Elijah Warren

PHIL 355E

2/21/20

Old Dominion University

CSR Case Analysis

When it comes to the use of private information, nothing hurts worse that when a company that doesn't allow you to change or monitor the information it collects on you then goes and has one of the biggest data breaches in history. They lose your information and therefore your identity. When you call to find out what happened and if you were affected, they have little information to offer you and can't tell you where your private information ended up. It is the responsibility of those that take our information to make sure that it is safe guarded. In this case analysis I will argue that Ubuntuism shows us that the Equifax breach harmed everyday citizens of this country by not properly protecting the information that they collected which was morally wrong.

Friedman argues that the social responsibilities of a business isn't actually the business making the decision. Rather it is those that work for the business that decides to do something that won't necessarily help the company grow but what is the ethically correct thing to do. I think that this is the focus of ubuntuism. Being able to come together as a society to do what is best for the majority rather than focusing on what the best thing for the one or in this case the company would be. In the case of Equifax, the issue arises when you find yourself in need of a loan. You go to a bank and ask for x amount of money; they say they will happily give you that amount after checking your credit score. Your credit score that is stored in a central location. A location that is run by a single company that collects all your payment history. This company has the information about your life on file and if anything is to happen to that information, you may find yourself in a place of insecurity.

After an investigation took place, information arose that Equifax wasn't taking the proper steps necessary to stop an attack from happening. Like a plane crash, multiple things must go wrong before an infosec disaster like this occurs. The first thing that happened was that attackers used a widely known web portal vulnerability to gain access to the servers. This vulnerability should have been patched by Equifax months in advance but because of failures in the internal process, the vulnerability remained. Once the hackers gained access, they were able to navigate to other servers and find usernames and passwords that were being stored in plain text. This meant that they now had access to millions of accounts. They then began removing terabytes of information through encrypted networks for months. They were able to do this because Equifax had failed to renew an encryption certificate on one of the security tools. To top it all off, they didn't release the information about the leak for more than a month after they had discovered it.

There were many steps that could have been taken in order to stop this ordeal from happening. If Equifax and their employees would have put forth the same actions that Friedman writes in his article, this could have been avoided. The same goes for the teachings of Ubuntu. If the employees that were responsible for the care of the network had made sure that the protection of the information was made a top priority, many of the issues that they were having would have been already fixed.

Anshen's article takes the stand that companies are more worried about how to use their resources to grow the company rather than making sure that they do it in an ethical way. They should be a vital part in society being there to better the community rather than profit off of it. He believes that there is a social contract between society and the businesses that serve them. This type of give and take allows for the survival of both the business and the wellbeing of its customers. When we bring this philosophy to the Equifax breach, we see a company that has no intentions of serving its community. What I mean by this is that they prioritize profits more than anything else. Even if the thing that they are leaving behind is the security of their customers. However, can you claim that for a business to put themselves first to be a morally incorrect thing? I would argue that you can.

When you agree to take the personal information of anyone, you are agreeing to a social contract of trust. This means that you will do what you can to protect the information from attackers that might want to gain it. By not doing all that you can, you are using the publics trust for your own personal gain. This is the morally incorrect thing to do. Ubuntu teaches that with everything that you do, you must be mindful of the thoughts of others. You must have kindness in your heart and good intentions. I think that all corporations should make this their top priority. If you put those that give you business first, then you will never have to worry about the growth of your company, things will take care of themselves.

When we look at the victims of the breach and how their daily lives where affected, you get a since of how important protecting information really is. 143 million people had their names, addresses, dates of birth, social security numbers, and drivers license numbers exposed. This information would allow anyone to be able to steal identities and steal money or crush the credit scores of millions of Americans. Credit scores play a huge part in the finances of millions of people, many wouldn't be allowed to purchase things such as houses and cars. Credit scores are also often used by companies when hiring to determine the reliability of a person. This means that a bad credit score could also cause someone to not be able to get a job.

We need to be able to look back at what happened and learn from the situation. Companies need to take more care in how they protect the information of the millions of accounts that they have. Protecting this information should be the top priority of any business that collects or stores the personal information of anyone. We as a society need to be more involved when it comes to how our information is stored and what it is used for. We have become numb to the process and prefer if we didn't know where our information went. We need to demand for more rights when it comes to deciding how businesses can use the information they collect. The EU has put into act laws like this to give their citizens more rights while also requiring companies to give information about how they are storing the information. If the United States put laws like this into act, I feel that there would be a substantial dip in the amount of leaks that happen within a year.