity theft, these responses can only be engaged once identity theft *has already occurred*. Therefore, even the most diligent of consumers can only mitigate the financial losses and some secondary costs associated with identity theft, but cannot prevent it from happening. Given the tremendous financial cost to the financial services industry and the pernicious, the lasting effects that identity theft imposes on victims, and the difficulty of tracking down identity thieves, prevention efforts such as limiting access to personal information must be part of the solution.⁸⁹

The difficulty of tracking the origins of electronic information and its use also means that good data on the extent to which breaches actually lead to identity theft is not available. However, notification can provide consumers with a specific point in time from which they need to employ heightened diligence in monitoring their credit reports. With appropriate warnings, consumers can place fraud alerts and active credit monitoring that can shorten the time required to detect fraudulent activity. The faster an identity theft incident is detected, the quicker its resolution time and the lower the ultimate financial cost.⁹⁰ Research indicates that self-detection on the part of consumers results in 48% lower average fraud amounts, 35% shorter detection times, and 36% lower consumer costs.⁹¹ Longer detection times result in higher ultimate financial costs and fraud amounts.⁹² Notification embodies the information-collecting

⁸⁷ RITA TEHAN, CONGRESSIONAL RESEARCH SERVICES, THE LIBRARY OF CONGRESS, PERSONAL DATA SECURITY BREACHES: CONTEXT AND INCIDENT SUMMARIES 3 (2005), available at

<http://www.opencrs.com/document/RL33199/> (citing Gartner report that says identity thieves have a 1 in 700 chance of getting caught, AVIVAH LITAN, UNDERREPORTING OF IDENTITY THEFT REWARDS THE THIEVES (2003)).

⁸⁸ See Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, forthcoming in 21 HARVARD J.L. TECH. ____ (2007)(arguing that lending institutions should disclose data on identity theft incidences because survey research of victims has known limitations).

⁸⁹ GAO IDENTITY THEFT REPORT at 11.

⁹⁰ JAVELIN RESEARCH, 2006 IDENTITY FRAUD SURVEY REPORT 2, Jan. 2006

⁹¹ *Id.*

⁹² *Id.* at 35.

organization's "duty to warn" of dangers,⁹³ which acts as a way for the party who has the knowledge of a danger or potential injury to warn those who lack such knowledge.⁹⁴

The problem arises when those who are warned either do not take act on the warning or do not know how to mitigate the risks. A recent survey shows that 11.3% of the American population, roughly 23 million people, have received a security breach notification within the last year.⁹⁵ Only about half of these initially thought that the communication, whether in letter, email, or telephone form, was an important piece of information; and about 39% originally thought it was junk mail, spam, or a telemarketing call.⁹⁶ There are no data indicating what proportion of recipients simply throw away notification letters, without realizing that it contains a notice of a compromise of their personal information.

How can notification requirements be improved?

The need for a uniform standard for all security breaches

Perhaps the most pressing issue regarding breach notification laws is the need for a uniform requirement. The complexity and variation of the state laws result in piecemeal disclosure of information coming out of the organizations that suffer a breach. For example, some companies may decide to take the least-common-denominator approach to breach notifications and send out notifications to consumers according to the most stringent state law requirements. Even those companies that do this however, may opt to not send out notifications to consumers who reside in states that do not have a state breach notification law. Therefore, not only is the information on the number of consumers affected by any given breach incorrect, but consumers who reside in no-notification states may get a false sense of security because they may believe that the breaches they read about in the news do not affect them. A uniform standard that applies to all security breaches would ensure that all consumers receive the same amount of information coming out of a security breach, and therefore have the same opportunities to protect themselves. The consistency of information disclosure is even more

⁹³ Thomas J. Smedinghoff, *Security Breach Notification – Adapting to the Regulatory Framework*, originally published in THE REVIEW OF BANKING & FINANCIAL SERVICES, 1-2 (2005), available at <http://www.bakernet.com/ecommerce/breachnotification.pdf>.

⁹⁴ *Id.* at 1-2.

⁹⁵ PONEEMON NOTIFICATION COSTS SURVEY at 2.

⁹⁶ *Id.* at 3.

important because one of the primary benefits of the security breach notification laws is that of heightening information exchange and awareness about information security and privacy issues.

Require notification to a centralized organization in addition to consumers

Tracking security breaches, particularly small ones, is difficult because in most states, there is no requirement to notify a central authority. In order for information security to become a characteristic that consumers can take into account when purchasing services, there must be consistent public information on which analysis and information-gathering can be based. Furthermore, a public database of security breaches can serve as an analytical tool for security professionals.

Since the main bite of security breach notification comes from the public notification aspect of the security breach notification laws, requiring organizations that suffer a security breach to take the additional step of filing with a centralized organization could increase the amount of information available about security breaches without compromising the security incentives that notification laws provide. This database would provide a standardized source of information to which security professionals can refer to gather statistics on security vulnerabilities. It would also give media outlets a reliable source of information. Keeping a public database of information would also assist enforcement agencies, such as the Federal Trade Commission, in keeping track of repeat offenders against whom enforcement actions may need to be brought.

Clarify definitions of forms of data storage exempt from notification standards

Encrypting personal information is one method of protecting against unauthorized access. The exemptions for encrypted data provided for in multiple state statutes reflect a general trust in the technology. However, the agencies implementing data security for the Gramm-Leach-Bliley Act chose not to include a blanket exemption for encryption because some implementations do not effectively protect customer information.⁹⁷ This decision reflects a disconnect between "encryption" in the state statutes and the level of encryption necessary to protect consumer data.

