Dylan Coulter February 13, 2025

ID#1896062

C405

# **CS405 Assignment 5-1 - Case Study**

**Introduction**

The Equifax data breach occurred between March 2017 and July 2017. This breach impacted over 140 million Americans. During this breach hackers were able to gain access to customers personal information. The personal information that was accessed and stolen was customers dates of birth, names, addresses, credit cards numbers. and social security numbers. The hackers were able to gain access to the Equifax through a vulnerability in Apache Struts Java framework. In July of 2019 Equifax came to a settlement with the Customer Financial Protection Bureau to pay fines and compensation amounting to 700 million dollars. The compensation would be distributed to the 147 million affected individuals (Kanaris Miyashiro, 2021).

**Name of case and link**

Equifax Data Breach (2017)

Link: <https://sevenpillarsinstitute.org/case-study-equifax-data-breach/>

**Date of case**

March 07, 2017

**Why did this case make the news?**

The Equifax breach was one of the biggest data breaches to ever happen and it had an impact on over 140 million Americans whose person information was stolen. The company would later come to a settlement amounting to 700 million dollars.

**Describe the breach**

**Type of security or data breach or combination**

This was a data breach as some gained unauthorized access to protected data. Hackers were able to gain unauthorized access to the Equifax network through a vulnerability in the Apache Struts framework. Not only did Equifax suffer a breach in 2017 they also did in May 2016 where over 400,000 were affected due to a breach of the Equifax W2 express website. The Equifax breech of 2017 was preventable but happened because the company failed to recognize and mitigate its cybersecurity risks. Equifax failed to implement security measure at one point they allowed up to 300 security certificates to expire. Equifax used custom built legacy systems and with the rapid growth of the company and the amount of data being stored lead to a very complex IT environment making the company vulnerable.

**Why was this company a target?**

Equifax like any large company that stores sensitive data in large amounts will always be a target. Equifax holds vast amounts of customers person information which if gets in the wrong hands can have a major impact the effected individuals’ life. It is the company’s job to ensure they are taking the best measures to protect users’ personal information. In this case there was a major oversight on Equifax end impacting millions.

**Identify the threat(s)**

**Immediate threat(s)**

Exposure of sensitive customer information this includes bank account details, social security numbers, credit scores, dates of birth, address, and names.

**Potential threat(s) if the vulnerability goes unresolved**

Hackers could learn how to exploit other similar systems. They also would been able to gain ever more access to other information. This all could open the door to more attacks in the future which could end up being equal or even more successful.

**What could a developer have done to prevent this breach?**

In this case acting faster when the company was alerted of the risks and vulnerabilities of the current Apache Struts framework. They could have worked on adding more authentication and authorization to prevent from unwanted entities from gaining access.

**Which policy or policies will help prevent this type of attack?**

With this attack not only would have certain policies have helped, but a faster response when they were informed of the security risk within the Apache Struts framework. The company was notified on March 08, 2017, of the vulnerability, but allowed for attacks to happen all the way until July 2017. This falls directly on the lack of accountability and management structure within Equifax. Policies around validating user input data would have help with this case as that is where the attackers found the vulnerability to exploit the system.

**Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.**

**Authentication**

Going forward after this breach Equifax should adopt certain authentication measures such as the implementation of multifactor authentication, regular credential updates, and strong password requirements. All of this would prevent unwanted entities from gaining access to the system. This will allow better assurance that who is accessing the system is who they say they are**.**

**Authorization**

Authorization policies should be enforced with aspects such as role-based access controls, least privilege principal enforcement, and regular access reviews. There is no need for someone to have more access than necessary to do their job functions. Allow to much access to users opens the door to future issues.

**Accounting**

Accounting policies should be adopted and some of these include real-time monitoring, comprehensive system logging, and regular security assessments. If Equifax followed these policies, they would have been able to trace and catch the breach quicker. They would also be able to identify other potential risks.

**Defense in depth**

Defense in depth should be implemented with a focus around network security, data protection measures, and applications security. There are many aspects to consider with which can be adopted such as physical controls, behavior analysis, network security controls, administrative controls, and antivirus. Adopting different policies and controls will help protect from unwanted entities gaining access. The more layers they need to go through the more difficult it will be. We just need to remember it we do more than is needed it can have a negative impact on performance.

**Resources**

Kanaris Miyashiro, I. (2021, April 30). *Case Study: Equifax Data Breach*

[*https://sevenpillarsinstitute.org/case-study-equifax-data-breach/*](https://sevenpillarsinstitute.org/case-study-equifax-data-breach/)