LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5052NI Risk, Crisis & Security Management

Assessment Weightage & Type

50% Individual Coursework

Year and Semester

2023-24 Autumn

Student Name: Angana Bhattarai

London Met ID: 22067110

College ID: NP01NT4A220074

Coursework Due Date: Friday, January 5, 2024

Coursework Submission Date: Friday, January 5, 2024

Word Count:2219

I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Table of Contents

Table of Figures

1. Introduction

1.1. What is Cyber Security?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes. (Cisco, 2023)

1.2. Cybersecurity Trends

Cyber security is a fast-moving sector, as both hackers and security providers vie to outsmart each other. New threats and innovative ways to combat them emerge all the time. In this overview, we explore the latest trends in cyber security. (Kaspersky, 2023)

Heading into 2024, the attack surface is set to expand even further, with threats likely to grow more and more elusive. Considering the increasing power and accessibility of tools based on artificial intelligence (AI) and large language models (LLMs), it will be imperative to stay several steps ahead of threat actors and know what tactics to expect in the coming year. (Zamir, 2023)

1. **Remote working cybersecurity risks**

   A critical cyber security trend is for organizations to focus on the security challenges of distributed workforces. This means identifying and mitigating new security vulnerabilities, improving systems, implementing security controls, and ensuring proper monitoring and documentation. (Kaspersky, 2023)

2. **The Internet of Things (IoT) evolving**

   The expanding Internet of Things (IoT) creates more opportunities for cybercrime. The Internet of Things refers to physical devices other than

computers, phones, and servers, which connect to the internet and share data. (Kaspersky, 2023)

3. **The rise of ransomware**

   Ransomware isn't a new threat – it's been around for about two decades – but it is a growing one. (Kaspersky, 2023)

4. **Social engineering attacks getting smarter**

   Social engineering attacks like phishing are not new threats but have become more troubling amid the widespread remote workforce. (Kaspersky, 2023)

5. **Data privacy as discipline**

   One of the key data security trends is the rise of data privacy as a discipline in its own right. (Kaspersky, 2023)

6. **Custom ChatGPT-like bots crafting convincing social engineering attacks**

   OpenAI's custom GPTs are prime examples of powerful new tools that hackers will be leveraging in 2024. Given their ease of use, they can be utilized by those with far less technical skill to engineer and launch highly convincing social manipulation attacks. (Zamir, 2023)

7. **The evolution of deception**

   Multi-modal machine learning models have granted attackers the capacity to generate convincing audio, images, and videos to trick unsuspecting employees. Such deception practices will continue to pose serious threats for countless organizations. (Zamir, 2023)

1.3. Aim and Objectives

The aim of this research is to recognize potential challenges before or after they arise and to develop a strategy for dealing with them.

The objectives of this report are:

1) To identify the risk in an effective manner, a thorough risk identification procedure must be carried out in order to identify the risk in an effective manner.
2) To analyze the risk entails locating possible risks, evaluating their impact and possibility, and creating management plans for them.
3) Prioritizing the risk enables businesses to concentrate their resources and attention on the most serious risks.
4) In order to manage the risk, solutions must be developed and put into action to either lessen the risk's impact.
5) The procedure of risk monitoring encompasses ongoing risk assessment, tracking, and success evaluation.

2. Background

Risk Management / Control

A risk is the potential of a situation or event to impact on the achievement of specific objectives. The project risk management process reflects the dynamic nature of project-word, capturing and managing emerging risks and reflecting new knowledge in existing risk analyses (APM, 2023) .

