Taking users' privacy for a ride: A Case Study on the Uber Data Breach

I. Introduction

Uber Technologies, Inc. owns and operates the largest ride sharing application globally, which allows customers to connect with drivers using their mobile device. The organization collects certain personal information from the customers and the drivers including- names, email address, phone number, license and registration number of the drivers, etc. (Uber Technologies Revised Complaint, 2018)

On November 2017, Dara Khosrowshahi, the new CEO of Uber announced a major breach of data, compromising personal information of about 57 million customers and drivers. He disclosed that the breach was discovered by Uber on November 2016 and he had been made aware of the incident only recently. At the time, the organization had paid-off the hackers with an amount of $132,000 to delete the data without notifying any of the affected customers and drivers or any legal authorities about the breach, causing a violation of the law in the areas they operated in. This violation cost the Organization $148 million to be paid in fines. (Sutton, 2017)

This paper explores the Uber data hack of 2016. It would begin with a chronology of the events and the technical aspects of the breach. It would then explore the response of the victim organization in the wake of the breach, the disclosure of the incident, the resolutions made and the consequences faced. Finally, the paper would analyze the steps taken by Uber following the breach and provide insights with ideal and effective responses.

II. The Specifics

A. Chronology and technical aspects

On May of 2014, the personal data of Uber's drivers were accessed by hackers from an Amazon S3 bucket, a public cloud storage service used by Uber to store their organizational data. The hackers gained access to the platform using an access key which was posted publicly on a GitHub repository, and came into possession of 100,000 drivers' personal information. The breach was detected by Uber's security team, by methods unknown, on September of that year and instead of promptly notifying the affected drivers and the Federal Trade Commission (FTC), they waited until February of the next year. Following the disclosure, FTC started an investigation into the matter. (Wright, 2020)

On the April of 2015, Uber hired their first Chief Security Officer, Joe Sullivan. On mid-November of 2016, Sullivan received an anonymous email making claims about procuring data from Uber's database by exploiting a vulnerability. (Wright, 2020) Investigations, by methods which were not disclosed by Uber, performed by their security team confirmed the breach. Two hackers gained access to a private GitHub repository used by the software engineers of Uber. There they came across login credentials, in plain text, which gave them access to the AWS account which Uber used to store the database of customers and drivers. This compromised names, email addresses and phone numbers of 50 million customers and 7 million drivers in addition to the names and license numbers of 600,000 drivers in the United States. (Newcomer, 2017)

On April of 2017, Uber sent a letter to FTC to close the investigation of the 2014 data breach claiming that they complied completely to the investigation and have implemented additional security to their third-party database to prevent further breaches. The letter did not mention the recent hack of 2016. FTC and Uber reached an agreement regarding the previous breach, which mandated to strengthen their privacy, undergo audits for 20 years every 2 year, and prohibit them from falsifying their security practices. (Wright, 2020)

B. Uber's Response

Following the email from the hackers, Sullivan and then-CEO Travis Kalanick decided to treat the situation as a "Bug Bounty program", which is a platform where organizations willingly pay to have their security vulnerabilities tested. After tracking down the hackers, a 20-year old from Florida and a Canadian (Anon., 2018), Sullivan offered them 100,000 USD disguising as a "Bug Bounty" to sign a non-disclosure agreement and delete the data. (Wright, 2020) They also chose not to notify any of the affected users or to disclose the incident to any government agencies, violating the state's data breach notification law and the agreement between the organization and FTC from the 2014 data breach. (Torre, 2019) They hid the fact from their Board of Directors as well. The board carried out an investigation on the activities of Sullivan and his security team and came to find out about the breach and the non-disclosure.

