WESTERN SYDNEY
UNIVERSITY

01005- PPC

Assignment on Ethics and Codes of conduct Report

Name: Quoc Lap Trieu

Student ID: 19263045

Contents

DATA BREACH IN ETHICAL CODE OF CONDUCTS

ABSTRACT

As the growth of the business, every member of the company in the workplace plays a vital role in its success. There needs to have a set of rules in order to reflect the behaviors of every person in an organization. By following these rules, it could make sure the development, as well as the benefit, are on the right track. Code of conducts and ethics are the rules that every large size business considers as a policy that needs to follow to achieve their success in the marketplace. This report discusses several case studies relating security data breach issue in different companies. The report analyzes each case in order to find out the issue in breaching the code of conducts of each company according to their codes. The author also compares these case studies together so as to give the conclusion of the report.

INTRODUCTION

Code of conducts and ethics are used to advise the direction of behaviors in a company which benefits the success of the organization. Ethics are used to influence the decision of employees in the company while conducts are used as rules of prohibiting specific actions that are considered inappropriate of employees. The ethical code of conducts that are related to security area is considered as an important code for every IT company since it contains detail information about the privacy of the user. In the other words, what each company should do to their user' personal information, what information they should collect from them and who they should share it with are the essential questions that each company need to answer in their code of conducts as it could affect greatly from the trust of their users.

In this report, I will discuss four case studies related to security area from different companies. The report will focus on the problem of breaching the code of conducts in different situations of the companies. Each case study describes the reasons and weaknesses in company security that lead to the serious problem of leaking a large amount of user data by hackers on the internet and its serious consequences. The first case study is about Yahoo, a large company supporting different services and also the victim of the largest data breach in history. On the second case, I discuss eBay, a popular e-commerce corporation that helps users connect each other by selling and buying products on its online website. On the third case, it is about Uber, a transportation network service. Finally, the case of a data breach of Heartland Payment Systems, an organization that helps customers to simplify the process of payment.

DATA BREACH

1. Yahoo – The biggest data breach in history

Yahoo is an application that comprises different tools including search engine, map, mail, news and plenty of web services to support users on the internet (Rouse, 2005). Each user needs to register an account from the application itself in order to fully utilize its services. For example, with an email account from Yahoo, users can fully access the Yahoo Answer web application to create or answer questions. Due to its powerful and useful services, Yahoo contains a large number of users as well as their information in different countries. It is also the main reason for being the target of hackers on the internet.

In 2016, according to (Armerding, 2018), Yahoo announced that it had been hacked and 500 million of user accounts including real names, telephone numbers, dates of birth, and email addresses had been leaked in 2014. The company also said that a large number of passwords had been hashed by using a strong algorithm for encryption in order to assure its users. However, a few months later, it had been revealed that 1 billion accounts had been stolen in the year of 2013.

The stolen data this time includes encrypted passwords with the only MD5 algorithm as well as questions and answers for security authentication. In fact, MD5 is a hashing algorithm that accepts any length as input and returns a fixed-length value which is used for authenticating original data. It is also important to note that MD5 hashing is no longer considered as a reliable method for encrypting sensitive data since there exist techniques that are capable of easily generating MD5. Therefore, stolen passwords which are encrypted by MD5 in the database could be easily decrypted by hackers and use for different purposes.

After estimating the total number of stolen accounts, Yahoo declared with the number of 3 billion Yahoo accounts at the end of 2017. It could be said that Yahoo breaks the record for the largest data breach in history with 3 billion user accounts including all their sensitive information in the database system (Interset, 2016).

As it could be seen that the attack occurred in 2014 but until two years later in 2016 that everyone could know the truth. The article (Interset, 2016) said that there is strong evidence that Yahoo knew the attack long before that but they keep hiding it. In fact, the company could warn their users to take action by changing their password in order to protect their sensitive data from being stolen by hackers, the company did nothing about it. This kind of action makes me think about one of the codes in the code of ethics from Yahoo Company, the Conflict of Interest. According to (Office, 2011), they state that every one of them must consider their efforts are not affected by the conflicts of interest in order to make sure the success of the company. In other words, they must be careful in their decision so that their decision would not be influent by their personal interests. In this case, the article (Interset, 2016) indicates that the company intentionally conceal the incident of attack from users without considering the importance of user's personal information, they only think about their interest first. It is opposite with what they declare in the code of ethics.

