Equifax Incident Report

Tyler J. Latshaw

Southern New Hampshire University

IT-659 Cyberlaw and Ethics

Dr. Derek Holbert

September 26, 2021

TABLE OF CONTENTS

Case Introduction

Regardless of industry, various aspects of cyberlaw and security have made their way into everyday business operations, given the ever-increasing threat of data leaks and breaches. Three overarching trends can be seen among these principles: adherence to the law, ethics, and societal and cultural expectations. In particular, these principles can be applied to the business and tech industry for companies like Equifax, which recently suffered one of the most significant data breaches ever, resulting in the personal information of over 143 million people being stolen directly from the company itself (Fruhlinger, 2020).

Cyberlaw and Security Principles

Taking a look at the business and tech industry as a whole, it is clear how these principles can apply. For example, there are numerous laws and regulations in the United States and other countries that focus efforts on lessening cybercrime and protecting valuable and sensitive data and users accessing the internet. Any industry operating in these areas need to comply with the given laws. The United States, in particular, has even established the Cybersecurity and Infrastructure Security Agency (CISA), which is tasked with being the "Nation's risk advisor" working both in public and private sectors (Cybersecurity & Infrastructure Security Agency, 2018). While debatably not complete, these laws allow the government to intervene in public matters such as data breaches and support government agencies such as the FBI and Department of Homeland Security (Cybersecurity & Infrastructure Security Agency, 2018).

Beyond the legal concerns, there are also ethical and cultural principles for industries to consider while conducting any business online. At any given time, a company can hold countless information on their network about hundreds of millions of people across the globe. It is their duty to protect it ethically, without harming anyone they have data for (Computer Ethics

Institute, 2005). The same could be said for cultural reasons. These companies are in the industry for a reason, so if they do not consider cultural expectations, they likely will suffer a significant loss of customer trust.

Equifax Data Breach

Equifax is a great example of a company that did not follow these basic principles before and after its major data breach in 2017. Known as one of the leading credit reporting agencies, Equifax is unique in that it spans multiple industries, including e-commerce, communications, and more, but it is primarily centered in the business services and technology industry. Due to relaxed security protocols, international hackers were able to gain access to names, addresses, birthdates, social security numbers, and more for more than 40% of the United States population (Fruhlinger, 2020).

According to documentation, the incident began on February 14, 2017, about three months before hackers first breached the website when Apache Struts was first notified of a vulnerability related to HTTP requests. The company developed an open-source framework that Equifax and other companies used for Java applications (Fruhlinger, 2020). After issuing a patch for the vulnerability a few weeks later, Equifax failed to make the necessary upgrade needed, resulting in the breach through a customer complaint portal on May 14 (Williams, 2018). The hackers were able to continue undetected for months until the end of July when they were discovered. Equifax patched the exploit the following day on July 30 (Williams, 2018).

Despite the company discovering the breach in July, Equifax neglected to inform the public about the data loss until more than a month later, on September 7, 2017 (Fruhlinger, 2020). During this time, a number of serious ethical and cultural questions were raised by the public and the federal government as a number of top executives, including the president, CFO,

and CRO, sold their shares of the company days after the breach was discovered, which was believed to be insider trading (Fruhlinger, 2020). Beyond this, in the aftermath of the breach, additional cyber and ethical concerns were found, including Equifax unintentionally directing users to a phishing website and retirement payouts of the CEO totaling $90 million (Williams, 2018). Had Equifax followed these security principles from the beginning, the situation could have been handled a lot better on their part without losing as much business or even have been avoided completely.

Case Analysis

Ethical Issues

In any major data breach or cybercrime, ethics inevitably will be a talking point when analyzing the breach, and Equifax is not an exception to this. In some instances, the ethical issues listed are also legal and regulatory concerns as well. First and foremost, it is widely documented and understood that Equifax was not proactive in its security measures and protocols. Ethically speaking, since the company had sensitive consumer information, they should have acted quickly to patch any open vulnerabilities to the system, yet they had not, which ultimately left the breach to occur (McCombs School of Business, n.d.). The company knowingly left the vulnerability open.

