Regulations to Reduce Data Breaches

David Mitchell

ICTN 6870 601

April 11, 2016

Abstract

Over the past years there have been targeted data breaches that affected many large corporation and even the federal government. Target store and Office of Personnel Management OPM were two of the biggest data breaches of 2015. Some of these data breaches could have been identified or remediated if the corporation or government agency reported proper notification or conducted compliance audits as required by law. The Communication Act of 1934 and Health Insurance Portability & Accountability Act of 1996 are some of the regulations that protect this type of information. These regulations are due for an update by state and federal legislators to bring laws current with technology. Legislators are starting to show some focus on regulation or compliance for data breaches and cybercrimes after the data breach of Office of Personnel Management.

Introduction

Recent data breaches have put a spotlight on concerns about the security of personal identifiable information stored by corporations. A data breach happens when sensitive information is stolen, lost or accessed by unauthorized personnel. Security and breach notification requirements and protections are regulated by federal laws such as Health Insurance Portability and Accountability HIPPA, the Gramm-Leach Bliley Act, Federal Information Security Management Act and Payment Card Industry Data Security Standard.

Former Attorney General Eric Holder has requested to Congress that America needs a national standard for notifying consumers and law enforcement of data breaches. A chorus of lawmakers is calling for a federal law to supersede the state regulations already in place. It took Target four days to inform customers about the hackers lifting data from 40 million customer credit cards accounts. Neiman Marcus informed the public about 10 days later. Only forty-six states have disclosure laws that require companies to inform the public about security breaches within a certain period of time for consumer protection. The different requirements have been a challenge for consumers and the government regarding data breaches. There shouldn't be more or less protection depending on the state in which you reside. The national attention on Target security breach brought the different protections laws to light. We will discuss some regulations or compliance used to reduce the impact of data breaches or cybercrimes in this paper.

Federal Communication Act

The Federal Communication Commission is asserting authority to regulate cybersecurity under the Communication Act of 1934. The FCC authority is to impose a forfeiture

penalty against any person who willfully or repeatedly fail to comply with any provision of the act (Black, Newman, & Tran, 2014). The Federal Communications Act contains strong data security and breach notification protection for consumers. It protects customer's use of telecommunication services such as location data and phone call histories (Consumer Groups Oppose H.R. 2205, Data Security Act of 2015, 2015). The Federal Communication Act now consider it a violation if the telecommunication company fail to properly protect consumer's propriety information when stored on a third-party servers (Pryor & Sabett, 2014). The law will apply to telecommunication carriers and vendors that the carriers use to obtain or store information about their customers. Section 222 (a) of the Communication Act establishes a duty to protect customer proprietary information (Kashatus, 2014).

The Federal Communication Commission's Enforcement Bureau processed its first privacy and data security settlement with Cox Communication for $595,000 because the company failed to protect the customers' personal information when their data was breached in 2014 (FCC Settles Cox Communications Data Breach Investigation, 2016). The hackers impersonated a Cox's information technology employee and convinced a customer service representative to enter their account IDs and passwords into a phishing web site. The hacker was able to gain access to the Cox customers' personally identifiable information. The FCC Enforcement Bureau monitored Cox's compliance for seven years.

Health Insurance Portability and Accountability

Health Insurance Portability and Accountability HIPAA requires businesses to provide notification following a breach of protected health information (Health Information Privacy, 2016). The HIPAA establish standards and requirements for transmitting health

information while protecting patient privacy. There is a requirement to report smaller breaches of fewer than 500 individuals as part of the HIPAA protection. Beach notification must be made no later than 60 days following the discovery of a breach. HIPAA requires that the affected individuals must be inform of the steps the breached company is taking to protect them from potential harm (HIPAA Journal, 2016). 94% of health care organizations suffered a data breach in the last two years. There was an average of 2,769 records lost or stolen per breach (HIPAA Rule Brings Changes to Breach Notification, 2013). Higher security standards are needed to keep pace with increased exchange of personal identifiable information. The HIPAA act protect individual's health information while permitting approved access to the information by health care providers. The purpose of the HIPPA was to ensure businesses are accountable to US Health & Human Services for protecting private information in companies care.

New York Presbyterian Hospital NYP disclosed 6,800 patient's information to Google and other Internet search engines during a reconfigure caused by a server (Kelly, 2016). The breach was caused when a physician attempted to deactivate a personally owned server on the network containing NYP patient data. The lack of technical safeguards while deactivating the server resulted in the data being accessible by Internet web search engines (Kelly, 2016). New York Presbyterian Hospital failed to implement processes for monitoring IT data system that were linked to patient data prior to the breach incident. NYP paid Health & Human Service three million dollars because of the lack of notification following the breach. NYP agreed to conduct a comprehensive risk analysis of security risks and vulnerabilities for all their data systems (Kelly, 2016).

