Equifax Breach Analysis

Anthony Wilson, Brianna Mears,
Brittany Kirkham, Charlie Smith,
Matthew Cragg, Nikitta Weston,
& Tracy Harvey

Olympic College, Fall 2023
IS 337: Information Assurance I
September 27, 2023

Section 1: Bri (Start – 25min)

In today's world, a credit score can determine how someone lives their life. It controls what types of loans a person can qualify for, what vehicles a person is able to purchase, if someone can afford to purchase a home instead of renting one. The credit score is incredibly important. In the United States, 3 companies calculate credit scores. These companies are Equifax, Experian, and Transunion. To calculate credit scores these companies use many types of personal identifying information (PII). Types of PII that get used include current and former addresses, vehicles owned, social security numbers, and birth date. Because of the types of PII used, when Equifax got hacked in 2017 many people's sensitive and personal data was leaked onto the internet, putting millions of people at risk of identity theft.

Unlike with other security breaches (like the Target breach in [insert year]) consumers are unable to choose to take their business elsewhere if they do not want to support a company that practices poor cybersecurity. They are unable to remove their information from these three companies, therefore, the public was powerless to protect their PII in the Equifax breach, if they even knew that a breach had occurred. Between 2015 and 2017 Equifax suffered three data breaches, though most of the public was only aware of the one in 2017.

Leading up to the breach, Equifax not only practiced poor cybersecurity, but poor internal communication between software vendors and IT staff, leading to a perfect storm where a crucial patch was not installed and a backdoor into their servers was created. Even though a vulnerability was discovered months prior to the breach, no action was taken to patch the vulnerability.

Section 2: Charlie (25min – 50min)

I reviewed the Equifax hearing from the 25-minute mark through the 50-minute mark. All the opening statements occurred up to this point, with several members questioning the CEO of Equifax about the procedures, protections, and failure to protect millions of Americans' personal information. My segment started with Richard Smith's testimony, the former CEO of Equifax.

After Mr. Smith's opening remarks concerning his acknowledgment of this breach and offering his apology, he described both the human and technical errors that occurred. He first tells how their technical team failed to put a software patch to their dispute portal earlier that year. He then describes how the scanner failed to detect that portal's vulnerability.

To project accountability and to correct their errors in the eyes of Americans, Equifax created a website, call center, and free services to assist the public with this breach. However, the website and call centers were overwhelmed, partly blamed on a hurricane that took out two of their call centers.

In response to being questioned on the 10-day delay between when events occurred and when the public was notified, Mr. Smith stated a forensic investigation was necessary to gather the information needed to inform consumers of the details and severity of the breach. This sounds plausible, but this delay further muddied Equifax's reputation in the eyes of those who were harmed. The CEO also blames the CIO for speaking of this breach as only "suspicious activity" and referred to it as an "incident", which delayed Mr. Smith's reaction when first notified of an issue a few months earlier.

From the segment of Mr. Smith's testimony, it is clear issues that arose were not taken seriously, the security team was not utilizing tools to routinely test the integrity of their systems, and the lack of communication within the organization was proven problematic.

Section 3: Matthew (50min-1:15)

In the section I reviewed the questions were non-technical, sort of a 30,000-foot view of things. Each line of questioning had its own sort of background to fuel the discussion but remained generalized outside of timelines and numbers.

There was a line of questioning about the frequency of meetings that the CEO had with both security and IT. It was answered that these meetings occurred, for both parties, at least quarterly but supplemented as needed should more be required. The CEO could not recall how many of these meetings had occurred in the roughly 9-month timespan of events. There should have been at least three, at which point none of the meetings contained any information about the security issues.