⁹⁷ Response Guidance, 70 Fed. Reg. at 15745.

"Encryption" is not defined in California's statute, although some states have defined encryption in their statutes.⁹⁸ However, the California Office of Privacy Protection did issue a set of "Recommended Practices on Notice of Security Breach Involving Personal Information" which recommends that data encryption meet the National Institute of Standards and Technology's Advanced Encryption Standard.⁹⁹ If encryption is truly a type of technology that secures personal information from unauthorized use, then notification laws should clarify what minimum levels of encryption technologies should be used to qualify for the exemption from notification. However, because encryption is an evolving technology, it seems better suited for definition and reevaluation by regulatory agencies than strict definitions in statutes.

In contrast, the President's Identity Theft Task Force has, instead, opted to exclude data on the basis of "unusability."¹⁰⁰ The Task Force invoked this concept to imply that organizations can render data unusable in ways other than using encryption. Aside from noting that "unusability is not a static concept and the effectiveness of particular technologies may change over time," the Task Force did not provide any further definition.¹⁰¹

Without further definition, "unusability" is a vague concept that does not necessarily assist organizations in deciding which technologies sufficiently exempt them from notification requirements. As a result, vague terminology should be replaced with guidelines, to be issued by a federal oversight agency, that specify what types of technologies may be considered to be adequate in preventing lost consumer information from being accessed and misused.

Timeline required for notification

Most of the notification statutes only require that organizations notify within "reasonable amount of time," and allow for delays where necessary to comply with law enforcement. However, some organizations that have suffered data breaches have delayed for long periods of time before notifying customers. For example, the University of California at San Diego waited nearly three months to notify students and alumni of a potential breach.¹⁰² These instances suggest that "reasonable amount of time" may leave too much room for interpretation.

⁹⁸ CIPPIC WHITE PAPER at 14.

⁹⁹ *Id.* at n. 50.

¹⁰⁰ COMBATING IDENTITY THEFT at 36.

¹⁰¹ *Id.* at 36.

¹⁰² See IDENTITY THEFT RESOURCE COUNCIL. 2005 DISCLOSURES OF U.S. DATA INCIDENTS (2005), available at <http://idtheftmostwanted.org/ITRC%20Breach%20Report%202006.pdf>.

On the one hand, shortening the time period during which companies must notify may give consumers the greatest amount of "head start" in monitoring their credit reports and minimizing financial losses from any potential misuse of information. On the other hand, each data breach is different in terms of scope and effort required to discover and diagnose, such that a rigid compliance window may actually cause more harm than good. In one case, a laptop theft triggered one company to prepare notifying millions of potentially affected customers. However, an investigation later revealed that the laptop was stowed away by a security guard for later removal, but had neither been accessed nor removed from the company's premises.¹⁰³ A rigid compliance window may have required this company to notify before its investigation was complete, and might have resulted in wasted consumer efforts in monitoring their identity files, and would at least have greatly contributed to envelope fatigue. Sometimes publicly admitting a breach may also make an organization more vulnerable to attacks for a short period of time if notification occurs before the company is able to patch the vulnerability.¹⁰⁴

A compromise of these two methods might be a two-part notification process. Organizations should have a set time limit (e.g. 30 days) during which they must provide notification to both the regulatory agency and to consumers if they can reasonably do so with an investigation of the breach. If, after 30 days, the organization cannot isolate the source of the breach or patch the vulnerability, the organization should notify the regulatory agency of the need for an extension, and specify why. In other words, this system provides for a 30 day safe harbor during which notification is presumed to be timely, while providing flexibility for situations in which 30 days is insufficient to remedy the breach or complete the investigation.

Provide consumer-targeted guidelines on the content of notifications

Notifications can only provide value to consumers if they have useful information about the incident and know what steps can be taken to mitigate the harm. Notifications provide an opportunity for consumer education that, unfortunately, has been bypassed by notification letters that focus more on obfuscated language and legal jargon than direct communication (see Appendix B for an example of a breach notification letter). Breach notification letters are difficult to read and understand; 28% of the individuals receiving a notification do not

¹⁰³ Reece Hirsch, *Ten Common Mistakes in Responding to a Data Breach Incident*, 5 PRIVACY AND SECURITY LAW REPORT 338 (2006).

¹⁰⁴ Donald G. Donald G. Aplin, *Panelists Advise Companies on Navigating the Notification, FTC 'Maze' After the Breach*, 5 PRIVACY AND SECURITY LAW REPORT 481 (2006).

understand the data involved or the potential consequences of the breach after reading the letter.¹⁰⁵ Notification laws, therefore, should incorporate some basic guidelines regarding clarity of language, a description of the incident, and steps that consumers can take to protect themselves to as to facilitate communication between the breaching organization and the consumer. A specific analysis of the failures of breach notification letters is being conducted by other members of the Samuelson Law, Technology & Public Policy Clinic. Their findings should contribute useful data to the discussion of what constitutes a "good" notification letter.