The Gramm-Leach Bliley Act

Personally identifiable information and financial information have been the focus of most data protection laws. The Gramm-Leach Bliley Act limits disclosure and use of customer information. The Gramm-Leach-Bliley Act is also called the Financial Services Modernization Act. This act was enacted by Congress in 1999 to provide rules regarding the privacy of nonpublic personal information collected by financial institutions such as insurance companies, commercial banks, higher learner institutions and investment banks (Nunn, 2007). The Gramm-Leach-Bliley Act applies to financial institutions that handle personal information including protection of customer financial records and other personal information. Financial institutions collect personal information from their clients including names, addresses, credit histories and social security numbers. States are allowed to formulate protections that exceed Gramm-Leach Bliley Act federal law (Gramm-Leach-Bliley Act and Compliance Regulations for Protecting Data-at-Rest, 2016). Financial institutions must takes steps to ensure confidentiality, security and privacy of customer records. Higher education institutions are consider financial institutions because they handle federal loans (Gramm-Leach-Bliley Act, 2016). Gramm-Leach-Bliley Act requires financial organizations to protect against unauthorized access information that could result in substantial harm to any customer (Gramm-Leach-Bliley Act and Compliance Regulations for Protecting Data-at-Rest, 2016). A financial institutions is required by the Gramm-Leach-Bliley to provide consumers a copy of the privacy notice. Gramm-Leach-Bliley Act also prohibits falsely impersonating someone in order to obtain their financial data.

Federal Information Security Management Act of 2002

The Federal Information Security Management Act was signed into law as part of the Electronic Government Act of 2002 to protect government information, operations and assets against threats (Rouse, n.d.). This act requires federal agencies to implement a set of process and system controls designed to ensure the confidentiality, integrity, and availability of information (Vanderburg, n.d.). Federal Information Security Management Act help to bring focus within the federal government to cybersecurity. Federal Information Security Management Act required the inspector general to conduct annual reviews of the agency's information security program. Office of Management and Budget will use the annual results to prepare reports to Congress on agency compliance. The NIST Special Publication 800-53 provide the guidance for the minimum security requirements and security controls for organizations (NIST - Special Publication 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations, 2014). The security controls in the NIST are designed to help both private and government to select the controls that protect mission critical services (Dumont, 2015).

The Inspector General found that Veterans Affair's did not comply with the agency's rules for securing data and allowed IT specialist access to databases beyond their security clearance (White, 2011). Federal agencies had problems implement Federal Information System Management Act due to unfunded mandates for additional work. The one challenge with the FISMA is that it relies on an agency's compliance with reporting (White, 2011).

Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard requirements are controls that require businesses to implement credit card data protection and compliance (Rouse, PCI DSS 12 requirements, 2012). There are twelve requirements that organizations must meet if they handle payment cards. The PCI DSS 12 requirements are as follows (Rouse, PCI DSS 12 requirements, 2012):

1. Install and maintain a firewall configuration to protect cardholder data.

2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

PCI DSS information security policies protect the confidentiality, integrity, and availability of payment card data and related information systems.

Sarbanes Oxley Act

The Sarbanes-Oxley Act of 2002 (SOX) was enacted on 30 July 2002. Sarbanes-Oxley Act provides data protection compliance requirement in section 302 and 404. These sections require that any financial information needs to be safeguard, and its integrity assured. SOX requires that specific internal security controls need to be identified that protect the data and the security posture re-assessed every year (Sarbanes Oxley Act Compliance Requirements, n.d.). Information Technology and corporate finance have to work together to ensure that financial and technological controls work together to protect financial data. Corporations should understand which processes, services and systems

need to be controlled (Sox, Security Standards and Building a Compliance Framework, n.d.).

Data Protection Acts

There have been several federal privacy bills introduced in 2015 to help with updating data protection in the United States. United States Senate Bill 1158 called the Consumer Privacy Protection Act help create a federal security breach notification law. The bill would override weaker state laws while leaving stronger state privacy laws in place (Data Protection in United States: Overview, 2015). This bill required that Homeland Security is notified if a security breach involving more than 5,000 individuals or federal databases. It would also make it a criminal offense for concealment of a security breach of computerized data contain personally identifiable information (S.1158 - Consumer Privacy Protection Act of 2015, 2015).