Besides, in (Office, 2011), Yahoo also states that the customers trust them to protect their private information and the company could use it according to their published policy. Users also are able to know what the services would collect and the way it would be used. Besides, the

company also assure the users that they would take measures to protect their personal information. They would not share the user's data with the other parties. However, not only billions of Yahoo accounts containing important data of users being stolen, the company also tried to conceive it from the public. That action could be considered as breaching the code of ethics from protecting user privacy.

2. EBay's Data Attack

eBay is one of the most popular multinational e-commerce corporations that connect users around the world together by the process of buying and selling products on their marketplace (HSIAO, 2017). On the one hand, the sellers can establish their store and organize their products for sale, on the other hand, the buyers can search for their interesting products and purchase them. With the purpose of supporting their customers, the application support for the different platforms including web application for desktop, a mobile application for mobile devices and even application programming interface (API) for third-party applications. In order to use the services on eBay, the user needs to create an account including important information such as name, credit card number, telephone number and so on. After establishing the account and filling necessary detail information, the user can start selling their products or buying ones they like. Due to the popularity of eBay, there are more than 170 million active users from the statistic of (Statista, 2018).

The company reported an attack occurring in the middle of the year of 2014 that exposed sensitive information of 145 million of user accounts including their names, dates of birth, addresses, and encrypted password. Fortunately, eBay said that financial information such as credit card numbers of users was still safe due to its database structure for storing in separate locations. The company also advised customers to change their password in order to protect their accounts from hackers.

However, according to (Pagliery, 2014), one of the most important thing about this attack is that the company did not email their customers to change their password even it had been more than 24 hours since the company reveals the attack. Even though the company always sends plenty of emails to their customer to advise them to buy different kinds of products, they did not send a single email to inform customers to change their password. From the code of ethics of eBay from (eBay, 2015), one of the codes about their responsibility state that it is important to always make the right decisions when dealing with ethical and legal issues. From their action of delaying notifying users to change their password, it is totally opposite to their code of ethics. They did not consider the importance of their customers. Besides, it is also criticized for its poor implementation in the process of renewing passwords.

It is also important to discuss the method of attacking. According to the suggestion of (Cawley, 2014), the employees of eBay had been deceived by the phishing attack from hackers. As described in (Fruhlinger, 2017), It is a kind of hacking method for stealing user data, it could be username and password or credit card numbers. It occurs when a person sends an opening an email, text message or instant message to the victim. The message contains a malicious link that deceives the recipient to click it, which can lead to the installation of malware that could free the system or steal important information from the victims. In the case of eBay employees, they could receive an email to inform them to log in and change their password. From the action of authenticating from employees in eBay, the hackers could easily obtain username and

password from their account. As a result, the hackers had successfully accessed the three employees account of eBay for 229 days and obtain user database (Armerding, 2018).

Another important point in the code of ethics of eBay is that they consider protecting the privacy of the customers is one major reason their customers trust them. They also state that they will keep the sensitive information of customers safe and use it only for legitimate business purposes, and always follow the privacy policy of the company. They will never share user's information with a third party. However, because of the attack, 145 million of user accounts had been stolen and being used for different purposes. It could be seen that the company could not follow the privacy code about protecting their user data.

3. Uber – Network Transportation

Uber is a company relating transportation network comprising ridesharing and food delivery services. The company contained more than 40 million monthly active users around the world in 2017 from (Quora, 2017). The application targets two types of user, the first type is the one who wants to earn money by using the application while the second type is the one who needs to use the service from the application and pay the money for the first type of users. In the other words, the first type of user is riders and deliverer, the second one is customers. Each user needs to have an account in order to use the application. The account could include much important information such as name, email address, date of birth, telephone number, and vehicle number plate. This information is very sensitive to users as it could be used for different purposes that could cause them trouble. Because of that, Uber is also one the targets for the data attack from hackers.

From (Armerding, 2018), In the late of 2016, the company discovered that 57 million of user accounts including telephone numbers, email addresses, and the name of users were exposed by two hackers. Besides the accounts, there were also 600 thousand of driver license numbers of users being exposed. Fortunately, the important data about credit card numbers, trip locations and numbers of social security were still safe.

The main reason for this attack is due to carelessness of Uber programmers (Ducklin, 2017). During the development process of the application, the developers of the company uploaded their username and password credentials to a GitHub repository. It is important to note that GitHub should a place that developers use to store the application source code for hosting and reviewing each other code and not the security credentials. Because of this action of developers, millions of user accounts had been stolen by hackers, affecting not only user members of Uber but also the company itself. Uber decided to fire the programmers uploading security credentials to the repository. However, what's worse is that the company actually hiding this fact from the users for nearly a year from the time of the attack. In fact, they actually paid 100 thousand dollars to the hackers in order to ask them deleting the data they stole without even knowing that whether the data were actually destroyed or not (Ducklin, 2017). They consider that money as the fee for finding the bug of the application.