Gather more information on the appropriate notification "trigger"

The overuse of breach notifications may present the danger of desensitizing consumers, even though they provide a valuable resource for security professionals. A deluge of notification letters threatens the amount of attention consumers will pay to the issue of data security. Of the types of data breaches that are being reported to consumers, it stands to reason that some forms of data breaches can be eliminated from the reporting pool without detriment to consumers' ability to protect themselves. For example, Chase Card Services notified 2.6 million Circuit City credit card holders that computer tapes containing their personal information were mistakenly thrown in the trash. Further investigation of the incident by "federal and local authorities" led Chase to believe that the tapes were "compacted, destroyed and buried in a landfill."¹⁰⁶ The records in this incident posed no threat of revealing personal information, yet Chase no doubt spent a considerable amount of money notifying the 2.6 million customers, and the letter might have hardened some of those 2.6 million consumers to the importance of data security. As David Walker of the Government Accountability Office noted, "Unnecessary notifications of breaches when there is little or no risk that the data will be misused might cause unnecessary risk or confusion, and might numb consumers to the notifications and cause them to fail to act when the threat is actually great."¹⁰⁷

This risk raises the importance of finding the correct "trigger" language that balances the amount of useful information about security breaches that can flow from the notification with the impropriety and impracticability of sending out notification letters in cases like the Chase

¹⁰⁵ PONEMON NOTIFICATION COSTS SURVEY at 11.

¹⁰⁶ See IDENTITY THEFT RESOURCE COUNCIL. 2006 DISCLOSURES OF U.S. DATA INCIDENTS (2006), "Chase Card Services," September 2006 (quoting Associated Press Newswires, Sep. 7, 2006).

¹⁰⁷ DAVID M. WALKER, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, PRIVACY: PREVENTING AND RESPONDING TO IMPROPER DISCLOSURES OF PERSONAL INFORMATION, Testimony Before the Committee on Government Reform, House of Representatives. GAO-06-833T, 14 (2006) [hereinafter GAO PREVENTING AND RESPONDING].

example above. Given the lack of reliable information available about the number of total security breaches and consumers' responses to them, more time is needed before this balance can be accurately reached. However, it is important to note the substantial difference between a standard that *exempts* notification when an organization finds that there is no risk versus a standard that requires notification *only* when an organization finds a risk of misuse. Both standards present obvious challenges. The former standard requires the investigation to prove a negative, and thus limits notice exemptions. The latter standard does not take into account the fact that organizations' investigative abilities regarding who has accessed the data are limited, and that organizations may not always be able to make a determination that the data is or is not likely to result in misuse. Where this determination is available, notification should depend on the results of that determination. However, when the investigation cannot make a determination on risk, notification should be required, because these are the situations in which consumer efforts to monitor and catch identity theft incidents on their own are most needed.

Conclusions and Directions for Further Research

While much is unknown about identity theft, it seems clear that identity theft remains a pervasive problem, and one that is becoming more complicated to diagnose and remedy. Even not knowing the degree of connection between identity theft and security breaches, the notification of security breaches that occur has resulted in certain benefits that push towards greater protection of consumer information. Chief among these benefits is an increase in the amount of awareness, attention, and vigilance that is dedicated to rectifying information security vulnerabilities through multiple levels of society--consumers, information security professionals, and management at different levels. The tools through which security breach notification laws exert an influence over organizations and consumers are public awareness, education, and self-regulation in the industry. Changes in security breach notification laws, therefore, should leverage these tools to maximize the informational advantages and to spread awareness to other topics that involve identity theft.

Much work remains to be done, however, in evaluating the effect of security breach notification laws for more resource-constrained organizations and for smaller organizations that are not as subject to public scrutiny as the organizations interviewed in this study. Information gathered from security breach notification letters suggests that educational institutions and government agencies report a large amount of data losses. These conclusions, of course, are

subject to the caveat that these organizations may just be reporting more incidents. While these institutions may be subject to the same type of reputation hit that private companies and non-profits endure, studies suggest that organizational limitations and funding pose more of a barrier to information security in these institutions.¹⁰⁸ More work needs to be done to understand how the issues around the protection of personal information are different from educational and government institutions, and how to best approach the solutions.

The larger the organization, the more important a brand name and reputation becomes to its ultimate success. The relationship between the tools wielded by security breach notification laws and smaller, private businesses are less clear. Smaller businesses may be more susceptible to customer churn, but they are also less likely to be caught if they choose not to notify. In fact, very few unrecognizable names show up on the lists of data breaches. Because of the resource constraints on small businesses, more research is needed to understand how to strike a balance between providing incentives to actually notify in cases of breaches and helping them to protect personal information without incurring staggering costs that could impeded their ability to operate at all.

¹⁰⁸ See, e.g., LINDA D. KOONTZ AND GREGORY C. WILSHUSEN, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION SECURITY: LEADERSHIP NEEDED TO ADDRESS WEAKNESSES AND PRIVACY ISSUES AT VETERANS AFFAIRS, Testimony Before the Subcommittees on Disability Assistance and Memorial Affairs and on Economic Opportunity, Committee on Veterans' Affairs, House of Representatives. GAO-06-897T (2006); CDW-G, CDW-G HIGHER EDUCATION IT SECURITY REPORT CARD 2006, 19 (2006) ("While administrators support their IT organizations and recognize the vital nature of network security, they are not backing them with enough IT funding or resources.").

APPENDIX A: Federal and State Regulations Regarding Breach Notifications

Regulatory compliance plays an important role on the list of priorities of information security professionals. In the CSI/FBI survey, policy and regulatory compliance ranked second in terms of what respondents perceived as the most critical computer security issues facing them.¹⁰⁹ This section summarizes only some of the major regulations and standards affecting information security at private institutions, and their effect on information security practices.