Student Digital Privacy and Parental Rights Act H.R. 2092 introduced by the United States House of Representative to prohibit operators from selling students' personal information to third parties or collecting for purposes unrelated to education instruction. It also requires the implementation of security procedures in cause of data breaches. Student Digital Privacy and Parental Rights Act requires schools to delete certain student information that is not required by the school within 45 days (H.R.2092 - Student Digital Privacy and Parental Rights Act of 2015, 2015).

The Data Broker Accountability and Transparency Act of 2015 S.668 requires data brokers to ensure accuracy of personal information they collect or maintain. This Act allow individuals to dispute the accuracy of their personal information with a written request. Individuals are provided a cost-free method to review their identifying

information (Data protection in United States: overview, 2015). These acts are a few of the regulations that law maker have introduced to help update our current data protection laws.

Security Breach State Legislation

There were around 25 states that considered security breach notification bills in 2016 (2016 Security Breach Legislation, 2016). These bills were introduced to amend existing security breach laws. Consumers or citizens are required to be notified if their personal information is breach in this laws. There are only three states that currently do not have consumer notification for security breaches involving personal information (2016 Security Breach Legislation, 2016). More than 50 bills have been introduced by these various states. Most of these bills are still pending a vote in their state legislation.

California legislation introduce Bill A.B. 259 that require agency with personal identifiable information to offer identify theft prevention at no cost for not less than 12 months if they have a security breach. Bill A.B. 2828 requires a person or businesses in California to provide notification if their data were breach by unauthorized person. A Georgia Senate Bill 306 made an amendment to their current protection removing telephone notification as a means of information a person of a potential breach of security. House Bill 1260 in the Illinois state legislation required businesses of security breaches notify the Attorney General and provide notice timelines (2016 Security Breach Legislation, 2016). This legislation from the state of Illinois is still pending for Governor's signature. Other state governments are adopting more security breach legislation in hopes that they would preempt federal laws (State Data Breach Laws Should Preempt Federal Laws, 2015). State governments are moving in the right direction with at least introducing or increase their security breach legislations to protect the citizens and businesses of their states.

Compliance Challenges

The current legislation for security breaches does not provide a uniform nation data breach standard for all personal sensitive information. The breaches are currently guided by different legislation of all state laws. The states that currently don't have data breach notification laws are Alabama, New Mexico and South Dakota. The states have different notification requirements for security breaches making the compliance very difficult and confusing for businesses (Government Focus on Cybersecurity Elevates Data Breach Legislation, 2013). Michael Bruemmer, the Vice President of Data Breach Resolution made the following statement "Regardless of where you do business, there is a complicated set of state laws and regulations for organizations to follow to ensure they are in complete compliance. A best practice to navigate the complex regulatory landscape is to identify and begin working with subject matter experts ahead of time to stay on track with response to a data breach (Government Focus on Cybersecurity Elevates Data Breach Legislation, 2013)." This shows the challenges that businesses have to overcome when dealing with security breaches in the various states. Another challenge in compliance is there are different laws that cover financial data or health related data for security breaches.

Conclusion

The high profile breaches of personally identifiable information affected millions of Americans have continue to drive the interest of lawmakers on the issue of security breaches or security compliance. There are different federal laws implemented to protect consumer data or require businesses to compliance with certain regulations to help reduce or elimination data breaches. There are no federal data breach standards but there are federal privacy laws that include data breach provisions including Gramm-

Leach-Bliley Act and the Health Insurance Portability and Accountability Act. Security breaches are starting to be the normal as more and more businesses continue to grow over the Internet. Congress will be forced to seriously consider legislation on a national level to tackle these growing security breach concerns by the citizens. The implementation or amendment of security breach laws in 49 states provide different data breach notification requirements according to their state regulations. Congress is considering a national data breach notification requirement to replace the confusing and challenging security breach notification requirements in the 49 states. State governments are looking at ways to modify existing statues or implement new ones while Congress consider a national requirement.

Congress will need to overcome several hurdles before it can adopt a national data breach standard. However, businesses and organizations would need to comply with the existing regulations and security breach notification laws. It is also critical that the current security breach laws are implemented or amended to bring the laws current with today's technology.