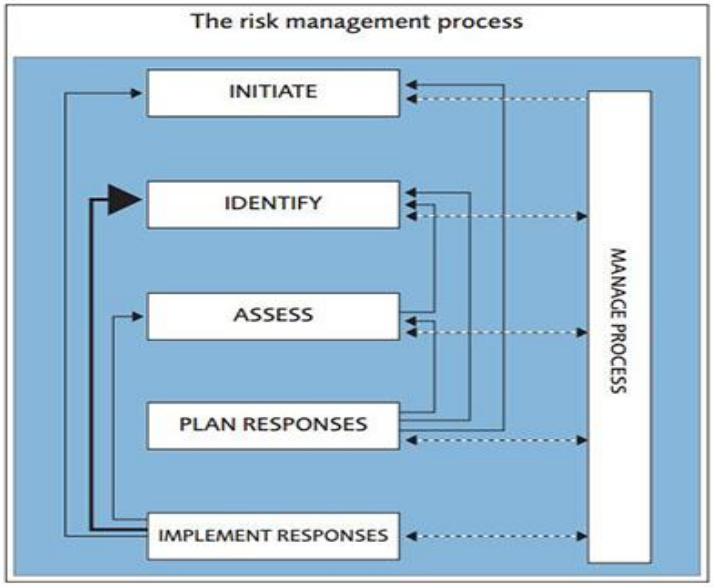

Figure 1: Risk Management Process

Source: (APM, 2023)

Three important steps of the risk management process are risk identification, risk analysis and assessment, and risk mitigation and monitoring.

- **Identifying risks**
- **Risk analysis and assessment**
- **Risk mitigation and monitoring**

. (IBM, 2023)

Risk control refers to a business strategy used for assessing and managing the affairs of a business in a manner that detects and prevents the business from unnecessary calamities that could hinder the organization’s operations and future plans. Hazards, unnecessary losses, etc. that may occur are avoided by incorporating risk control measures**.** (Shrivastav, 2023)

3. Literature review

This report is based on the research of a data breach that occurred in 2017, “Equifax Data Breach”. Equifax, one of the three largest consumer credit reporting agencies in the United States, announced in September 2017 that its systems had been breached and the sensitive personal data of 148 million Americans had been compromised (Epic.org). This data breach report is analyzed on the basis of risk management/control.

3.1. Case Study

A significant cybersecurity breach that impacted one of the biggest credit reporting organizations in the US was the 2017 Equifax data breach. Around 147 million Americans' sensitive personal information, including names, addresses, social security numbers, and credit card information, was compromised. The hack went unnoticed for several months as the attackers took use of a flaw in the website software used by Equifax.

Since Equifax was aware of the vulnerability but did not quickly fix it, the organization came under pressure for how it handled the breach. Top executives resigned as a result of the affair, which also set off an outbreak of legal actions and government investigations. In 2019, Equifax and the impacted parties came to a settlement agreement whereby Equifax agreed to pay up to $700 million in compensation and to put in place measures including free credit monitoring services. The hack served as a reminder of the value of strong cybersecurity procedures and the necessity of promptly patching vulnerabilities in order to safeguard private customer data. (Epic.org, 2023)

3.2. Findings

3.2.1. Identifying Data Breach

In the years leading up to the breach, Equifax struggled with outdated cybersecurity policies and instruments. In April of 2015, former CSO Susan Mauldin implemented Equifax's first patch management policy. An internal audit of the policy later that year revealed numerous security deficiencies, including over 8500 unresolved software vulnerabilities (PSI). In May of 2016, Equifax's W-2 Express website was also hacked, resulting in the leak of 430,000 names, addresses, social security numbers, and other types of personal information (Brewster). By 2017, most of Equifax's security deficiencies had not been remediated, allowing hackers to breach Equifax's network and harvest the PII of 147 million consumers' personal information (PSI). (Miyashiro, 2021) On September 7, 2017, Equifax announced that it had breached the data of approximately 143 million U.S. consumers. The same announcement stated that some UK and Canadian consumers had been affected as well, but did not give a specific number. The company stated that the unauthorized access occurred from mid-May through July 2017. The hackers did not access the data from Equifax's core consumer credit reporting databases, but from the company's U.S. online dispute portal web application. The data included Names, Social Security Numbers, Birth Dates, Addresses, and Driver's License Numbers. (Epic.org, 2023)

3.2.2. How did the breach occur?

The breach occurred between May and July 2017, as cyber criminals exploited a remote code execution vulnerability in Apache Struts 2, an open-source framework for developing Java web apps. (Irwin, 2023) The vulnerability that caused the breach was vulnerability Apache Struts CVE-2017-5638. (Epic.org, 2023) Apache learned of the vulnerability two months earlier, in March 2017, and released a patch. However, Equifax failed to install it, leaving a known vulnerability on its systems for criminals to find and exploit. (Irwin, 2023)

