https://doi.org/10.48009/4_iis_2015_86-94

Issues in Information Systems
Volume 16, Issue IV, pp. 86-94, 2015

AFTER THE DATA BREACH: NOTIFICATION LAWS AND MORE

Janet C. Ford, Western Carolina University, jford@catamount.wcu.edu
Barbara Jo White, Western Carolina University, whiteb@email.wcu.edu
Kristin M. White, North Carolina State University, kmwhite3@ncsu.edu

ABSTRACT

After a data breach occurs, organizations typically implement an incident response plan, which includes some form of discovery, notification, and remediation. While IT professionals play a central role in these activities, they are joined in their efforts by others internal to the organization as well as external specialists. For example, the internal data breach response team often includes members from the legal department who provide counsel, participate in contacting law enforcement where necessary, and coordinate other law-related activities. In addition, law firms that specialize in data breaches may provide additional expertise to guide the organization through notification and possible remedial measures such as call centers and identity theft protection for affected parties. This paper, aimed at IS/IT academics and professionals, describes data breach characteristics, costs, and response steps, while primarily focusing on the variations in state data breach notification laws and, to a lesser extent, the proposed federal Personal Data Notification and Protection Act of 2015. Examples from state statutes illustrate the range of legal obligations IT professionals face with respect to events that trigger a notification requirement, who must provide notification, the time frame for and methods of notification, compliance and enforcement.

Keywords: Data Breach, Legal Issues, Security

INTRODUCTION

Data breaches, which are becoming increasingly likely for businesses of varying sizes, are costly for businesses both in the U.S. and worldwide. For example, data breach related expenses for the recent data breach at Target not only cost upwards of $160 million dollars and cost Target customers and sales but also may have cost the CEO his job [34]. Data breaches have changed over the last decade and so have the laws associated with them. A challenge for IT professionals is the fact that all but three states have their own data breach notification laws, and they vary widely. However, not all of the factors that differentiate the different state laws exhibit the same level of variation. In addition, state laws continue to be amended in the direction of more protection for individuals affected by a data breach [16].

Gartner, Inc., a leading IT research firm, forecasts that by 2020, intrusion detection and security incident response will require the majority of the security budget for large firms [12], and therefore firms need to not only develop the skills of their IT employees working in security but also look outside their firms for additional security and other appropriate incident response skills such as legal skills [14]. It is important that IT personnel, from IT students and professors to IT professionals, become familiar with legal issues associated with data breaches. In many steps associated with a typical data breach response, from discovery of the breach to resuming business as usual, IT personnel interact with or utilize the expertise of legal personnel.

While many legal resources exist that address data breach notification laws, these resources, such as law reviews and journals, legal workshops, and seminars are typically directed primarily to legal academics and practitioners. Few legal resources are aimed at an IT audience. This paper, aimed at IS/IT academics and professionals, first describes data breach characteristics, associated costs, and typical data breach response steps. Then, the paper discusses in depth variations in state data breach notification laws, including the events that trigger a notification requirement, who must provide notification, the time frame for and methods of notification, compliance and enforcement. The paper then covers the proposed federal Personal Data Notification and Protection Act of 2015 [32], and concludes with limitations and future research.

DATA BREACHES, ASSOCIATED COSTS AND DATA BREACH RESPONSE STEPS

Data breaches vary due to many factors, including parties responsible for the data breach, mechanisms or methods used to perpetrate the data breach, and a variety of other characteristics. For nearly a decade, Verizon has published annual studies analyzing 500 to 1000 data breaches spread fairly evenly across companies of all sizes [36, 37, 38, 39, 40, 41, 42, 43]. Besides Verizon, IBM has also shown an interest in data breaches and has sponsored research by the Ponemon Institute [1] that examines costs of data breaches, including costs associated with legal actions related to data breaches. Specifically, the Ponemon Institute has conducted surveys and in-depth interviews relating to the costs associated with data breaches with companies that actually experienced a data breach. The sample includes anywhere from 14 companies in 2006 to 61 companies in 2014 [1]. Examining these studies over time helps to identify data breach trends. Moving to activities following a data breach, a variety of firms related to credit cards, from credit card processing to credit score agencies, have gotten involved in publishing actions or steps that firms can undertake if or when they discover a data breach [13, 14, 44].

