Data Breach in the Service Sector: Problems and Solutions

ISBN 978-1-943295-24-1

Kishwar Joonas
Ahmed Y. Mahfouz
Antoine Banks
Dinah Murphy
Tiara Johnson
Jasmine Napper
Larry Luellin
Prairie View A&M University
(kajoonas@pvamu.edu)
(aymahfouzs@pvamu.edu)
(banks.antoine@sbcglobal.net)
(ddmurphy12@pvamu.edu)
(tjohnson180@pvamu.edu)
(jnapper@pvamu.edu)
(lluellen@pvamu.edu)

A classic success story in the service sector is Uber Technologies, Inc., which is a pioneer in the ride-sharing industry. Despite facing significant competition in the field, Uber Technologies, Inc. continues to be the market leader. The company's web site, uber.com, supports the real world of ride-sharing with through a digital system. We examine the phenomenon of multiple data breaches suffered by the company in the past. We also discuss the company's risk mitigation strategies to protect against data compromise, achieve a smoother digital operation, and maintain its market position.

Keywords: Management Information Systems, Marketing, IOS, Android, MFA, Risk Factors, Data Breach

1. Introduction

1.1 Industry Background

The development of the Uber Company was based on a simple idea by the co-founders of facilitating access to a ride through the use of the phone. Paris experienced the infamous blizzard incident in December 2009. When Travis Kalanick and Garrett Camp were unable to hail a cab during a storm, they quickly came up with the concept for the startup UberCab (Blystone, 2022). After encountering two, Travis Kalanick and Garrett Camp spent their time looking for new business ideas to fit their aspirations until morning. One of the many ideas floated that evening was for a timeshare limousine service that customers could book using a mobile app. Camp, who was eager to move on to the next great thing, continued to develop the idea once he returned to San Francisco and acquired the domain name UberCab.com. The next step was to convince Kalanick to join the venture, and after his involvement in the company, Uber was launched in 2009.

The startup obtained its first significant funding, a $1.25 million round headed by Inaugural Round Capital, after beginning in 2009 and launching its first ride in 2010. 2011 was a significant year for the expansion of Uber. The business expanded to New York, Seattle, Boston, Chicago, and Washington, D.C. early in the year after raising an $11 million Series A fundraising round headed by Benchmark. It also opened an office in Paris. In the second series of the fundraising, the company was able to raise $37 million where the funds were from key investors Menlo Ventures, Jeff Bezos, and Goldman Sachs. The business expanded its selection in 2012 when it introduced UberX, which offered a less-priced hybrid automobile as a substitute for a black car service. After its investment rounds, Uber became globally the highest valued startup at $51 billion as of July 2015. Uber then received an additional $3.5 billion from Saudi Arabia's national wealth fund in June 2016.

Uber is associated with numerous acquaintances where they have a program for food delivery under uber eats. This is cooperation with a credit card and Uberpool in the merchant delivery program. Uber and GV announced on July 9th, 2018 that they would be investing in the electric scooter rental business line (GOOG) and later with Uber self-driving cars. The company is associated with various challenges in terms of its policy like its surge of pricing where Uber algorithms are involved in raising prices based on the demand and supply in the market. Paying drivers' benefits based on pretax earnings rather than after-tax earnings, and other cases of discrimination and high competition from the rival Lyft. The company has experienced a wild ride with annual revenues of over $11 billion, a market capitalization rate of $74 billion, over 19,000 workers, and various corporate controversies. The company has undergone a transition in the last three years with the greatest change being during the pandemic when the company was involved in laying off more than 400 drivers. This is in addition to the security issues facing the company from cybercrime.

