Equifax Data Breach 2017

Janae Craig

Old Dominion University

CYSE 300

Dr. Joseph Kovacic

May 19, 2024

Equifax Data Breach of 2017

In 2017, Equifax encountered a major data breach, exposing personal data belonging to about 147 million Americans. This incident has prompted major questions about how well organizations protect our personal information. This paper will look at what happened during the Equifax attack, why it matters, and what we can learn from it to avoid such events in the future. We'll look at the causes, consequences, and aftermath of the incident to understand what this means for cybersecurity practices and regulations. By carefully investigating this occurrence, we intend to contribute to the continuing discussion about how to keep our data secure in today's digital environment.

Numerous vulnerabilities were exploited during the Equifax data attack, worsening the damage. The most significant compromise came from a severe hole in Apache Struts, a popular software framework used in Equifax's web platforms. Despite the existence of available patches for some time, Equifax failed to implement them on time. Weak network segmentation and authentication standards additionally allowed illegal access. investigations also revealed that Equifax was aware of several vulnerabilities but failed to resolve them appropriately. This underscores the importance of proactive security measures such as regular upgrades, strong authentication, and good insider threat detection in preventing such large-scale attacks.

Cybercriminals use these vulnerabilities to acquire unauthorized access to sensitive personal information such as names, Social Security numbers, birth dates, residences, and, in some cases, driver's license numbers. The Equifax data attack had severe repercussions, affecting millions of people as well as data security in general. Victims were at higher risk of identity theft and financial fraud, which made it difficult to track their accounts and resolve identity theft issues. In addition, the breach harmed public trust in Equifax and the larger credit reporting

sector, prompting calls for greater transparency and accountability in handling consumer data. Equifax faced considerable attention from authorities, lawmakers, and the public, resulting in investigations, lawsuits, and significant fines. This incident underlined the critical necessity for enterprises to strengthen their cybersecurity procedures to avoid incidents like this in the future. Overall, the Equifax breach highlighted the necessity of securing personal data in today's digital age, leading to calls for more restrictive regulations and industry-wide reforms to protect consumer privacy and security.

To avoid the Equifax data breach, numerous cybersecurity precautions could have been implemented. First, timely patching of software vulnerabilities, such as the Apache Struts issue, might have prevented attackers from exploiting known vulnerabilities. Equifax's delay in implementing these patches underlines the need for proactive patch management. Furthermore, installing tight network segmentation as well as access controls may have constrained attackers' ability to move within Equifax's systems, thereby reducing the impact of the incident. Using stronger authentication mechanisms, such as multi-factor authentication, could have prevented fraudulent access attempts. Regular security audits and penetration assessments may have identified and rectified vulnerabilities before attackers exploited them. Improving employee training to spot phishing and other social engineering efforts may have prevented the incident from occurring in the first place.

The Equifax data leak is an important example of the significance of strong cybersecurity safeguards, as well as the need for businesses to prioritize consumer data safety. The Equifax data leak serves as a reminder of the crucial role of cybersecurity in our interconnected world. The vulnerabilities that enabled this intrusion, ranging from unpatched software weaknesses to inadequate network security policies, underline the critical necessity for enterprises to adopt

strong cybersecurity measures. The Equifax breach has severe consequences, harming millions of people and decreasing public trust in information security policies. Furthermore, the incident demonstrated the importance of legislative reforms and industry-wide standards for effective customer data protection. Lessons acquired from the Equifax incident must inform future proactive cybersecurity initiatives, such as prompt vulnerability patching, improved network security controls, and extensive employee training programs. Organizations may better protect sensitive data and reduce the destructive impact of data breaches on both individuals and the community as a whole by taking proactive actions to improve cybersecurity defenses.

References

Abagnale, Abagnale, Frank W., & Big Think, publisher. (2019). *The great hack : A famous fraudster explains the Equifax data breach.*

DeMarco, Edward J., Jr, & Mason, B. (2017). THE EQUIFAX DATA BREACH AND ITS CONSEQUENCES. *The RMA Journal*, *100*(3), 80.

Robbins, J. M., & Sechooler, A. M. (2018). ONCE MORE UNTO THE BREACH: WHAT THE EQUIFAX AND UBER DATA BREACHES REVEAL ABOUT THE INTERSECTION OF INFORMATION SECURITY AND THE ENFORCEMENT OF SECURITIES LAWS. *Criminal Justice (1986)*, *33*(1), 4.