References

*(2016, February). Retrieved from HIPAA Journal: http://www.hipaajournal.com/hipaa-compliance-checklist/

2016 Security Breach Legislation. (2016, March 16). Retrieved from National Conference of State Legislatures: http://www.ncsl.org/research/telecommunications-and-information-technology/2016-security-breach-legislation.aspx

Black, E., Newman, T., & Tran, P. (2014, October 29). *FCC Brings Its First Data Breach Enforcement Action*. Retrieved from Haynesboone: http://www.haynesboone.com/news-and-events/news/publications/2014/10/29/fcc-brings-its-first-data-breach-enforcement-action

Consumer Groups Oppose H.R. 2205, Data Security Act of 2015. (2015, December 8). Retrieved from Consumer Federal of America: onsumerfed.org/press_release/consumer-groups-oppose-h-r-2205-data-security-act-of-2015/

Data protection in United States: overview. (2015, July 01). Retrieved from Practical Law: http://us.practicallaw.com/6-502-0467

Data Protection in United States: Overview. (2015, July 01). Retrieved from Practical Law: http://us.practicallaw.com/6-502-0467

Dumont, C. (2015, November 6). *NIST 800-53 Rev 4 Report*. Retrieved from Tenable Network Security: https://www.tenable.com/sc-report-templates/nist-800-53-rev-4-report

FCC Settles Cox Communications Data Breach Investigation. (2016, Febuary). Retrieved from ProQuest: http://search.proquest.com.jproxy.lib.ecu.edu/docview/1764323177?pq-origsite=summon

(2013). *Government Focus on Cybersecurity Elevates Data Breach Legislation.* Experian.

Gramm-Leach-Bliley Act. (2016, 03 17). Retrieved from University of Missouri System: https://www.umsystem.edu/ums/fa/glb/act

Gramm-Leach-Bliley Act and Compliance Regulations for Protecting Data-at-Rest. (2016, 03 24). Retrieved from Vormetric Data Security: http://www.vormetric.com/compliance/gramm-leach-bliley

H.R.2092 - Student Digital Privacy and Parental Rights Act of 2015. (2015, May 01). Retrieved from Congress: https://www.congress.gov/bill/114th-congress/house-bill/2092

Health Information Privacy. (2016, March). Retrieved from U.S. Department of Health & Human Services: http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

(2013). *HIPAA Rule Brings Changes to Breach Notification.* Marsh.

Kashatus, J. (2014, December 11). *FCC Forges New Ground on Enforcement of Data Security Duties under Communications Act*. Retrieved from Technology's Legal Edge: https://www.technologyslegaledge.com/2014/12/fcc-forges-new-ground-on-enforcement-of-data-security-duties-under-communications-act/

Kelly, R. E. (2016, March). *Data Breach Results in $4.8 Million HIPAA Settlements.* Retrieved from HHS: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/new-york-and-Presbyterian-hospital/index.html

NIST - Special Publication 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations. (2014, January 15). Retrieved from HIMSS: http://www.himss.org/ResourceLibrary/GenResourceReg.aspx?ItemNumber=28823

*Nunn, T. (2007, March 12). *Protecting customer data under the Gramm-Leach Bliley Act*. Retrieved from Insurance Journal: http://www.insurancejournal.com/magazines/legalbeat/2007/03/12/77898.htm

Pryor, M., & Sabett, R. (2014, October). *The FCC Begins to Regulate Data Security.* Retrieved from Cooley: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwi5lvOQt9_LAhVGZCYKHYsIB-0QFggcMAA&url=https%3A%2F%2Fwww.cooley.com%2FPdfManager%2Fgetpublicationpdf.aspx%3Ftype%3Dalert%26show%3D70415&usg=AFQjCNGlHIwSKgm_tQuFUuFj0hjCawCt_A&cad=rj

Rouse, M. (2012, March). *PCI DSS 12 requirements*. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/PCI-DSS-12-requirements

Rouse, M. (n.d.). *Federal Information Security Management Act*. Retrieved from Techtarget: http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act

S.1158 - Consumer Privacy Protection Act of 2015. (2015, April 30). Retrieved from Congress: https://www.congress.gov/bill/114th-congress/senate-bill/1158

Sarbanes Oxley Act Compliance Requirements. (n.d.). Retrieved from Vormetric Data Security: http://www.vormetric.com/compliance/sarbanes-oxley

Sox, Security Standards and Building a Compliance Framework. (n.d.). Retrieved from TechTarget: http://searchsecurity.techtarget.com/feature/SOX-security-standards-and-building-a-compliance-framework

**State Data Breach Laws Should Preempt Federal Laws*. (2015, July 8). Retrieved from HIPAA Journal: http://www.hipaajournal.com/state-data-breach-laws-should-preempt-federal-laws-says-naag-8012/

Vanderburg, E. (n.d.). *Information Security Compliance: Which regulations relates to me?* Retrieved from Jurinnov: http://jurinnov.com/information-security-compliance-which-regulations/

White, D. M. (2011). Federal Information Security Management Act of 2002: Potemkin Village. *The Fordham Law Review*, 360-406.