Z

by X Y

Submission date: 16-Apr-2023 02:26PM (UTC-0400)
Submission ID: 2066048926
File name: UKS31435.docx (33.81K)
Word count: 2794
Character count: 15163

RISK MANAGEMENT

Table of Contents

1.0 INTRODUCTION

The following assignment talks about the 2017 data breach which happened in EQUIFAX, one of USA's credit reporting companies that rate the fiscal status of almost everyone in the US. The breach paved the way for a lot of controversies which included EQUIFAX being blamed for their lack of security and notice. The report shall also outline the critical analysis on the holistic nature of risk management within organizations using qualitative and quantitative approaches. And how internal and external factors influence approaches to risk management and disaster planning.

1.1 BACKGROUND INFORMATION ON THE EQUIFAX CASE STUDY:

In the year 2017, in March a credit reporting company in the United States namely EQUIFAX was subject to a data breach and being a company monitoring the citizen's fiscal health, they had access to their sensitive details like usernames and passwords and were subsequently hacked and infiltrated. Such Infotech disasters are usually a result of numerous multi-level failures which also ends up highlighting numerous security slip ups. Initially, the breach happened due to a botched consumer complaint feature, as the hackers took advantage of that vulnerability and used the portal to hack into the system as it was the bug was initially fixed by Equifax like it should have been (equifax, 2023). The hackers successfully moved from just the portal to their other domains as the systems had poor cyber surety measures and they were able to pull out data without being noticed for months in an encrypted form as the company has basically failed to renew certain encryption certificates on a particular internal security tool. The company hid and did not expose the breach to the public until a month had passed after they came to know and this led to accusations of insider trading by the top officials.

1.2 PURPOSE OF THE REPORT

The purpose of the report is to study the case of Equifax during their 2017 data breach situation and produce a critical analysis of the above and on the holistic nature of risk management within top and important organizations, like, Equifax, who deal with sensitive citizen information using qualitative and quantitative methods and how internal and external factors influence the approaches to risk managements and disaster management.

2.0 LITERATURE REVIEW

According to the US National Institute of Standards and Technology, cybersecurity incident handling is defined as analysing incident related data and then determining the appropriate solutions to minimise the effects, including communication strategies needed for incident related info with respect for outsider parties like consumers, stakeholder, partners etc.As

demonstrated by studies on the impact of market valuations by Cavusoglu, Mishra, and Raghunathan (2004) and the study of Yahoo data breaches by Wang and Park (2017), public communication on cybersecurity incidents is crucial for handling the incident and managing any subsequent corporate crisis because of it direct relation with business reputation and execution. In a 2017 study by Wang and Park , they proposed a comprehensive communication model for the public for dealing with data breach situations like the one similar to Equifax and the Yahoo data breach. It contained essential strategies of communication of denial. Diminish, rebuild bolstering and timing.

2.1 OVERVIEW OF RISK MANAGEMENT

According to, "***Fruhlinger, 2023***", the concept of Risk Management has a few key factors, which includes , identification, assessing and analysing, and ultimately responding to the risk and reviewing the response later. Constructive Risk Management is acting in a proactive manner rather than a reactive way , in an effort to influence events that might come up in future and as a result this could diminish the likelihood of a potential risk coming up and endangering the organisation and their clients. In the case of Equifax they made assumptions about accepting a bigger risk would enable them to make more income and were fixated that this would be a good gamble for the company, however due to the massive data breach they lost their gamble completely.Unfortunately for Equifax the reason why they were subject to such a big data breach was because of a small rectifiable bug and the breach was avoidable only if they paid more attention to it and fixed it before it was taken advantage of.

2.2 TYPES OF RISKS

The term "risk" usually makes one hesitant and wary and immediately think about potential harm , however some risks can have a positive connotation too.

- Positive risk

Positive risk is a circumstance or event that will enable one to advance a project's goals and since they are favourable , one may promote it as they are advantageous. Enhancing the scope of the event occurring or its consequences is the reaction plan.

- Negative risk

As the name suggests a negative risk has the potential to harm or impact the project negatively and therefore one must identify and eliminate the impact or lessen its chance of happening.

- Issues

These are circumstances where a stakeholder of the project disagrees with something.

- Known Risks

Risks which one is aware of prior to it happening and take appropriate steps and measures to eliminate its effects.

- Unknown Risks

Usually these are risk which are unidentified and stays unknown until it actually takes place, and because of their unidentified status usually one has to come up with solutions to tackle it on spot

- Risk Tolerance

Low tolerance refers to a refusal to accept risks until the reward surpasses the danger, whereas high tolerance denotes a desire to do so.This refers to the sensitivity towards risks of the said organisation or stakeholders of an organisation/project.

- Risk Threshold

This refers to the amount of risk a certain organisation is able to accept and deal with,. It's also a next step into risk tolerance.

- Residual Risks

After the intended risk response has been put in place, these are those risks that an organisation anticipates that can occur.