It was also asked if the CEO inquired about the nature of security issues. It wasn't crystal clear what verbiage was used but there was a time when security informed the CEO of an issue. What type wasn't specified, and the CEO didn't question this or ask for the nature of the breach. The issues I see here are with structure, management involvement, questioning attitudes, and overall communication. Obviously, these breaches happened because of a failure to protect information. But there are also issues with the responses. Why would the CEO not question what sort of issue was had? What sort of information was discussed at these briefings? If you have a quarterly meeting with two major departments, would you not remember having any additional? And as mentioned, if protection of peoples personally identifiable information is truly your number one objective, why is security briefing the CEO only once a quarter and not discussing such a massive breach?

I think it's clear there are organization wide flaws here. There is some extreme lack of communication that once a breach was identified it was not scoped and applicable personnel were not made aware of it. They need to have a restructuring or at least centering of their

leadership and work teams to determine the root of this issue. Aside from the security gap itself, I heard a lot about how the organization fumbled this problem. Some causal analysis and a deeper dive into the reason that communication error(s) was made is warranted.

Section 4: Tracy (1:15-1:40)

This section's questions were not really technical about the breach. There were a few places where committee members asked questions about how the breach was discovered and what was done in the immediate timeline following the discovery of the breach. But all in all, it revolved more around the astronomical amount of data that credit reporting companies like Equifax have collected on consumers, who owns that data and whose job it is to protect that data.

According to one line of questioning it was revealed that the breach was detected using a piece of technology called a decrypter, which reversed the encryption on the data that it was applied too, which allowed Equifax's network security professionals to realize that they were under attack and take steps to cut off the dataflow going out of the network. Equifax had data forensics people look at the system to see if anything had been compromised. Equifax had the ability to trace the attackers back to their IP address but that isn't really a smoking gun.

According to the examples given by some of the committee members, like a 130-page credit report. Equifax has so much data on people, but the CEO seems to indicate that it is the consumers job to secure their data, when the average American probably doesn't even begin to understand just how much data companies like this have on each one of them. There was constant reference to an app coming out that would allow consumers to lock and unlock their credit files at the push of a button as if this were the end all be all answer to the breach. How can the CEO of a company that mines for and collects consumers' financial data not seem to believe that his company has any responsibility for the security of that data?

There was also a line of questioning regarding the selling of large amounts of stock by two of the company's upper management and if they had any prior knowledge of the breach when they sold the stock, which again the CEO defended.

From what I saw large companies like this do not seem to believe that they should have any repercussions from things like this because they do not believe that they are responsible for securing the data, it is the consumers' responsibility. Which kind of makes me wonder exactly how seriously they take their data and network security?

Section 5: Anthony (1:40-2:05)

Encryption at rest is encrypting data that is being stored on storage media that is non-volatile. (Ensures that data remains intact over time and can be accessed again when needed). This ensures that the data remains confidential and secure even when it's not actively being used or transmitted over a network. One of the many issues Equifax had was that the PII was at rest was not safeguarded. When information is being stored and is not being used it is at rest and should still be protected. This would protect the information from unauthorized access. Richard Smith reported that the system that was compromised was not encrypted at rest. With all the sensitive information under the control of the Equifax organization, every system they control should be highly protected. Complacency is a big issue with this breach. There were more than enough people on the job to patch programs. This is a human error only. Technology needs to be activated by a human to do a job. This is not technology's fault. Equifax needs a system of checks and balances so people can be held accountable.

Encryption of data at rest is a very important step to secure information stored on storage devices. This ensures that unauthorized people cannot gain access to this data without the proper access keys. There are about eight different types of resting encryption techniques. Here are a

few that are listed. Key management is essential for data that is at rest encryption. These keys should be stored securely and managed. Self-Encrypting drives (SEDs). They have self-encryption built into the system. This system encrypts data as it is saved to the device and decrypts it when read. Network-attached storage systems in an enterprise environment have features to protect data at rest. This can be applied at the hardware level or by using software-based encryption solutions. Protecting data at rest is a fundamental step in protecting sensitive data from breaches and unauthorized access. To provide comprehensive protection of the systems' data this can be used in conjunction with other security measures such as access controls and data classifications.