Federal and Industry Regulations and Standards

Gramm-Leach-Bliley Act (GLB Act) and Enacting Interagency Guidelines

Title V of the Gramm-Leach-Bliley Act provided authority for each of the agencies governing financial institutions (the Federal Deposit Insurance Corporation, Office of Comptroller of the Currency, Federal Reserve System, Federal Savings & Loan Insurance Corporation, and the Office of Thrift Supervision) to establish and enforce guidelines to ensure the security of and protect against unauthorized access to or use of customer data.¹¹⁰ These agencies have issued two Interagency Guidelines requiring financial institutions to safeguard personal data by developing reasonable security measures and requiring financial institutions to develop a formal response plan to deal with data security breaches.¹¹¹ The security guidelines require that financial institutions conduct risk assessments where the particular security measures will depend on the risks presented by the complexity and scope of the business.¹¹² They also require that financial institutions "consider, and adopt what is appropriate of, the specific security measures enumerated in the Guidelines, including access controls on customer information systems, background checks for employees, and incident response programs."¹¹³ Furthermore,

¹⁰⁹ LAWRENCE A. GORDON, MARTIN P. LOEB, WILLIAM LUCYSHYN AND ROBERT RICHARDSON, COMPUTER SECURITY INSTITUTE, CSI/FBI COMPUTER CRIME AND SECURITY SURVEY, 4 (2006). Data protection (data classification and encryption) and application software vulnerability security was listed as the most critical computer security issue, while identity theft and leakage of private information came in third.

¹¹⁰ 15 U.S.C. § 6801-09.

¹¹¹ Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (2005) [hereinafter Response Guidance]; Interagency Guidance Establishing Information Security Standards, 69 Fed. Reg. 77620 (2004) [hereinafter Security Guidance].

¹¹² *Id.*

¹¹³ *Id.*

the guidelines require the financial institutions monitor its service providers' compliance with these guidelines through contracts.¹¹⁴

The security breach program set up by the Interagency Guidelines has two aspects. First, the financial institution must immediately notify its oversight regulatory agency the moment a financial institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.¹¹⁵ The Guidelines do not require that individual consumers be notified of a security breach unless, upon reasonable investigation, the financial institution determines that misuse of the customers' personal information has occurred or reasonably possible.¹¹⁶ The Guidelines, however, do not exempt information protected by encryption based on its encrypted status alone, because "there are many levels of encryption, some of which do not effectively protect customer information."¹¹⁷

Sarbanes-Oxley internal controls requirement (§ 404)

Sarbanes-Oxley section 404 requires companies that are registered under the 1933 Securities Act build a sufficient system of internal controls "around the safeguarding of assets related to the timely detection of unauthorized acquisition, use or disposition of an entity's assets that could have a material effect on the financial statements."¹¹⁸ Because personal information gathered from employees, customers, and consumers and maintained in databases are unique assets for a publicly-traded company, protecting personal information becomes a compliance requirement under Section 404. Public companies must disclose, in their annual filings, the system of internal controls that the company has in place to protect information and report inaccuracies, and must also attach an internal report of how the internal controls are working. Internal controls therefore "cover an enormous range of methods and procedures that an organization employs to ensure it is using resources as intended, preventing fraud, protecting assets from damage, and so on."¹¹⁹ Penalties for non-compliance under Sarbanes-Oxley include

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 15745.

¹¹⁸ Kim Getgen, *Ten Questions About Sarbanes-Oxley Compliance*, COMPUTERWORLD, Mar. 30, 2005, <http://www.computerworld.com/securitytopics/security/story/0,10801,100646,00.html>.

¹¹⁹ Anindya Ghose and Uday Rajan, *The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare*, Working paper submitted to Workshop on Economics of Information Security 2006, 3 (2006).

investigations by the Securities Exchange Commission, criminal and civil prosecution, and monetary and criminal penalties.¹²⁰

Health Insurance Portability and Accountability Act (HIPAA)

Passed in 1996, but implemented through regulations issued by the Department of Health and Human Services, these standards for protecting identifiable health information cover healthcare providers, health plans, healthcare clearinghouses (i.e., processors of health information), and business associates that contract with these entities to provide services that involve the use of health information.¹²¹ The standards regulate the manner in which identifiable health information, that is, any information that is created or received by a covered entity and relates to health condition, provision of health care, or payment for provision of health care and that identifies the individual, is protected and exchanged among covered entities.¹²² The standards set forth three sets of requirements regarding Administrative Safeguards, Physical Safeguards, and Technical Standards that cover standards that must be followed to ensure the security of identifiable health information, but are flexible enough to allow different entities to implement according to their specific characteristics.¹²³

Payment Card Industry Data Security Standard (PCI)

The PCI standard differs from the regulations mentioned because it is an industry-promulgated standard, rather than a government regulatory standard. The five major credit card brands announced in September 2006 that they would establish a formal council to oversee the implementation of the PCI standard. Thus far, there has been low compliance with the standard, although card issuers are now emphasizing compliance as a result of security breaches.¹²⁴ The council releases security standards that any entity that processes, stores, or transmits credit card information is required to implement. Requirements may differ among merchants, because they

¹²⁰ Kim Getgen, *Ten Questions About Sarbanes-Oxley Compliance*, COMPUTERWORLD, Mar. 30, 2005, <http://www.computerworld.com/securitytopics/security/story/0,10801,100646,00.html>.

¹²¹ 45 C.F.R. § 160-64.

¹²² 45 C.F.R. § 160.103.

¹²³ 45 C.F.R. §§ 164.308, 164.310, 164.312.