- Secondary Risks

These are risks that can occur due to the implementation of a certain solution to an already indemnified risk.

- Risk Triggers

These can be classified as the warning signs which can indicate a risk is about to occur and utilized to alert the people in action.

2.3 RISK ATTITUDE AND RISK APPETITE

According to, "***Hillson and Murray-Webster, 2011***", everyone approaches RISK differently; some actively seek out risk, while others choose to avoid it and this depends on one's risk-taking attitude. Risk Attitudes are usually influenced by Perceptions, tolerances, and other biases.

Depending on their risk attitude, organisations and stakeholders determine how willing they are when it comes to accepting varying degrees of risk.

A company's risk appetite could be highlighted as high or low depending on how many chances it is prepared to take. If a company doesn't take many risks, its risk appetite is low. It basically means that the amount of risk an organisation or stakeholder is willing to take in exchange of any form of compensation.

2.4 BUSINESS CONTINUITY MANAGEMENT

Business continuity planning sets risk management practices and procedures that seek to prevent disruptions of mission-critical services and swiftly restore full operations to the organisation. It refers to the ability of an organisation to continue their essential functions at the period of and after a crisis takes place. According to, "***Gibb and Buchanan, 2006***", it is the ability to keep the basic functions running during said crisis and to be able to operate at its full capacity as fast as possible. A Business Continuity Plan takes various events which are unpredictable in nature into account, like, natural calamities, cyberattacks, pandemics and health outbreaks etc.

2.5 CRISIS MANAGEMENT

According to, "**Herbane *et al*. 2004**", it refers to handling a crisis in a way that limits harm and helps the impacted organisation to restore its operations into full effect swiftly. This also helps maintain Public Relations for an organisation which is very beneficiary .There are many different types of crises, hence it is advised that a corporation develop a crisis management strategy in advance.

- Accidental Disasters
- Natural Disasters
- Technology Disasters
- Conflict of Interest Crisis

3.0 THE CASE STUDY OF EQUIFAX

According to, "***Team, 2023***", a credit reporting firm in the United States, EQUIFAX, experienced a data breach in March of 2017. As a company that monitors the financial health of its customers, EQUIFAX had access to sensitive information including usernames and passwords which was under jeopardy as their systems were hacked and information was taken out in an encrypted mode for months before they could detect it which was a result of a vulnerability in their customer complain domain.

Apache Struts, an open source framework for developing corporate Java applications also used by Equifax had a vulnerability detected dubbed as the CVE-2017-5638. The Software foundation came out with a patch on 9th of March for the said vulnerability for any systems that may have been affected by the bug as Equifax was, but personnel at Equifax failed to do so. After forensic analysis , it was revealed that the breach on the web portal happened due to the Struts vulnerability but wasn't until May 13.2017, when Equifax reported a separate incident when the hackers actually started exfiltrating data and moving into other parts of the

network. Infotechs like Equifax are usually armed with softwares that can help in decrypting , analyze and then reversing it back so that they can detect any activities regarding infiltrations and these services usually require a certification which usually is a third party certification and is updated annually which helps in keeping their services afloat . However Equifax had failed to renew one of such certifications which basically meant these services weren't working for them at the time.

According to, "***corporatefinanceinstitute, 2023***", because Equifax deals with the personal information of the citizens including fiscal health ,the hackers were able to access just sensitive personal information without much hassle and around 143 million people were impacted by this,Names, Social Security Numbers, Residence addresses , date of birth etc were all in jeopardy. Around 200,000 of the affected also had their credit card info saved with the company which used it to check their own credit report.

4.0 BUSINESS CONTINUITY MANAGEMENT AND CRISIS MANAGEMENT BY EQUIFAX

According to, "***Harmer, 2023***", Equifax publicly disclosed a significant data breach on September 7, 2017, announcing it impacted 143 million US individuals (nearly half the country's population initially but later when the dust settled they disclosed 146.6 million Americans, almost 15 million Britons, and 19,000 Canadians had been affected. Equifax had the luxury of arranging its own announcement since it had discreetly spent six weeks looking into its incident.

- They conducted an apparently stellar press release.
- They hired cyberlawyers from the law-firm King and Spalding LLP
- They had the incident reported to the FBI.
- The consumers could check if they were affected by the breach or not and could apply to the remedial package.
- They set up call centres to also help the affected. Which basically meant training thousands of people in customer service in just 2 weeks.
- The company created a "robust package of remedial materials," according to Smith, that included "(1) consumer credit files being monitored throughout the trio of bureaus, (2)the accessibility to the Equifax files of credit , (3) the capability to lock the file, (4) insurance to take care of the identity thefts that might have occurred and (5) scans on the dark web for social security numbers

According to, "***Sullivan and Crocetti, 2023***", on paper everything was fine, but in reality, it all went south. Equifax was looking at more than 240 lawsuits by the affected, which were brought by the institutions of finance and stockholders, in 2 months of the breach. They published that they were working with the governments of all levels containing the international ones in order to seek information. This also included the District of Columbia and Puerto rico , FTC, CFPB, SEC etc.

