An Analysis of the Human Factor in the Equifax Data Breach

Melissa Genovese

Collin County Community College

CYBR-4320.201

Professor Ted Sanders

April 21, 2023

Table of Contents

An Analysis of the Human Factor in the Equifax Data Breach

Introduction

The Equifax data breach that occurred in 2017 was unprecedented in the sense that it affected many companies and over a hundred million people in the United States. This data breach was preventable, but as a result of multiple mistakes, Equifax was unable to prevent this data breach, and this allowed the attackers to continue to steal personal identifiable information (PII). When the breach was eventually discovered, Equifax was slow to tell the public, and their remedies to try and help those who were victims were underwhelming, and it was believed that this had made the situation worse. The public and the government lost confidence in Equifax, and investigations had to be conducted and completed. Once those were completed, Equifax had to pay fines and reparations, then was required to change how their operations were run, and they are accountable to government oversight. This case study will focus on how the human factor contributed to the data breach and how these mistakes were allowed to continue for as long as they did, conclusions will be drawn, and solutions will be proposed to avoid a similar situation in the future.

Background

Equifax is the largest of the three main credit reporting agencies after it made a company goal to expand in 2006 and acquired 18 different companies in a span of a decade (Kabanov et al., 2021). Consumers and businesses rely on credit reporting agencies for many things ranging from obtaining loans and getting employment; thus, credit reporting agencies hold very sensitive

personal identifiable information and are trusted to safeguard this information with the utmost care. In their own 2016 annual report, Equifax said that they hold data on 91 million businesses and 820 million consumers, so the fact that 143 million consumers were impacted with such sensitive personal identifiable information is egregious (Kabanov et al., 2021). When they told the public, the impact on the company was also enormous, as their stock fell 13% and lost 34% of their company's value (Kabanov et al., 2021). What makes this particular breach interesting is that it was avoidable and how the human factor played a huge part in the process of how this breach happened.

On the surface, how the breach happens seems mostly inhuman if one looks at the events leading to the breach and the results afterward. On March 8, 2017, US-CERT notified members of Equifax of the Apache Struts 2 CVE-2017-5638 vulnerability, and they performed a scan, but on the wrong directory, so they think they are okay (Kabanov et al., 2021). On May 13, 2017, the attackers had access to Equifax ACIS, and for 76 days, the extraction of data went unnoticed until July 29, 2017, when the breach was first detected and then 40 days later, Equifax finally notified the public (Kabanov et al., 2021). Additionally, this can seem like the fault of systems or tools, but humans played a very important role. According to Calvin Nobles, humans are the cause of 90% of cyber incidents, and training in cybersecurity is lacking investment, and it goes mainly towards technology instead (Nobles, 2018). Some of the common mistakes cybersecurity professionals make are network misconfigurations, vulnerabilities in technology, actions that are directed by leaders, being non-compliant, violating operational procedures, and being mentally distracted (Nobles, 2018).

Many of these reasons mentioned played a part in the Equifax data breach in 2017. Humans are creatures of habit, can be influenced by various factors, make mistakes, and in essence, cannot be

made to follow the rules strictly as if they are programmed with lines of code. It is important to consider human nature and psychology in what will be referenced as the "the human factor" and how it plays into Equifax's non-functioning program operations that led to the data breach.

Contributing Factors

Prior to the breach, certain events happened that could have prevented the breach from ever occurring if Equifax's program operations had been functioning correctly. The only way to have their program operations functioning correctly is to have humans capable of making the operations set in place so they can work as they should and, once set in place, make sure that humans are doing their roles as described in the program.

One contributing factor was that they were using an inefficient manual way to manage SSL certificates. Equifax realized that they needed a better solution to manage their hundreds of SSL certificates in 2016 by utilizing an automated tool, but their tool had not completed implementation by the time of the attack (Kabanov et al., 2021). If the humans involved in the decision-making process had decided the priority of this automated tool, this would have been recognized sooner or implemented quicker before the breach occurred. However, because humans did not make the correct judgement calls, SSL certificates were still expired, and this kept the IDS/IPS from analyzing traffic as it should have been able to. The Snort rule that was put in place on IDS/IPS on March 14, 2017, did not detect the exploitations, and the ISec Team thought everything was functioning correctly because they thought the IDS/IPS was functioning as it should (Kabanov et al., 2021). This shows a faulty program and how it operated, and the humans involved did not have the capacity to resolve this issue and also complacency to not think with defense in depth which would point to human laziness. They may have been doing

their jobs, but they were not thinking about the seriousness of the issue, and the employees were only doing the bare minimum.

Another contributing factor that happened before there was a vulnerability found in Apache Struts 2 was that threat actors could have found out that they were using Apache Struts 2 via Google dorking (Kabanov et al., 2021). This means that their ACIS technical details were out to the public for consumption and should have never been allowed if following proper governance (Kabanov et al., 2021). This could have been prevented through proper documentation to protect sensitive information such as their technical details, and again, human lack of thought about needing these necessary policies is evidence of faulty program operations.

