

**ASSESSMENT 2**

**MIS607 (CYBERSECURITY)**

**THREAT MODEL REPORT**

**Submitted by: Submitted to: Mandeep Singh Dr Arezou Pour Mirza**

**A00030931 Dr. Ian Storey**

# 

**INTRODUCTION**

As per the case scenario, The Business and Communication Insurance dealt their business related confidential as well as authentic information with their client through emails in order to keep a proof. However, it has become a risk factor and threat for this institution as they are facing several cybersecurity attacks.

The CEO consulted the senior management and they acted promptly to investigate the risk factors and threats with the aid of cybersecurity specialists. This paper will therefore highlight the various threats, how to manage those threats, promote awareness and initiate action to mitigate those problems. In this record, I will also discuss Level 0 DFD diagram and context diagrams and presenting the diagram in the report body.

**RISK FACTORS RELATED WITH CYBERSECURITY**

Cyberspace is a concept that explains about a widespread interconnected digital technology. This concept was first coined after the diffusion of the internet. It is a global domain under an information environment, which consists of multiple interdependent networks, including computer system, internet, telecommunications and many more. These cyber-attacks are usually aimed to change or destroy the sensitive and confidential information, extort money from the users and ruin the reputation of the company or any other institution.

As stated by Utente (2018), a cookie policy is a declaration for the users on what cookies is active on their websites, what the purpose of the data are, for which they are tracking and where in the world this data is sent. This policy creates potential privacy risk as it can track the behaviour of the user. Data policy are the high-levelled principles, which forms guiding framework, in which data assets in the Commission can be managed.

All business firms undergo certain risk assessment, which affect the performance level of the organisation. The core values of these risk and the compliances demonstrate on defining the risk so that the organisation may proceed with standard and regulation. As stated by Florakis, Louca, Michaely and Weber (2020), the various threats related to cybersecurity are ransomware, hacking, data leakage, inside threat, third party vendor risk, phishing and improper way to secure the sensitive information, trust betrayal clients and many other. Ransom emails are usually forwarded through unreliable external networks that are outside the company’s security and trust boundary.

In the regard to case study, ransomware and hacking are the main risk occurred in this profile. Ransomware is form of malicious software that attempt to scramble the data and then extort a ransom in order to release an unlock code. Most often, this ransomware is released through malicious emails. In this case, too, through several malware emails, the company’s sensitive information is hacked by the outsider. As argued by Newhouse, Keith, Scribner and Witte (2017), hacking is yet another procedure, which can ruin a company’s confidential information. Gaining access and information from IT system from outside the organisation still provide a huge opportunity for the criminals to hack the company information and even the bank details or credit card database. The intellectual property is yet another source of value for them where they use the staffs to reveal the users name and passwords, social engineering and creates a threat for the company.

# PROMOTING STAFF AWARENESS AND MANAGEMENT OF THE RISK

As beautifully stated by some famous author “A leader is one who knows the way, goes the way and shows the way”. “Leadership is all about the vision and the responsibility, not the power”, therefore the team should be guided by an efficient leader who can show them the right path in this regard. As stated by Johnson and Hackman (2018), the art of communication is the language of the leaders.

Communication can solve these risk factors, as the more we communicate, the more we can understand the kind of problem arises at any circumstances. A responsible leader will develop their own communication skills as well as motivate the team to exercise this skill within power in order to achieve the best result. The management should guide and train their staffs effectively in order to avoid these technical mistakes.

As mentioned by Sarker et al. (2020), the hackers are waiting to grab the situation where the user left holes or gaps in their performance. Therefore, it is necessary to promote awareness among the staffs or employees and they should be aware of the unsolicited emails specifically those, which ask for prompt response. Firstly, the employees should be provided enough of training session on this cybersecurity concept, how and when the threats occurs and how to manage those threats before it can totally ruin the company’s important documents.

Secondly, they should know how to handle both the software as well as the hardware data. In order to avoid risk factor updated software are needed. Thirdly, in case of ransomware risk factor, installing a malware protection and maintaining a good anti-virus is highly needed. As stated by Alahmari and Duncan (2020), underestimation of cybersecurity threats by several small or medium organisation can also lead them to face the challenges of the increased vulnerabilities and risk factors. Therefore, in this regard management should identify the key aspects and the factors such as threat, behaviour, practice, awareness and decision-making.