¹²⁴ "The PCI Data Security Standard has thus far prompted relatively little action by merchants. Visa recently estimated that only 22 percent of the largest merchants (those that handle more than 6 million credit card transactions per year) are PCI-compliant today, but it expects that number to climb dramatically by the end of 2006. Visa also estimates that 72 percent of the largest merchants have conducted an initial PCI audit, identified their deficiencies and have a remediation plan in place to achieve full compliance." Reece Hirsch, *Merchants Can No Longer Ignore The PCI Data Security Standard*, 5 PSLR 1408 (Oct. 9, 2006).

are separate into four levels of standards depending on the volume of credit card transactions they perform on an annual basis. Enforcement is delegated to individual brands, where each individual brand sets up certification requirements that follow the guidelines and establishes fines for non-compliance. The PCI standard sets out specific guidelines with which merchants must comply, including technical standards (such as encryption standards under which credit card information may be stored), and process standards (for how long credit card information may be stored).

Federal Trade Commission enforcement actions

The Federal Trade Commission has become an active regulator of security policies. The FTC has instituted enforcement actions against numerous companies, arguing that the failure to implement sufficient security protection constitutes "unfair" or "deceptive" trade practices in violation of the FTC Act section 5(a), regardless of whether the investigated company had made any false representations as to its state of security.¹²⁵ As opposed to the other regulatory instruments that apply to specific industries, FTC actions have essentially expanded information security concerns and regulation to unregulated industries, taking action on at least 8 instances of data security breaches: Eli Lilly, Microsoft, Guess, Petco, Superior Mortgage Corp, BJ's Wholesale Club, DSW Shoe Warehouse, and Choicepoint.¹²⁶

State breach notification laws

California sets the precedent – S.B. 1386

Growing concerns about identity theft and a particularly well-publicized data breach incident at the Stephen P. Teale Data Center that compromised the personal information of 265,000 state employees prompted the California legislature to enact the country's first state-level security breach notification law, effective July 1, 2003.¹²⁷ Known as the Security Breach

¹²⁵ Steven C. Bennett, *Data Security Breaches: Problems and Solutions*, 5 PRIVACY AND SECURITY LAW REPORT 1619, 1620 (2006); see also Thomas J. Smedinghoff, *The Corporate Duty to Provide Information Security*, 5 PRIVACY AND SECURITY LAW REPORT 178, 179-80 (2006).

¹²⁶ Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007).

¹²⁷ SB-1386 was originally introduced as a way of clarifying that personally identifiable information that was collected by a state agency pursuant to a privacy policy was not subject to public records disclosure requirements. See SB-1386 as introduced, February 12, 2002; Senate Judiciary Committee Analysis, April 2, 2002; Senate Floor Analysis, April 4, 2002; Senate Floor Analysis, April 11, 2002, available at http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=0102&house=B&site=sen. The data breach incident at the Stephen P. Teale Data Center was characterized by a delay of over a month between the breach and discovery, and a delay of another two weeks before employees were notified, during which time unauthorized persons had attempted to access

Information Act, or Senate Bill 1386 (SB-1386), the statute requires any agency, or personal or business that conducts business in California, and "that owns or licenses computerized data that includes personal information" to notify affected residents of California of any security breach in the resident's personal information was, or is reasonably believed to have been accessed by an unauthorized person.¹²⁸ The key elements of the statute are as follows:

Affected Entities – The disclosure and notification requirement of SB-1386 reaches "any person or business that conducts business in California," provided that such person or business "owns or licenses computerized data that includes personal information." Sections 1798.82-1798.84 do not specifically define "owns or licenses," but the preceding section 1798.81.5¹²⁹ states that "the phrase 'owns or licenses' is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates."¹³⁰ Notably, the statute does not apply to organizations that are in mere possession of data, or those who process it on another organization's behalf. The duty to notify applies to state agencies, but not county or city-level government entities.

Type of Data Affected – California's notification statute generally covers any type of computerized data that includes "personal information," where "personal information" means "an individual's first name or first initial and last name in combination with any one or more of" a social security number, driver's license or California Identification Card number, OR account, credit, or debit card number in combination with any security or access code or password that would allow access to said account.

However, only a breach that results in unauthorized acquisition of unencrypted personal information, where any of the data elements named above is not encrypted. Therefore, if a laptop is stolen, but all the personal information contained on the laptop is encrypted, notification would not be required.

the accounts of several employees whose data was compromised in the breach. The controversy surrounding this breach motivated the original supporter of the bill to modify the bill to require active public notification in cases where personal information was acquired by unauthorized persons. *See* Analysis of the Assembly Committee on Judiciary, S.B. 1386, June 18, 2002, available at http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1386&sess=0102&house=B&site=sen.

¹²⁸ S.B. 1386, codified at Cal. Civil Code, §§ 1798.29, 1798.82-1798.84.

¹²⁹ Note that section 1798.81.5 was enacted after S.B. 1386.

¹³⁰ Cal. Civ. Code § 1798.81.5.

Notification Trigger – Under SB-1386, disclosure and notice is mandated when personal information "was, or is reasonably believed to have been, acquired by an unauthorized person." While "unauthorized person" is not defined, the statute excludes good faith acquisition of personal information by an employee or agent from the notification requirement, "provided that the personal information is not used or subject to further unauthorized disclosure."

Notification Timeline – Notification must be made in the most expedient time possible and without unreasonable delay, although the statute allows for delay in order to comply with law enforcement's attempts at a criminal investigation or other procedures necessary to determine the scope of the breach and restore the integrity of the data.