Data Breach Evolution from 2008-2013

Various characteristics associated with data breaches, such as breaches that were largely avoidable and attacks that were considered low difficulty showed increases from about 85% in 2008 [36] to 97% in 2012 [40] (see Figure 1 below). Meanwhile other characteristics, such as the percent of victims that were opportune targets showed slight decline over a similar period. The 25% increase in data breaches discovered by third parties in the 2011 report [39] is likely due to the higher concentration of smaller organizations compared to the 2010 report [38]. Smaller organizations with fewer IT resources are less likely to discover breaches compared to third parties [39]. Although the 2011 report described a record number of data breaches, there were fewer records that were compromised. The over 20-point drop in the percentage of records compromised from servers and applications, from 98% in 2010 [38] to 76% in 2011 [39], can be attributed to the fact that in 2011, in these smaller organizations there were no breaches that involved millions of records (see Figure 1 below).

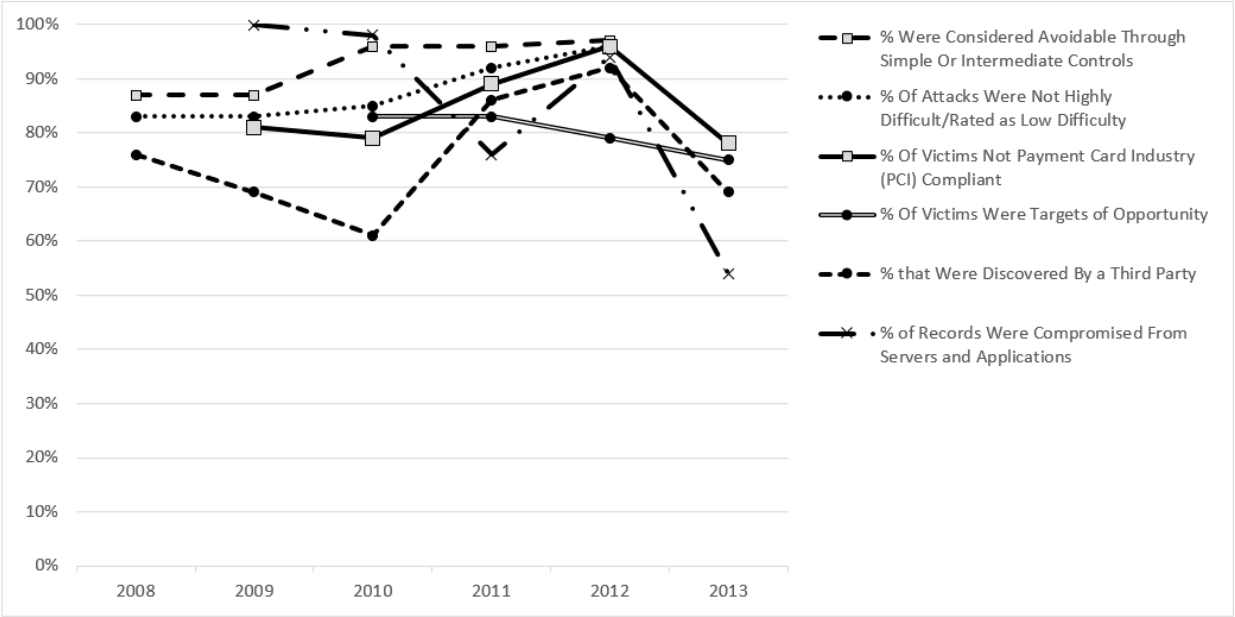

Figure 1. Data Breach Characteristics [36, 37, 38, 39, 40, 41]

Regarding data breach mechanisms or methods (see Figure 2 on the following page), there was a dramatic increase in the percentage that resulted from hacking and malware, from about 40% in each area in 2010 [39] to 69% for malware and 81% for hacking in 2012 [40]. In fact, for hacking or using malware, the rate of growth from 2011-2012 and subsequent decline from 2012-2013 nearly mirrors the rate of decline from 2011-2012 and subsequent

increase from 2012-2013 for the data breach methods of physical or social attacks or data breaches caused by privilege misuse [39, 40, 41]. A more recent phenomenon is the data breaches associated with activist groups or actors affiliated with the state. In 2013, 58% of data breaches were linked to activist groups while 19% were tied to actors affiliated with the state [41].