Fourthly, the management should keep a data backup system in order to manage the stolen data that will allow the company to recover from an unencrypted version of a file. In this regard regularly testing the backup system can be a good idea. Fifthly, in order to stay protected from the hackers use network firewalls, data access security, user awareness and training as well as removing access.

Sixthly, as stated by Desolda et al. (2019), the CEO should remain vigilant of phishing risk factor, which is done to gain sensitive or classified information while demonstrating as a reliable contact. The managers and the leaders should keep in mind that the company should not ask for sensitive information. It is the work of the hacker, who will fir gain the trust of the user and then will track their information and further put them in a trap. Seventhly, spam filters should be turn on, remain suspicious about the unexpected mails and use anti-malware soft wares.

The data leakage factor is yet another issue usually faced by several companies. The use of smartphones and tablets has become widespread. The portable and cheap characteristics of portable storage devices make it a useful tool for backup and transferring sensitive information (Sun et al., 2018).

Therefore, in this regard the management should check that each of their employees should have a strong password code and ensure that the GPS mode should always be turned on. The user should maintain their mobile device and keep track on paperwork, because if ever the data thieves stole and hack their backup data, then the paperwork can help the user. Inside threat is yet another factor, which usually cannot be tracked.

It happens in some situation, in which the employee of an organisation leaks the data, by mistake or by taking commissions (Xin et al., 2018). The potential for document leaking to do harm cannot be overstated. Therefore, in this regard, educate the team to remain alert of these situations and handle them carefully. Control the use of portable storage devices and protect their digital assets.

# 

# ETHICAL DECISION MAKING AND IMPLEMENTATION OF SERIOUS MEASURES

In order to protect the company’s reputation and the sensitive information from cybersecurity attack, the management should ethically take decision and promote awareness among their staffs and initiate serious action. As a cybersecurity specialist, our team provide some important guidelines and steps, which if followed can be avoided the risk to some extent (Crumpler & Lewis, 2019).

Changing passwords and updating their device can keep them protected from the data thieves. The password should be unique as well as strong enough to beat their range. They can communicate to all involved both internal as well as external. It is important for all the stakeholders including clients, customers and others to understand what has happened.

Besides, as suggested by Crumpler and Lewis (2019), the executive managers and other leaders should stay alert in every respect to track and detect the threats before they touch the company’s documents fully. If appropriate, they can involve third party expert for better advice on corrective action and they can even report this incident to action fraud and keep the contact to the bank official credit card companies.

As stated by Radziwill and Benton (2017), cybersecurity cost of quality can improve and manage the risk factor. Ethical decision should be taken by the management in this regard and serious action should be initiated as soon as possible to track the criminal and get them punished.

**MITIGATION PLAN USING STRIDE MODEL**

The risks have been identified and mitigation strategy has been discussed too in the above paragraphs. Succinctly, I would like to categorise the mitigation plan with STRIDE model.

**SPOOFING**: Strong passwords, as well as other security measures such as fingerprint scanning or two-factor authentication must be implemented. Furthermore, encryption should be implemented to prevent unauthorised access to private information.

**TAMPERING**: Authorization levels must be clearly defined, and each task must be prioritised. To ensure data integrity, it must be checked and confirmed on encryption and decryption.

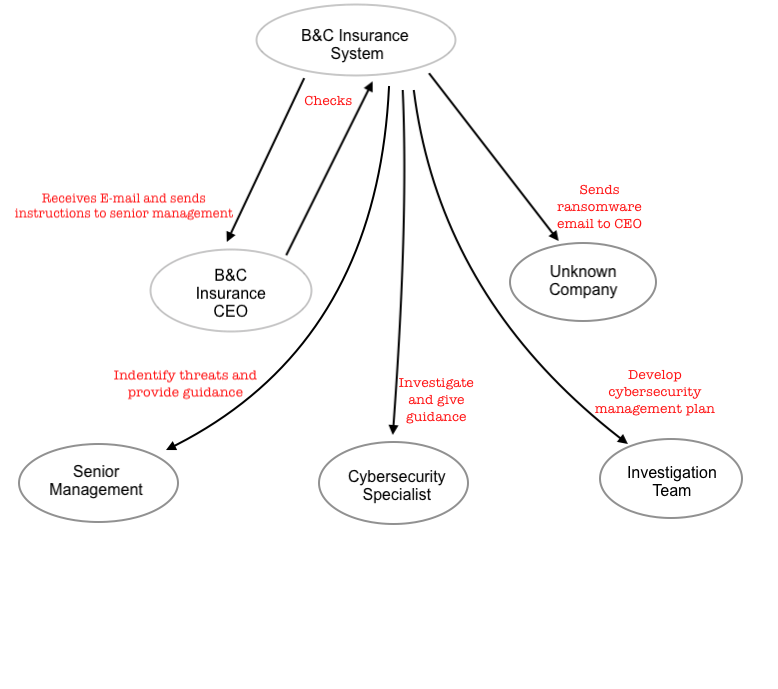
**REPUDIATION**: Each activity such as the valid and unsuccessful login attempts, cookies, and so on, must be logged.

