Hanah Deering

5-1 Case Study: Triple A and Defense in Depth

CS 405 Secure Coding

Southern New Hampshire University

The *Yahoo* data breach was the biggest data breach ever to be reported, effecting at least three billion accounts. Due to the amount user accounts getting exposed during this hack, the news reported it as securing the number one stop of data breaches thus far since it happened in 2013. A link to the article can be found at: https://www.ukessays.com/essays/computer-science/analysis-of-the-yahoo-data-breaches.php .

As the *Yahoo* data breach goes down in history, there are still many questions as to what really happened as it is unclear just how the hackers were able to steal three billion peoples account information There were many business, financial, and public reputation implications surrounding this incident. *Yahoo* took two years to report the issue. Due to the negligence, the personal information of many users was placed at risk for a prolonged period. This data breach that compromised the three billion accounts resulted in a $35 million charge from the Securities and Exchange Commission. *Yahoo* was also asked to provide free credit monitoring service for over 200 million impacted people of the data breach just to ensure that no identities were stolen. But most importantly, the ramifications of the data breach extended to impact *Yahoo’s* reputation, as end users lost trust and confidence in the company.

*Yahoo* could have avoided this massive data breach if cybersecurity risks had been appreciated earlier. I believe this was a combination of security and data breach as the proper security protocols were not followed there was a delayed response to the breach from *Yahoo*.

The information from all three billion accounts was put up for sale, being purchased by just three entities. Two of these three entities are known spammers and the last entity appeared to be interested in the data for espionage purposes. It is said that *Yahoo’s* account management tool and user database was accessed by installing a backdoor on one of the *Yahoo* servers, allowing the hackers to install user databases onto their personal computers. Access cookies were then generated through a script that was installed on the *Yahoo* server. If this vulnerability goes unresolved, it can lead to the misuse and abuse of end user sensitive proprietary information being used/sold.

Regular assessments and audits of systems could have prevented this type of data breach. Yahoo had not been doing work on their end to ensure the safety of end user information. Adding extra layers of security would help with not exposing information.

The Triple A and Defense in Depth approach can be used to prevent any future attacks. Authentication needs to be set up to verify the identity of all users through obtaining credentials. If users can pass the authentication processes, then the system moves to the authorization process to see what level of access the user has. People within the company need to be held accountable for their accounts and their role in keeping all information safe. Using DiD (Defense in Depth) implies that multiple layers of security are placed through without the system so that redundancy is applied in the event that one security control fails, or a vulnerability is exploited.