Equifax Breach

Genesis, Savannah, Chris, Kevin

Saint Leo University

2 December 2017

Equifax Breach

Along with Experian and TransUnion, Equifax is known as one of the largest credit reporting agencies. Equifax is in charge of monitoring millions of Americans credit score. Equifax job is to collect personal and financial data on people and then send the credit history and credit score to the lender. From there, the lender has the ability to deny or approve the loan based on the information provided by Equifax, they also have the ability to tell you what your interest rate will be. The Equifax breach affected about 143 million customers. The hackers' compromised customer's personal data including names, birth dates, Social Security numbers, driver license numbers and physical addresses, and credit card numbers. The breach occurred from Mid-May to July of 2017, the breach occurred due to a vulnerability in the software. The Equifax website is built on a software called Apache Struts, a widely used framework for creating programs that help companies manage large amount of data online. In March, the Apache foundation which oversees structs announced the existence of a vulnerability in a software code. However due to a bug, hackers were able to access customers personal data.

Reports have said that more than 145 million American citizens have been affected by this breach and three months ago they announced that an additional 2.5 million people were affected. The releasing of personal to financial information has left the industry in a critical stage and people in fear. With the public attention toward this issue begging for a reason/solution to this company mess up, it only leads to the entire company taking a down fall. Stock holder's

percentages have dropped a minimum of 35%, which in the stock market is extremely rare and fatal. This shows that everyone involved in this company was affected, whether it was credit card users, stockholders or simply the people running the company. It is definitely a huge hit to the economy and mentality of the public knowing now that big companies cannot guarantee security over their most personal and private information of their customers.

"As Equifax apparently has a vulnerability management process that involves regularly scanning and patching its systems, many are questioning how this intrusion came to be, and why the company's processes failed to identify and apply the patch. In examining the root cause of this data breach, here are three key things to consider:" (Burnette). First, accidents will always happen, and in the case of the breach for Equifax's data, they most likely had a robust security program in place. However, the Apache Struts vulnerability was suppressed in the reporting system, and that caused it to not appear in the report activities. If it did show up, they would have been able to notify the responsible areas. Secondly, cyber attacks are inevitable, with the large troves of sensitive data, they should expect the threats. Luckily, Equifax was aware of the threats, but the approach they had for the cybersecurity, that was the best strategy for safeguarding against any attackers. Lastly, a layered, defense-in-depth strategy can help. The defense-in-depth strategy, LBMC Information Security, includes multiple layers of protection in the security, so they do not depend of single control for complete protection. If the secondary vulnerability scanning process was implemented, the breach could have been sooner detected and could have been addressed sooner.

This market disappointment isn't extraordinary to data security. There is little change in the well being and security of any industry until the point where government officials venture in. Consider pharmaceuticals, automobiles, planes, restaurants, and work environment conditions.

Definitely, find a way to shield yourself from identity fraud in the wake of Equifax's data break, nonetheless perceive that these means are just compelling on the edges and that most information security is out of your hands. According to Schneier, there is a possibility that the Federal Trade Commission will get involved, however without confirmation of "unfair and deceptive trade practices," there's no other option for it. Maybe there will be a legal claim, but since it's difficult to draw a line between any of the numerous data breaks you're subjected to and a particular mischief, courts are not prone to favor you. (Schneier, 2017)

Work Cited

C. (2017, October 02). Equifax data breach affected millions more than first thought. Retrieved November 29, 2017, from https://www.cbsnews.com/news/equifax-data-breach-millions-more-affected/

How did the massive Equifax breach happen? Former CEO answers. (n.d.). Retrieved November 26, 2017, from https://www.housingwire.com/articles/41469-how-did-the-massive-equifax-breach-happen-former-ceo-answers

"How the Equifax Data Breach Happened: What We Know Now." *CNNMoney*, Cable News Network, 18 Sept. 2017. November 30, 2017, from money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html.

How to Check If You're Affected by the Equifax Data Breach. (2017, October 06). Retrieved November 28, 2017, from https://www.lifelock.com/education/how-to-check-if-youre-affected-by-the-equifax-data-breach/

Schneier on Security. (2017, September 11). Retrieved December 02, 2017, from https://www.schneier.com/essays/archives/2017/09/don't_waste_your_brea.html

"The Equifax Data Breach: How Did It Happen?" LBMC, www.lbmcinformationsecurity.com/blog/the-equifax-data-breach-how-did-it-happen.