The 2017 Equifax Data Breach

CYSE 300 - Professor Kovacic

Brandon Creech

Old Dominion University

The 2017 Equifax Data Breach

Data breaches in the cybersecurity sector has become a deadly tool of destruction for cybercriminals against large corporations. It has led to astronomical financial deficits for the corporations involved and exposed security for the customers, exploiting weaknesses that exist within security infrastructures. In recent years, financial conglomerates have become more frequently targeted. Equifax, a credit reporting bureau, has fell victim to a data breach in 2017 that surpasses their previous one in 2015, exposing approximately 144 million US consumers. The brief research paper will provide an overview of what vulnerabilities caused the data breach, what threat exploited it, the repercussions of the incident, and what cybersecurity measures could have been taken to mitigate the consequences or prevent it from happening.

Corporations become victims of data breaches for a variety of reasons such as: lack of employee knowledge, weak security infrastructure, or internal malicious actors. Equifax is a corporation added to the long list of victims that have to make a substantial recovery. According to Hal Berghel in their scholarly article "Equifax and the Latest Round of Identity Theft Roulette," it is suspected that the cybersecurity breach was due to the Apache Struts software, which displayed improper executions of file uploads (Berghel 2017). It is important for corporations to ensure that all parts of their sectors, including software, are running smoothly before they can be implemented. Software needs to be tested for bugs and in certain cases, also be put in a simulation scenario to determine whether it is ready for launch to customer devices.

According to DeMarco Jr. et al. (2017), the vulnerabilities within Equifax's faulty software were exploited by unnamed hackers who gained access to numerous personal information that belonged to customers such as social security numbers, birthdates, addresses, and driver's licenses (DeMarco Jr. et al., 2017). This left many customers in fear of whether they will become

a victim of additional criminal offenses such as identity theft since now that their personal information was exposed. It also leaves customers with distrust in relations to Equifax as relationships are often important between the two. When incidents like this happen, it can shake up the trust and cause distress among customers, leading them to leave the corporation for a competitor which hurts them not just financially but also economically.

The 2017 Equifax data breach resulted in permanently affected lives as customers had to adjust to this sudden event. When incidents like this happen, it puts customer security under scrutiny and makes us question: how secure really is our personal information? Customers are forced to live with the fear of whether they are more vulnerable to another future threat or if their personal information is practically being sold on the black market right now as a result of the data breach. A scholarly article by Novak and Vilceanu expanded on this stating that an estimated 144.5 million US consumers have been put at risk for identity theft, which consequently means that they will face this risk for the rest of their lives. This triggered chaos in the political sphere, as a couple state governors filed lawsuits and investigations into the incident (Novak & Vilceanu 2019).

There are cybersecurity measures that could have been taken to mitigate the consequences or prevent the incident. Data breaches happen because they exploited a weakness within a corporation's security infrastructure. In this case, the hackers exploited the bug that existed with their new server update. This could have easily been prevented if they tested the update for bugs before it was rolled out live for customers. Testing bugs ensures that minimal problems will arise and in turn will reduce the risk of potential harm to anyone. There also should have been a quick response plan in case if something were to happen as a result of the update (Fortinet). This would involve having a swift action immediately upon awry activity to minimize the damage possible.

In conclusion, the 2017 Equifax data breach brought immense consequences to both the corporation and the customers. The hackers exploited the malfunctioned Apache Struts software update that compromised the personal information of 144 million customers. This caused outrage among customers because they now have to deal with the additional risk of identity theft for the rest of their lives now that their personal information is exposed. The political sphere was heated as well, where several lawsuits were filed against Equifax as a result of the incident. This could have easily been prevented through traditional protocols of testing the update before launching. The incident shows that any sort of mistake made on part of a corporation, even the smallest, can lead to devastation for everyone.

References

Berghel, H. (2017, December 18). Equifax and the Latest Round of Identity Theft Roulette | IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/8220474/

DeMarco, Edward J., Jr, & Mason, B. (2017). WASHINGTON Wrap-up. *The RMA Journal, 100*(3), 80-83. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/washington-wrap-up/docview/2043172601/se-2

Novak, A. N., & Vilceanu, M. O. (n.d.-b). *"The Internet is Not Pleased": Twitter and the 2017 Equifax Data Breach*. Old Dominion University Libraries - Remote Login. https://research-ebsco-com.proxy.lib.odu.edu/c/lnv5pa/viewer/pdf/tzy5ffjks5?auth-callid=a175f7a0-5d7a-43b5-8151-d621184d7b58

What Is a Data Breach and How to Prevent It? Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/data-breach