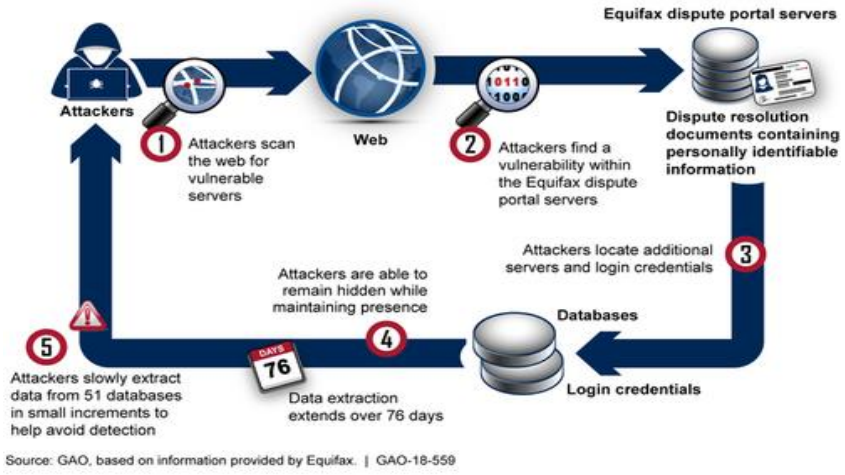

Figure 2: Exploitation of vulnerabilities from attackers in Equifax

Source: (GAO, 2018)

3.2.3. Post-breach actions

After learning of the breach, Equifax GVTM teams attempted and failed to locate Apache struts on servers by conducting multiple network scans. (Miyashiro, 2021). Equifax reported that it took steps to mitigate these factors and attempted to identify and notify individuals whose information was accessed. The company's public filings since the breach occurred reiterate that the company took steps to improve security and notify affected individuals. (GAO, 2018)

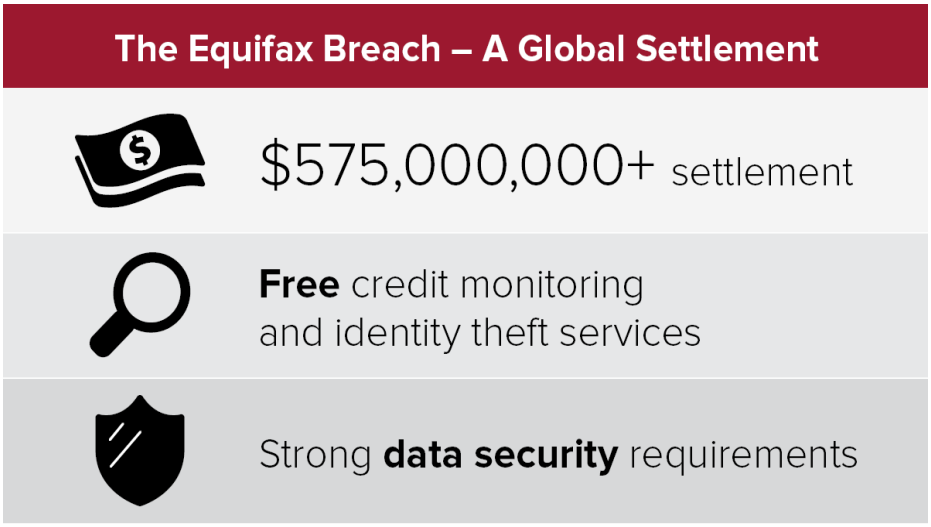

Figure 3: Settlement for Equifax Data Breach

Source: (FTC, 2019)

Equifax agreed to pay up to $700 million (about £561 million) as part of a settlement with US regulators following its mammoth data breach in 2017.The FTC (Federal Trade Commission) claimed that Equifax hadn't taken reasonable steps to secure its systems, which led to the records of more than 147 million people being compromised (Irwin, 2019) .