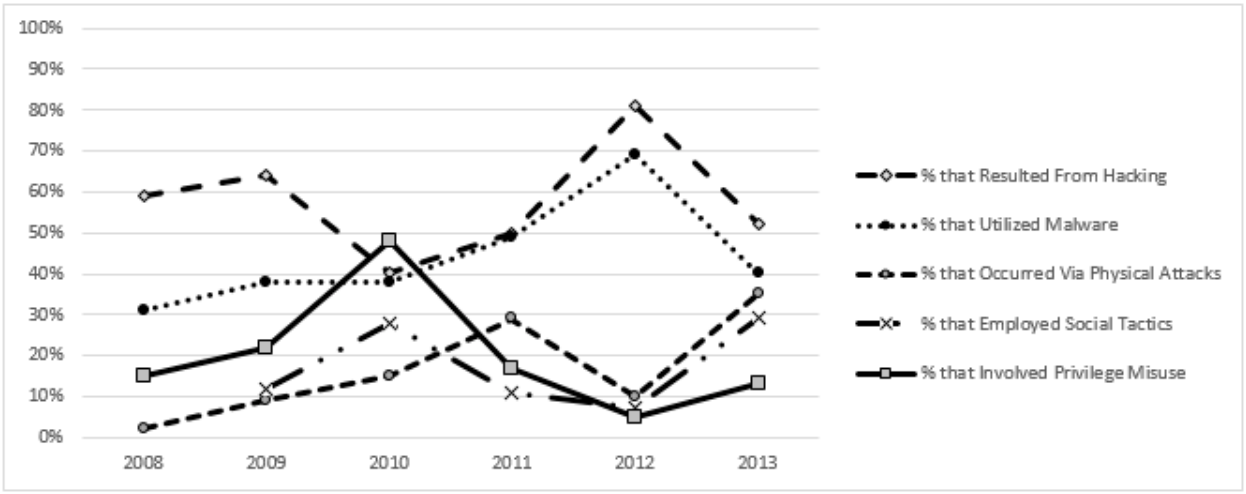

Figure 2. Data Breach Mechanisms [36, 37, 38, 39, 40, 41]

In addition to data breaches varying by the mechanisms used to perpetrate the breach and by basic characteristics of the breach, the party or parties responsible for data breaches also varies (see Figure 3 below). The percentage of data breaches resulting from external sources had a yearly growth rate of about 5% from 2008 to 2013, while the percentage of data breaches caused by insiders had a yearly declining rate of about 5% over the same period. Also, during the same period, the percentage of data breaches caused by multiple parties had a declining rate of about 25%. The percentage of data breaches that implicated business partners experienced the greatest decline with a 50 % drop over the period from 2008 to 2013 [36, 37, 38, 39, 40, 41].

