Module 2 Group Drop Box

Group: Anthony, Brianna, Brittany, Charlene, Matthew, Nikitta, Tracy

Section time 1:15 – 1:40

This sections 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?