UNIVERSITYOF HERTFORDSHIRE

School of Engineering and Computer Science

Student name: Kola Dheeraj

SRN: 18021370

Impact of Data Breach on Brand Image and Employee Loyalty-A Case Study of Uber

Table of Contents

1. Introduction

Security breach or data breach has become one of the serious threats nowadays for multinational companies and also for SMEs (small and medium sized companies). In last few years, some big names around the world such as British Airways, Facebook, Coca Cola, Tesla and Google experienced data breach incidents that hampered their operations and brand image in various manners (Gressin 2017). It is obvious that such data breach exposes data of users or employees or both. However, the question is whether such data breach affects the organizations or not. Some companies lose their brand image however, is it all? Some scholars have argued that along with losing brand image business organizations also lose their employees' trust and loyalty along with trust of customers after such incidents. This report intends to research on two factors that are brand image and employee loyalty. This research intends to find out whether data breach or security breach can have severe negative impact on brand image or an organization by losing trust of the customers and can affect loyalty of the employees. For this purpose, the case study of Uber is selected here that was hit by a data breach in 2016 when both its customers' and employees' data were stolen. Besides, this research also will find out proper solutions and will provide policy recommendation to prevent occurring of such incidents in the near future.

1.1 Rationale

According to Janakiraman *et al*. (2018)), data breach can be defined as an event through which sensitive, protective and confidential data is stolen by an individual of group. In spite of the fact that regulations for example HIPAA and/or PCI Data Security Standards were developed to help companies to handle sensitive information, numbers of data breaches have increased year after year. For example, in 2019 a total of 7,098 data breach cases were seen through which 15.1

billion records were exposed or stolen (helpnetsecurity.com 2020). This was a growth of 1% than the year of 2018. It is anticipated that the number will grow in 2020. Therefore, it is the high time for the companies to properly realize how data breach can affect them; not only financially (through fines) but also through negative brand image and lack of employee loyalty. That is why; it was decided to continue with this topic.

On the other hand, the case of Uber is selected as during the data breach of 2016, not only customer data, but also employee (Uber drivers) data of the organization was also stolen. This case study will help to understand how such data breach can affect brand image of an organization (through negative customer loyalty) and employee loyalty.

1.2 Research Aim

The aim of this research is to identify how data breach can affect brand (through negative customer loyalty) and employee loyalty of an organization.

1.3 Research Objectives

- To identify the impact of data breach 2016 on customers of Uber
- To analyze the impact of data breach 2016 on employees of Uber
- To recommend solutions to prevent such data breach in the future

1.4 Research Questions

- How data breach in 2016 affected customer loyalty of Uber?
- How data breach of 2016 affected employee loyalty of Uber?
- How can Uber avoid such incidents in the future?

2. Background

In the year of 2016, Uber experienced a major data breach that exposed the data of 57million customers. On the other hand, this data breach also exposed data such as license numbers, of 600,000 Uber drivers (techcrunch.com 2017). As per The Guardian magazine, data of 3.7m drivers were stolen (Hern 2018). There were several arguments about whether Uber could get prevent this data breach by strengthening their network or not. However, the shocking thing was instead of reporting this incident to the regulators or the customers or the drivers, the organization paid $100 million to the hackers to delete the data (Hern 2018). After the incident, Bloomberg reported that CEI Kalanick was aware about the data breach from November 2016 however, he did not revealed it until the next month when it became public (Hern 2018). This situation occurred even after Uber tried to increase its security measures. Because of this data breach, European operation of Uber was fined £385,000 for this data breach. Later, it also paid additional $148m for not notifying its drivers about the data breach. Uber, after this data breach stated that it is working to improve to its data security to ensure avoidance of such situation in the future.

3. Research Methods

In order to conclude this research in a proper manner, this research will follow both primary and secondary data collection methods.

By following positivism philosophy, deductive research approach and mixed methods, though journals, articles and websites, it will collect secondary data about how Uber was affected due to this data breach. The focus will be on identifying how its customers and employees reacted after this data breach.

In terms of primary data, both qualitative and quantitative data will be collected. For collecting qualitative data, telephonic interviews will be organized with 4 managers of Uber who are serving the organization since 2016. In terms of collecting quantitative data, by following random sampling method, survey questionnaire will be shared with 200 customers of Uber. Those questionnaires will include close-ended questions and the main goal of those questions would be to find out how they think about Uber after the data breach. Further, to find out what the employees think about the organization after the data breach, a separate questionnaire will be developed that would also include close-ended questions. That questionnaire will be shared with 100 random Uber drivers.

Both the questionnaires will be shared through social media sites such as Facebook or through e-mails. The participants will be able to take part in the research only after completing the consent form. They will be given 48 hours of time to submit their responses.

References

Gressin, S., 2017. The equifax data breach: What to do. *Federal Trade Commission*, 8.

helpnetsecurity.com, 2020. *In 2019, A Total Of 7,098 Reported Breaches Exposed 15.1 Billion Records - Help Net Security*. [online] Help Net Security. Available at: <https://www.helpnetsecurity.com/2020/02/11/2019-reported-breaches/#:~:text=2019%20saw%20an%20increase%20in,2019%20incidents%20come%20to%20light.> [Accessed 7 September 2020].

Hern, A., 2018. *Uber Fined £385,000 For Data Breach Affecting Millions Of Passengers*. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked> [Accessed 7 September 2020].

Janakiraman, R., Lim, J.H. and Rishika, R., 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), pp.85-105.

techcrunch.com, 2017. *Techcrunch Is Now A Part Of Verizon Media*. [online] Techcrunch.com. Available at: <https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAL-R-URPZNhSs9M4pXfzm6Wb6daz14ZnqhvZSNYZ7Rmdexa_0SC9SyNbhFWEN6Q99eP-KimkYUBDgKFCukZbJ26GZNU4d873daj7lc6BnUcawPPL6xkccM3GZn75q-

_d7xKpTARTl6vGZwKbN9o4QRsScVE26AojdnCkAhQPMAs1> [Accessed 7 September 2020].