Type of Notice Required – A company that suffers a security breach must provide notice in one of the three forms provided for under the statute – written notice, electronic notice (if the person affected as previously consented to receiving electronic records in place of paper records, as allowed for under 15 U.S.C. § 7001), or substitute notice if the agency, person or business demonstrates that the cost of providing notice under the preceding two forms would be greater than \$250,000, or the number of affected persons is greater than 500,000. Substitute notice must take the form of e-mail notice where possible, posting information related to the breach on the organization's website, and notification to major statewide media. However, the statute also provides an organization that develops their own notification procedures as part of an information security policy for the purposes of protecting personal information will be deemed to be in compliance with the notice requirement if they provide notice in accordance with their own procedures and they meet the timing requirements of the statute (i.e., as expedient as possible, without impeding efforts to recover / restore the data or investigate the security breach incident).

Other states follow

At last count, 36 other states have enacted similar data breach notification laws since California's statute went into effect.¹³¹ While most of these states follow California's examples in many ways, there are some key differences between the statutes. Because many organizations that collect personal information conduct operations in more than one state, and because it requires too much effort to cater notification plans in response to each individual state, most organizations will notify customers according to the most stringent set of requirements.

¹³¹ See COMBATING IDENTITY THEFT at 32. See also <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>.

Furthermore, some companies will notify consumers even in states without notification requirements, because once the breach becomes public information, consumers who were affected but did not receive notice feel "slighted," resulting in a public relations disaster.¹³²

Affected Entities – Almost all of the other state statutes follow California's applicability to any agency, person or business that "owns or licenses" personal information, although a few states exempt government agencies from some of the sanctions associated with non-compliance.¹³³ Illinois and Delaware expanded California's definition to include all anyone who handles, collects, or otherwise deals with personal information.¹³⁴ In contrast, Georgia's breach notification statute only applies to the much smaller subset of organizations covered under its definition of "information brokers."¹³⁵ Furthermore, some states exempt organizations that are already covered under the provisions of and regulations associated with the Gramm-Leach-Bliley Act.¹³⁶

Type of Data Affected – All of the states have defined "personal information" at least as expansively as California's statute, and many states have expanded the definition to include various others forms of personal information. These types of personal information include, among others, the following types of information:

- Email address
- Mother's maiden name
- Date of birth
- Alien registration number
- Passport number
- Employer or tax ID number

¹³² See David Bender, *Security Breach Notification Laws and FTC Activity Induce Enhanced Security*, 23 THE COMPUTER & INTERNET LAWYER, 3 (2006).

¹³³ Florida H.B. 481, effective July 1, 2005 (exempting government agencies from administrative fines stemming from failure to notify consumer reporting agencies under the specified conditions).

¹³⁴ Illinois H.B. 1633, effective Jan. 1, 2006; PERKINS COIE, SECURITY BREACH NOTIFICATION CHART (2005) [hereinafter PERKINS COIE NOTIFICATION CHART], available at <http://www.perkinscoie.com/statebreachchart/>. See, e.g., Delaware Code, s. 12B-102(b), online: <<http://www.delcode.state.de.us/title6/c012b/index.htm>> [Delaware Act]. CIPPIC WHITE PAPER, 17.

¹³⁵ Georgia S.B. 230, effective May 5, 2005. PERKINS COIE NOTIFICATION CHART. "Information brokers" under the Georgia statute is defined as "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes." *Id.*

¹³⁶ CIPPIC WHITE PAPER at 16-17.

Medicaid or food stamp account number
Biometric data / fingerprints
Medical records
Insurance policy number
Department of Transportation operator's number
Unique electronic number, address or routing code

In Montana, a social security number alone, without additional information, constitutes "personal information."¹³⁷

Notification Trigger – The area in which the state statutes show the most variation is the event that triggers customer notification, and to whom the organization must provide notification. Most states follow California's example in requiring notification whenever there is a reasonable belief that unauthorized acquisition of personal information has occurred, and exempting good faith acquisitions by employees or agents provided that the information is not further disclosed. Connecticut and New Jersey broaden this even further, requiring notification whenever there is unauthorized access of personal information. However, many states have also narrowed California's notification trigger by exempting notification to consumers only if, upon a reasonable investigation, the organization reasonably determines that harm is not likely to result to individuals whose information is compromised by the breach.¹³⁸ Vermont requires that, if an organization makes such a determination, the organization must provide notice and an explanation to the Attorney General or to the applicable department of banking, insurance, securities and health care administration.¹³⁹

Notification Timeline – Some states have enacted statutes that require specific timelines for notice. Florida requires that businesses that own data must notify within 45 days of discovery of the breach, and businesses that license data must notify within 10 days.¹⁴⁰ Ohio requires notification within 45 days of discovery. Most other states, however, follow California's standard, and allow for delay where notification would impede investigation by law enforcement.¹⁴¹

¹³⁷ *Id.* at 11-14.

¹³⁸ Alabama, Arkansas, Connecticut, Delaware, Florida, Louisiana, New Jersey, North Carolina, Pennsylvania, Rhode Island. *Id.* at 16.

¹³⁹ *Id.* at 16.

¹⁴⁰ *Id.* at 18.

¹⁴¹ *Id.* at 18.