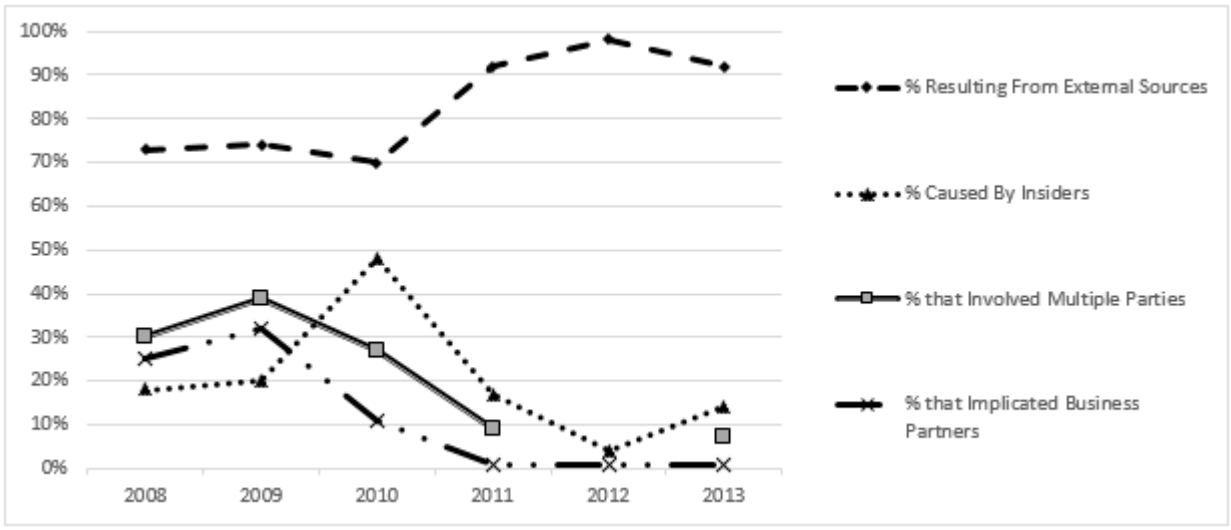

Figure 3. Parties Responsible for Data Breaches [36, 37, 38, 39, 40, 41]

Data Breach Response Life Cycle

The likelihood that firms will experience data breaches varies across industries. The Ponemon Institute suggests that the likelihood of a data breach is nearly 19% with retail, education, and public sector companies having above

average likelihoods of a data breach compared to research, industrial and energy companies which have a lower than average likelihood [1]. With a nearly one in five chance of experiencing a data breach, a variety of firms, including credit card companies like Visa [44], credit reporting services such as Equifax [13] and global information services firms such as Experian [14], have a vested interest in helping their current or potentially future customers successfully navigate a data breach. The guidance they offer, which is typically freely available and updated frequently, runs the gamut from a short checklist [13] to much more detailed information [14, 44]. Once a data breach occurs, there are various steps that businesses must undertake in response, starting with detection or discovery of the breach, which requires knowledgeable IT security employees. In fact, the most sought-after technical skills deal with detection [12] and firms are increasingly using security consultants to provide expertise or to supplement their existing knowledge [2]. Following detection, steps proceed with appropriate notification and ultimately, resuming business as usual [14] (see Table 1 below).

Table 1. Data Breach Response Steps

Data Breach Response Steps(cite)	Interaction between IT and Law Personnel
1. Discover the Breach	Within the first 24 hours, it is recommended that legal counsel be contacted for guidance [14]. During the discovery and investigation stages, many state laws do not require notification if after an appropriate investigation, it is determined that the breach will not likely result in harm to the individuals affected [3]. The Ponemon Institute study reports costs associated with discovering the breach and determining the root cause in 2014 were approximately $418,000 in the United States, which represents about a 6% increase from the previous year [1].
2. Investigate and Remediate	
3. Assemble Internal Response Team	The response team, often called an internal response team (IRT) or computer security incident response team (CSIRT), manages incidents. The lack of a security incident management process may lead to increased costs and legal action [47]. It is recommended that the IRT have members from the legal department [13].
4. Contact Law Enforcement (if Applicable)	Consult with legal counsel to determine whether it is necessary to notify law enforcement [14].
5. Employ Vendors Such as Forensics, Data Breach Resolution, Law, PR Firms	It is not required to hire an external law firm, and while it is possible to use in-house counsel, hiring legal counsel with expertise in data breach notification can be beneficial. On the IT side, Gartner, Inc., a leading IT research firm, recently suggested that security services could serve as an interim solution while the firm works to develop internal skills of its security personnel [12].
6. Begin Notification Process, Purchase Identity Theft Protection Services for Affected Persons	Some states such as California require that identity theft protection be offered to those affected by the data breach in some situations [8].
7. Make Public Announcement, Launch Website for Breach	While the default form of notification is typically in a written, electronic or telephonic format, prominent notices on websites or statewide media can serve as substitute notice if the cost of sending the default form or the number of notifications exceed state thresholds
8. Mail/Email Notifications	Costs associated with notification have experienced slight decline over the last decade [1].
9. Respond to Inquiries	Some states such as New Hampshire require that data breach notifications include contact information for the company whose system was breached [28].
10. Resume Business as Usual	It is best to establish and maintain relationships with external counsel before a data breach occurs [14].

Industry observers have noted that "[i]ncident response planning . . . is currently complicated by the existence of 47 different state breach notification laws and those of additional jurisdictions. . . The variety is no doubt confusing and

increases the compliance costs for [businesses]" [6]. While trying to understand 47 different state laws seems daunting, mastering the fundamental elements of data breach notification laws is more easily achieved.

