CSEC620

Assignment 1

Megan Bell

University of Maryland University College

This examination was part of a class exercise. This report represents a layman's perspective and not an attorney's legal review.

Table of Contents

Using U.S. Regulatory Frameworks to Improve Cybersecurity

Introduction

Recently, the central bank of Bangladesh lost more than $80 million dollars from accounts held by the U.S. Central Bank of New York.(Javers & Liesman, 2016). Bank investigations identified three different hacking groups in the bank's networks. Two groups were performing reconnaissance while a third group was stealing money. This incident became the most recent incident where the U.S. Security and Exchange Commission (SEC) provided warning that current private industry cybersecurity protections do not adequately address cyber risks. For this reason, the SEC and other Federal entities have made private industry information security a high priority as part of U.S. Federal and state security (White House, 2009).

This paper explores the relationship between the U.S. regulatory regime's approach to cybersecurity and the impact on private industry. This includes review of the U.S. Constitution's role in defining individual rights and the roles of Federal and state government. Specific points of importance include privacy, legislative sectoral practices and the use of executive orders (U.S. Congress, 2013). The impact of private industry practices are discussed with respect to minimum security enablement, the FTCs use of enforcement to improve standards, and private industry practices such as PCI that can improve broader cybersecurity best practices.

Government Jurisdiction and Sources of Authority

U.S. cybersecurity is primarily regulated by a combination of U.S. Federal and state entities (U.S. Congress, 2013). At both Federal and state government levels, regulation and governance originate from elected legislatures that pass laws, administrative branches that implement laws, and judiciary that interpret laws and resolve conflict (Hamilton, 2005). Federal

and state agencies that implement legal statutes also conduct oversight and enforcement actions. The overall U.S. approach to cybersecurity governance has been labeled a sectoral approach to governance (Swire & Ahmad, 2013).

Rationale for Regulation of Cybersecurity

The Federal government's authority to regulate cybersecurity is primarily derived from U.S. Constitutional mandates to protect the rights of U.S. citizenry, to maintain national security and protection of U.S. interests, and to share power with states (Hamilton, 2005). The first ten amendments of the Constitution stipulate protections for individuals and the limitations of Federal government. The Tenth Amendment indicates that powers not held by the Federal government are the purview of state government and creates one of the most notable limitations to the role of Federal government by placing substantial regulatory authority at state level. Additionally, the U.S. tradition of British common law adds further legal precedent. When a specific law does not define rules and standard of conduct, common law duties of care and negligence still present obligations. In the case of cybersecurity, best practices can fall outside of specifically defined statutory requirements and still be required under a duty of care (Shackelford, Proia, Martell, & Craig, 2015).

Individual Protections

The U.S. Constitution was created with the intention to empower individual freedoms and limiting governmental intrusion. While individual privacy was not explicitly stated as a fundamental right, privacy was eventually defined as a right through judicial interpretation of legal doctrine (Warren & Brandeis, 1890). In an interconnected world, the Federal regulatory regimes balance cybersecurity against privacy rights ascribed to individuals. This boundary may be most noted in monitoring and surveillance activities carried out by government. For instance,

the National Security Agency (NSA) collects information on millions of phone calls as part of its cybersurveiilance programs as part of compliance with the Patriot Act (Fisher, 2015). In a recent court decision on the level of lawful call information collection, the Second Circuit Court of Appeals in New York ruled that the NSA illegally overcollected call information. The judiciary addressed a specific balance between individual privacy rights and the needs of national security.

Legislative Power

According to Article 1 of the U.S. Constitution, Congress is endowed with the authority to create laws (Hamilton, 2005). The powers bestowed to Congress enable Congress to consider broad legislation, but Congress is traditionally biased toward enacting targeted legislation rather than broad legislation. One reason for the Congressional approach is the Tenth Amendment. Another important reason for more focused regulation is the structure of Congressional elections (Durr, Gilmour & Wolbrecht, 1997).

The Congressional approach to legislation is visible in the process to develop and enact cybersecurity legislation. Each year in Congress, legislation is defined as a set of legislative proposals. The legislative proposals are developed by specific committees such as the Homeland Security and Governmental Affairs Committee in the Senate and then approved for voting after hearings and development of negotiated legislative language. The complexity of this laborious process can be observed in the recent passage of the Cyber Intelligence Sharing and Protection Act (CISA). In 2011, President Obama's administration sent a proposal to Congress (White House, 2011). At the same time, a 12-Member House Republican Task Force issued a series of recommendations for the development of cybersecurity legislative proposals (U.S. Congress, 2013). In 2015, CISA was finally passed by both houses of Congress and signed by the President

as part of an omnibus budget-package (Risen, 2015). The legislation took more than four years to pass Congress and was passed budgetary reasons rather than its own merits.