Another major problem with their program operations concerned the lack of an adequate password policy, which again could be pointed to the human factor and lack of imagination, will, or concern for securing Equifax's network and systems. Their password policy was not strong, even for privileged accounts; one database that the attackers accessed "was protected with a four lower-case password, which matched the database's name," and they were also not encrypted and did not utilize the principle of least privilege. (Kabanov et al., 2021). This allowed the attackers, once they were moving around laterally within the network, to freely and easily move around, which is another level of showing the lack of competency of those in charge to be in charge and do what was necessary to protect the systems.

Part of having a program that operates correctly has knowledgeable humans in place to do their jobs, which means having other humans hire the right people to fill these positions. The lack of will or wherewithal for those in charge to do this simple task can end up in a horrible situation regardless of the role, but in this case, it led to another contributing factor of how the exploitation was not detected, so immediate remediation could take place.

The ISec team performed the scan to find the CVE-2017-5638 on the wrong directory (the root directory) instead of the subdirectory, where Apache struts were actually located, and the main reason for this was their lack of knowledge of how Apache Struts 2 worked; thus, IT was never told about the vulnerability and on top of that, communication between IT and ISec was lacking. (Kabanov et al., 2021). This is an example of how having people in positions that were lacking knowledge did not help the situation, and those that hired them did not do their jobs either (could be for any reason of the human factor). The lack of communication further shows how operations within the program were severely falling short due to the humans involved in the process, and the vulnerability was allowed to gain a foothold in Equifax's network from the beginning.

To have a program operating at its best to avoid situations such as the Equifax data breach, one has to have communications in place between the right departments and then communication between those working within those departments. This communication is not only necessary from department to department, but it works from the top down as well as from the bottom up. Not having these working communications in place is part of the human factor of not addressing the issue, and this allowed for another gap of people not being aware of a potential problem giving more opportunity for the vulnerability to slip into Equifax's network, allowing for the disaster to occur the way it did.

There were major communication problems in alerting those needing to know of the vulnerabilities. The ISec team receives alerts from US-CERT, but the ACIS operator was not alerted to it because they were not on the list to be contacted, and the senior vice president's team also failed to alert ACIS (Kabanov et al., 2021). This failure to notify the vulnerability of those who needed to know was a direct result of the human factor in a program not operating correctly. If measures had been made to ensure that the ACIS operator was on the list or that the

vice president's team would have contacted the appropriate team members about the vulnerability, then there probably would have been an opportunity for those who were responsible for putting a patch in place that would have possibly halted or stopped the vulnerability from gaining a foothold in Equifax's network and systems.

Equifax's programs were operating horribly on every single level, and the following contributing factors discuss how humans had failed to take into account when it is appropriate to be either proactive or reactive when it came to issuing patches showing that their program's operations led to massive gaps that allowed the exploitation to exist in their network and systems for as long as it did. Another issue is how taking an auditor's recommendations seriously and implementing them when told to is a human factor contributing to gaps in their operations.

Equifax had implemented a reactive program when it came to patching vulnerabilities even when an audit conducted internally in October 2015 had recommended that Equifax go with a proactive approach instead and was given a deadline of December 31, 2016, for this to be completed, but because it was not within the IT teams priorities, it was not finished until May 2017 (Kabanov et al., 2021). Additionally, the lack of people with the ability to make such decisions in the IT department shows how incapable they were of being able to prioritize and implement the proactive approach to patching properly. When the program was finally finished late in May of 2017, it was too late as the vulnerability was exploited, and data was allowed to be exfiltrated for 76 days by the attackers until the expired SSL certificates were finally found months later (Kabanov et al., 2021). The inability to properly prioritize what needs to be fixed is instrumental for any organization, let alone Equifax, and it shows how humans were very lacking in their ability to make sure that their program was robust and operating as it should.

One of the most egregious inactions that Equifax failed to do was how they handled their PII. The PII was not encrypted, and if it had been then, the information that the attackers had gathered could have been a non-issue at best, or the risk reduced further at the least, and this also made them PCI-DSS non-compliant since credit card information was also stolen, they collected and stored unnecessary data, and they did not have a data loss prevention (DLP) system in place (Kabanov et al., 2021). This again highlights how their program operations were lacking on another level and again points to human laziness for not doing the bare minimum and creating proper policies or adhering to them if they were in place. If this had been properly in place, with the right crew in place to take these actions and encrypt the PII, then the whole breach could have been a non-issue. Then the pure negligence of not being PCI-DSS compliant is another way the human factor came into play. It seems that with a combination of poor program operations and all the factors that make humans human, this was allowed to slip as well.