VARIATION IN DATA BREACH NOTIFICATION LAWS

As of January 2015, forty-seven states, the District of Columbia, and the U.S. territories of Guam, Puerto Rico, and the Virgin Islands have laws that require private and governmental entities to notify individuals whose personal information has been exposed in a data security breach [27]. The first such law was passed in California with an effective date of July 1, 2003 [17]. A survey of those laws reveals that, while they are not entirely uniform, they share many common elements, such as definitions of who is responsible for notification and what kind of data security breach will trigger the obligation to notify, an expectation that notification will occur promptly, subject in many cases to the needs of law enforcement to investigate the breach, how notification must be made, and exemptions to the notification obligation. Within each of the preceding elements, state laws contain a range of possibilities with respect to legal obligations. To determine the range of possibilities for each of the above elements, all relevant state laws were examined.

In addition to the commonalities that exist across the state laws, some state laws also include provisions addressed to third parties who have access to personal information [8]. Additionally, some state laws, such as Alaska, require additional notification to other private entities such as credit reporting agencies [3], government officials, such as an attorney general, or state administrative agencies such as a department of insurance [21]. Generally, each state law applies to whoever collects or owns personal information concerning a state resident, so entities that collect or own personal information on residents from multiple states must comply with a variety of notification requirements.

Who Must Provide Notification?

State data breach notification laws generally apply to any person or entity who does business in the state and who collects, owns, or licenses personal information concerning a state resident. Arkansas, along with most states, also include government agencies who collect, own, or license personal information [5]. Most state security breach notification laws do not extend a notification obligation to third party non-owners of personal information, but they must notify the owners or licensees of that information should those third parties experience a data security breach. Third parties, in Arizona for example, typically must also cooperate with the owners or licensees of the information [4]. A number of state security breach notification laws exempt entities that are regulated by other state or federal laws if those laws provide greater protections to personal information and have similar disclosure requirements [4].

Notification Requirement/Triggering Events

Key to the application of state security breach notification laws is the unauthorized access, release, or use of personal information that compromises the security, confidentiality, or integrity of that information [24]. Many state laws contain language similar to that of Idaho: "Good faith acquisition of personal information by an employee or agent of an agency, individual or commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure" [19]. Wyoming and many other states define "personal information" to include an individual's first name or initial and last name combined with one or more of the following items if they are not redacted: Social Security number, driver's license number or government-issued identification card number, account number, including credit or debit card account numbers, combined with a security code, access code, or password that would allow access to those accounts [49]. Unauthorized acquisition of personal information that has been encrypted, redacted, or otherwise rendered unusable will not trigger a notification obligation in Alaska [3] or many other states. Ohio, like many other states, excludes from the definition of "personal information" material that is publicly available from federal, state, or local government sources or from widely distributed media sources [30].

Notification Timing

Notification ordinarily is not required if, after conducting an investigation upon discovery of the breach, the covered entity determines that harm or misuse of the information is not likely to occur as is the case in Arkansas [5]. In such a situation, New Jersey, for example, requires the covered entity to retain documentation of its investigation and

conclusion [29], while Florida requires consultation with law enforcement officials [15]. Otherwise, as in Arkansas, the covered entity must provide notification to the affected individuals in "the most expedient manner possible and without unreasonable delay" [4]. The vast majority of states include some variation of either "most expedient manner possible" or "without unreasonable delay," or both. All states allow a reasonable delay of notification if notification of the data security breach would impede a law enforcement investigation. Most states also allow a reasonable delay in notification for an internal investigation to determine whether the breach is likely to result in harm and also to "restore the reasonable integrity of the computerized data system" [19].

A few states place an outer limit on the amount of delay allowed for law enforcement and internal investigations. Florida places a thirty day maximum period within which notification must be made following discovery of the data security breach [15]. Ohio [30], Vermont [45], and Wisconsin [48] each require notification no later than forty-five days following discovery of the breach. The state of Washington will join this group effective July 24, 2015, when an amendment to its laws takes effect [46]. The state of Maine requires that notification be made no later than seven business days after law enforcement determines that notification will not impede its investigation [24]. The territory of Puerto Rico requires a covered entity to report a data security breach to the Department of Consumer Affairs within ten days after the breach has been discovered. The Department must then issue a public announcement of the breach within 24 hours of receiving that report [31].