According to their code of conducts about Privacy of Data Collection and Uses in (UBER, 2017), Uber states that they collect information from users and use it help improve the reliability and convenience of delivery and network transportation services. Besides, they want to use the collected information to:

- To improve the services relating to security and safety of users.
- To support users
- For research and development
- To connect users together
- To provide promotions or contests
- For legal proceedings

More importantly, Uber declares clearly that it does not share or sell the personal information of users to the other party.

It could be seen that the action of hiding from users and paying the hackers the money to keep the secret is equivalent to the action of sharing sensitive data of users to the others. What if the hackers did not delete the data they got from Uber and they continued to use it for different purposes such as selling data to the other parties. This kind of action from Uber is opposite to the code of conducts they create. Moreover, in the conducts, the company wants to keep the trust from users, but by hiding the fact that their important data had been stolen by hackers, how they could be able to gain trust from their users. It is just like if you do not care about your user's information, how they continue to trust you.

4. Heartland Payment Systems

Heartland Payment Systems is a provider of technology and process of payment. They provide different services for all sizes of business with the purpose of simplifying the process for their customer. The company contains a large number of credit cards due to the number of transaction per month. In January 2009, it was estimated that there were 100 million transactions in a month for 175 thousand merchants at that time. It was also the time for the data attack from hackers. There were 134 million credit cards that were exposed during the attack. The company was considered as a victim of one of the largest data breach attack in the US (SECUREWORKS, 2012).

According to (SECUREWORKS, 2012), the data breach method is a SQL injection attack on the website of the company in the early of 2018. About several months later, in the middle of May 2008, the malware from the SQL injection transfer from the corporate network to a network of payment processing and the important thing is that Heartland Payment Systems had no idea about this. In the late of October 2008, HPS found out the issue based on the notification from by one of the major card brands, Visa and MasterCard. The company tried to hire many experts to analyze their IT security network but all of them declared that the system did not contain any malware. Until the January of 2009, HPS staff found the malware. As a result, the company had to suffer a loss of $170 million, only 20 million dollars was covered by the insurance.

The main method for the attack is through SQL injection on the website of the company. This technique is one of the most common web hacking techniques that is used to cause damage to the database system by placing malicious code in SQL statements with the purpose of using that code to retrieve data from the system (Rouse, 2010). However, at the time of the attack that happened, SQL injection was well recognized as one of the popular methods for hacking data, even many security experts had warned about the vulnerability of this technique for serval years in order to help many web applications deal with it. There were even existing solutions that were easy to implement to prevent the SQL injection. Due to the carelessness in the implementation of the web application, 134 million credit cards had been stolen by hackers and its

consequences could not be estimated totally. According to the code of business conducts and ethics of Heartland Payment Systems from (Wesley Fredericks, 2013), the company claims that they would build the quality products and services for the customers but their developers could not deal with a common attack from SQL injection. Moreover, one of the most important rules in the code of ethics from the company state that they will protect all proprietary data of the customers or suppliers give to them according to their agreements, so did they protect it successfully?

The answer is a no, they could not protect it and even let their customer's data being stolen by hackers without realizing it. Until the January of 2009 when the company was notified by Visa and MasterCard from detecting suspicious transactions of the accounts (Armerding, 2018). The credential data being stolen by using the simple but common technique in web hacking is the failure of the company, but another serious failure of the Heartland Payment System is that they could not realize that their data had been exposed by the hackers until being notified by the third parties. How serious could it be if they did not even realize the attack coming from their websites? How many credit card could have been stolen without knowing? As a result, the company had to pay around 145 million dollars in compensation for the loss in payments.

5. Comparison

It could be seen that it is the same for the three company Yahoo, Uber and eBay. Even though each of the company uses different methods to handle the incident of data attack, at the end they always tried to conceive the event from the public for their own interest. Yahoo did not reveal the truth for several months even though the data had been stolen for two years. They also use the reason for investigating to delay the process. Uber Company instead paid the money for hackers to delete the data and conceive the attack for nearly a year without informing users to change their passwords, and eBay did not even send a single email to their customers to inform them to reset password even though it had been more than 24 hours since the company revealed the attack. In the case of Heartland Payment Systems, it is very dangerous that due to the poor implementation of the system, they could not detect the malware casing by SQL injection technique for more than a year. This issue made them suffer a huge loss in the marketplace.