Beyond this, there are also concerns of timely notification once the breach has occurred. According to the McCombs School of Business at the University of Texas at Austin, "Equifax officials became aware of the hack on July 29, 2017, more than a month before they let consumers know" (McCombs School of Business, n.d.). Consumers typically would feel that it is the company's ethical responsibility to properly notify anyone affected immediately so they can monitor their credit instead of allowing more than a month to pass. During this time, more

concerns were raised when four executives collectively sold millions of dollars in shares of the company (Fruhlinger, 2020). This insider knowledge of the data breach and the company's devaluation in the stock market gave them an unfair advantage. According to Georgia Law, where Equifax is located, the company does not have a specific timeframe in which they need to notify consumers; it just needs to be reasonable (OCGA § 10-1-912). By this, Equifax did not break any law in delaying a month unless someone contests it, but it is still not ethical in most perspectives.

Legal Compliance

In the aftermath of the data breach, extensive investigations were conducted, and it was found that Equifax was not fully compliant with various regulations, according to the Federal Trade Commission (FTC). In the lawsuit against Equifax, one of the biggest noncompliance issues mentioned by the FTC was the lack of security measures briefly mentioned above. This directly breaks the Safeguards Rule, 16 CFR Part 314, which mandates the protection and confidentiality of customer information by financial institutions and credit bureaus like Equifax (*Federal Trade Commission v. Equifax Inc.*, 2019). As proof of the infractions, the FTC specifically cited that the company received notification of the vulnerability from Apache Struts, issued a notification email from the security team to the employees that would make the changes for the patch, but then never actually followed through with the changes (*Federal Trade Commission v. Equifax Inc.*, 2019).

Further, it is noted in the lawsuit that Equifax was negligent in making even the most basic security measures to prevent attacks such as cross-site scripting or SQL injections. Despite the size of the company and the amount of properly trained security personnel, Equifax relied on automatic code scanning for threats, but the code was not even properly configured (*Federal*

Trade Commission v. Equifax Inc., 2019). This was also accompanied by the company failing to implement adequate controls for data access. Equifax stored administrative logins in plain text, unencrypted format as well as had live customer data including social security numbers available for testing, but the data was accessible to employees that did not need to view it, and when they did, there was no logging to notify the security team (*Federal Trade Commission v. Equifax Inc.*, 2019). All of these accusations directly breach the Safeguard Rule.

Societal and Cultural Impact

Unlike similar data breaches of the time and current, the Equifax breach did not target a specific demographic or social group purely for the fact that it affected over 40% of American citizens. However, the entire attack itself was targeted from China to the United States and was sponsored by the Chinese military (Fruhlinger, 2020). The breach as a whole did have a significant impact on the United States, namely over concerns of how Equifax was so relaxed with its security measures and the fact that there were a lot of deceptive practices at play (McCombs School of Business, n.d.). Additionally, it started to raise important questions about some of the nuances behind data protection and the moral and ethical compliance issues surrounding it. It can be argued that Equifax became a catalyst for the recent increase in individuals becoming more aware of data privacy.

In general, data breaches are something that affects almost everyone at some point in their lifetime. Just before the Equifax breach, a 2016 study found that only 26% of respondents remembered receiving notice of their data being compromised in the past year, but this number would have increased to at least 40% due to Equifax (Ablon et al., 2016). While it would be hard to say one way or another if a specific demographic is targeted until it is understood what data was stolen, it is clear that, on average, more than half of the individuals that have received notice

of a breach had been involved in two or more attacks in the same timeframe (Ablon et al., 2016). This is likely due to consumer habits or being more open with their personal information. Additionally, the same study found that typically higher-income and better-educated individuals better understand what is involved with a data breach and are more likely to remember it (Ablon et al., 2016).

Incident Impact

Regulations

The Equifax data breach has significantly impacted both the ethical and legal regulations surrounding data protection and information technology in general. In 2017 alone, Congress introduced three separate acts that would expand current legislation and add protection for citizens, as well as a host of other proposed changes. Known as the Data Broker Accountability and Transparency Act of 2017, proposed legislation was introduced to the Senate that would significantly increase the power of the FTC to enforce laws for data brokers and institutions (O'Connor, 2017). The legislation would act as a catch-all statement that allows the FTC to create new regulations as it sees fit.