Forms of Notice

State data breach notification laws require that notice be made in a written form, such as a mailing, and electronic form, or, in some states, telephonically [35]. The majority of state laws allow substitute notification to be made in cases where the cost of notification or the number of individuals to be notified exceeds a certain threshold or the covered entity has insufficient contact information [33]. Substitute notification thresholds for cost and affected individuals range from a high of $250,000 or 500,000 state residents, adopted by the majority of states as in Tennessee [33], to a low of $5,000 and 1,000 state residents in Maine [24] and New Hampshire [28]. Wyoming has a two-tiered threshold for substitute notice depending on whether the covered entity is based in Wyoming. For an entity that is based in Wyoming, substitute notice is permitted if the cost of notice will exceed $10,000 or if the number of state residents to be notified exceeds 10,000. For an entity that is not based in Wyoming, substitute notice is permitted if the cost of notice will exceed $250,000 or if the number of state residents to be notified exceeds 500,000. Where substitute notice is allowed, as in Kansas [20], it typically must consist of either email communication with the individuals affected, a conspicuous posting on the covered entity's website, or notification to major statewide media. Some states also specify what must be included in the notification, such as a description of the incident, the type of information exposed, toll-free numbers for major credit reporting agencies, and information or advice on how the individuals affected can protect themselves from the misuse of their personal information [8].

Under some state security breach notification laws, a covered entity must provide notification not only to individuals whose personal information has been exposed but also to other individuals or agencies. In California, for example, a security breach that will require notification to more than 500 California residents triggers a requirement that the state attorney general also be notified by means of a sample copy of the notification [8]. In Alaska, a security breach that will require notification to more than 1,000 state residents triggers a requirement that consumer credit reporting agencies who maintain nationwide files on consumers also be promptly notified [3].

Compliance, Waivers, and Enforcement

As mentioned previously, many state data breach notification laws exempt entities from the notification requirement if those entities are subject to, and in compliance with, other state or federal laws or regulations that provide greater protections to personal information and that have similar disclosure-of-breach requirements [4]. Colorado, like many states, also exempts entities from the notification requirement if those entities have implemented, and complied with, their own internal policies for notification in the event of a data security breach provided that those internal policies are consistent with the statutory requirements [9]. One popular exemption explicitly mentioned in some state laws applies to entities that are subject to the Gramm-Leach-Bliley Act of 1999 [3].

Some states preface their security breach notification laws with statements of findings and legislative purpose to establish the government's intent behind the acts. Arkansas, for example, notes in its legislative findings that the legislature's intent is to protect sensitive personal information and "to encourage individuals, businesses, and state agencies that acquire, own, or license personal information about the citizens of the State of Arkansas to provide reasonable security for the information [5]." Other states, such as Maryland, stress the importance of personal information security by including provisions in their laws that the protections of the notification requirements cannot be waived by contract or otherwise, and that any waivers would be considered void as against public policy [23].

Finally, the enforcement mechanisms and penalty provision for violations of the data security breach notification laws vary widely from state to state. In most states, the attorney general [11] or a regulatory body is designated as the enforcement authority [19]. Enforcement actions by government actors typically seek injunctions against future violations, compensation for individuals who have been injured because of the violation, and often, civil penalties with aggregate caps ranging from $10,000 in Arizona [4] to $750,000 in Michigan [25]. In addition to enforcement actions by government officials or agencies, the District of Columbia and some, but not all, states allow individuals who have been harmed as a result of a violation of the notification requirements to bring private actions to recover actual damages and sometimes attorney fees and court costs [10]. As to both government enforcement actions and private civil actions, numerous state laws distinguish between relief granted when a covered entity has knowingly, willfully, or repeatedly violated the notification law and relief granted when a covered entity has only been negligent [28]. The majority of state laws specify that a violation of the security breach notification provisions constitutes a violation of the individual states' unfair or deceptive business practices laws, and refer to the enforcement and remedies thereunder [15]. Montana not only allows imposition of a fine of not more than $5,000 for a violation, but also allows for imposition of a jail term of not more than one year, or both a fine and imprisonment [26]. Since only individuals, and not entities, may serve jail time, individuals within a covered entity that collects personal information on Montana residents have a strong incentive to comply with their data breach notification laws.

The Personal Data Notification and Protection Act of 2015 – A Nationwide Standard?