3.2.4. Factors that contributed to the breach

According to the survey, the following aspects are the possible factors of the breach that occurred.

a. IT and Security Management

The attackers pulled data out of the network in encrypted form undetected for months because Equifax had crucially failed to renew an encryption certificate on one of their internal security tools (Frulinger, 2020). Communication among employees on the remediation of security vulnerabilities was inconsistent (Miyashiro, 2021).

b. Lack of Comprehensive IT Asset Inventory

At the time of the breach, Equifax lacked a complete IT Asset Inventory, meaning they did not know the locations of the Apache struts application on their network. Instead, IT had to conduct network scans, which failed to detect the software. (Miyashiro, 2021)

c. Failure to follow Patch Management Policy

Equifax's security policy mandated critical vulnerabilities be patched within 48 hours of discovery, but the lack of IT Asset Inventory made meeting this deadline impossible. IT conducted multiple network scans but could not find instances of the vulnerable software. After failing to locate the application, IT and security took no further action to find Struts, and management did not check the vulnerability had been remediated. (Miyashiro, 2021)

d. Failure to Maintain Cybersecurity Technologies

Hackers encrypted their activities on Equifax servers, but because the certificate had expired, incoming traffic was not decrypted, and Equifax had no knowledge of suspicious activities on the online dispute portal (Miyashiro, 2021).

3.3. Analysis

Equifax was exposed to CVE-2017-5638, a critical Common Vulnerabilities and Exposure of Apache Struts. This exposed extremely sensitive information from about 143 million customers in the United States and Canada between May and July 2017. Personal information such as social security number, physical address, date of birth, and more was leaked. This vulnerability was publicly disclosed (with a fix that had to be implemented) in March 2017, but Equifax did not patch it. While introducing numerous servers, network equipment, web services, and DBMS, which are the basis for business expansion and operation, systematic management of them was neglected. There was no clear equipment status and no minimum manual to respond to emergency situations, and it insensitively responded to security warnings, alarms, and security patch

recommendations for CVEs from various computer systems. Even if there was no dedicated organization, manpower, and manual to respond to cyber incidents, if the technical defense system had been preemptively equipped, the worst could have been avoided. However, the hacker was able to take copious amounts of data from the Equifax system for two months without detection (Bond, 2023).

Certain changes could help this organization fix the damage and even prevent the unknown risk that might occur in the future.

- For Equifax organization

i. Reform the industry by giving consumers control over their credit reports.

Instead of the current setting, which allows virtually anyone to pull someone's credit report, credit reporting agencies should establish a credit freeze for all disclosures, with free and easy access for consumers who wish to disclose their report for a specific purpose. (Epic.org, 2023).

ii. Improve Breach Notification

The federal standard should require immediate and efficient notification of impacted consumers, regulators, and the public to limit the damage caused by data breaches. (Epic.org, 2023).

iii. Promote innovative technology to minimize the collection of personal data.

There are already initiatives to improve privacy protections in the field of data science, and these efforts could be adopted and further developed by the companies responsible for protecting consumer data. (Epic.org, 2023) .

iv. Increase Confidentiality, Integrity and Availability

Ensuring that sensitive data is encrypted, implementing data integrity checks and implementing disaster recovery plans will help in limitation of risks or damage.

v. Secure Authorization, Authentication and Accounting

Implementing robust user authentication mechanisms, regular auditing of logs and authorization mechanisms can help build better security in the organization. Equifax could have reviewed and restricted unnecessary privileges to limit the potential damage from a compromised account.

4. Conclusion

Due to the evolving nature of technology and its increasing use in daily life and business life new cybercrimes are being developed or committed on a frequent basis. These crimes range from totally new technologies to committing types of cybercrimes to applying previous cybercrime methodologies to new targets as new technology is embraced. Cybercrime has become so prevalent, that many people are more worried about cybercrimes such as identity theft than home burglaries.

At the time, the Equifax data breach was unprecedented and represented the largest most complex data breach known. The breach was caused due to a known vulnerability that was published by the vendor and Equifax received several warnings to apply the patch that would prevent the vulnerability. In such data breaches and cyber-attacks, it is very important to look after the risk management/control process. Analyzing the risk, managing the potential solutions, eradicating the risk/vulnerability, mitigating the issues and solving the damage done will thoroughly do better for any organization who face data breach.