Lawmakers introduced additional legislation to both the Senate and the House of Representatives, known as the Freedom from Equifax Exploitation (FREE) Act and the Personal Data Notification and Protection Act of 2017 (PDNP Act). At the time of the data breach, consumers may have needed to pay up to $10 to freeze their credit from things like new loan applications, so the FREE Act would have wiped this requirement as well as created a universal way to freeze credit reports with all three major agencies since, at the time of writing, each had its unique process and potential fee (O'Connor, 2017). The PDNP Act also had direct ties to Equifax and worked on increasing regulation for proper notification after a breach. As previously

mentioned, Equifax would have needed to follow Georgia's law since there is no federal law for timely notifying individuals. The proposed act would remove all state laws and create a common requirement and template that companies would need to follow, which would enforce a 30-day window to notify consumers (O'Connor, 2017).

Standards

Not only was Equifax non-compliant in several laws and regulations, but they were not up to the standards that would be expected of a company its size, especially dealing with the nature of the information they had on consumers. In general, it can be expected that any company will at least have a protocol or procedure in place to detect and respond to attacks, yet Equifax did not find the attackers in the system for months (Fruhlinger, 2020). Beyond that, the company properly notified the correct teams when the vulnerability notice was issued to them, but no one ever implemented the fix for it, despite actually having a defined process for this (*Federal Trade Commission v. Equifax Inc.*, 2019).

As noted by the FTC, there were also several industry standards that Equifax did not follow that partly contributed to the data breach. These standards included not using proper security measures to segment databases from application servers, failing to enforce access controls related to the storage of plain text social security numbers and logins previously mentioned, as well as failure to provide adequate training in computer security to its software engineers and company as a whole (*Federal Trade Commission v. Equifax Inc.*, 2019). While it did have a defined privacy policy listed on its website at the time, Equifax failed to follow even its guidelines (*Federal Trade Commission v. Equifax Inc.*, 2019). Privacy policies are a baseline standard within online industries such as this.

Cultural Impact

The Equifax data breach was one of the largest and costliest cyberattacks ever recorded in terms of severity. The impact to individuals across the country and even the world is incomputable given the scope, but it is also important to note the cultural impact that has resulted from the attack and other similar instances. Debatably, this one example affecting almost half of the country had the power and influence to shift attitudes of technology and use of consumer data negatively. According to Forbes, the breach has started raising the discussion across consumers about how much of a tradeable asset they are instead of a customer and how helpless they are against major corporations. Additionally, the impact has started shifting the discussion from consumers to lawmakers who advocate based on the new views of cyber communication (Disparte, 2017).

While cultural attitudes toward cyber communication around this scenario have been negative, some of the impacts have remained positive. As a result of Equifax's attack, senior managers across all companies, both small and large, have started becoming more familiar with and involved with their own company's policies. Instead of simply meeting the minimum standards, companies are now aiming for higher standards of security controls and protocols (Talley, 2017). They are finally adopting the mindset of "it won't happen to us" and moving more toward "it can and will happen to us." Globally, Equifax is just one data breach in a long list of others, and it will not completely change the way people look at technology, but it did have some level of impact, both positive and negative.

Recommendations

Organizational Changes

According to news articles, the hackers were able to hack into the system through an open vulnerability in a customer complaint form since Equifax was using the Apache Struts framework. The vulnerability, known as CVE-2017-5638, was announced by Apache on March 7, and the hackers gained access just three days later, on March 10 (Fruhlinger, 2020). In theory, if Equifax had implemented the patch that Apache provided promptly, the entire attack and breach could have been avoided, and no one would have been affected or had their data stolen. According to the same article, an administrator at Equifax had initiated a request to have the vulnerability patched, but the employee responsible for it failed to fix it. A later code scan revealed a significant number of vulnerabilities in the systems (Fruhlinger, 2020).

Given this information, Equifax's information technology department would have benefitted from several organizational changes that could have protected the company from the attack. First and foremost, the department should have implemented an official process for requests like these that are a security matter for the company. It should have been made clear through documentation and training what the expectation was for implementing it, the potential for a catastrophic breach, and the consequences of not following protocol. Further, the administrator who initiated the request should have been responsible for following up regarding it or delegated it to another manager if they were not suitable. Ultimately, the department should have been organized to have a clear hierarchy of responsibility for situations surrounding security.

Ethical Guidelines

Given the size of Equifax, the company's IT department should have a formal code of ethics documented for its employees to follow, or at least subscribe to a publicly available version such as the Information Systems Security Association's (ISSA) code of ethics (Information Systems Security Association, Inc., 2019). A code of ethics is a great way to have a set of expectations and guidelines for a team or department to follow if there is no specific company rule in place. Depending on the company, not following the ethics agreed upon could result in disciplinary action as the guidelines are implemented to make the company better and help protect its customers and its employees.