1.2 Statement of the Problem

On 13th September 2022, Uber discovered a compromise in its computer network. This resulted in the company's locking up several systems, while assessing the severity of the data breach. Uber informed its employees about the attack, which occurred after the company's Slack staff messaging app was hacked (Conger, & Roose, 2022). The publishing of an explicit image on an internal company information page suggested the hacker had access to other internal systems causing the company to shut down the slack system (Milmo, 2022). Similar issues are associated with Uber, where in the past, the business has been hacked. Joseph Sullivan, the company's former chief security officer, is currently facing charges that he conspired to pay $100,000 to hackers to conceal a 2016 attack that resulted in the theft of the personal data of around 57 million users and drivers.

After Uber was hacked, the company came up with strategies to mitigate the losses in the company. Uber identified, among other issues, employee accounts that were impacted, and either their access was disabled, or a password change was enforced. For several affected tools, keys on internal systems were changes, thus resetting access (Uber Team, 2022). Restricted access to the source to stop further code additions. The user was also involved in the process where they were required to re-authenticate to regain access to internal tools. Additionally, to prevent the occurrence of a similar case the company was involved in enhancing our multi-factor authentication (MFA) guidelines while increasing internal environment monitoring to keep a closer check on any new questionable behavior. Technology was crucial in enabling the company to track software and servers that were hacked allowing them to take control of the system.

1.3 Addressing the Problem

Since being hacked, Uber has made their top priority to keep their databases safe for the interest of the company and its customers. The rideshare platform has a host of drivers and riders on a global scale! To put it into perspective the last hack affected nearly 40 million people. The data breach included personal and private information of users. The company deployed multi-factor authentication guidelines in an attempt to elevate data security and protect against future data compromise.

Besides ensuring data security, compromised accounts were either blocked or identified as an account that required a password reset. Employees were required to re-authenticate when refreshing internal tools to ensure no one has unauthorized access. Most importantly, the company integrated a more detail-oriented process for internal monitoring to prevent suspicious activity.

Although being hacked is never good news, the company used this as an opportunity to research the cause and how to prevent it going forward. Several digital forensic firms were hired to investigate how the attackers were able to hack their systems. Investing the money to strengthen their policies, practices, and technology shows the company takes pride and values its customers.

As a precaution the company also takes down some of the software tools when the app has been threatened or potentially compromised. These preventive steps have grown from the last hack in 2017 when the company attempted to pay the hackers off. To strengthen the MFA security the company could implement security keys which would make it more difficult for hackers to intercept the two-step authenticator.

2. Description of the Case Study

A social engineering attack is a series of malicious activities through human interaction, in other words, tricking a person into divulging security details to break a security breach (Mackay, 2022) If the mathematical formula of an encryption algorithm is cracked the key to the randomly generated binary number added to the algorithm is a huge challenge that will take millions of years to crack. Cracking encryption algorithms is not an easy process; hence social engineering attacks are often the preferred method of hackers.

On September 15, 2022, Uber Technologies Inc suffered a network breach that forced a shutoff many engineering and messaging systems (Robb, 2022) The company disclosed that the hacker “Lapsus$” compromised an employee’s Slack account, a messaging app that enables access to the information they seek and allows everyone within an organization access to the same shared and searchable information via the web site slack.com.

The teenage hacker confessed that they stole the password on an employee, and deceived them broke into approving the attacker’s push notification for Uber’s multi-factor authentication, or MFA. This was how they attacked Uber’s systems. (Whittaker, 2022).

Multi-Factor Authentication calls for at least two types of authentications for verification of users. According to the hackers, Uber was using Push authentication, where users responded by verifying their identities from their mobile devices. The targeted employee continued to receive push notifications until the hackers eventually contacted them via WhatsApp in the name of an Uber employee in the IT department, saying they needed to accept the authentication request. The employee accepted the request, and the hacker added their device. (Winder, 2022)

This is a prime example of a data breach through the means of social engineering. It wasn't until after the damage was done that the employee realized he was a victim of cybersecurity, and most likely they still didn't know it was their execution that led to the breach until contacted internally by Uber. The human factor is the biggest contributor to data breaches, unfortunately, most employees' only interaction with the term is once a year during annual compliance training if even at that time. In general, employees consider cybersecurity to be a problem for IT and above their pay grade and knowledge base (*7 reasons why*, 2024).