5. References

Cisco.,2023. *Cisco.* [Online]
Available at: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html
[Accessed 2023].
Project., *Risk Analysis and Management Guide.* 2nd Edition ed. s.l.:s.n.
APM, 2023. [Online]
Available at: https://www.apm.org.uk/resources/what-is-project-management/what-is-risk-management/
APM, 2023. *Project Risk Analysis and Management Guide 2nd edition.* 2nd ed. s.l.:s.n.
Bond, M., 2023. *CS.UCF.* [Online]
Available at: https://cs.ucf.edu/~mohaisen/doc/teaching/cap5150/fall2022/cap5150-proj2.pdf
CFPB, 2023. *CFPB.* [Online]
Available at: https://www.consumerfinance.gov/equifax-settlement/
Cisco, 2023. [Online]
Available at: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html
Cisco, 2023. [Online]
Available at: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
Epic.org, 2023. [Online]
Available at: https://archive.epic.org/privacy/data-breach/equifax/
Epic.org, 2023. [Online]
Available at: https://archive.epic.org/privacy/data-breach/equifax/
Epic.org, 2023. [Online]
Available at: https://archive.epic.org/privacy/data-breach/equifax/
Epic.org, 2023. *Archive Epic.* [Online]
Available at: https://archive.epic.org/privacy/data-breach/equifax/

Frulinger, J., 2020. *CSO.* [Online]
Available at: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
Frulinger, J., 2020. *CSO.* [Online]
Available at: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
FTC, 2019. *ftc.gov.* [Online]
Available at: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach
GAO, 2018. [Online]
Available at: https://www.gao.gov/products/gao-18-559
GAO, 2018. [Online]
Available at: https://www.gao.gov/products/gao-18-559
GeeksForGeeks, 2023. [Online]
Available at: https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/
Governance, 2023. [Online]
Available at: https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important
Governance, I., 2023. [Online]
Available at: https://www.itgovernance.co.uk/what-is-cybersecurity
Governance, I., 2023. [Online]
Available at: https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important
Governance, I., n.d. [Online]
Available at: https://www.itgovernance.co.uk/what-is-cybersecurity
[Accessed 2023].
HashedOut, 2019. [Online]
Available at: https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/

IBM, 2023. [Online]
Available at: https://www.ibm.com/topics/risk-management
Irwin, L., 2019. *IT Governance.* [Online]
Available at: https://www.itgovernance.co.uk/blog/equifax-to-pay-561-million-to-settle-data-breach
Irwin, L., 2023. [Online]
Available at: https://www.itgovernance.co.uk/blog/equifax-to-pay-561-million-to-settle-data-breach
Kaspersky, 2023. [Online]
Available at: https://usa.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends
Miyashiro, I. K., 2021. [Online]
Available at: https://sevenpillarsinstitute.org/case-study-equifax-data-breach/
Shrivastav, A. K., 2023. [Online]
Available at: https://www.wallstreetmojo.com/risk-control/
Zamir, T., 2023. [Online]
Available at: https://www.helpnetsecurity.com/2023/12/28/2024-cyberattacks-trends/
Zamir, T., 2023. [Online]
Available at: https://www.helpnetsecurity.com/2023/12/28/2024-cyberattacks-trends/

6. Appendix

6.1. Appendix A: Introduction

Why is Cyber Security important?

Cyber security is important with the following criteria:

- **The costs of cyber security breaches are rising.**

Organizations that suffer cyber security breaches may face significant fines. There are also non-financial costs to be considered, like reputational damage. (Governance, 2023)

- **Cyber-attacks are increasingly sophisticated.**

Cyber-attacks continue to grow in sophistication, with attackers using an ever-expanding variety of tactics. These include social-engineering, malware and ransomware. (Governance, 2023)

- **Cyber security is a critical, board-level issue.**

The board needs assurance from management that its cyber risk strategies will reduce the risk of attacks and limit financial and operational impacts. (Governance, 2023)

- **Cybercrime is a big business.**

According to a study, the world economy loses more than $1 trillion each year due to cybercrime. Political, ethical, and social incentives can also drive attackers. (Governance, 2023)

6.2. Appendix B: Background

Risk Management/Control

Risk analysis and risk management is a process that allows individual risk events and overall risk to be understood and managed proactively, optimizing success by minimizing threats and maximizing opportunities and outcomes.