At a minimum, the implemented code of ethics should include a reference to following all generally accepted security practices for the field, following all local, state, and federal regulations and laws, and properly managing and handling confidential information, both surrounding the company and its customers. In addition, it could include references to not attempting to access or view information that is not essential for the employee's direct job and treating every task or system as if they were the customer — having ethically sound employees could have prevented this attack because the employees would have known proactively to treat the Apache patch as a higher priority situation.

External Standards

Based on the information presented in the case against Equifax, the main laws and regulations surrounding credit reporting companies focus primarily on safeguarding information by whatever means necessary by the company; however, they do not go into specifics (Federal Trade Commission v. Equifax Inc., 2019). What one company might deem as appropriate might be completely less than another company. It would be beneficial in situations like this to have a

clearer understanding of the minimum standard of protection. Further, since the company has sensitive information such as social security numbers, it should properly document and register its security practices with the government. If the government knew Equifax was using Apache Struts, they could have followed up with Equifax directly to ensure they implemented the patch.

Global Considerations

International Compliance

Given that Equifax collects data from across the globe, the company needs to comply with various international standards. The primary set of compliance standards for any organization, let alone credit reporting agencies is through the International Organization of Standards (ISO). The ISO is the foremost authority on global standards across different areas, let alone information technology, information systems, and information security. The ISO has a specific family of standards known as the 27000 family. This set of standards specifically aims to provide companies of any size a minimum and expected standard for the security of information systems (ISO, 2013). Equifax was more relaxed on its security policies based on the information already discussed. Still, this family of standards could have helped prevent the breach because of needing to comply with ISO. It is worth noting that there are other additional standards that Equifax could comply with, such as ISSA mentioned above, but none are as prominent and widely accepted as ISO.

Cultural Impact

Considering the entire Equifax data breach affected more than 40% of the entire United States population, saying that it had a significant domestic and international impact on the culture of information systems and security is an understatement. Immediately following the breach, news traveled fast, making headlines across the globe. Not only was the attack bad

enough, given the size and scale of it, but it was also found to be directly sponsored by the Chinese military (Fruhlinger, 2020). In America alone, one survey found that as many as 84% of Americans were aware of the data breach, a higher number which can be attributed to how fast the news spread (Brown, 2018).

The overarching question raised around this incident is that individuals do not have any control over whether or not their information was included in credit reporting databases such as the ones at Equifax (Brown, 2018). Unlike other data breaches of the time, such as Target, customers had the option of not having their information included by not going to the store, but they did not voluntarily provide information to Equifax in most cases. While this seemingly has not led to any loss of commerce related to the company, this has caused individuals to worry if their data is safe. After the attack, there was a significant spike of over 57% of individuals checking to see if their data was compromised related to the breach. While the incident was not a positive event and caused a lot of financial strain on impacted individuals across the globe, it did create a small culture of being more aware of what information is available on individuals and what new laws and regulations are necessary to protect it.

In general, the connection humans have with computers and technology is a unique one that closely parallels our relationship with other individuals. Originally published by Nass and Moon in 2000, an experimental study found that humans tend to have an anthropomorphic approach to computers. Essentially, the average person approaches and treats a computer as if it were a human instead of a machine, although they fully understand it is not human nor has any level of consciousness (Nass & Moon,

2000, p. 93). This close connection between mind and machine can become frayed from incidents like the Equifax data breach. Just as how someone could lose trust in a friend or colleague if they shared private information about them with a third party, humans have the same potential to gain distrust in technology. As the world progresses further and relies more than ever on technology and security for everything from use in surgeries to flying an airplane safely, it is imperative for forward movement and trust in computers.

Global Technology Environment

Based on research, there has been little impact on new regulation on the global scale based on the Equifax impact. However, several new standards and regulations could be implemented similar to the ones mentioned previously. These include requiring reporting agencies like Equifax to register their security practices and software that they use, as well as requiring a specific minimum standard. That being said, there were a number of laws that were created or proposed domestically in the aftermath of the breach. Two primary bills in Congress include the Data Broker Accountability and Transparency Act of 2017, which creates new privacy and security standards, and the Personal Data Notification and Protection Act of 2017, which forces stricter requirements on notifying customers of breached data. Additional bills on the state level were proposed, including the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017, altogether banning social security numbers from being used in credit bureaus, effectively making that data less desirable for hackers to steal (O'Connor, 2017).

