Cybersecurity P (ELEC-E7470)

Group ASRG (Nathan Atta, Kevin Silbereisen, Janne Valo)

Case Study Report

Table of Contents

Introduction

Uber Technologies, Inc. is a company based in the United States best known for its ride sharing mobile application that was initially launched in 2010. The application allows drivers to provide car rides for people and provides a platform for booking and paying the rides. Essentially, Uber offers a taxi service without directly employing the drivers. The company has since branched out to other areas as well, and currently offers for example also a food delivery service called Uber Eats and a freight service called Uber Freight in some countries. On May 10th, 2019 Uber made its entrance in the NASDAQ stock exchange in one of the highest valued IPOs (Initial Public Offerings) since Facebook and Alibaba went public.

Uber currently operates in over 700 cities in 63 countries around the world. The users of the app use the service for over 14 million trips daily (Uber Technologies, Inc., 2019). The company has not released exact numbers of its users, but the statistics company Statista estimates the number to be around 110 million.

Uber has been in the news for several different controversies, scandals and data breaches. The scandals and controversies have ranged from workplace bullying and sexual harassment to blatant disregard of the users privacy and unfair business practices. The company has also been at odds with regulators and lawmakers in several countries (Taylor & Goggin, 2019). Finland is one example: before the legislation was changed in 2018, the service was deemed unlawful and several drivers were fined, and the service actually withdrew from Finland for a while (Hern, 2017).

Uber has been hacked during the years several times, but in this paper, we are focusing on the largest and most well known incident. Between October and November 2016 Uber was hacked, and the attackers gained access to the data of 57 million users around the world. The breach included data from both drivers and riders (Khosrowshahi, 2017). The breach itself was nothing special: the stolen data was not sensitive, and despite covering 57 million users, in the grand scheme of breaches, the hack was not an especially large one. What makes the breach stand out from others, however, is the peculiar and irresponsible way the company handled the breach.

In this paper, we will take a closer look at what led to the breach, what happened after the breach and how the company handled the situation. We will also consider the effects the hack had on Uber and its users. To conclude, we will review what lessons the breach and the reaction to it offer to other companies in handling cyber security or data breaches.

Background: the 2014 Breach

Even though this paper focuses specifically on the 2016 breach, an introduction of a previous breach that took place in 2014 is in order since similar mistakes that led to the 2016 breach were made before, and even the mistakes made in responding to the earlier breach were similar and repeated later.

In May of 2014, a hacker gained access to names and driver's license numbers of more than 100,000 Uber drivers. The breach was discovered in September 2014, but it was only disclosed 5 months later, in February 2015 (Lewis, 2015).

When disclosing this first breach, Uber already showed a serious lack of responsibility and transparency, and the significance of breach was downplayed. The company first reported that only 50,000 users were affected, and later was forced to correct the statements since the number of affected users was actually 100,000. It also took the company 4 months to discover the breach and 5 more months to notify the victims of the hack. The hacker had been able to access the driver data on Amazon Web Services (AWS), according to the Federal Trade Commission (FTC) of the United States. An access key to AWS had been publicly posted by an Uber engineer to the code sharing website GitHub (Brewster, 2017).

After this incident, Uber was fined by the state of New York and the FTC did order the company to up its security game (Brewster, 2017). The next sections will show how seriously it took this order.

The 2016 Breach

On November 14, 2016 an attacker approached Uber via e-mail, informed them that he or she had exfiltrated Uber’s data and demanded “a six-figure payout”. Uber rather quickly determined that the attacker had gained access to archived copies of Uber databases and files that were stored on Amazon Web Services (AWS) in a Simple Storage Service (S3) bucket.

The company launched an internal investigation that concluded that the attacker had – as with the 2014 breach – gained access to the AWS S3 credentials through a private GitHub repository used by Uber engineers. The engineers had used the GitHub repository to store code that included the AWS S3 credentials (Flynn, 2018). And as the credentials were stored in plaintext, the breach of the GitHub repository opened a door to S3 bucket as well.

