**Equifax**

1. Listen to a podcast about the Equifax data breach that occurred in 2017. As you listen, pay close attention to the multiple lapses that allowed this attack to be carried out successfully.

<https://www.spreaker.com/user/jacintheagalpin/equifax>

2. Answer the following questions regarding the breach itself:

How did the threat actors breach the network?

As stated on the podcast The US Department of Homeland Security issued a warning about an Apache Struts vulnerability on March 8, 2017, and urged users of the program to immediately install Apache to fix the problem. According to former Equifax CEO Richard Smith, on March 9, 2017, a warning notice was prepared to be sent to Equifax IT staff, which would have triggered repair within 48 hours. However, the employee in charge of distributing the warning notice failed to do so, and the routine internal scans did not detect the Apache Struts vulnerability leaving Equifax systems wide open to hackers who were aware of the Apache Struts vulnerability where they gained access to Equifax systems by exploiting the vulnerability in Apache Struts.

An open-source software called Apache Struts is used to build Java web applications on its online dispute gateway, a user interface where users could dispute their credit scores, Equifax had been using Apache Struts.

How did Equifax know there was a problem?

On July 29, Equifax security discovered suspicious behaviour related to its online dispute site. Security blocked the activity right away and started keeping a close eye on the portal for any additional suspicious activity.

What did they do to contain the breach?

Access to Equifax systems and data exfiltration ceased on July 30 after numerous instances of suspicious traffic related with the gateway. As a result, access to Equifax systems and data exfiltration ceased on August 2. To determine precisely what had occurred, they hired a forensic consulting company and retained experienced legal counsel, within two weeks, they informed the FBI that they might have been hacked. Equifax was aware of the amount of the harm caused by the hackers.

3. Answer the following questions regarding the aftermath of the attack:

What actions did Equifax take to assist customers?

Richard Smith stated that Equifax will take care of their clients. He promised all of them and to all of the esteemed partners: to help customers and improve our data security skills in the process. Many thanks To aid customers, Equifax created the www.equifaxsecurity2000and17.com website, which offered free credit reports and consumer credit protection as well as the ability for customers to determine whether they had been affected by the hack. Equifax also significantly improved its security environment by three things: one, isolating and containing sensitive data via enhanced network segmentation so even if a hacker got into, say, the online dispute portal, they wouldn't automatically have access to sensitive data; two, installing additional application firewalls; and three, implementing additional logging to identify unusual behaviours.

What actions did Equifax take to improve its security posture?

Also, Equifax significantly increased its security environment by restricting and isolating sensitive data through improved network segmentation so that even if a hacker had access to, for example, the online dispute portal, they wouldn't immediately have access to critical data. Two more application firewalls were implemented, and attack-blocking tuning signatures were also installed. More logging was added in three places to look for odd behaviours.

What was the political fallout (who got fired), and why?

Equifax completely reorganised its leadership. There was a belief that anything that had gone wrong began at the top and that cultural regeneration could only occur with a new beginning when Richard Smith resigned along with the organization's chief information and chief security officers.

4. What are some of the problems the podcast author highlights in terms of the failures leading up to this breach, as well as how Equifax responded to and handled it?

A warning alert was prepared on March 9 to be forwarded to Equifax IT staff, which would have prompted repair within 48 hours in compliance with Equifax internal policy. The employee in charge of distributing the warning notification supposedly failed to do so, patching was not performed, and normal internal scans failed to detect the Apache struts vulnerability as a result, according to former Equifax CEO Richard Smith. Equifax systems were now completely accessible to hackers with knowledge.

What could Equifax’s IT security team have done to prevent this attack from occurring?

Equifax IT security team could have taken immediate action towards the warning notice that was drafted and sent to Equifax IT personnel, which would have triggered remediation within 48 hours per Equifax internal policy.

Why do you think Equifax’s senior management didn’t pay more attention to the state of their IT security?

They didn’t pay much attention because they believed in their security methods they had in place, or they had too much commitments before the incident.