From my point of view, in four case studies, the case of Uber is the one that needs to consider carefully. It could be seen that the problem of the four case studies is the same about data breach attack. However, the main point I want to mention here is that how each company handles the problem according to their ethical code of ethics. In Uber case, it is a serious problem that they know how dangerous it would be when their user's data were stolen but they keep hiding the truth and even paid the hackers 100 thousand dollars to delete the data. In fact, they actually did not know what would happen to the data and they even did not care what would happen to their customers if the information were exposed to the third parties for bad purposes.

CONCLUSION

In the end, every company should learn mistakes from the events in the past in order to avoid an unnecessary incident that could cause a breach of an ethical code in conducts of the company. They should understand the importance of following the code of conducts. It is used to guild every member of the organization in the right direction and help them make the correct decision which benefits businesses of the organization.

BIBLIOGRAPHY

Armerding, T., 2018. *The 17 biggest data breaches of the 21st century.* [Online]
Available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
[Accessed 02 MAY 2018].

Cawley, C., 2014. *The eBay Data Breach: What You Need To Know.* [Online]
Available at: https://www.makeuseof.com/tag/ebay-data-breach-need-know/
[Accessed 03 MAY 2018].

Ducklin, P., 2017. *Uber suffered massive data breach, then paid hackers to keep quiet.* [Online]
Available at: https://nakedsecurity.sophos.com/2017/11/22/uber-suffered-massive-data-breach-then-paid-hackers-to-keep-quiet/
[Accessed 02 MAY 2018].

eBay, 2015. *CODE OF BUSINESS CONDUCT & ETHICS.* [Online]
Available at: https://www.ebayinc.com/assets/Uploads/eBay-CodeofEthics-external-080615.pdf
[Accessed 03 MAY 2018].

Fruhlinger, J., 2017. *What is phishing? How this cyber attack works and how to prevent it.* [Online]
Available at: https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
[Accessed 03 MAY 2018].

HSIAO, A., 2017. *What is eBay?.* [Online]
Available at: https://www.thebalancesmb.com/what-is-ebay-1140195
[Accessed 02 MAY 2018].

Interset, 2016. *THE COMPLICATED ETHICS OF DATA-BREACH DISCLOSURE.* [Online]
Available at: https://interset.com/2016/10/06/the-complicated-ethics-of-data-breach-disclosure/
[Accessed 02 MAY 2018].

Office, Y. E. a. C., 2011. *Yahoo.* [Online]
Available at: http://files.shareholder.com/downloads/YHOO/660619262x0x239565/4f32ddd0-82e5-47c2-ac71-75403ebbb404/YahooCodeOfEthics_Ext_1008.pdf
[Accessed 04 MAY 2018].

Pagliery, J., 2014. *eBay hasn't emailed all customers about the attack.* [Online]
Available at: http://money.cnn.com/2014/05/22/technology/security/ebay-hack-email/index.html
[Accessed 03 MAY 2018].

Quora, 2017. *Has Uber's Ridership Been Impacted By Its Various Scandals?.* [Online]
Available at: https://www.forbes.com/sites/quora/2017/04/03/has-ubers-ridership-been-impacted-by-its-various-scandals/#6d77eb2c2dee
[Accessed 02 MAY 2018].

Rouse, M., 2005. *Yahoo.* [Online]
Available at: https://whatis.techtarget.com/definition/Yahoo
[Accessed 01 05 2018].

Rouse, M., 2010. *SQL injection.* [Online]
Available at: https://searchsoftwarequality.techtarget.com/definition/SQL-injection
[Accessed 03 MAY 2018].

SECUREWORKS, 2012. *A Famous Data Security Breach & PCI Case Study: Four Years Later.* [Online]
Available at: https://www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland
[Accessed 03 MAY 2018].

Statista, 2018. *The Statistics Portal.* [Online]
Available at: https://www.statista.com/statistics/242235/number-of-ebays-total-active-users/
[Accessed 03 MAY 2018].

UBER, 2017. *UBER.* [Online]
Available at: https://privacy.uber.com/policy/
[Accessed 03 MAY 2018].

Wesley Fredericks, E., 2013. *CODE OF BUSINESS CONDUCT AND ETHICS for DIRECTORS, OFFICERS AND EMPLOYEES of HEARTLAND PAYMENT SYSTEMS, INC.* [Online]
Available at: http://corpdocs.msci.com/ethics/eth_108887.pdf
[Accessed 03 MAY 2018].