Uber has not disclosed in detail how the attackers gained access to the GitHub repository (Sharwood, 2018), but admitted that the company did not use multi-factor authentication before the breach (Flynn, 2018). In other words, GitHub did offer two-factor authentication, which can already be described as a rather basic security measure offered by several less critical consumer services as well. And, to emphasize, Uber did not use the feature even though it already got hacked once before in a similar manner.

The attackers gained access to data of over 57 million Uber users in total. The breached information included names, e-mail addresses and phone numbers of all users. Additionally, for a subset of 600,000 drivers in the United States, the data included their driver’s license numbers (Khosrowshahi, 2017). The information also included “in some cases” Uber user IDs, location of the user when signing up, user tokens, and hashed and salted passwords (Flynn, 2018). The company claims that no trip location history, credit card numbers, bank account numbers, dates of birth or social security numbers were accessed (Flynn, 2018), and no evidence of such data being breached has surfaced.

After the breach, Uber paid $100,000 to the attacker through the bug bounty service HackerOne. Uber claims that it received “assurances” that the data had been destroyed after the payout (Flynn, 2018). Uber has not provided details of what such assurances were, but there are no signs that the hackers have publicized the data anywhere.

Generally, companies participating in bug bounty programs pay out rewards for hackers who discover vulnerabilities in the systems of the participating companies. However, an essential part of a bug bounty program is the responsible disclosure of the vulnerability to the company in question (see e.g. HackerOne, 2019). In other words, the idea of the bug bounty programs is to reward hackers for disclosing the vulnerabilities to the company in a responsible manner instead of selling them to the highest bidder or using them themselves for nefarious purposes.

In Uber’s case, it would thus seem more appropriate to classify the payout as ransom or hush money instead of participating in a bug bounty program. And indeed, when testifying before a subcommittee of the United States Senate, the chief information security officer of the company admitted that “*the bug bounty program is not an appropriate vehicle for dealing with intruders who seek to extort funds from the company*” (Flynn, 2018). Classifying the payout is not relevant to the issue, however, even if it would not by any objective standards meet the general characteristics of a bug bounty reward.

After the breach happened and the internal investigation concluded what had happened, the company kept quiet and did not tell either the users or the relevant authorities. The breach was publicly disclosed in November 2017, almost exactly a year after it was discovered (Khosrowshahi, 2017). The disclosure was only done after the current chief executive officer (CEO) Dara Khosrowshahi took over the company.

Uber said it discovered the breach as a result of a board investigation into the business practices of the company (Isaac, Benner & Frenkel, 2017). The previous CEO, Travis Kalanick, resigned in June 2017. Even though the resignation happened after a series of scandals including discrimination, sexual harassment and bullying (see e.g. Wong, 2017), the data breach seems not to have been a direct factor in the resignation. However, it has been reported that the deal with the attackers was done “under the watch” of Kalanick (Isaac, Brenner & Frenkel, 2017).

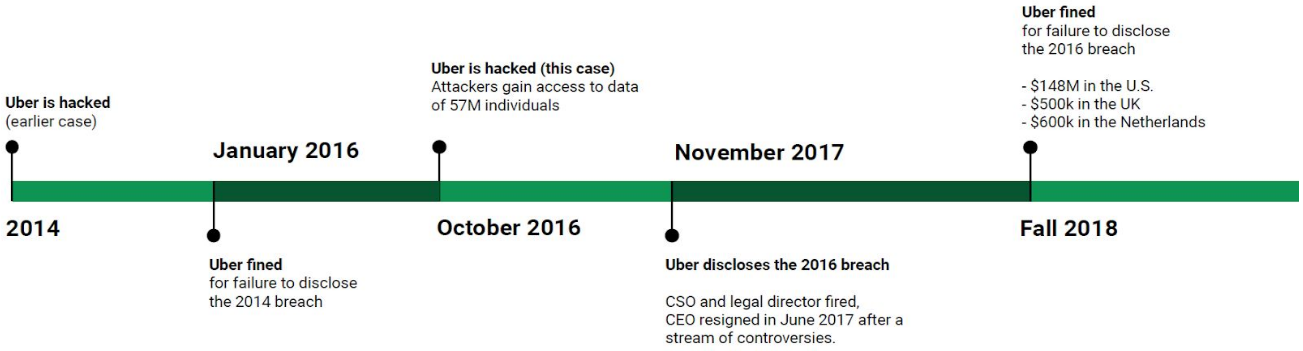

Figure 1: Timeline of the events.