The patchwork of state laws has naturally led to numerous calls for a federal law that would impose a single nationwide standard. In a January 12, 2015 speech before the Federal Trade Commission, President Obama announced a proposal to create such a standard [7]. The proposed bill has garnered both critics and supporters, as it is perceived to strengthen some protections while weakening others. Some observers doubt that this bill will make it any further in the legislative process than any of its predecessors, in at least one case giving it only a 1% chance of passing [18]. Others speculate that presidential support and new provisions may enhance the bill's chance of passing. However, if it is to pass, it will probably undergo significant revision and clarification [16]. Introduced in Congress on March 26, 2015, House Bill 1704, commonly known as the Personal Data Notification and Protection Act, applies to any business that "uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period". A key provision of this bill is that it will preempt existing data breach notification laws [32].

Critics of the bill point out, among other things, that it will preempt existing state laws that provide greater protection for individuals whose information is compromised. In response, supporters argue that while some stricter state provisions may be preempted, the bill will ensure greater protection than currently exists in many states, including the three states that do not have such a law [6]. Another criticism of the bill is that it eliminates the possibility of private causes of action that are available under some state laws. However, this bill does allow the attorneys general of the states to file actions in federal court seeking injunctive relief and/or civil penalties for violations. Under the bill, those civil penalties can be up to $1,000/day/individual up to a total of $1 million per violation. An open question concerns the meaning of "violation." Does it refer to failure to notify a particular individual or does it refer to the breach incident? The $1 million dollar cap, which is higher than any existing civil penalty cap under state law, does not apply where the violation is willful or intentional, thus opening the door to virtually unlimited penalties. Some legal practitioners speculate that this provision may make the bill more acceptable to state governments, and thus enhance the bill's chance of passage [16]. Finally, there is concern about the applicability of the bill to business entities that collect sensitive personally identifiable information on fewer than 10,000 individuals in a twelve month period. Are those entities still subject to the existing state laws, or are they altogether exempt from any notification requirement? The fate of H.B. 1704 is far from certain. Whether it passes or

not, IT professionals are well-advised to be proactive in preparing for stricter notification requirements, if not under the federal bill then possibly under the increasingly aggressive state notification laws [16].

CONCLUSIONS

In this day of expanding accumulation of personal information and its potential for misuse, it has become conventional wisdom in the IT industry to speak in terms of not if, but when a breach occurs. Preparation can make all the difference and it starts with an effective incident response plan [22] outlining the data breach response steps from discovery to notification, to remediation and ultimately to resuming business as usual [14]. While IT professionals play a central role in the incident response activities, they must be prepared to interact with other professionals, particularly those in the legal field, whether they are inside or outside of the organization. Elements of state data breach notification laws, including who must provide notification, triggering events, the timing and methods of notification, compliance, and enforcement were compared to identify ranges of possible values. The elements of state data breach notification laws do not exhibit the same degree of variation. For example, one element that varies widely is the circumstances under which substitute forms of notice may be used. By contrast, one element that is relatively consistent from state to state involves the requirement that collectors, owners, and licensors of personal information must provide notice to individuals affected by a data breach.

A limitation of this study is that only one lawyer determined the common elements and range of values within those elements in state data breach notification laws. Future research could involve the development of a system to code state data breach notification laws. For each element, a coding system could be defined to describe the range of possible values. Inter-rater reliability could be assessed if two or more lawyers independently code each state law using the agreed-upon definitions.