October is Cybersecurity Awareness Month highlighting the importance of cybersecurity, but should it stop there? Some employees have clicked on a test phishing email following an annual compliance training. Several companies have suffered a network compromise, despite the use of multi-factor authentication. Each day, employees exemplify they are well equipped in the day-to-day task of their job requirements, along with other attributes making them the greatest asset of any company, however, surveys reveal they are also the weakest link in the data security chain. According to a report published by Knowbe4, nearly 25 percent of employees at cybersecurity-conscious companies from diverse industries such as healthcare, finance, and technology, believe suspicious links pose no threat at all. (Worrall, 2022)

Annual meetings are just not enough anymore. Employees need constant reminders to prioritize data security in their day-to-day activities. If they were trained more frequently, they would absorb more information (Page, 2016).

3. Solution

3.1 Strategy for Change

While investigation is still ongoing, Uber ensures the security monitoring is enhancing its ability to support Android and IOS interfaces. Internally the company has identified any employee accounts that have been compromised, or at risk of being compromised or any defeats with network access. Which leads Security to be able to respond quickly by locking down the database and preventing new code changes from being created. This can help by preventing potential allies of the current hacker Joe Sullivan. Since the company had previously had a two-step authentication process the company had decided to restore the access to internal tools which will cause all internal employees to conduct a two-factor authentication process after resetting their access. This will consistently be monitored by the company's internal environment so they can seek out any unfamiliar activity in their operating systems. Uber is taking the necessary steps to undertake and find solutions to prevent another attack.

3.2 Role of Technology

Technology was the backbone of the company which in this case became its biggest weakness regarding the cyber-attack as evidenced in Figure 1. The hacker was able to navigate and understand the interfaces and applications in the security department. Since Uber owns and operates a mobile platform that allows the riders to connect with the nearest Uber riders using their mobile phones. There are personally identifying data such as names, email addresses, and phone numbers. The company even has the payment information of the Uber riders. The payment information that had been compromised is being monitored to support both applications by providing a cashless system. Customers can use a debit card or credit card or use a promotion code. The Payment Card Industry Data Security Standard is important to comply with. Uber chose to partner with Braintree. Data collected from the drivers include license, licensing authority, and vehicle registration information. Other information collected by Uber consists of the geographical data for both riders and drivers in real-time (Chatterjee et al., 2019). The company must also be in compliance with the NIST 800-171 – Federal Requirements for Controlled Unclassified Information. The National Institute of Standards and Technology (NIST) published NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, in June of 2015. As a part of the NIST 800 Series, SP 800-171 is one of many government publications setting policies, procedures, and guidelines for computer security. Even though people's information was compromised, and trust was broken within the company overall Uber has done its best to solve this issue (Figure 1. Uber's IT Network).

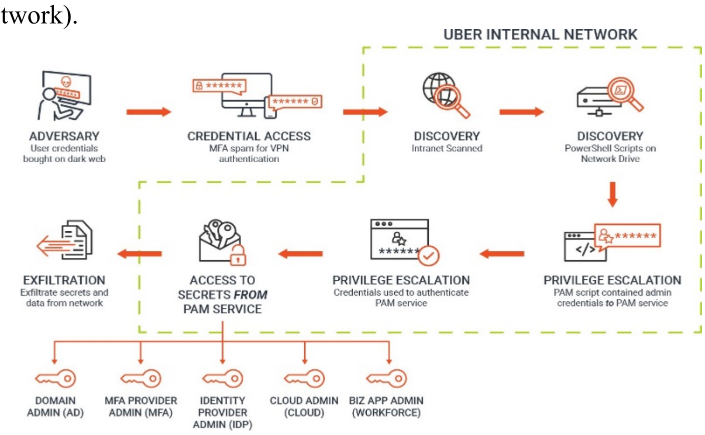
UBER INTERNAL NETWORK
ADVERSARY
User credentials bought on dark web
CREDENTIAL ACCESS
MFA spam for VPN authentication
DISCOVERY
Intranet Scanned
DISCOVERY
PowerShell Scripts on Network Drive
PRIVILEGE ESCALATION
PAM script contained admin credentials to PAM service
PRIVILEGE ESCALATION
Credentials used to authenticate PAM service
ACCESS TO SECRETS FROM PAM SERVICE
EXFILTRATION
Exfiltrate secrets and data from network
DOMAIN ADMIN (AD)
MFA PROVIDER ADMIN (MFA)
IDENTITY PROVIDER ADMIN (IDP)
CLOUD ADMIN (CLOUD)
BIZ APP ADMIN (WORKFORCE)