The Aftermath

After the company finally disclosed the breach in November 2017, authorities in several countries quickly announced investigations into the matter and expressed dismay at the fact that Uber had tried to cover up the breach by paying the attackers instead of disclosing the breach to the data subjects, the users of the app, the authorities or the general public (Finkle & Somerville, 2017). The investigations led to several fines, which are discussed in more detail in the *Economic Damage* section.

As Uber disclosed the breach, it also announced that it had fired the chief security officer of the company as well as the legal director of security and law enforcement. The two had led the response to the incident and the subsequent cover up (Finkle & Somerville, 2017 & Khosrowshahi, 2017). The company also hired an external company (Mandiant) to “conduct a thorough analysis of the data at issue”, i.e. investigate what had been stolen (Khosrowshahi, 2017).

After the disclosure, Uber announced that the company would individually notify the drivers whose driver’s license number was stolen. These drivers were also offered free credit monitoring and identity theft protection services (Khosrowshahi, 2017).

Uber was faced with great amount of backlash and distrust towards the company due to their decision to not only keep the data breach a secret but also to bribe the hackers into secrecy. This was however in vain in the end, and the hack was eventually made public and made worldwide news. This of course led to the big question and speculation of whose information was actually stolen (not surprising, as Uber had not informed the affected users personally).

The debate around the breach and how Uber handled it gained major traction in the social media amongst the users of Uber. Especially, Twitter seemed to be a popular platform for the affected users to voice their opinions in this blatant violation of trust between them and the company. While data breaches always damage a company's reputation in some way, the cover up and the public reaction of this kind was nonetheless unheard of. For example, even when the users' banking information was involved in cases of data breaches at PayPal, the transparency towards their users was what prevented major trust losses and reduced the overall media coverage due to the lack of outrage from the users. Not so with Uber.

Additionally, this was not the first misstep that the now resigned CEO of Uber Travis Kalanick had made and as such, the impact of the incident in question was even greater (Spiegel, 2017). Furthermore, the attempted cover-up initiated a thorough discussion of the responsibility and accountability of the company towards the public. As such, among the many critics of Uber's decision to stay silent about the data breach, California Attorney General Xavier Becerra and U.S. Senator Richard Blumenthal voiced their opinion by calling the secrecy "*a blatant violation of the public's trust*" (Conger, 2018) and "*a form of obstruction of justice*" (Stoller, 2018).

#UberHack

As previously stated, one of the main reasons this data breach generated this level of discussion was not the size of the company nor the number of files or records that had been stolen. The files also were not made public, even though the attackers gained access to them. Therefore, the traditional media did not really turn it into much of a headline until the delay of the response was revealed and the hashtag "#UberHack" was established in social media. Having the users already in and angered state made it easy for larger media to add to the discussion and maintain it as an issue over an extended period of time. Uber also was not a very sympathetic subject in the public at the time due to the previous scandals and controversies and the arrogant attitude of the company and its management towards users, media and the public.

The continuous attention of the media and the social media users made it harder for Uber to reconnect to their users in attempts to regain their faith and trust in the company. However, not only users but also employees started to look at the company they were working for in a different light. An often-overlooked affected group are the employees whose credentials had been used to steal the data from the GitHub repository in the first place. Since this incident revealed that the information was not properly guarded by the company either, it caused a lot of people to, if not turn their backs on the company, at least distance themselves from the brand and demanded retribution and an official apology from the company to the victims.