While the Equifax breach has not had a significant impact on laws and regulations on the global level, it has started a new conversation surrounding data protection and has spurred the movements listed above. The impact of the attack will likely be seen for many years to come,

given the depth of the number of records and information stolen. Despite this, it has started an extremely important conversation both with general consumers globally and the lawmakers and non-profits that set the regulations that companies need to follow. It will be a long process to implement any new laws formally, but when they do, Equifax will be following them to avoid another catastrophic failure.

Summary

Equifax is the perfect example of why laws change over time. Technology develops, hackers get better, and laws become less relevant or no longer adequately encompass their original intent. After a careful analysis of the Equifax data breach, it is clear how fragile information security can be and how problematic it can be if a breach occurs. Even a simple process that is lacking on the business side of a company can have major downstream effects. For example, Equifax had a formal process established to implement security patches; however, it was not followed by the employees it was built for. As a result, hackers could exploit a small vulnerability, penetrate a secure system, and steal data for hundreds of millions of people.

Additionally, Equifax failed to have a proper security control even to detect the hackers within their system. While it can never be said with complete certainty, it can be hypothesized that if Equifax had better embraced a sense of security and followed industry and global standards, they could have avoided this entire event. Had the employee responsible for the patch issued it when required, the company would not have needed to pay massive fines to consumers and the government.

Further, it can be concluded that the current laws surrounding the protection of information systems are somewhat vague. For example, the GLBA previously mentioned has a specific Safeguards Rule that dictates companies must make an adequate attempt to protect

sensitive information, but it does not say how. Before the breach occurred, an internal audit may have found the current protections perfectly sufficient, but clearly, a data breach still happened. Laws similar to this are a viable way to instill a small sense of urgency with companies, but they give the impression that the government can only enforce them after it is too late – after a data breach or cyberattack occurs.

References

Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. Rand Corporation. https://www.rand.org/pubs/research_reports/RR1187.html

Brown, M. (2018, October 29). *One Year Later: The Impact of Equifax's Data Breach*. Transforming Data with Intelligence. https://tdwi.org/articles/2018/10/29/biz-all-impact-of-equifax-data-breach.aspx

Computer Ethics Institute. (2005). *The Ten Commandments of Computer Ethics*. Computer Professionals for Social Responsibility. http://cpsr.org/issues/ethics/cei/

Cybersecurity & Infrastructure Security Agency. (2018). *About CISA*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/about-cisa

Disparte, D. A. (2017, October 2). The Equifax Breach And The Case For Digital Identity. *Forbes*. https://www.forbes.com/sites/dantedisparte/2017/10/02/the-equifax-breach-and-the-case-for-digital-identity/?sh=785328f84e24

Federal Trade Commission v. Equifax Inc., (United States District Court for the Northern District of Georgia July 22, 2019). https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf

Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO Online. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Ga. Code Ann. § 10-1-912 (Lexis Advance through the 2021 Regular Session of the General Assembly)

Information Systems Security Association, Inc. (2019). *ISSA Code of Ethics*. ISSA International. https://www.members.issa.org/page/CodeofEthics

ISO. (2013). *ISO/IEC 27001 Information security management*. International Organization for Standardization. https://www.iso.org/isoiec-27001-information-security.html

McCombs School of Business. (n.d.). *Equifax's Breach of Trust*. Ethics Unwrapped; The University of Texas at Austin. https://ethicsunwrapped.utexas.edu/video/equifaxs-breach-of-trust

Nass, C., & Moon, Y. (2000). Machines and Mindlessness: Social Responses to Computers. *Journal of Social Issues, 56*(1), 81–103. https://doi.org/10.1111/0022-4537.00153

O'Connor, B. J. (2017). *After Equifax Data Breach, Here Are 8 Changes Lawmakers Propose*. LifeLock; NortonLifeLock Inc. https://www.lifelock.com/learn-data-breaches-after-equifax-data-breach-here-are-8-changes-lawmakers-propose.html

Talley, K. (2017, October 17). *Equifax breach's positive impact: CIOs and CEOs talk more to each other about cyber issues*. FierceCEO; Questex LLC. https://www.fierceceo.com/technology/equifax-important-conversation-starter

Williams, H. (2018, November 28). *Equifax Breach Timeline*. GracefulSecurity; Akimbo Core Ltd. https://gracefulsecurity.com/equifax-breach-timeline/