

The 2017 Equifax Data Breach: Social Science Case Study

Obi Oputa

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

4/21/26

Introduction

This case study will focus on the 2017 Equifax data breach. The Equifax data breach is one of the most significant in the history of American cybersecurity. In March of that year Chinese hackers were able to access the company's systems via a vulnerability in the Apache Struts software that the company used. For 78 days, these hackers remained undetected and had access to the company, during which time they collected the personal data of over 147.9 million Americans. Equifax had to spend \$1.38 billion to settle with those who were impacted by the breach and to implement various cybersecurity improvements for their systems. While the technical failures of Equifax played a significant role in the breach of their data, the human and organizational failures that the company exhibited are also important to understand and learn from (Amishav, 2026).

Analysis

When looking at the Equifax breach from a psychological perspective, it shows the list of human factors that contributed to the breach. As discussed in this course, human factors is the application of knowledge about human capabilities and limitations to the design and development of tools, devices, systems, environments, and organizations (Yalpi, 2026). Equifax's security team was aware of the critical patch that was available for Apache Struts but did not apply it to their systems. This is a human factor, as it is well known that the human mind tends to disregard risk factors that cannot be seen or experienced directly. Furthermore, their SSL certificate had expired, leading to their network being without monitoring for over half a year, another sign of complacency and disregard for security (Amishav, 2024)

Now shifting perspectives and looking at this event from a sociological lens, the structural functional theory helps to explain how the breakdown of the coordination between Equifax's

security and IT teams led to the data breach and the fact that it remained undetected. Also, the cybersecurity culture within Equifax must not have adequately established norms and procedures for tasks like patching and monitoring for potential threats; covered in this course, the norms established within an organization's culture have a direct impact upon how its employees treat their security responsibilities (Yalpi, 2026).

Solution

There are many solutions to this problem, but they must address the technical and human elements of the issue. Equifax can enforce timelines for applying patches to the systems and verifying that the monitoring tools are working properly. Additionally, Equifax should focus on embedding cybersecurity into their culture. The main barrier to implementing these solutions will be the resistance to change from those within the organization. From the conflict theory perspective, the leaders of the organization will not seek out these changes until an event actually occurs. (Yalpi, 2026)

Conclusion

The Equifax breach helps show that cybersecurity is more than just a technical issue. No matter how sophisticated a system is, if people have a tendency to ignore security practices, the data will always be vulnerable to hacks out there. Combining the principles of social sciences with cybersecurity creates a more complete understanding of the problem and how to avoid cybersecurity breaches such as the 2017 Equifax breach. By looking at cybersecurity through the lens of social sciences, people can understand how much of a role the human factor plays in creating and avoiding cybersecurity threats.

References

Amishav, J. (2024, December 8). *Equifax Data Breach Case Study: Causes, Who Was Affected, and Settlement*. BreachSense. <https://www.breachsense.com/blog/equifax-data-breach/>

Yalpi, D. (2026). *CYSE201S: Cybersecurity and the social sciences* [Course Modules 4, 5, 8, 9, 10]. Old Dominion University.