Equifax Data Breach 2017

Lilibeth Rodriguez Sanchez

Old Dominion University

CYSE 300

Malik A. Gladden, MS.CYB

1/21/2024

Description on Equifax Data Breach 2017

In September of 2017, Equifax unfortunately was hit with a data breach. Equifax is considered to be one of the three largest credit reporting agencies in the United States. “This data breach allowed for hackers to be able to receive 147 million individuals’ personal information” (Federal Trade Commission). This data breach allowed hackers to be able to access information like social security numbers, driver’s license numbers, names, home addresses, phone numbers, and much more. Not only was personal information accessed by these hackers but also “the credit card numbers of approximately 209,000 consumers were also breached” (Epic). Unfortunately, such information being stolen, it is easy for these malicious users to use that information for malicious purposes. These hackers having access to individuals’ personal information allows for these malicious users to be a capable to really affect individual’s personal lives. Identity theft is a terrible crime due to the harm that they can cause towards a person’s life. Identity theft can completely affect a person’s financial future as well as their personal life. Some ways that these criminals can affect a victim’s life is by opening bank accounts, applying for credit cards, taking out loans, and conducting other financial activities. “Some examples of consequences of identity theft include, being denied of credit card and loans, being unable to rent an apartment or find housing, paying increased interest rates one existing credit cards, having greater difficulty getting a job, suffering severe distress and anxiety, etc.” (Epic). Those are just a few examples on how the consequences of having your personal information accessed by these malicious users can derail your financial future.

Cybersecurity Vulnerabilities regarding data breach

While researching this data breach I was able to conclude that the vulnerability was due to the Apache Struts web application software. This is a tool used when using the Equifax

dispute portal. A patch was available two months before the breach but unfortunately Equifax did not keep up with proper security measures and failed to ensure that their systems were updated. Not only was this the main vulnerability but there were also other factors that allowed the data breach from easily happening. Some of those factors included “insecure network design which lacked sufficient segmentation, potentially inadequate encryption of personally identifiable information, and lastly ineffective breach detection mechanisms” (Epic). These were some of the vulnerabilities that caused for this data breach to occur and negatively affect many people’s lives.

Threats

The main threats of this crime included four Chinese military men who were able to discover the flaws in the software that was used to dispute issues with their Equifax credit reports. These men were able to discover the vulnerabilities in the Equifax system allowing them to be able to gain access to the information of these consumers. “These hackers were able to operate unseen for about 76 days” (Epic). These hackers were the main threats by gaining access to the personal information of 147 million individuals.

Repercussions

This breached allowed for several repercussions including a significant drop in share prices, loss of trust of the system, and a significant drop in fines. These repercussions were extremely difficult to regain immediately. Not only were there repercussions for Equifax but also for the consumers. The consumers repercussions included potential identity theft and fraud. The repercussions have negatively impacted the victims making it difficult for victims to return to their normal financial life.

Mitigation Measures

The Equifax system has many vulnerabilities that allowed for the hackers to easily be able to breach the data. To prevent such consequences from happening it is crucial that there are mitigation measures in place. The breach could have been prevented by ensuring that updates are being made repeatedly as well as making sure the systems are being patched. Another way to prevent such breaches from happening would be developing a robust cybersecurity framework that would include vulnerability assessments, intrusion detection systems, and specialized response plan would allow prevention of such consequences from happening.

Such incidents like these are prime examples of the consequences that can happen when not having the correct cybersecurity measures in place that can help prevent such incidents from occurring. Data breaches involve many threats, vulnerabilities and repercussions that can be avoided. Ensuring that their mitigation measures in place will allow such consequences form happening and ensure that the systems are operating in a safe way.

References

Center, E. P. I. (n.d.). Epic - Equifax Data Breach. Electronic Privacy Information Center. https://archive.epic.org/privacy/data-breach/equifax/

Ritchie, J. N. & A., & Technology, T. O. of. (2022, December 20). Equifax Data Breach Settlement. Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement