## 

## **Business report investigating and analyzing the data breaches of**

## **UBER and Yahoo!**

**Done by: Arijeet Roy**

**Date Submitted:** April 29, 2019

**Actual Word Count:** 2131 words

|  |  |
| --- | --- |
| *Title* | *Page* |
| [*Introduction*](#Introduction) | ***3*** |
| [*UBER Data Breach 2016*](#UBER_Data_Breach_2016) | ***4*** |
| [*Yahoo Data Breach 2013 and 2014*](#Yahoo_Data_Breach_2013_and_2014) | ***5*** |
| [*Similarities and Differences between the attacks*](#Similarity_Differences_between_attacks) | ***6*** |
| [*Lessons learnt between UBER and Yahoo!*](#Lessons_learnt_between_UBER_and_Yahoo) | ***6*** |
| [*Advices to the board*](#Advices_to_the_board) | ***7*** |
| [*Conclusion*](#Conclusion) | ***8*** |
| [*References*](#References) | ***9*** |

***Table of contents***

Ctrl + Click on the titles to navigate to respective pages.

***Introduction***

The purpose of this report is to inform the board about the issues relating to the impact of data breaches to organizations from a business perspective. These organizations - Uber and Yahoo! were impacted by a data breach and were reported during the same time period. Uber is a global transportation company that offers services including peer-to-peer ridesharing, ride service hailing, food delivery, and a bicycle-sharing system. Similarly, Yahoo is an Internet portal that incorporates a search engine and a directory of World Wide Web sites organized in a hierarchy of topic categories. These organizations will be further discussed in the report.

The report covers information of Uber and Yahoo’s experiences of how they unsuccessfully dealt with data breaches, similarities and differences of the two data breaches, how these organizations can learn from each other and propose advices to the board so that all organizations can prevent these types of data breaches.

***UBER Data Breach 2016***

In October 2016, two unauthorized individuals hacked into Uber’s third-party, cloud-based service Amazon Web Services (AWS) account to access personal data of 57 million Uber users worldwide. This includes the user’s names, phone numbers and email addresses. Among those 600,000 driver’s license numbers of drivers in the United States were stolen at the time (Etherington 2018). Luckily, sensitive information such as location data, credit card numbers, bank account numbers, social security numbers, and birth dates, had not been stolen.

Before the attack, GitHub advised to all users “never store access tokens, passwords, or other authentication or encryption keys in the code. If developers must include such items, they should use extra security procedures to prevent unauthorized access or misuse” (Kahn 2017). Uber failed to implement a secured multifactor authentication while developing the system under their GitHub account. This led hackers to routinely hunt for vulnerabilities and codes posted publicly to GitHub for passwords and private encryption keys that developers had left visible.

Uber did not report the incident to regulators or to affected customers, but instead paid ransom of $US100,000 to “hackers” to get rid of the data and cover-up the data breach, according to the report (Wong 2017). According to the California state law, “companies are to notify state residents any breach of unencrypted personal information and must inform the attorney general if more than 500 residents are affected by a single breach” (Wong 2017). Uber fired its Chief Security Officer (CSO) Joe Sullivan because of the breach, specifically for his role in keeping the cyberattack secret.

Uber’s data breach in 2016 should have been avoidable. The company should have considered the possibility of security failures and anticipated malicious behavior of any users. Therefore, they have to constantly monitor, evaluate and analyze the behavior of all users and entities in their landscapes. After the breach, Uber improved their data security by removing their access tokens, passwords, and other authentication or encryption keys in the code except open sources in GitHub database (Sharwood 2018). Before the breach Uber could have enabled a two-factor authentication to provide additional security layers which ensures that a hacker who has discovered the password will not be able to log into the account if the passwords were stored since the data breach and use IP whitelisting to connect to AWS.

Uber’s Cyber Insurance was not used after the 2016 data breach. Uber could have used this insurance as an extortion. Extortion in the cyber insurance is defined when the perpetrator threatens to seize, damage or release electronic data owned by the victim. Although their insurance covers extortion in this scenario, the US state law enforcement officials leveraged $US148 million against Uber for concealing the data breach and not complying the states’ law to report data breaches (Cameron 2018). Britain’s Information Commissioner’s Office (ICO) and Dutch Data Protection Authority also fined Uber $490,000 and $690,000 respectively (Dillet 2019).

***Yahoo Data Breach 2013 and 2014***

Personal information of around 3 billion Yahoo users were compromised, which included user names, e-mail addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers (BBC 2016). Security experts stated that although most of the Yahoo passwords used the **bcrypt** **hashing algorithm,** but many use the **MD5 algorithm** which can be cracked easily (Goodin 2016). The hackers developed web cookies to forge the login credentials which allowed them to gain access to all the accounts without the need of actual username or passwords (Newman 2016).

According to Yahoo’s SEC report, Yahoo itself was responsible as they were aware of the attack in late 2014 but failed to investigate the circumstances of the breach properly until 2 years later when a hacker claimed to have huge amount of data related to Yahoo users (Peterson 2016). Yahoo claimed the attack as a state-sponsored one but did not disclose the country behind it. The Federal Bureau of Investigation, FBI, who investigated the attack also confirmed the claim of Yahoo, suspecting Russia behind the attack. Nevertheless, the claim was never confirmed to be true and the reason to target Yahoo for the attack was also never disclosed.