**INFORMATION DISCLOSURE**: It is critical to safeguard information using cryptography, a high degree of authorisation, and limiting access to only trusted and authorised individuals in order to keep it secret.

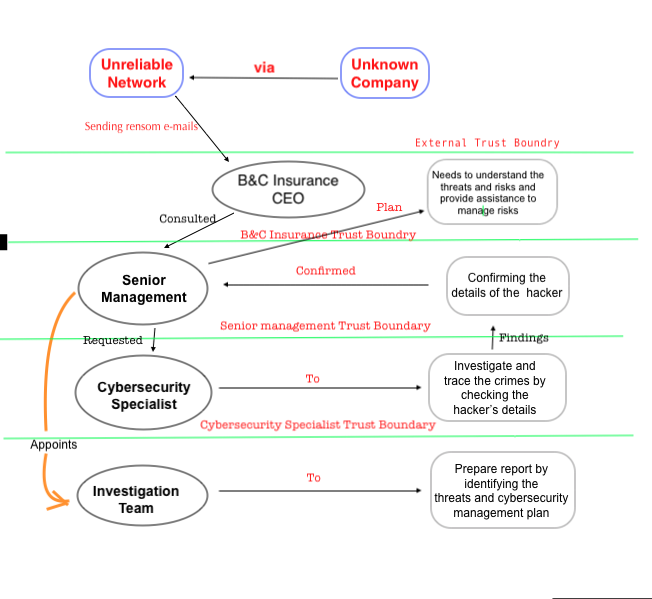
**DENIAL OF SERVICE**: Information security must be discussed with all team members and no one should be allowed to bring portable devices inside the premises from outside, and no one should have access to sensitive information.

# PRIVILEGE ELEVATION: Any user with permitted access should have restricted privileges and access.

**CONTEXT DIAGRAM**



**LEVEL 0 DATA FLOW DIAGRAM**

****

**CONCLUSION**

From the above report, it can be concluded, “cybersecurity is a new area where equality will exist to allow intelligence to succeed”. However, cybersecurity undergoes certain risk factors, which destroys the company’s reputation and damage the important documents and information. Therefore, in order to protect the company’s reputation, the management should identify the threats, their behaviour and pattern, make ethical decision and initiate strong action.

This paper highlighted the basic concept of cybersecurity risk, how to manage them, promoting awareness among the staffs and implementing serious measures. “Success is not final, failure is not fatal, it is the courage that continues the count”, a famous quote of Winston Churchill who always motivates and encourage the business dealers and the management not to lose hope in any situation.

# 

**REFERENCES**

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-5

Crumpler, W., & Lewis, J. A. (2019) *The cybersecurity workforce gap* US: Centre for Strategic and International Studies (CSIS)

Desolda, G., Di Nocera, F., Ferro, L., Lanzilotti, R., Maggi, P., & Marrella, A. (2019). Alerting users about phishing attacks. In *International Conference on Human-Computer Interaction*, 134-148

Florakis, C., Louca, C., Michaely, R., & Weber, M. (2020) *Cybersecurity Risk* (No. w28196) US: National Bureau of Economic Research

Johnson, C. E., & Hackman, M. Z. (2018) *Leadership: A communication perspective* US: Waveland Press

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication*, *800*(2017), 181.

Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. *arXiv preprint arXiv:1707.02653*

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, *7*(1), 1-29.

Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE communications surveys & tutorials*, *21*(2), 1744-1772.

Utente, G. (2018). Informative Privacy-Cookies Policy. *Policy*, *18*, 07

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365-35381