On November 21st of 2017, Uber's new CEO Dara Khosrowshahi released an official statement in which he goes into the details of the data breach which were by and large already publicly known at that point. Moreover, he promised that all the victims would be individually notified and informed about the details of what of their data had been stolen (Khosrowshahi, 2017).

Economic Damage

The breach has generated different kinds of economic consequences at different scales for the company. In fact, Uber has been fined in different countries around the world for its failure to protect the users' information, and some of the settlements have included payouts to the affected users. Also, as said previously, hackers have been paid to remain silent and to delete the stolen data. And finally, some internal and less easily quantifiable costs have to be taken into account as well, such as costs from the reorganization of the company structure, the loss of confidence of the customers and so on.

First, let's discuss about the amount Uber paid the hackers. As discussed, Uber did not tell authorities or the users of the app about the breach, but instead chose to stay quiet and pay the hackers $100 000 to keep the breach secret, and to delete the stolen data.

A few months after the breach happened, in June of 2017, the CEO at the time, Travis Kalanick resigned after a stream of controversies unrelated to the 2016 data breach. In November of 2017, Uber disclosed the breach and the chief security officer of the company and a legal director got fired. Once the breach was revealed, Uber has been investigated and fined by authorities in the United States, in the United Kingdom and in the Netherlands.

In the United States, Uber got fined $148 million for failing to notify users they had been hacked. "*This is one of the most egregious cases we've ever seen in terms of notification; a yearlong delay is just inexcusable,"* Lisa Madigan, the Illinois Attorney General told the Associated Press (2018). The settlement payout was divided among the states based on the number of drivers each had. Illinois's share was $8.5 million, said Madigan, who planned at the time to provide $100 to each of the affected Uber drivers in Illinois. The payout was similar to what several other states had estimated.

In the European Union, Uber has been fined as well for failing to protect the customers' personal information. The Information Commissioner's Office (ICO) in the United Kingdom fined the company £385,000 ($490,760) while the Dutch Data Protection Authority imposed a 600,000 € ($678,780) fine.

When discussing the fines in Europe, it bears worth noting that the breach occurred before GDPR, the General Data Protection Regulation of the European Union, came into force in May 2018. In other words, the fines were based on the previous national legislation. GDPR would have empowered the European data protection authorities to issue fines up to 4% of the company's global turnover. In 2016, Uber reported a revenue of $6.5 billion, meaning the maximum fine could theoretically have been around $260 million. While this is the theoretical maximum, it can easily be speculated that the fine might have been substantial, since the failure to disclose the breach in a timely manner and the conscious effort to cover up the incident would have been gross violations of the GDPR. The regulation requires the data breaches concerning personal data to be notified to the authorities within 72 hours and in certain cases to the data subjects themselves as well.

Reasons

The breach revealed several points and ways in which Uber failed in its procedures. First, some important security aspects and practices were neglected. In fact, Uber software developers stored sensitive login data on a third-party repository, GitHub, which allowed the hackers to get access to Amazon Web Service data storage. Moreover, multi-factor authentication should have been used. In 2016, multi-factor authentication already was a rather basic security measure, especially in more critical or sensitive systems.

In addition to the lax security regarding GitHub, it is worth noting that the AWS credentials were stored in plaintext in the service, and the attackers thus had easy access to them. Uber also said that it implemented AWS credential rotation after the incident (Flynn, 2018).

What makes the neglected security especially egregious was the fact that the 2016 breach was not the first time a similar omission led to another breach. In 2014, hackers found a login key in code that Uber's developers publicly posted on GitHub, which resulted in the theft of data on 50,000 Uber drivers. This breach, too, was only disclosed much later, and Uber was fined in the state of New York for the failure to disclose the earlier breach. This, of course, does not give a flattering image of the company's culture regarding transparency and responsibility.

Conclusion

When assessing the initial reaction of Uber, it is noteworthy to remember that the breach did not include sensitive data. For the vast majority of affected users, the data in question included their names, e-mail addresses and phone numbers. The exception to this are the 600 000 users whose U.S. driver's license number got stolen, which exposes them to identity theft. While of course embarrassing for Uber and definitely a breach of privacy of their users, the incident still was not as near as critical of a breach than for example the Home Depot breach of 2014, which affected almost an identical number of people. In that case, it was credit card details that the attackers gained access to, in addition to e-mail addresses (Stempel, 2016).