Although the attack was avoidable, but the company failed to, as said by the ICO deputy commissioner of operations, James Dipple-Johnstone - "Yahoo! UK Services Ltd had ample opportunity to implement appropriate measures, and potentially stop UK citizens' data being compromised." (Shephard 2018).

The attack caused Yahoo to pay $50 million to victims and their UK branch was further fined for €2.5 million (Shephard 2018). The company also spent $35 million on lawyer fees (Leithauser 2018).

***Similarity and Differences between the attacks***

Uber and Yahoo share distinctive similarities and differences in the data breach between 2014 and 2016. These organizations informed sensitive personal information such as names, emails and phone numbers were gained access by unauthorized users during the breach, for which they had to pay outstanding fines. In 2016, both of the organizations were aware of the data breach but did not disclose to the public because they were afraid of the upcoming fines and penalties from domestic and international laws that they have to face due to this.

The differences between Uber and Yahoo is that data stolen from Uber users were comparatively less harmful as it included only names, phone numbers and email addresses. But stolen data from Yahoo was critical because it not only led to a single system but to users’ connections to their banks, social media profiles, other financial services and users’ friends and family. Hackers achieved these data breaches by routinely scan for vulnerabilities and perform different techniques to gaining access into the organization’s system. They used false login credentials to bypass the security by not using actual usernames and passwords to breach into Yahoo’s system thus, accessing user accounts and encrypted passwords. On the other hand, Uber’s login credentials were placed in a public site GitHub, which allow hackers to easily breach into Uber’s AWS account through the fault of developers and warnings given from GitHub before the breach. Finally, Uber was fined $US148 million against Uber for concealing the data breach and not complying the states’ law to report data breaches (Cameron 2018). Britain’s Information Commissioner’s Office (ICO) and Dutch Data Protection Authority also fined Uber $490,000 and $690,000 respectively (Dillet 2019). Whereas Yahoo paid $50 million to victims, $35 million on lawyer fees and their UK branch was further fined for €2.5 million. Although yahoo had a post data breach claim, which was later investigated by the FBI, Uber had no idea on who had done it. Unlike UBER, Yahoo did not have to pay any ransom amount as they claimed it to be a state-sponsored attack.

***Lessons learnt between UBER and Yahoo!***

Group member – Kasumi Jolley (43679838)

Although it may be argued that the data breaches of Yahoo and Uber themselves could have been avoided through more effective cyber security management, it is important that the companies recognize their faults in the handlings of each breach and what can be learned from them. Not only did the concealment of the breaches result in legal and financial consequences for both companies, arguably the most significant impact was the loss of confidence and trust from their respective users. Due to the similarities in both cases, it is important that the companies acknowledge the faults of their peers and attempt to gain insight into the proper proceedings of an event such as a large data breach. As such, had Uber considered the scale and impact of Yahoo’s data breach and concealment, their own scandal could have potentially been avoided.

The hacking of Yahoo in 2013 is the single largest data breach to date, compromising the information of all its 3 billion users (Amerding 2018). The scale of this breach and its subsequent concealment highlight the responsibility of a cybersecurity standard of care that must be implemented and adhered to by companies in order to prevent a breach of sensitive user information (Trautman & Ormerod 2017). Not only should companies take initiative in preventative security methods, it is imperative that they display transparency in the cases where user data have been compromised. Therefore, there is an important lesson to be learnt in the management of data security breaches and the responsibility of corporate directors to disclose such incidents to shareholders and users. Had Uber observed and considered the negative repercussions that Yahoo faced, as a result of its failure to disclose its data breaches, the ride-sharing company may have been able to improve the handling of its own breach. Yahoo’s failure to disclose within an appropriate timeframe ultimately resulted in a loss in confidence and trust by its users. In the absence of transparency, the company failed to enforce its duty of care, an event later echoed by Uber on a smaller scale. Both breaches should be lessons in management of cyber-attacks and highlight the responsibility of company directors to disclose such events to the public.

***Advices to the board***

The Uber data breach could have been prevented through more diligent cyber security practices as the breach has been described by cyber security experts as an unsophisticated attack (Nizri, 2017). The aftermath of how Uber initially handled the data breach has come under scrutiny and the board requires assistance with how to prevent anything like this to ever occur again. The board needs to implement the use of, or strengthen the countermeasures used to protect the data Uber stores. Helms et al. (2000) discusses preventative measures which will help a company protect its data. Identifying all critical information such as banking details, client lists and information etc. is vital to the protection of the company’s data makes it easier to analyze any threats to see how vulnerable your data can be to hackers. It is then at that point where you should assess the risk of what happens to your company if this critical information is released to the public and only then should you update and implement countermeasures to protect your company. This can include releasing security updates on a regular basis, hiring highly trained cyber security professionals to ensure the security of your data and can also include educated the non-skilled employees of your company how to keep their data and the company’s data secure.