Three important steps of the risk management process are risk identification, risk analysis and assessment, and risk mitigation and monitoring.

- **Identifying risks**

Risk identification is the process of identifying and assessing threats to an organization, its operations and its workforce. (IBM, 2023)

- **Risk analysis and assessment**

Risk analysis involves establishing the probability that a risk event might occur and the potential outcome of each event. (IBM, 2023)

- **Risk mitigation and monitoring**

Risk mitigation refers to the process of planning and developing methods and options to reduce threats to project objectives. (IBM, 2023)

The process of risk control measures is listed below:

- The primary step is the analysis of the business environment in which the business operates.
- After that, analyze the possible circumstances which could affect the business activities, whether they are adverse or favorable, called risks.

- Then finding out the measures which could be applied to control or it could not be prevented or controlled fully then to minimize the effect thereof. (Shrivastav, 2023)

6.3. Appendix C: Case Study

Literature Review:

The data breached included names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also breached. The Equifax breach is unprecedented in scope and severity. There have been larger security breaches by other companies in the past, but the sensitivity of the personal information held by Equifax and the scale of the problem makes this breach unprecedented. (Epic.org, 2023)

Findings:

About Equifax:

Equifax is a multinational credit reporting agency, founded in 1899 and headquartered in Atlanta, Georgia. One of three major US credit reporting agencies, including Experian and Transunion, Equifax holds the information of millions of consumers and businesses worldwide. Equifax sells both commercial credit reports and consumer credit reports. Additionally, Equifax sells credit monitoring services, including credit fraud and identity theft prevention services (Equifax). (Miyashiro, 2021)

How did the breach occur?

The vulnerability was left unpatched until July 29, 2017 when Equifax's information security department discovered "suspicious network traffic" associated with its online dispute portal and applied the Apache patch. On July 30, 2017, Equifax observed further suspicious activity and took the web application offline. Three days letter the company hired cybersecurity firm Mandiant to conduct a forensic investigation of the breach. The investigation revealed that the data of an additional 2.5 million U.S. consumers had been breached, bringing the total number of Americans affected to

approximately 145.5 million. Equifax disclosed in the same announcement that 8,000 Canadians had been impacted and stated that the forensic investigation related to UK consumers had been completed, but did not state the amount of UK consumers affected. A later announcement from Equifax stated that the data of 693,665 UK citizens was breached. (Epic.org, 2023)

Events Timeline:

April, 2015: Former CSO Susan Mauldin implemented Equifax's first patch management policy. (An internal audit of the policy later that year revealed numerous security deficiencies, including over 8500 unresolved software vulnerabilities) (Miyashiro, 2021).

May 2016: Equifax's W-2 Express website was also hacked (resulting in the leak of 430,000 names, addresses, social security numbers, and other types of personal information) (Miyashiro, 2021).

By 2017: Most of Equifax's security deficiencies had not been remediated (allowing hackers to breach Equifax's network and harvest the PII of 147 million consumers' personal information) (Miyashiro, 2021).

March 7, 2017: Apache publicized and provided a patch for Apache Struts. (an easily exploitable software vulnerability) (Miyashiro, 2021).

March 8, 2017: The Department of Homeland Security's US-CERT team notified Equifax of the software flaw, and an alert was distributed to 400 employees by Equifax's Global Threats and Vulnerability Management team (Miyashiro, 2021).