Figure 1 *How Data Breach Occurred in Uber's IT Network*
Source: *Major Cyber-Attacks in Review: September 2022*

3.3 Implementation

While there are many reasons why companies may fail to report such breach, such as regulatory oversight, company reputation at stake, and expenses, there are worse consequences than executives must be aware of when they fail to report such a breach due to lack of knowledge of knowing how to suspect unusual activity (Nandaniya, 2024). The company's iOS application messages are powered by the Twilio telecommunications provider. Uber is indeed required to implement push notifications using Apple's "Push Notifications Service". For the Android app Uber is using Google Cloud Messaging (GCM). The notification and the disclosure are recommended to all companies that might have experienced a cyber-attack. The decision to either disclose must be weighed carefully while considering the effects on consumer expectations, industry cyber security regulations and the company reputation. These facts come ahead of the company's reputation. It's been advised that Uber must also have an experienced legal counsel that would help determine whether a breach occurred and how the breach can be disclosed without harming the corporation's reputation. Uber plans to keep the user and suppliers safe and informed with the updates on the ongoing investigation.

3.4 Lessons Learned

Many are unaware that this is not Uber's first rodeo as it relates to a Cybersecurity attack. Uber experienced its first attack in 2016, and was kept a secret up until 1 year ago. Considering this is their second time being targeted, a few changes are now being put in place in order to mitigate future attacks. One task being, taking a second look at the system's multi-factor authentication. Uber was using MFA, which more than half companies do, but the system failed when the attack happened. Needless to say, the program was ineffective. Secondly, it's important for Uber to understand their organization's risk factors. Questions that Uber should ask themselves as a company are: What are the company's vulnerabilities? If a breach is broken, how much would it cost the company? In the future, Uber should create a roadmap and fill in missing mitigation components to better gauge effective and non-effective metrics. Cyberattacks will continue to happen especially to organizations that are not well equipped and protected. The best way Uber can handle these types of situations is by executive level buy-in. This can minimize the attacks from happening in the future.

3.5 Outcomes

Phishing attacks have proven to be detrimental to both a company and its customers. Companies and their networks are at a constant risk of being targeted and the only way to minimize the risk is to raise awareness. There has been an increase in courses and training on preventing such attacks. Informing employees on the signs that would indicate an attack could lower the chances of one being successful. Uber also has features where employees have to do a face scan to verify their identity before being granted the access of the platform. In addition, the use of MFA has also been a contributing factor to lower success rates of hackers. Like any other company, Uber's database is vulnerable to being hack, but overall, there has been a good protection of sensitive information over the lifespan of the business.

4. Conclusion

In conclusion, a jury in U.S federal court pronounced former Uber security chief Joe Sullivan as "guilty". The charge was failure to disclose a breach of Uber customers and driver data to the Federal Trade Commission. In view of the foregoing discussion, it is evident that Uber will be taking new preventive measures to protect their assets and avoid future attacks. Though many businesses experience trial and error, experience will serve as a major lesson to Uber in hopes that changes will happen soon rather than later considering this was not the first attack faced by the company. In their best efforts in keeping the business assets safe and cyberattack free, they should now invest in executive level buy-ins, compare and contrast qualitative metrics, and create a pros and cons list for what has happened in the past and revise it to create a better future.