It is also important to educate the board on the way that the company handled the data breach. The issues by not reporting the data breach for over a year after the incident. Not only is it illegal to report a data breach in the US and in Europe which has resulted in the company receiving fines the ethical issues regarding not informing the 57 million Uber users that they have had their data compromised. From a company who on their websites says they care about the community, and that they are dedicated to making the community safer the decision to pay the ransom to the hackers and not disclose the data breach has got to have let the public think how can they trust Uber to keep their information safe? After all, Uber relies on their customers for how successful the company is, so the board needs to realize this and put the customers first.

***Conclusion***

The purpose of this report was to investigate and analyze the issues related to the data breach of the two companies – UBER and Yahoo and provide advices to the board of the companies. The report clearly identifies that advancements in cyber security has been increasingly necessary for organizations, particularly since technical advances have increased their range, to bring the organizations a competitive advantage. The report also identifies lessons that other organizations could learn from these breaches. Because the data stolen from companies can be used in numerous destructive ways by the hackers, resulting in harm both for the users and the companies. Although no security system of any company can prevent an attack, but the companies should harden their security culture to defend an attack in the best possible way.

***References***

Amerding, T 2018, ‘The 18 biggest data breaches of the 21st century’, *CSO*, 20 December, viewed 28 April 2019, <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

BBC 2019, Yahoo ‘state’ hackers stole data from 500 million users, viewed 12 April 2019, <https://www.bbc.com/news/world-us-canada-37447016>

Cameron, D 2018, Uber To Pay Record $204 Million Fine For Concealing 2016 Data Breach. [online] Gizmodo. Available at: <https://www.gizmodo.com.au/2018/09/uber-to-pay-record-204-million-fine-for-concealing-2016-data-breach/>

Dillet, R 2019, French data protection watchdog fines Uber $460,000 for data breach. [online] TechCrunch. Available at: <https://techcrunch.com/2018/12/20/french-data-protection-watchdog-fines-uber-460000-for-data-breach/>

Etherington, D 2018, Uber data breach from 2016 affected 57 million riders and drivers. [online] TechCrunch. Available at: <https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers/> [Accessed 19 Mar. 2019].

Goodin, DG 2016, ‘Yahoo says half a billion accounts breached by nation-sponsored hackers’, viewed 12 April 2019, <https://arstechnica.com/information-technology/2016/09/yahoo-says-half-a-billion-accounts-breached-by-nation-sponsored-hackers/>

Helms, MM, Ettkin, LP and Morris, DJ (2000) Shielding your company against information compromise, *Information Management & Computer Security* vol. 8 no 3. pp.117-130.

Kahn, J 2017, Uber data breach shows vulnerability of software code-sharing services. [online] <https://www.livemint.com>. Available at: <https://www.livemint.com/Technology/E3QAV7NHJuk6t4geJwbwHJ/Uber-data-breach-shows-vulnerability-of-software-codesharin.html> [Accessed 19 Mar. 2019].

Larson, S 2017, Uber's massive hack: What we know. [online] CNNMoney. Available at: <https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html> [Accessed 19 Mar. 2019].

Leithauser, TL, ‘$35M settlement reached for Yahoo data breach’, viewed 13 April 2019, <http://simsrad.net.ocs.mq.edu.au/login?url=https://search-proquest-com.simsrad.net.ocs.mq.edu.au/docview/2049976598?accountid=12219>

Newman, LHN 2016, ‘Hack brief: Hackers breach a billion Yahoo accounts. A billion’, viewed 12 April 2019, <https://www.wired.com/2016/12/yahoo-hack-billion-users/>

Nizri G (2017) How Uber Could Have Prevented Their Latest Cybersecurity Breach [online] Ayehu. Available at: https://ayehu.com/uber-prevented-latest-cybersecurity-breach/

Peterson, AP 2016, ‘Yahoo discovered hack leading to major data breach two years before it was disclosed’, viewed 13 April 2019, <https://www.washingtonpost.com/news/the-switch/wp/2016/11/10/yahoo-discovered-hack-leading-to-major-data-breach-two-years-before-it-was-disclosed/?utm_term=.ad9904ccadb8>

Sharwood, S 2018, Uber quits GitHub for in-house code after 2016 data breach. [online] Theregister.co.uk. Available at: <https://www.theregister.co.uk/2018/02/07/uber_quit_github_for_custom_code_after_2016_data_breach/> [Accessed 19 Mar. 2019].

Shephard, SA 2018, ‘Yahoo handed euro 250,000 fine over 2014 data breach’, viewed 12 April 2019, <http://simsrad.net.ocs.mq.edu.au/login?url=https://search-proquest-com.simsrad.net.ocs.mq.edu.au/docview/2053825266?accountid=12219>

Trautman, LJ and Ormerod, PC 2017, ‘Corporate directors’ and officers’ cybersecurity standard of care: The Yahoo data breach’, *American University Law Review,* vol. 66, no. 5, pp.1231-1291.

Wong, J 2017, Uber concealed massive hack that exposed data of 57m users and drivers. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack> [Accessed 19 Mar. 2019].