On the June of 2017, following various scandals, Travis Kalanick stepped down as CEO and on August of that month, Dara Khosrowshahi was named the new CEO of Uber. On the September of 2017, Sullivan was asked to brief Khosrowshahi about the breach of data that occurred in late 2016. Following this, Khosrowshahi fired Sullivan and a senior lawyer from his team, Craig Clark, for not disclosing the breach and for paying off the hackers. (Wright, 2020)

C. Disclosure and Resolutions

On the 21st November of 2017, Khosrowshahi disclosed the breach in an open letter where he laid out the details of the attack and how it was handled at the time to secure to the data. He also mentioned that according to their outside forensics' experts, there has been no indication of trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth of the users being accessed or downloaded. In his letter he also mentioned about strengthening the security of their cloud-based storage systems, which would prevent further unauthorized access and the firing of the people responsible for the breach and the cover-up. The letter also included various steps that he had taken to remedy the situation and earn back the trust of their customers. They are:

i. Notifying regulatory authorities
ii. Individually notifying the affected drivers.
iii. Providing the drivers with free credit monitoring and protection from identity theft.
iv. Monitoring the affected accounts and flagging them for fraud protection. (Khsorowshahi, 2017)

In addition to the above, according to a statement from Uber's Chief Legal Officer Tony West, Uber hired Ruby Zefo, the former leader of Intel's global privacy and security legal team, as their Chief Privacy Officer and Matt Olsen, a co-founder of a cybersecurity consulting firm and former general counsel of the National Security Agency and director of the National Counterterrorism Center, as their Chief Trust and Security Office, as an initiative from the company to alleviate any weaknesses in their security and privacy practices as part of their mission to move forward from the negative image created by the data breaches. (Korosec, 2018)

III. Legal Ramifications

A. Upon learning about the 2016 breach and the cover-up, the Federal Trade Commission announced a withdrawal of their previous settlement with Uber and further filed a detailed formal complaint about the organization's practices. It went on to disparage their security practices and criticized their collection of user data under false pretenses of security. The grounds for their complaints were that Uber failed to closely monitor and audit and provide reasonable security for the database of their users' personal information as per their promises. The other complaint was regarding Uber's failure to disclose the breach of 2016 to the affected consumers and the commission until about a year after it occurred. (Uber Technologies Revised Complaint, 2018) Following the complaint, they agreed upon a revised settlement with Uber stating that the organization would be subject to civil penalties for failure to disclose any further security breaches or incidents regarding their users' data. (Wright, 2020)

B. As a result of the 2016 breach, Uber came to a settlement with the state Attorney Generals of 50 states and the District of Columbia, mandating Uber to adhere to model data security and breach notification practices and maintain an integrity program for their employees to report unethical behavior. They were furthermore required to hire an outside security firm to evaluate their security practices. In addition, the settlement required Uber to pay a penalty of $148 million, which is the biggest data-breach payout to-date. This payout included a settlement from the suit filed against Uber by the Attorney General of Washington state for flouting the state's data breach notification law by failing to promptly notify the breach to the 10,888 drivers based in Washington and the Attorney General of the state. The lawsuit excluded the passengers, as the breach notification law of Washington requires notification only in cases where the names of the individuals along with any of their sensitive data (such as- financial account numbers, driver's license number, or Social Security number) is exposed. In the cases of the passengers, no such evidence was found. (Torre, 2019)

IV. Analysis and Insights

The massive data breach of 2016 exposing personal information of 57 million users of Uber's application was convoluted by the fact that they failed to timely notify the incident to the legal authorities or the users whose data were compromised.

Firstly, they should have taken heed of their public cloud storage security, considering that it contains data of sensitive nature, right out of the gate and should have taken steps to prevent further unauthorized access after the initial hack of their database on 2014. Moreover, they should have closely monitored and regulated the information that were being shared in the GitHub repositories, as the login credentials of the AWS database were found by the hackers in one of the repositories maintained by the Software engineers of Uber in plain text. (Trend Micro, 2017)

Even though paying-off the hackers and having them sign a non-disclosure may have momentarily resolved the issue, and were even applauded by some, the act is generally seen as encouraging criminals and funding organized crime. According to Kevin Beaumont, a British Cyber Security expert, paying ransoms to hackers are creating a market for unethical behavior and demonetizing these activities would cause them to be "teenagers in bedroom breaching companies for fun". (Isaac, et al., 2017)

