Michael Chillemi

04/04/2022

Information Assurance & Security

Dr. Aakash

Case Study 2 Questions

1. How does Equifax's business model work? What is the role played by consumers’ in Equifax’s product offerings?

- Equifax is a credit score company. How their business model work is the company accepts financial information from different institutions. Once they have this information they compile the data into score and reports that would reflect on the individuals information. This company also provides other services like fraud detection and identity threat detection services. These services are very useful for consumers. What makes them useful is the ability to produce the scores and reports for people or companies who are looking into other people. It’s a great way for companies to take a look at what kind of person they could be potentially hiring. Also it is a positive service for everyone because you can review the reports they reproduce which can give you insight on what you can change to make your score better than what it currently is. They also provide services protecting their consumers information which is very appealing to all consumers.

2. Was Equifax lax or unlucky to be cyber-breached in this way?

- In the event of Equifax having a security breach it can be determined that they were box unlucky and lazy. They were unlucky based on the fact that they had a security breach. But in lots of other cases you can infer that the company was lazy. First of all the company did not have a lot of security to begin with. The company failed to update known vulnerabilities that they had in there current systems or they were very late on patching their systems. Other an issue the company had was a lack of communication and the teams corelation was poor. One big issue that I felt was the responsibility of the teams. In the article it explained that the way things worked were only the IT department was able to install software on devices. Then after they installed the software the security team was then able to configure the software. Depending on how efficiently the teams work this can work out but as explained earlier the team corelation was poor which leads to many problems. The company was also not up to date on specific certificates and the servers were not segmented which can leads to many complication if the system is breached. That is some of the many ways Equifax was lazy and unlucky.

3. How well did Equifax responded to the breach? What do you think accounts for the delay in informing the Board?

- Equifax did not do well in responding to the breach. First they were very transparent to the public about the data breach. At first it took them a long time to inform the public about this breach. Also when they informed they said that only a small amount of information was leaked. But then later on saying the breach was way more severe than they originally thought even though they knew the whole time. Some of the actions that the company took lead to a delayed response to the board. One action is that the company an outside source to investigate their vulnerabilities. Another delay was also the lack of communication team members sent emails to the security team but since the team was divided into two branches which made it difficult for people to get in touch with the correct person. These and many more factors lead to the poor delayed response to the breach.

4. To what extent would you hold Equifax's board accountable for the company’s lack of

Cybersecurity preparedness? Assuming you are serving on the company’s board, what

questions you’d ask to know about the security preparedness of the company?

- I would hold the companies board very accountable for the lack of preparedness in their security. One of the big mistakes the company made was hiring the new CFS who had no knowledge of security. This was a very poor and irresponsible decision on their part. Another action that you can hold them responsible for is the fact that they did not take any action once the breach occurred. If I was on the companies board I would ask many questions to understand the companies security. One question I would ask is how often does the security team test their systems? Another question I would ask is how up to date is the security tools are and what the likelihood that the systems can be breached? My last question for the board would be how much experience does the security have and if the team needed more than one percent of the funding?

5. In your view, how should Equifax have prepared for the breach and the subsequent

response?

- Equifax should have done a lot more then they did to prepare for the breach. To start off the company should have updated all their systems to the most recent update. Also they should have updated their certificates in order to determine properly how prepared their security is. Plus they could also rearrange their servers so they are not all connected in one spot. Equifax should have also looked more into the CFS they hired. If they hired someone else that had more experience they could have been way more prepared to deal with this breach. Which could also have lead to the company having a less severe breach. In regards to the subsequent response they should have let the public know a lot sooner and been more open about what has happened. Also they should have notified the board a lot sooner then they did. I feel that if they reported to the board they would have helped the situation. This is how Equifax should have prepared for the breach and their response.