REFERENCES

1. 2014 Cost of Data Breach Study: United States. The Ponemon Institute, May, 2014. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03017USEN&attachment=SEL03017USEN.PDF#loaded
2. Ahlm, E. (2012, November 07). Report Highlights for Market Trends: Data Loss Incidents Accelerate the Data Breach Response Service Market. (2012), Gartner, Inc. Available: https://www.gartner.com/doc/2229815/report-highlight-market-trends-data
3. Alaska Stat. §§45.48.010 et seq. (2014).
4. Ariz. Rev. Stat. § 44-7501 (2015).
5. Ark. Code Ann. §§ 4-110-101 et seq. (2015).
6. Bailen, P., (2015, February 27). "Examining the President's Proposed National Data Breach Notification Standard Against Existing Legislation" Westin Research Center. Available at https://privacyassociation.org/news/a/examining-the-presidents-proposed-national-data-breach-notification-standard-against-existing-legislation/).
7. Barack Obama, Speech before the Federal Trade Commission (January 12, 2015), available at https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission
8. Cal. Civ. Code § 1798.29 (2015).
9. Colo. Rev. Stat. § 6-1-716 (2014).
10. D.C. Code § 28-3853 (2015).
11. Del. Code Ann. Tit. 6, §§ 12B-101 et seq. (2015).
12. D'Hoinne, J. & Scholtz, T. (2015, February 19). CISSOs Should Review Their Enterprise's Security Skills Portfolio Now. 2015, Gartner, Inc. Available: http://www.gartner.com/document/2988219
13. Equifax (n.d.). Data Breach Ready. Available: http://www.equifax.com/international/canada/documents/Data_Governance_and_Loss_Checklist.pdf
14. Experian Data Breach Resolution (2014). Data Breach Response Guide: 2014-2015 Edition. Available: http://www.experian.com/assets/data-breach/brochures/2014-2015-data-breach-response-guide.pdf
15. Fla. Stat § 501.171 (2015).
16. Giszczak, J.J. and Paluzzi, D.A., (2015, Feb. 12). President Obama's New Personal Data Notification & Protection Act: Overview, Analysis, and Challenges [webinar]. In idExperts Available at

https://www2.idexpertscorp.com/resources/single/president-obamas-new-personal-data-notification-protection-act-overview-ana/r-general.
17. Goel, S., Shawky, H.A. (2014, January). "The Impact of Federal and State Notification Laws on Security Breach Announcements," Communications of the Association for Information Systems. (2014).
18. govtrack.us, "H.R. 1704: Personal Data Notification and Protection Act of 2015," (accessed May 15, 2015). Available at https://www.govtrack.us/congress/bills/114/hr1704.
19. Idaho Code Ann. §§ 28-51-104 et seq. (2015).
20. Kan. Stat. Ann. § 50-7a01 (2013).
21. Mass. Gen. Laws § 93H-3(b) (2015).
22. McMillan, R. (2012, July 19). Prepare for the Inevitable With an Effective Security Incident Response Plan. (2012), Gartner, Inc. Available: https://www.gartner.com/doc/2086516/prepare-inevitable-effective-security-
23. Md. Code Ann., Commercial Law, §§ 14-3501 et seq. (2014)
24. Me. Rev. Stat. tit. 10, §§ 1346 et seq. (2014).
25. Mich. Comp. Laws § 445.72 (2015).
26. Mont. Code Ann. § 30-14-142 (2014).
27. National Conference of State Legislatures, Security Breach Notification Laws. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
28. N.H. Rev. Stat. Ann. § 359-C:20 (2015).
29. N.J. Stat. Ann. § 56:8-163 (2015).
30. Ohio Rev. Code Ann. §§ 1347.12 and 1349.19 (2015).
31. P.R. Laws Ann. tit. 10, § 4052 (2011).
32. Personal Data Notification and Protection Act, H.B. 1704, 114th Congress (2015).
33. Tenn. Code Ann. § 47-18-2107 (2015).
34. Trefis Team (2014, May 8). Target's CEO Steps Down Following The Massive Data Breach And Canadian Debacle. Available: http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-and-canadian-debacle/
35. Va. Code. Ann. § 18.2-186.6(A) (2015).
36. Verizon (2008). 2008 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/security/databreachreport
37. Verizon (2009). 2009 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp
38. Verizon (2010). 2010 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg
39. Verizon (2011). 2011 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg
40. Verizon (2012). 2012 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg
41. Verizon (2013). 2013 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg
42. Verizon (2014). 2014 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg
43. Verizon (2015). 2015 Data Breach Investigations Report. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg
44. Visa, Inc. (2013). What To Do If Compromised. Available: http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf
45. Vt. Stat. Ann. tit. 9 §§ 2430 et seq. (2015).
46. Washington Chapter 64, Laws of 2015.
47. Wheatman, J. (2010, October 10). Five Reasons Why You Need a CSIRT, Even If You Think You Don't. (2010), Gartner, Inc. Available: https://www.gartner.com/doc/1448133/reasons-need-csirt-think-dont
48. Wis. Stat. §134.98 (2015).
49. Wyo. Stat. §§ 40-12-501 et seq. (2014).