Type of Notice Required – Most states follow California’s standard for written notice, but also allow for some other form of notice in place of written notice under special circumstances. Most states allow for substitute notice through electronic mail or by media reports to statewide media, although the circumstances under which companies may utilize substitute notice may be more lax than those provided by California. Ohio and Delaware permit telephone notice in addition to notice by mail.¹⁴² In Maine, for example, substitute notice is permissible if the cost of notification is greater than \$5,000 or the number of consumers affected is more than 1,000.¹⁴³

Other Provisions – State statutes enacted since California’s statutes have also added provisions that did not exist in California’s statute. Most notably, some statutes require that companies provide notification to a state regulatory agency in addition to providing notice to the consumers, and/or establish a particular state agency as an oversight agency for monitoring compliance with the statute. New York, in particular, requires that companies must notify the Attorney General, the Consumer Protection Board, and the State Officer of Cyber Security and Critical Infrastructure Coordination, and that this agency notification must contain information about the number of individuals affected, and the timing and distribution of the notice.¹⁴⁴ The New York’s Office of the Attorney General recently announced they reached the first settlement under the notification law with CS Stars, LLC, a Chicago-based claims management company, for not notifying consumers affected by a breach for two months.¹⁴⁵ The Texas statute, in addition to allowing the attorney general to enjoin the activities of the business for failure to comply, also provides for civil penalties, and equitable and declaratory relief for identity theft victims.¹⁴⁶

State statutes vary in some additional ways. Some states require that consumer reporting agencies be notified if the security breach passes certain thresholds, such as the number of consumers affected.¹⁴⁷ Some states that did not have data destruction laws preceding the enactment of the security breach notification laws added a data destruction requirement to their

¹⁴² *Id.* at 17.

¹⁴³ *Id.* at 17.

¹⁴⁴ *Id.* at 18.

¹⁴⁵ Sharon Gaudin, *N.Y. AG Gets First Settlement Under Security Breach Notification Law*, Information Week, Apr. 27, 2007, http://www.informationweek.com/software/showArticle.jhtml?articleID=199202218&cid=RSSfeed_TechWeb (last accessed Apr. 30, 2007).

¹⁴⁶ Texas S.B. 122.

¹⁴⁷ Minnesota (more than 500); Indiana (more than 1,000); Florida.

notification statutes.¹⁴⁸ Lastly, some states also added specific "security freeze" provisions, allowing consumers affected by security breaches (and others) to place a security freeze on their credit reports that would require all third party requests for credit information to be pre-approved by the consumer.¹⁴⁹

¹⁴⁸ Arkansas; Montana; Nevada; Rhode Island; Tennessee.

¹⁴⁹ CIPPIC WHITE PAPER at 19.

APPENDIX B: Example of a Breach Notification Letter— LexisNexis



June 6, 2006

A.B. Anyname
123 Any Street
Anytown US 01234-5678

Dear A.B. Anyname:

I am writing to you on behalf of LexisNexis because we believe a law enforcement customer's user ID may have been used in an unauthorized manner that allowed some personal information about you to be viewed. That information may have included your name, address, Social Security number and/or Driver's License number. We understand that such unauthorized use or exposure may create a risk of identity theft and we treat it very seriously. Although we have no evidence that your information has been misused, we are notifying you so that you can, if you deem appropriate, take additional steps to protect your personal information. We deeply regret that individuals like you, who are the primary beneficiaries of LexisNexis® products and services, may have been affected by this incident.

How LexisNexis Will Assist You

We are committed to assisting you through this unfortunate situation and providing you with the tools to correct any problems that may arise.

To that end, we are working with Equifax®, a credit management and identity theft protection service, to help you monitor your credit reports for one year at no cost.

Equifax will help you protect your identity and your credit information through these steps:

1. Placing a fraud alert on your credit file at Equifax and the other two credit reporting agencies, TransUnion and Experian; and
2. Enrolling you in Equifax Credit Watch™ Gold identity theft protection service and obtaining your 3-in-1 Credit Report for you.

These services are being provided to you at no cost. This letter and the attachment include everything you need to sign up for this free service.

If there is reason to believe that you have been a victim of fraud as a result of this incident, we have arranged for you to have access to the Equifax Fraud Victim Assistance Program. This program includes one-on-one counseling from an Equifax Fraud Specialist and provides you with:

- **Fraud Education Providers** – a Fraud Specialist will provide you with information that will help you proactively protect yourself from identity theft and provide information to you regarding the credit reporting agencies, such as telephone numbers, Web sites and mailing addresses; and
- **Fraud Assistance** – a Fraud Specialist will provide you with a step-by-step process to reduce your exposure to further fraud and clear up any negative credit inferences in your name by helping you write letters that you may send to dispute fraudulent accounts at credit bureaus and with creditors.

How to Enroll

Equifax has a simple Internet-based verification and enrollment process. Go to www.myservices.equifax.com/lexis, and follow these steps:

- **Step 1 – Registration:** Complete the form with your contact information (name, address, telephone number, Social Security number, date of birth, e-mail address). The information is provided in a secure environment.
- **Step 2 – Verify Your Identity:** Equifax will verify your identity by asking you one or two security questions.
- **Step 3 – Order Summary:** During the "check out" process, provide the following promotional code **LEXIS-9999999999** in the "Enter Promotion Code" box. (This code eliminates the need to provide a credit card number for payment.)
- **Step 4 – Go to the Member Center,** where you can access the 3-in-1 Credit Report. You will receive a follow-up e-mail confirmation of your enrollment in Equifax Credit Watch Identity theft protection service.

If you prefer, you can order the enrollment materials to be delivered via U.S. Mail. Please call the Equifax Customer Service Center at 1-866-572-1424, provide the promotional code from Step 3 above and their Customer Service representative will assist you in ordering these services.

Additional Resources

In addition to the support through Equifax, you may also wish to utilize one or more of the following resources:

- We have created a special Web site with the information contained in this letter, plus additional information regarding identity security. Visit the site at <http://privacyfacts.lexisnexis.com>. If you prefer to speak with someone at LexisNexis, you may reach us at 1-866-293-3894.
- Most states have a consumer fraud division, and you can also enlist their help. A list of state offices is available on the special LexisNexis Web site listed above. You may also call us at 1-866-293-3894 to obtain this information.
- For more general educational information on identity theft, visit the Federal Trade Commission Web site, www.consumer.gov/idtheft, or call at 1-877-IDTHEFT (1-877-438-4338).