Uber's biggest mistake, however, was hiding the breach from the legal authorities and failing to notify the affected customers, causing a violation of the data breach notification law. According to the statement from New York's Attorney General, Barbara Underwood, the huge fine imposed on Uber was a message about the "zero tolerance" policy of the law when it comes to personal information of customers and employees being mishandled. (Carr, 2018) Instead of hiding the fact, they should have worked with the legal authorities and security experts which might have helped them save millions of dollars and their reputation.

V. Conclusion

As per the case study, it is clear that data and personal information are sensitive elements and need to be protected from threat agents with the same effort that goes into protecting any other valuable assets, if not more. Organizations should take notice of and control the data that goes into their cloud storage systems and should ensure proper security of these data through encryption and other methods, even more so if these data are of sensitive nature. Uber's data breach cover-up has cost them their reputation and millions of dollars in fines. Moreover, it is likely that paying-off the hackers has provided encouragement for criminals to pursue executing offenses of similar nature in the future, driven by the desire of a monetary reward. All in all, the case of the Uber data breach has been a lesson for all organizations regarding what to avoid doing in the case of a sensitive data breach.

Since the breach, Uber has been taking steps to improve their organizational values and security practices. Dara Khosrowshahi has been cleaning house since being appointed as the CEO of the San Francisco based company, which has gained a reputation for flouting laws and regulations, and has summarized their new set of values as "doing the right thing. Period." (Isaac, et al., 2017) Despite making mistakes initially, Uber is heading in the right direction by developing contingency measures and strengthening their security team in order a to avoid a recurrence of the unfortunate incident. While this won't change the past, it certainly would help heal their tarnished reputation as an organization and eventually gain back their customers' trust.

References

Anon., 2018. *Sydney Morning Herald.* [Online]
Available at: https://www.smh.com.au/business/companies/uber-to-pay-204m-to-settle-data-breach-cover-up-20180927-p5069k.html
[Accessed 27 September 2018].

Carr, A., 2018. *Bloomberg.* [Online]
Available at: https://www.bloomberg.com/news/articles/2018-09-26/uber-to-pay-148-million-in-settlement-over-2016-data-breach
[Accessed 27 September 2018].

Isaac, M., Benner, K. & Frenkel, S., 2017. *The New York Times.* [Online]
Available at: https://www.nytimes.com/2017/11/21/technology/uber-hack.html
[Accessed 21 November 2017].

Khsorowshahi, D., 2017. *Uber.* [Online]
Available at: https://www.uber.com/newsroom/2016-data-incident/
[Accessed 21 November 2017].

Korosec, K., 2018. *Tech Crunch.* [Online]
Available at: https://techcrunch.com/2018/09/26/uber-to-pay-148-million-in-data-breach-settlement/
[Accessed 27 September 2018].

Newcomer, E., 2017. *Bloomberg.* [Online]
Available at: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data
[Accessed 22 November 2017].

Sutton, M., 2017. *ABC News.* [Online]
Available at: https://www.abc.net.au/news/2017-11-22/uber-data-breach-was-not-disclosed-ceo-says/9179168
[Accessed 22 November 2017].

Torre, L. F. d. l., 2019. *Medium.* [Online]
Available at: https://medium.com/golden-data/case-study-uber-technologies-inc-data-breach-7261484d6471
[Accessed 14 May 2019].

Trend Micro, 2017. *Trend Micro.* [Online]
Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users
[Accessed 22 November 2017].

Uber Technologies Revised Complaint (2018) Secretary of Federal Trade Commission.

Wright, R., 2020. *Search Security.* [Online]
Available at: https://searchsecurity.techtarget.com/news/252488361/The-Uber-data-breach-cover-up-

A-timeline-of-events
[Accessed 31 August 2020].