Web patches are a very important part of web development and security. The patches help applications evolve and adapt to changes. They also help with vulnerabilities and issues that might arise. “Organizations that prioritize patch management demonstrate a commitment to the security and satisfaction of their users, ensuring that their web presence remains robust and resilient in the face of an ever-evolving threat landscape.” The best practices for web patch implementation are regular updates, reviewing and applying patches as needed. Testing, test the patch before applying and do this in a staging envvironment before applying them to a system. Prioritization, prioritize focusing on critical vulnerabilities first. Documentation always keeps a detailed record of the patches applied, the purpose and any issues that might have been encountered. Lastly always keep a Back-up and perform these on a regular basis. Not implementing web patches regularly can lead to serious consequences, such as system failure. It is important to stay up to date with web patches to ensure the safety and functionality of your system.

Section 6: Nikitta (2:05-2:30)

Rep Gene Green poses a good question on the relationship between LifeLock and Equinox where he suggested that Equinox benefits from being breached because every time someone uses LifeLock as a response to data breaches, some of the money goes to Equinox because of Equinox's has stake in LifeLock. CEO Richard Smith claimed he didn't know then 10 seconds later said they had the opportunity to directly come to us when breaches happen. If Rep Greens assertion are true, then the proper response would be to have a contract with an independent managed security service provider (MSSP), where Equinox doesn't have any influence or stake to gain from data theft.

Rep Mullin states the vulnerability that caused this data breach wasn't identified for at least 30 days. When it comes to finding vulnerabilities in software there are some techniques that can identify them. The one that is best at finding zero-day vulnerabilities would be threat hunting and penetration testing. This is where you hire a third-party or make your own team of cyber security officials to proactively look for threats in your systems. Sometimes third-party vendors are seen as the better option because they might have less bias toward the infrastructure and a different perspective.

Rep Walters goes into detail about the slow response to Equinox's customers stating it is taking too long to hear any feedback on their current situation. CEO Richard Smith agreeing in part that they had a backlogged situation. The well-known cyber security tirade, confidentiality, integrity, and availability, states that these 3 pillars must be used to achieve a holistic secure environment. If availability is slow to the point it takes 5 business or more days to hear feedback about a data breach, then it is failing a critical cyber security pillar. To ensure this doesn't happen they could either hire more staff and buy more infrastructure that provides access to their servers or use cloud which ensures availability through a concept called elasticity.

Section 7: Brittany (2:30-3:00)

During the final portion of the interview touched on many concerns which arose due to the breach. Some concerns were reiterations of previous points, while others were more specified and unique questions. A prominent procedural assurance issue was highlighted when Mr. Smith was asked about the timeline of the patch rollout. The questioner had information stating the patch took 3 days to create once the problem was identified; however, in reality, the patch took several weeks to be issued. Mr. Smith attributes this delay to procedural compliance and the quality testing regulations required for a major patch, regardless of urgency. For there not to have been emergent response procedures in place was a sever oversight.

Another notable issue that was detailed in this portion of the interview was the technical problems associated with the website launched to address the breach. Once the breach became public knowledge, Equifax created and launched a website to provide information on services available to consumers who were affected. However, it quickly came out that the website in question was poorly designed and managed. It was stated in the interview that the website failed to have protections in place against phishing attempts, and a programmer even created a scam website nearly identical to the Equifax website to highlight this security issue. The website also had additional technical issues in that it couldn't handle the volume of traffic it received.

Corrections to the website's design, security features, and access scalability would all need to be completed to address the technical issues. The procedural issues of patch rollouts need to be addressed by the creation of emergency procedures and teams for expediting casualty response.

References

House Energy and Commerce Subcommittee Hearing on Equifax Data Breach. (2017, October 3). [Video]. C-SPAN.org. https://www.c-span.org/video/?434786-1/house-energy-commerce-subcommittee-hearing-equifax-data-breach