Equifax Data Breach of 2017

CJ McDonald

Department of Cybersecurity, Old Dominion University

CYSE 300: Introduction to Cybersecurity

Professor Malik Gladden

September 10, 2023

Equifax, founded in 1899 and headquartered in Atlanta, Georgia, is one of the three major credit reporting agencies in the United States. It collects and maintains extensive consumer credit information, aiding lenders and businesses in assessing creditworthiness and financial decisions. Equifax offers credit reporting, scoring, and identity theft protection services globally, although it is widely recognized for its role in the U.S. financial sector. The company faced notoriety due to a significant data breach in 2017, which exposed sensitive personal information of millions of Americans, prompting increased scrutiny of cybersecurity and data protection practices in the credit reporting industry.

For starters, Equifax had numerous cybersecurity vulnerabilities. The root of the problem came from a vulnerability in Apache Struts, an open-source development framework for creating Java applications used by Equifax. The vulnerability was given the name CVE-2017-5638 and classified as critical with remote code execution risks. Equifax had other issues that contributed to the vulnerability and breach though. First, they had a lack of comprehensive IT asset inventory, la complete IT asset inventory, not knowing the locations of the Apache Struts application on their network. Instead, network scans were conducted by IT, and failed to detect the software. They also failed to follow their patch management policy. Equifax's security policy mandated that vulnerabilities labeled as critical, such as CVE-2017-5638, be patched within 48 hours of discovery. The lack of asset inventory made this difficult. Many scans were conducted by IT but they couldn't find instances of the vulnerable software. After not finding the vulnerabilities, no further action was taken.

Threats that exploited the stated vulnerabilities were allegedly members of the Chinese Army. On February 10, 2020, the US Department of Justice indicted four hackers and members

of China's People's Liberation Army, a sector of China's military. The names of the cyber attackers behind the crime were Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei.

As this was one of the largest and most significant data breaches in history, there were bound to be severe repercussions. The breach had compromised 147 million Americans, 15.2 million British citizens, and 19,000 Canadian citizens. Data such as social security numbers, birth dates, addresses, and driver's license numbers were all scraped. The breach also led to many financial losses, primarily from lawsuits and compensation checks. The city of San Francisco sued Equifax over violations of California's unlawful, unfair, or fraudulent business practices law. Also, the city of Chicago sued for the violation of the Illinois Personal Information Privacy Act, the Illinois Consumer Fraud and Deceptive Business Practice Act, and the Chicago Consumer Fraud Ordinance. Along with two cities, Attorney Generals Maura Healy and Curtis Hill also sued on behalf of their states, Massachusetts and Indiana. Equifax also gave a $125 compensation check to those whose data had been scraped in the breach. Lastly, Equifax spent $1.4 billion on security upgrades.

In retrospect, some measures could've mitigated or prevented the incident. The most basic of the solutions are patching and updating their software. Equifax could've prevented the breach by applying security patches and updates to the Apache Struts software and having an effective patching regimen. Equifax could also invest more in security awareness and training. Training and awareness programs should've been put in place to educate staff about the importance of cybersecurity and to help recognize and report potential vulnerabilities. Equifax also could've implemented stronger network segmentation to limit access to sensitive data and isolate systems. This would've made it harder for cyber attackers to move laterally within the network. Then there are intrusion detection and response systems, which, in place, could've

quickly identified and responded to suspicious activities on their network. Finally, there's encryption and access controls. Equifax's sensitive data should've been encrypted and access controlled to ensure that even if a breach had occurred, the stolen data remained unusable to unauthorized parties.

References

Bomey, N. (2020, February 10). *How Chinese military hackers allegedly pulled off the Equifax data breach, stealing data from 145 million Americans*. USA TODAY. https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/

DOJ. (2020, February 10). *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax*. Www.justice.gov. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

Equifax Reveals Extent of 2017 Data Breach, Details Number of Stolen Records - Security News - Trend Micro USA. (2018, May 9). Www.trendmicro.com. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/equifax-reveals-extent-of-2017-data-breach-number-of-stolen-records

FBI. (2020, February 10). *Chinese Hackers Charged in Equifax Breach*. Federal Bureau of Investigation. https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

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/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html#:~:text=The%20crisis%20began%20in%20March

Miyashiro, I. (2021, April 30). *case study: Equifax Data Breach*. Sevenpillarsinstitute.org. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

What can Others Learn in the Wake of the Equifax Breach? - Security News - Trend Micro USA. (2017, September 19). Www.trendmicro.com. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-can-others-learn-in-the-wake-of-the-equifax-breach