Post-breach actions:

The Internal Revenue Service (IRS), Social Security Administration (SSA), and U.S. Postal Service (USPS) three of the major federal customer agencies that use Equifax's identity verification services conducted assessments of the company's security controls, which identified a number of lower-level technical

concerns that Equifax was directed to address. The agencies also made adjustments to their contracts with Equifax, such as modifying notification requirements for future data breaches. In the case of IRS, one of its contracts with Equifax was terminated. The Department of Homeland Security offered assistance in responding to the breach; however, Equifax reportedly declined the assistance because it had already retained professional services from an external cybersecurity consultant. In addition, the Bureau of Consumer Financial Protection and the Federal Trade Commission, which have regulatory and enforcement authority over consumer reporting agencies (CRAs) such as Equifax, initiated an investigation into the breach and Equifax's response in September 2017. (GAO, 2018)

Two years after the breach, the company said it had spent $1.4 billion on cleanup costs, including “incremental costs to transform our technology infrastructure and improve application, network, and data security.” (Frulinger, 2020)

Analysis:

Certain changes could help this organization fix the damage and even prevent the unknown risk that might occur in the future.

- For Equifax organization

I. Reform the industry by giving consumers control over their credit reports.

Credit reporting agencies should change the default on access to credit reports by third parties. Instead of the current setting, which allows virtually anyone to pull someone’s credit report, credit reporting agencies should establish a credit freeze for all disclosures, with free and easy access for consumers who wish to disclose their report for a specific purpose. CRAs should also provide free monitoring and easy access to credit history (Epic.org, 2023).

II. Improve Breach Notification

They should set national, baseline data breach notification standards to limit the damage caused by data breaches. The federal standard should require immediate and efficient notification of impacted consumers, regulators, and the public (Epic.org, 2023).

III. Promote innovative technology to minimize the collection of personal data.

There are already initiatives to improve privacy protections in the field of data science, and these efforts could be adopted and further developed by the companies responsible for protecting consumer data. These are the techniques that Equifax and other credit reporting agencies should invest in to limit harm to consumers going forward (Epic.org, 2023) .

IV. Increase Confidentiality, Integrity and Availability

Ensuring that sensitive data is encrypted both in transit and at rest can help maintain confidentiality. Equifax should implement data integrity checks to detect any unauthorized alterations or tampering of information within its systems. Equifax should implement disaster recovery plans to quickly restore services after an incident.

V. Secure Authorization, Authentication and Accounting

Implementing robust user authentication mechanisms ensures that only authorized individuals can access sensitive systems and data. Enforcing strong password policies helps protect against password-related vulnerabilities. Equifax could have implemented comprehensive logging to record user activities, system events, and potential security incidents. Regular auditing of logs could have

helped detect anomalies or suspicious activities early on. Authorization mechanisms ensure that authenticated users have the appropriate level of access to resources based on their roles and responsibilities. Equifax could have reviewed and restricted unnecessary privileges to limit the potential damage from a compromised account.

- For Consumers

VI. Check your credit reports on your own

According to a Federal Trade Commission study, one person in five finds an error in their credit reports. When you check yours, be prepared to take steps to fix incorrect information. Information on credit reports and sample dispute letters can help the consumers with this process (CFPB, 2023).

VII. Consider placing an initial fraud alert on your credit file

Another way to protect your credit proactively is to place a fraud alert on your file. To do this, you can contact any of the three credit reporting companies. The credit reporting company you make the report to must communicate your alert to the other two credit reporting companies (CFPB, 2023).

VIII. Consider freezing your credit

One way to protect your credit proactively is to contact the three credit reporting companies and place a freeze on your credit. When you freeze your credit, lenders won't be able to access your credit information. If you apply for things like employment, apartments, or insurance, necessary credit checks can still go through (CFPB, 2023).

IX. Self-awareness for social engineering

The consumers must stay alert and aware about the social engineering attacks too. Such cases can exploit a lot of their personal information and no technical security can solve them.

At the time, the Equifax data breach was unprecedented and represented the largest most complex data breach known (Frulinger, 2020). The breach was caused due to a known vulnerability that was published by the vendor and Equifax received several warnings to apply the patch that would prevent the vulnerability. However, enterprise systems management and cybersecurity is very complex and even though Equifax had a presumably large IT division, they were not able to use standard digital forensic techniques of systems management practices to identify and track the infiltration (Frulinger, 2020).The utilized an outside security firm to conduct forensics investigations. The simple act of failing to apply a patch and failing to check properly and to see if the patch was installed enabled a devastating cybercrime with far-reaching ramifications.