When Equifax published its first-quarter 2018 report, the business had already invested $242.7 million in the incident. A settlement between Equifax and the FTC, the CFPB, and 50 U.S. states and territories was reached in July 2019, and it included payments of up to $700 million.

5.0 ANALYSIS OF THE EQUIFAX CASE STUDY

The March 2017 data breach of Equifax , was a result of negligence due to which sensitive data of millions of citizens were leaked and the company faced a number of lawsuits. This crisis could have been averted if the patches by the Apache were applied on time and their certificates were renewed timely. Even after 2 years the incident took place , the company ended up spending around 1.4 million USD in transforming their infrastructure and network with improved network and security. In 2019 there was a decline in the company's credit rating and the company as a result has to invest even more on infosec. The FTC and Equifax also settled a deal in 2019, July which made the company liable to pay almost upto 1.38 billion USD to address the consumer claims which would come as a result of that deal

6.0 CONCLUSION

Despite breaches occurring, over $75 billion was spent globally on security goods and services in 2017. If one doesn't take the time to learn about the dangers associated with operating systems that handle vast volumes of delicate customer data they can be vulnerable. Organisations have been reducing the usage of sensible security practices (such testing, deploying, and monitoring) for far too long because they think doing so will reduce their income by prioritising revenue over customer security.Due to the length of time before notification, both the integrity of Equifax as a company and its leadership team were instantly questioned..Los Angeles Times wrote about Equifax being irresponsible by not revealing data about the data breach and potentially jeopardising the customers sensitive details and waited for 6 more weeks to disclose making them even more vulnerable . The company failed to provide an explanation for the delay and to take proactive steps.Their crisis management team also weren't successful with handling the compromise either.

7.0 RECOMMENDATIONS

- The data breach of Equifax could have been avoided if the company had identified the risk in a better way earlier and would have taken the necessary steps to secure their systems. Equifax should maintain regular checks and update their security systems regularly and be more aware of the actions and programmes that are being run on their symptoms which contain sensitive info
- They should put a better risk management team in place, capable of handling big breaches like this and capable of detecting it on time or the possibility of it happening again so that a crisis like this can be averted.
- From the Equifax breach , individuals should make themselves more aware about cyber crime and they should monitor their financial accounts including credits cards , protect their bank accounts by insuring the two factor authentication

Reference list

Cavusoglu, H., Mishra, B. and Raghunathan, S., 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), pp.70-104.

equifax (2023) Who we are, Who We Are. Available at: https://www.equifax.com/about-equifax/who-we-are/ (Accessed: April 15, 2023).

Fruhlinger, J. (2023) Equifax Data Breach FAQ: What happened, who was affected, what was the impact?, CSO Online. CSO. Available at: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (Accessed: April 15, 2023).

Gibb, F. and Buchanan, S., 2006. A framework for business continuity management. International journal of information management, 26(2), pp.128-141.

Harmer, B. (2023) In Equifax Data Breach, three hard lessons in risk, CSO Online. CSO. Available at: https://www.csoonline.com/article/3229508/in-equifax-data-breach-three-hard-lessons-in-risk.html (Accessed: April 15, 2023).

Herbane, B., Elliott, D. and Swartz, E.M., 2004. Business continuity management: time for a strategic role?. Long range planning, 37(5), pp.435-457.

Hillson, D. and Murray-Webster, R., 2011. Using risk appetite and risk attitude to support appropriate risk-taking: a new taxonomy and model. Journal of Project, Program & Portfolio Management, 2(1), pp.29-46.

Sullivan, E. and Crocetti, P. (2023) What is business continuity and why is it important?, Disaster Recovery. TechTarget. Available at: https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity (Accessed: April 15, 2023).

Team, P.M.V. (2023) Risk averse, risk attitude, risk appetite, risk tolerance, PM Vidya. Available at: https://pmvidya.com/blog/risk-attitude-risk-appetite-risk-tolerance-risk-threshold-risk-averse/ (Accessed: April 15, 2023).

Wang, P. and Park, S.A., 2017. COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING. Issues in Information Systems, 18(2).

Z

ORIGINALITY REPORT

9%	7%	1%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	web.archive.org Internet Source	2%
2	www.csoonline.com Internet Source	1%
3	Submitted to UOW Malaysia KDU University College Sdn. Bhd Student Paper	1%
4	Submitted to University of Derby Student Paper	1%
5	www.termpaperwarehouse.com Internet Source	1%
6	Submitted to Colorado Technical University Student Paper	1%
7	pmvidya.com Internet Source	1%
8	Submitted to St James Lutheran College Student Paper	1%
9	Submitted to De Montfort University Student Paper	<1%

10	Submitted to Middlesex University Student Paper	<1%
11	www.canberra.edu.au Internet Source	<1%
12	Submitted to University of Portsmouth Student Paper	<1%
13	"SP9-PC-22_HR", ActEd Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		