While 57 million affected users is a very large group of people, the breach was not an especially large one either, compared to for example Equifax or the breaches of Yahoo! reported in 2016 (Isaac, Benner & Frenkel, 2017). The Equifax breach affected over 145 million users and the first Yahoo! breach affected over 300 million users. The other Yahoo! Breach affected all 3 billion of their users, having the dubious honor of being the largest data breach ever. Considering these facts, it would seem that there would have been no reason to try to hide the breach. Of course, it would have probably been news and caused some negative publicity, but for a more limited amount of time and the company could have tried to be as transparent as possible towards the users and provide them assistance in mitigating the effects of the breach (which it did, a year later, when it offered e.g. credit monitoring to those whose driver's license number was stolen).

It is also noteworthy that the 2016 breach was not the first one to hit Uber: as we discussed earlier, in May 2014 the company was breached, and names and driver's licenses of over 50,000 drivers were stolen. The company only discovered the attack later in 2014 and this breach as well was disclosed much later, in February of 2015 (Isaac, Benner & Frenkel, 2017). And in fact, Uber was fined for the failure to disclose this breach as well.

The response after the disclosure seems like the one that should have been made immediately, and if we look at those actions separate from their context, they actually provide a rather good example of how companies could act when breached. Uber hired an external company to do forensics, explained what happened in a somewhat transparent manner and offered identity theft protection and credit monitoring services for those users whose driver's license number was stolen.

All this, however, is shadowed by the initial reaction that seems to be an exceptionally clear example of how not to do things. First, the company neglected to take care of basic information security measures (two-factor authentication). Then, they chose to pay ransom to the attackers to keep them quiet, and trust them to delete the stolen data (ironically enough, this is the part that actually seems to have worked). After that, they did their best to hide the breach from the data subjects or the authorities. But as California Attorney General Xavier Becerra noted, trying to sweep the breach under the rug was "*consistent with [Uber's] corporate culture at the time*" (Salinas, 2018). It seems safe to guess that the slew of other controversies and scandals the company had recently been through had an impact on the decision to try to keep quiet, and it can easily be seen as an attempt to control the public image of the company. While the hack initially was kept secret for a while, in the long run, the cover up turned against the company.

References

CONGER, Kate, 2018. Uber Settles Data Breach Investigation for $148 Million. *The New York Times* [online]. 26 September 2018. [viewed 13 May 2019]. Available from: https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html

FINKLE, Jim & SOMERVILLE, Heather, 2017. Uber breach, cover-up trigger government probes around the globe. *Reuters* [online]. 22 November 2017. [viewed 11 May 2019]. Available from: https://www.reuters.com/article/uber-cyberattack/uber-breach-cover-up-trigger-government-probes-around-the-globe-idUSL1N1NS189

FLYNN, John, 2018. *Testimony of John Flynn to the Subcommittee on Consumer Protection, Product Safety, Insurance and Data Security; Committee on Commerce, Science and Transportation; United States Senate.* 6 February 2018. [viewed 9 May 2019]. Available from: https://www.commerce.senate.gov/public/_cache/files/7d70e53e-73e9-4336-a100-67b233084f12/75728554E990488D71625DFA69B05494.uber---john-flynn---testimony.pdf

HACKERONE, 2019. *Vulnerability Disclosure Guidelines* [online]. [viewed 9 May 2019]. Available from: https://www.hackerone.com/disclosure-guidelines

HERN, Alex, 2017. Uber presses pause on primary taxi service in Finland until 2018. *The Guardian* [online]. 6 July 2017. [viewed 12 May 2019]. Available from: https://www.theguardian.com/technology/2017/jul/06/uber-pop-primary-unlicensed-taxi-service-regulation-helsinki-finland-until-2018