Why Does LexisNexis Have This Type of Information?

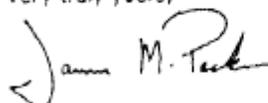
LexisNexis provides information such as public records, publicly available information and non-public information (such as Social Security numbers and Driver's License numbers) to business, government and legal professionals for legitimate business uses.

LexisNexis only provides access to non-public information to customers with a legally permissible purpose. These customers include law enforcement agencies, federal homeland security departments, prospective employers, banking and financial services companies and insurance carriers. Examples of the ways LexisNexis products and services are used include:

- Banks verifying their customer information for new accounts or loan applications;
- Insurance companies verifying their customer information to reduce applicant and claims fraud in efforts to keep insurance rates lower; and
- Telecommunications companies verifying their applicant information for instant cell phone service.

Again, we regret any trouble this incident may cause you. We pledge our continued commitment to reducing this type of incident. We will continue to work with our customers and appropriate authorities to improve data safeguards and privacy protections.

Very truly yours,



James M. Peck, CEO
LexisNexis Risk Management Group

Direct Correspondence:

LexisNexis Regulatory Compliance
9443 Springboro Pike
Miamisburg, OH 45342

LexisNexis and the Knowledge Durst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Equifax is a registered trademark and Equifax Credit Watch is a trademark of Equifax Inc. Other products or services may be trademarks or registered trademarks of their respective companies.
© 2006 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

APPENDIX C: Security Breach Notification Impact Study Interview Questions

Length: 60 minutes

SECTION I: OPENER / ICEBREAKER QUESTIONS

Length: 5 minutes

How do you spend your time as _____?

Are you responsible for issues other than security?

Of the issues you mentioned, which tend to dominate your time?

How many people work in your department?

SECTION II: FACTORS

Length: 20-30 minutes

Which departments, other than yours, play a role in the security policies and/or implementing the security initiatives at your organization? Describe your interactions with these departments and how they affect how security decisions are made.

I am going to read off a list of external factors that may or may not affect a company's security investment decisions. Please indicate which of these factors play an important role in your own investment decisions:

Legal compliance (such as SB-1386, Sarbanes-Oxley, Gramm-Leach-Bliley)

If important, which one stands out as most important?

Market competition

Media reports of security breaches at other organizations

Reputation of your company among consumers

Reputation of your company among your customers

Customer response to a past security breach

Industry security standards

Threat of lawsuits from consumers

Attention of privacy advocacy organizations or other non-governmental agencies
Regulatory scrutiny
If so, which agencies?

Are there other forces that have driven your company's development of security mechanisms?

Of all the factors we have discussed thus far, both internal and external, what are the most important motivating factors you consider when you make security investment decisions?

If you think back on the most significant security upgrades or security evaluations that you have undertaken in your time as [insert professional title], what would you say was the single most important catalyst for that undertaking? What was the undertaking?

Are there specific things / events / aspects about your company that have shaped its approach to security? How?

SECTION III: SECURITY BREACH NOTIFICATION

Length: 15 minutes

Specific Responses to SB-1386:

When did you first become aware of the security breach notification requirements of California SB-1386? What is your understanding of what these requirements are? What is your understanding of what the consequences for failing to comply are?

When you first became aware of the requirements of SB-1386, did you take any steps directly to respond to the requirements? Did you take any specific steps to enhance the security procedures of your organization? If so, what were they? Who in your organization was involved in implementing these steps?

As compared to other external factors that impact your security investment decisions, how strong of an influence would you say that security breach notification laws have had on your decisions?

SECTION IV: REPUTATIONAL IMPACT ON INVESTMENT DECISIONS

Length: 15 minutes

To what extent do you feel that your company's success depends on consumers trusting you with their information? [rank scale, 1 = trust is critical to the success of the company, 10 = trust is not a factor at all] In what ways?

Have you suffered a security breach at your organization that has required public notification?

If so, what do you consider to be the most substantial impact on your company from a public notification of a security breach? To what extent have these consequences driven your security investment decisions after the breach?

If not, what would you consider to be the most substantial impact on your company from the public notification of a security breach, were it to occur?

Has your company ever attempted to quantify the impact that these consequences have on your profitability?

Does the public notification requirement increase your willingness to engage law enforcement or other regulatory agencies for assistance in responding to the security breach?

In some states, notification statutes require notification be provided **both** to the individuals affected as well as a state regulatory agency, such as the department of consumer affairs or the attorney general. How would your perception of the impact that notification has on your company change if the law **only** required notification to some sort of regulatory agency? What would be your greatest concerns about the effects of notification in this scenario?

SECTION V: INDUSTRY STANDARDS

Length: 15 minutes

What role do professional associations and trade groups play in the development of your company's approach to security? Are there any that you consider particularly influential?

Do you have a sense that a set of "best practices" in security has developed?

Are they sector-specific or can they be generalized?

Is your company's practices influenced by these "best practices"?

What do you think has been the driving force behind these standards?

Do the security breach notifications of other organizations impact:

Your perception of how a breach notification will affect your own organization?

Your perception of how likely it is that a security breach will occur at your own organization?

Your own security mechanisms?

Your own breach notification procedures?

SECTION VI: CONCLUSION

Length: 5-10 minutes

Thinking back on the issues that we have discussed thus far, are there any additional points that you would like to add to your answers?