Governmental Response and National Security Impact

The Equifax data breach was so egregious that there was a massive response from many different entities within the United States. Investigations were conducted by the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), FBI, and the Securities and Exchange Commission (SEC) along with the Atlanta US attorney were involved because of an Equifax stock sale (two-million dollars) around the time of the breach with 34 attorney generals from other states also investigating (Miyashiro, 2021).

There were investigations by various Senate and House committees, such as the Homeland Security Permanent Subcommittee on Investigations, the Senate Commerce, Science, and Transportation Subcommittee, the House Financial Services Committee, the House Energy and

Commerce Committee, the Senate Banking, Housing, and Urban Affairs Committee, the Senate Banking Committee, and the Senate Judiciary Subcommittee on Privacy with most concluding that Equifax was at fault for being neglectful (Miyashiro, 2021).

Equifax was sued by various state and local governments, such as San Francisco as well as Chicago, for violating the Illinois Personal Information Privacy Act, the Chicago Fraud Ordinance, and the Illinois Consumer Fraud and Deceptive Business Practices Act and were sued by the Attorney Generals of Massachusetts and Indiana (Miyashiro, 2021).

Equifax settled with the FTC, forty-eight states, Puerto Rico, D.C, and the CFPB in July 2019 on behalf of the 147 million people affected by the breach for $700 million for compensation and fines, of which $300 million went to those whose information was exposed (Miyashiro, 2021). They also paid $100 million for civil penalties to the CFPB, and $175 million was paid to states, with $125 million being paid for compensation to consumers for out-of-pocket costs as needed. There were also settlements of $19.5 million and $18.2 million made independently with two states, Indiana and Massachusetts, respectively, with Equifax. (Miyashiro, 2021).

FTC said that Equifax had not been compliant with the Gramm-Leach-Bliley Act's Safeguards Rule in which they had failed to "develop, implement, and maintain a comprehensive information security program to protect the security, confidentiality, and integrity of customer information" (Miyashiro, 2021). Part of the agreement was that they were required to put into place a complete information security program to make up for their failings to do so previously (Miyashiro, 2021).

They were also to provide six additional years for consumers who filed claims to receive free credit monitoring services after their initial four years expired and were eligible to be

compensated for the time spent overcoming fraud and identity theft, as well as identity restoration services (Miyashiro, 2021).

After the FTC settlement, there were strong desires for legislation to be drawn in order to hold credit reporting agencies accountable with written legislation, and in 2018, Senators Mark Warner and Elizabeth Warren presented legislation called the Data Breach Prevention and Compensation Act in direct response to the Equifax breach (Miyashiro, 2021). It would penalize if consumer data was not protected in a measure to better protect consumers and have supervision over CRAs data security, as well as compensate consumers if their data was stolen again, with $100 per each consumer who had compromised personable identifiable information with $50 for additional compromised PII; however, it is still not law (Miyashiro, 2021).

Another piece of legislation was passed in March 2018 called Economic Growth, Regulatory Relief, and Consumer Protection Act which gives consumers the ability to freeze their credit for free and to put fraud alerts for one year on their accounts (Miyashiro, 2021).

Besides the massive impacts that the Equifax data breach had on consumers, companies, and the various governments in the United States, there was also a huge national security risk implication to the United States. The first attack was made by hackers with little skill who probably used a hacking kit to achieve infiltration, but soon they were in over their heads and realized how much valuable the breach was and likely sold their advances to more skilled hackers who were backed by the Chinese state (Fruhlinger, 2020). Investigators have reason to believe that Equifax's data breach is related to two previous big breaches that were not as impactful as PII was not disseminated on the dark web, to the 2018 hacking of Marriott's Starwood hotel brands and the 2015 hacking of the U.S. Office of Personnel Management (Fruhlinger, 2020).

The big question is understanding why the Chinese government would want data from Equifax, and that would be that there appears to be an operation to collect data on millions of Americans to create a "data lake" in order to learn about U.S. intelligence operations and government officials, and spies in order to learn of potential avenues for blackmail or bribery if they were in financial trouble (Fruhlinger, 2020). Suppose over a third of Americans had sensitive, personable identifiable information stolen, which is now in the Chinese state's hands; In that case, there is a good chance that information is known about important American politicians and officials who could put the welfare of the country in a dangerous state if they were in a state to accept a bribe. In an exceptional act (because the U.S. wants to avoid any sort of retaliation against American operations), the United States Department of Justice charged four Chinese military members with the attack (Fruhlinger, 2020). The fact that the Equifax data breach was so flagrant that The United States Department of Justice made an unprecedented move against the Chinese government is not a thought to shrink from.