ISAAC, Mike; BENNER, Katie & FRENKEL, Sheera, 2017. Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data. *The New York Times* [online]. 21 November 2017. [viewed 13 May 2019]. Available from: https://www.nytimes.com/2017/11/21/technology/uber-hack.html

KHOSROWSHAHI, Dara, 2017. 2016 Data Security Incident. *Uber Newsroom* [online]. 21 November 2017. [viewed 8 May 2019]. Available from: https://www.uber.com/newsroom/2016-data-incident

LEWIS, Dave, 2015. Uber Suffers Data Breach Affecting 50,000. *Forbes* [online]. 28 February 2015. [viewed 13 May 2019]. Available from: https://www.forbes.com/sites/davelewis/2015/02/28/uber-suffers-data-breach-affecting-50000/

SALINAS, Sara, 2018. Uber will pay $148 million in connection with a 2016 data breach and cover-up. *CNBC* [online]. 26 September 2018. [viewed 12 May 2019]. Available from: https://www.cnbc.com/2018/09/26/uber-to-pay-148-million-for-2016-data-breach-and-cover-up.html

SHARWOOD, Simon, 2018. Uber quits GitHub for in-house code after 2016 data breach. *The Register* [online]. 7 February 2018. [viewed 11 May 2019]. Available from: https://www.theregister.co.uk/2018/02/07/uber_quit_github_for_custom_code_after_2016_data_breach/

SPIEGEL, 2017. 57 Millionen Menschen betroffen Uber hielt großen Hackerangriff geheim. *Spiegel Online* [online]. 22 November 2017. [viewed 10 May 2019]. Available from:

https://www.spiegel.de/wirtschaft/unternehmen/uber-hielt-grossen-hackerangriff-geheim-57-millionen-menschen-betroffen-a-1179646.html

STEMPEL, Jonathan, 2016. Home Depot settles consumer lawsuit over big 2014 data breach. *Reuters* [online]. 8 March 2016. [viewed 12 May 2019]. Available from: https://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCN0WA24Z

STOLLER, Daniel R., 2018. Uber Answers for Data Breach, Alleged Cover Up in Senate Probe. *Bloomberg BNA* [online]. 6 February 2018. [viewed 13 May 2019]. Available from: https://www.bna.com/uber-answers-data-n57982088428/

TAYLOR, Kate & GOGGIN, Benjamin, 2019. 49 of the biggest scandals in Uber's history. *Business Insider* [online]. 10 May 2019. [viewed 13 May 2019]. Available from: https://www.businessinsider.com/uber-company-scandals-and-controversies-2017-11

UBER TECHNOLOGIES, INC., 2019. *Form S-1, Registration Statement under the Securities Act of 1933*. United States Securities and Exchange Commission. 11 April 2019. [viewed 8 May 2019]. Available from: https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm

WONG, Julia Carrie, 2017. Uber CEO Travis Kalanick resigns following months of chaos. *The Guardian* [online]. 20 June 2017. [viewed 8 May 2019]. Available from: https://www.theguardian.com/technology/2017/jun/20/uber-ceo-travis-kalanick-resigns

ASSOCIATED PRESS, 2018. Uber fined $148m for failing to notify drivers they had been hacked. *The Guardian* [online]. 26 September 2018. [viewed 14 May 2019]. Available from: https://www.theguardian.com/technology/2018/sep/26/uber-hack-fine-driver-data-breach

LORHMANN, Dan, 2017. After Uber Data Breach: Lessons for All of Us. *Government Technology* [online]. 2 December 2017. [viewed 12 May 2019]. Available from: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/after-uber-data-breach-lessons-for-all-of-us.html

BREWSTER, Thomas, 2017. FTC: Uber Failed To Protect 100,000 Drivers In 2014 Hack. *Forbes* [online]. 15 August 2017. [viewed 14 May 2019] Available from: https://www.forbes.com/sites/thomasbrewster/2017/08/15/uber-settles-ftc-complaint-over-secuirty-and-privacy/#7a1edfae88da