5. References

1. 7 reasons why security awareness training is important (2024, October 15). Retrieved on November 15, 2024, from https://www.cybsafe.com/community/blog/7-reasons-why-security-awareness-training-is-important/
2. Blystone, D. (2022, October 23). The story of uber. Investopedia. Retrieved October 25, 2022, from https://www.investopedia.com/articles/personal-finance/111015/story-uber.asp
3. Chatterjee, S., X. Gao, S. Sarkar, and C. Osmanoğlu. (2019). Reacting to the scope of a data breach: The differential role of fear and anger. Journal of Business Research: Elsevier.
4. Conger, K., & Roose, K. (2022, September 16). Uber investigating breach of its computer systems. The New York Times. Retrieved October 25, 2022, from https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.htmlxx
5. Konger, Kate (2022, September 15) Uber Investigating Breach of Its Computer Systems https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html
6. Kurth, A. (2022, October 6). Former Uber Security Chief Found Guilty in Criminal Trial for Failure to Disclose Breach to FTC. Hunton Blog. Accessed on November 15, 2024 from https://www.huntonak.com/privacy-and-information-security-law/former-uber-security-chief-found-guilty-in-criminal-trial-for-failure-to-disclose-breach-to-ftc
7. MacKay, J. (2022, October 15). 5 Examples of Social Engineering Attacks. MetaCompliance. https://www.metacompliance.com/blog/phishing-and-ransomware/5-examples-of-social-engineering-attacks
8. Mackenzie, Jackson (2022, September 16) Uber Breach 2022 – Everything You Need to Know https://blog.gitguardian.com/uber-breach-2022/
9. Major cyber attacks in review: September 2022. SOCRadar® Cyber Intelligence Inc. (2024, February 14). https://socradar.io/major-cyber-attacks-in-review-september-2022/
10. Milmo, D. (2022, September 16). Uber responding to 'cybersecurity incident' after Hack. The Guardian. Retrieved October 25, 2022, from https://www.theguardian.com/technology/2022/sep/15/uber-computer-network-hack-report
11. Nandaniya, H. (2024, October). How To Build an App Like Uber - Step-by-Step Guide. Maruti Techlabs. Accessed on November 15, 2024, from https://marutitech.com/build-an-app-like-uber/
12. Page, D. (2016, August 30). Employee Cyber Security Training: What You Should Do. SecurityMetrics. Retrieved on November 15, 2024, from https://www.securitymetrics.com/blog/employee-data-security-training-what-you-should-do
13. Robb, B. (2022, October 3). The State of Ransomware in 2022. BlackFog. Retrieved October 23, 2022, from https://www.blackfog.com/the-state-of-ransomware-in-2022/
14. Uber Team. (2022, September 19). Security update. Uber Newsroom. Retrieved October 25, 2022, from https://www.uber.com/newsroom/security-update/

15. Whittaker, Z. (2022, September 19). How do you stop another Uber hack? TechCrunch. Retrieved November 15, 2024, from https://techcrunch.com/2022/09/19/how-to-fix-another-uber-breach/
16. Winder, D. (2022, September 18). Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door to Hacker? Forbes. Retrieved October 23, 2022, from https://www.forbes.com/sites/daveywinder/2022/09/18/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/?sh=6e1d516d6056
17. Worrall, W. (2022, January 4). Lack of Employee Awareness of Cybersecurity Is a Catastrophe Waiting to Happen. Hacked.com. https://hacked.com/lack-of-employee-awareness-of-cybersecurity-is-a-catastrophe-waiting-to-happen/
18. Uber. (2024). Accessed on November 15, 2024, from https://www.uber.com/newsroom/history/