Industry Impact

Americans rely on credit reporting agencies (CRAs) for many things in their lives, including getting loans for cars and houses, the ability to acquire credit, and even the ability to obtain employment in some circumstances. Therefore, CRAs hold the very livelihoods of Americans in their hands. They cannot opt out of having their personal identifiable information collected by the credit reporting agencies, so CRAs have a duty to keep this data confidential and secure with its full integrity because if the integrity were to be lost or if the data was stolen, this could impact a person's credit score and possibly their ability to make purchases and potentially affect their ability to be financially stable (Miyashiro, 2021).

Credit reporting agencies must keep PII secure to keep it from being stolen and used to steal a person's identity. If the integrity is broken, then banking industries that assess this data to decide whether to give loans or make other financial decisions regarding their customers will no longer value the data that CRAs supply them, and this could impact the American economic infrastructure (Miyashiro, 2021). This incident affects not only the American population and American security in the world but also America's economy.

Going forward, Equifax has to prove that they have learned from its mistakes and prove that they are handling American's most sensitive data correctly and with the respect that it deserves in order to gain the trust back from those who were victimized. Legislation needs to hold all credit reporting agencies to this high standard that they must meet. CRAs must be transparent in the way that Equifax was not once they found out that a breach had occurred, and this breach also showed how inadequate the payments given to victims were as they were so small and could not possibly match the harm that could have been caused to certain individuals (Miyashiro, 2021).

For all these reasons, in summary, CRAs have a high threshold to meet on all levels in order to hold the trust of American consumers and to ensure that the American economy will not be affected, as well as to keep American national security safe.

Conclusions

After reading through the contributing factors and considering the impact it had on financial and credit reporting agencies, all the tax-payer money spent by the government to perform their investigations and put legislation into law, how consumers were harmed, victimized, and treated with so little care after, and then to think about how Equifax put the United States's national security in harm's way, it is very easy to say that the 2017 Equifax data breach was

unprecedented. For this to happen, as was shown in the contributing factors, the program had to have failed on many different levels, and this could point to the fact that policies were either not created or were not adhered to.

The one underlying theme in all the failings that led to the Equifax breach and the events after is the human factor. If there had been more competent humans in the roles discussed in the contributing factors before, during, and after the breach, then it is possible that policies and plans would have been in place to form a program that would have prevented this incident. Considering the fact that no matter how robust a program is, humans will still make mistakes, it should cover those few mistakes if a defense in depth approach is factored in.

This incident should be studied in every facet in order for other companies that manage and control consumers' PII to ensure that a disaster like this incident never happens again.

Internal Audit Plan Recommendations

There were internal audits that were completed before the breach, such as the 2015 finding that a reactive approach towards patching was not working and that a proactive approach needed to be implemented. However, it was not completed in time for the attacks, so it was of no use. For the purpose of this analysis, the recommended audits are more human-focused in regard to making a strong vulnerability program with the appropriate policies, procedures, and plans in place.

One of the first steps would be to look at the policies that make up the program and read through them to ensure there are no gaps. Included in this would be written ways instructing people how to communicate in case of an incident, vulnerability, or problem occurs and testing to make sure that those communications actually work. The second would be to ensure that the security program is thorough with the correct procedures and topologies to ensure that the network is

secure at all times and encrypted. Thirdly would be to check that there are policies in place to make sure that the network is secure, even with a few human errors, considering defense in depth.

Lastly, measure and test the working culture in the Equifax environment. As humans seem to be the common denominator in all of the events that contributed to the breach, this is especially important. Checks would need to be conducted to make sure that those who need to communicate can and are comfortable in doing so, that knowledgeable people are put in their proper roles upon hire, and that there are policies in place to address these issues and then go back and check to make sure they are being followed on a regular basis.

Appendix A- Acronyms and Abbreviations

ACIS- Automated Consumer Interview System

CFPB- Consumer Financial Protection Bureau

CRA- Credit Reporting Agency

DLP- Data Loss Prevention

FTC- Federal Trade Commission

IDS- Intrusion Detection System

IPS- Intrusion Prevention System

PCI-DSS- Payment Card Industry Data Security Standard

PII- Personal Identifiable Information

SEC- Securities and Exchange Commission

SSL- Secure Sockets Layer

Appendix B- References

Fruhlinger, J. (2020, February 12). *Equifax Data Breach FAQ: What happened, who was affected, what was the impact?* CSO Online. Retrieved April 4, 2023, from https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Kabanov, Ilya & Madnick, Stuart. (2021). Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. MIS Quarterly Executive. 20. 4. 10.17705/2msqe.00044.

Miyashiro, I. K. (2021, April 30). *Case study: Equifax data breach*. Seven Pillars Institute. Retrieved March 30, 2023, from https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

Nobles, C. (2018, March 15). *Shifting the Human Factors Paradigm in Cybersecurity*. NIST. Retrieved March 24, 2023, from https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/17.pdf

Appendix C- Peer Review

This case study was peer-reviewed by [redacted] on April 13, 2023.