Executive Orders

An Executive Order is a legally-binding order issued by the President that carries the legal weight of laws enacted by Congress (McNicholas & Mohan, 2015). With respect to cybersecurity, President Obama has made significant use of Executive Orders to enact protections. One recent well-known Executive Order is 13636 for Improving Critical Infrastructure Cybersecurity. This order enabled the development of the National Institute of Standard and Technology (NIST) Cybersecurity Framework which was designed as a set of best practices for organizations to voluntarily achieve better cybersecurity standards (Gregory, 2014). Private industry embraced the NIST standards, Shortly after the release, AT&T CEO Randall Stephenson indicated that AT&T would employ the NIST Framework as a baseline of requirements across its organization and for suppliers. Longer-term, it is hypothesized the NIST Framework could result in a global cybersecurity duty of care and that regulatory bodies such as the Federal Trade Commission (FTC) could use the NIST Framework as a private industry guideline to assess potential privacy enforcement actions (Shackelford, Proia, Martell, & Craig, 2015).

The Complexity of State Regulations

As previously mentioned, the Tenth Amendment limited an overly powerful centralized government by delegating powers to states (Hamilton, 2005). This has led to substantial complexity in cybersecurity regulation where the complexity is most evidenced in forty-seven states with differing data breach laws. On the more complex side, states such as Massachusetts require particular technical controls such as encryption to protect data at rest. In the event of a

data breach, Massachusetts requires notification to all impacted individuals and the attorney general. Massachusetts also established the right for individuals to seek potential damages (Swire & Ahmad, 2012). In contrast to Massachusetts, Wyoming uses a harm-based threshold that permits a legal analysis concerning notification, and notification is not automatic.

Impact of Private Industry's Cybersecrurity Compliance

Regulatory Enablement and Minimal Cybersecurity Standards

Overview. Even with the advent of the NIST Cybersecurity Framework, the U.S. sectoral approach to achieving cybersecurity governance introduces the opportunity for minimal standards and practices. Review of a case scenario for a hypothetical small tourist business located in New Mexico illustrates a potentially realistic scenario concerning the risks of minimal regulatory requirements and minimal cybersecurity practices.

Example Case. New Mexico does not mandate data security requirements or have data breach notification laws concerning disclosure of customer data. Without state-level cybersecurity requirements, the hypothetical tourist business can practice *de minimis* information security (Cole, 2015). The company is not required to employ the most basic of security defenses such as a firewall appliance. In the event of data breach, New Mexico does not impose security standards or notification to customers, and this tourist business could lack awareness about the need for other states' reporting requirements of security incidents or exposed customer data. The lack of security standards and notification requirements means that this tourist business could experience multiple data breaches and theft of customer data without having to be responsible for poor security practices. Finally, New Mexico does not offer individuals legal recourse to seek monetary damages for failure to notify individuals because of a breach incident. The lack of legal

recourse could lower the likelihood that this tourist business would comply with data breach reporting requirements in other states.

Since 2009, the White House has indicated that cybersecurity is everyone's responsibility (White House, 2009). However, state-level variability in cybersecurity governance has contributed to private industry minimum cybersecurity standards that contribute to national security risks.

FTC Promulgation of Data Security as an Enforcement Agency

Many private-industry businesses function in industries that lack cybersecurity standards (Swire & Ahmad, 2012). This often includes many small businesses. Cybercriminal and other hacking groups target these industry segments and small businesses because of low barriers to compromise (Yacowicz, 2012). For instance, more than 70% of all data breaches are targeted at small businesses with less than 100 employees, and nearly all credit card breaches in involve small business (Verizon, 2012). The Federal Trade Commission (FTC) has stepped in to advance privacy and data security standards through the use of its enforcement powers.

The FTC has expanded its role in fair trade practices to become an enforcement agency for private industry businesses that risk consumer safety with poor privacy and better data security practices (FTC, 2014). As of 2014, the FTC brought enforcement actions in over 130 spam and spyware cases and filed more than 40 privacy lawsuits. FTC settlements have included 20 years of required information security audits, changes in marketing programs, and even business closure in the case of Pairsys, Inc. Pairsys was found to have tricked seniors into payment for services related to software that was known to be free. One recent FTC court victory includes winning an appeal from the First Circuit Court of Appeals that upheld a verdict against Jerk.com for misrepresenting the use of mined consumer data (Morran, 2016). Privacy and data

security are components of cybersecurity programs, but the costs associated with FTC enforcement have contributed to private industry's adoption of better information security practices in lieu of potential FTC enforcement action.

Private Industry Initiatives toward Better Cybersecurtiy

There are cases where private industry has proactively set standards for cybersecurity, and the Payment Card Industry (PCI) is one such organization (PCI, 2011). PCI is well-known for tools such as the PCI Data Security Standards (PCI DSS). The evolution of PCI DSS has led to explicit minimum security requirements rather than mere guidelines (Shwayri, 2013). PCI DSS minimum requirements have delivered continual advances with each revision to further expand minimum security requirements. The importance of PCI DSS importance is evidenced through codification in legal statutes such as Nevada state data breach laws. Nevada laws regarding the security of personal information state, "If a data collector doing business in [Nevada] accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard" (NRS603A.215). Since most industries use major credit card brands for financial transactions, PCI has achieved broad private industry adoption of information security standards.

Conclusion

Private industry cybersecurity implementations are highly customized and variable. Cynersecurity practices range from non-existent compliance to exceptionally developed programs that influence broader adoption of better security standards. The Federal government seeks to close the variability in cybersecurity standards and practices in order to strengthen U.S. defenses against nation-states and terrorists. Through standards and legal enforcement, the U.S. regulatory regime also hopes to establish controls that create enduring cybersecurity.

References

Cole, T. (2015, March 30). Senate panel blocks New Mexico's data breach bill. Retrieved from http://www.govtech.com/state/New-Mexico-Senate-Panel-Blocks-Data-Breach-Bill.html

FTC. (2014). 2014 data and privacy security update. Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

Gregory, Holly. (2014, February 23). White House releases NIST Cybersecurity Framework. Harvard Law School Forum on Corporate Governance and Financial Regulation. Retrieved from https://corpgov.law.harvard.edu/2014/02/23/white-house-releases-nist-cybersecurity-framework/

Hamilton, J. (2005). Branches of government. Edina, MN: ABDO Publishing Company.

Javers, E., & Liesman, S, (2016, May 18). At time of Fed hack, Bank of Bangladesh targeted by others: Retrieved from http://www.cnbc.com/2016/05/18/at-time-of-fed-hack-bank-of-bangladesh-targeted-by-others-source.html.

McNicholas, E., & Mohan, V. (2015). Cybersecurity: A practical guide to the law of cyber risk. New York, NY: Practicing Law Institute.

Morran, C. (2016, May 18). Court upholds judgment against Napster co-founder in Jerk.com case. Retrieved from https://consumerist.com/2016/05/18/court-upholds-judgment-against-napster-co-founder-in-jerk-com-case/

Nevada Security of Personal Information, § 603A.215 (2015). Retrieved from http://www.leg.state.nv.us/nrs/nrs-603a.html

PCI. (2011, September 29). PCI DSS quick reference guide. Retrieved from https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Risen, T. (2015, December 18). A controversial cybersecurity bill rode a must-pass budget package to become law. US News & World Report. Retrieved from http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package

Shackelford, Proia, Martell, & Craig. (2015). Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Texas International Law Journal. Volume 50, Symposium Issue 2. Retrieved from http://www.tilj.org/content/journal/50/14%20SHACKELFORD%20PUB%20PROOF.pdf

Shwayri, R. (2013, November 2013). The impact of new payment card industry standards on business. International Association of Privacy Professionals (IAPP). Retrieved from https://iapp.org/news/a/the-impact-of-new-payment-card-industry-standards-on-business/

Swire, P. P. & Ahmad, K. (2012). U.S. private-sector privacy: Law and practice for information privacy professionals. NH: International Association of Privacy Professionals.

U.S.Congress. (2013). Federal laws relating to cybersecurity discussion of proposed revisions (E. A. Fischer, Author) [Cong. Rept. R42114]. Washington, DC: Congressional Research Service, Library of Congress.

Verizon. (2012). Verizon data breach report. Retrieved from http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

Warren & Brandeis. (1890). The right to privacy. Harvard Law Review, IV(5). Cambridge , MA: Harvard University Press. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

White House. (2009, June 4). Cyberspace policy review. Retrieved from https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

White House. (2011). Fact sheet: Cybersecurity legislative proposal. Retrieved from https://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf

Yakowicz, W. (2013). The big business of small business hacking. Inc. Magazine. Retrieved from http://www.inc.com/will-yakowicz/big-business-of-hacking-small-businesses.html