Literature Review

Student's Name

Institutional Affiliation

Literature Review

Introduction

Information and communication technologies (ICTs) enable people to meet different educational, commerce, entertainment, and communication needs. Despite the benefits of communication technologies, they have also contributed to new forms of criminal activity referred as cybercrime. The crimes are perpetrated by online attackers and hackers, and when directed towards organizations, they have an impact on finances and reputation. The theoretical framework that can better explain cybercrime is the Routine Activity Theory. Based on this framework, cybercrime happens when an offender comes across a suitable target, and there are no mechanisms to prevent them from committing the crime. In addition, cybercrimes take place in locations that lack guardians who can protect the target. This literature review will examine the impact of cybercrime on an organization's financial well-being and reputation. The review draws from various studies that highlight the financial and reputational impact of cybercrime.

Literature Review

Numerous studies suggest that cybercrime affects the financial standing of an organization and its reputation. In a study conducted by Raghavan & Parthiban (2014), the researchers evaluated the effect of cybercrime on a bank's finances. Based on the study, cybercrime can be regarded as a growing threat since organizations and individuals have become reliant on the internet. The results of the study indicate that approximately 114 billion USD is lost to cybercrimes every year, and the cost of combating this crime is twice the amount. Moreover, banks lose a lot of money in recovering from the crimes and also spend huge amounts to prevent the occurrence of cybercrimes in the future. Thus, cybercrime has a huge financial impact on financial institutions such as banks.

Chevers (2019) conducted a study similar to the one by Raghavan & Parthiban (2014). In his study, Chevers sought to understand the impact that cybercrime has on e-banking. The study found out that cybercrime hinders the adoption of electronic banking by financial institutions. For instance, victims of phishing are unlikely to adopt electronic banking, because they fear losing money when conducting online transactions. Besides, identity theft has a negative impact on the decision by banks to adopt electronic banking. From the results, 61% of cybercrime victims report their credit card having being misused while 33% report that identity thieves misuse of their wireless accounts or savings.

Another similar study conducted by Malik & Islam (2019) sought to classify cybercrime as an emerging threat in Pakistan's banking sector. The purpose of the study was to understand the impact that cybercrime incidents have on the banking sector in Pakistan. The researchers studied 302 bank employees in Pakistan and used the survey design method. Based on the findings, incidents of cybercrime affect organizational performance negatively. However, the negative impact that cybercrime has on the performance of organizations is weakened by information security awareness. The research illustrates the need for organizations to establish security training courses as a way of increasing the awareness of employees on cybercrimes.

A study by Agrafiotis et al (2018) examined the harms of cybercrimes and how cyber-attacks are propagated. The researchers observe that technological advances have contributed to the digitization of operations. As a result, most transactions are conducted online, and this has led to an increase in cybercrimes. The results of the study indicate that cyber-attacks have both direct and indirect impacts on the finances of an organization. Therefore, cybercrime has economic harm, which relates to the negative economic or financial consequences on organizations. Additionally, customers are likely to become victims of financial fraud, and this

leads to the loss of customers, which has a negative effect on an organization's financial performance. Financial damages to the organization are also likely to be manifested in the stock market.

Arcuri, Brogi, & Gandolfi (2017) conducted a study to highlight how cybercrime affects firms. The research established that cybercrime is one of the greatest risks for companies in today's world. Furthermore, the risk of cyber-attacks poses a threat to institutions in both the private and public sectors because it leads to financial losses, as well as loss of stakeholders and damages reputation. Stakeholders have little confidence in an organization whose systems are prone to cyber-attacks and this affects brand reputation negatively. In another study, Ali (2019) sought to indicate how cybercrimes pose a threat to the business sector and limit its growth. The study used a survey questionnaire to collect data from bank employees in the Gulf Countries Council (GCC). Based on the results, the effects of cybercrime are more than the financial impact it has on business sectors and financial institutions. The study is similar to that of Malik & Islam (2019) as it illustrates the need for financial organizations to be knowledgeable about online threats and adopt appropriate measures to address them.

Dupont (2019) examined the cyber-resilience of financial institutions with regards to its significance and applicability. The researcher argues that the severity, frequency, and sophistication of cyber-attacks that target institutions in the financial sector highlight the impossibility of these organizations to completely protect their computer systems. Based on the results, cyber-attacks have reputational damage on financial institutions and their efforts to rebuild is costly. Findings of the study highlight the need for financial institutions to invest in cyber-resilience and cybersecurity. Lagazio, Sherif, & Cushman (2014) conducted a study to understand how cybercrime affects the financial sector. The study found out that financial

institutions are unlikely to share information about incidents of cybercrime as a way of protecting their market share and reputation. Moreover, the study established that cybercrime has both direct and indirect losses. The direct losses include damage, monetary loss, and suffering that the targeted users experience due to cybercrime. The indirect losses include overall damage to reputation, loss of customer trust, and competitive disadvantage.

A research by Yadav & Gour (2014) studied cyber-attacks in relation to the impact they have on organizations. The research is a systematic study evaluating the cost of cybercrime incidents on organizations. The results indicate that cybercrime has diverse impacts on organizations, which range from economic, reputational, loss of sensitive information, and lack of trust. Organizations prone to cybercrime experience financial losses, negative brand reputation, loss of sensitive information relating to business, and customers lack trust. In another study, Antonescu & Birău (2015) evaluated the financial and non-financial implications of cybercrimes. The results of the study indicate that it is important for organizations to consider the non-financial implications of cybercrime. Reputational damage is one of the non-financial effects and it leads to negative publicity, declined customer confidence, and diminished business productivity.

Conclusion

Based on the review of literature, cybercrime is an issue of concern for organizations because it affects their financial well-being and reputation. The studies reviewed in this literature demonstrate the financial losses undergone by companies due to cyber-attacks, as well as the extent to which customers lose confidence on organizations whose data is accessed by online attackers. The literature provides essential insights on the need for organizations to develop

appropriate approaches of addressing cybercrime attacks. Moreover, the studies add to the existing body of knowledge on the adverse effects of cybercrime on organizations.

References

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S. & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1-15. https://doi.org/10.1093/cybsec/tyy006

Ali, L. (2019). Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *Journal of Developing Areas, 53*(1), 253-265.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*.

Antonescu, M. & Birău, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance, 32*, 618-621.

Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. *International Conference on Information Resources Management (CONF-IRM) 2019 Proceedings, 11*, 1-9.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity, 5*(1), 1-17. https://doi.org/10.1093/cybsec/tyz013

Lagazio, M., Sherif, N., & Mike, C. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, 1-32.

Malik, M. S. & Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. *Journal of Financial Crime, 26*(1), 50-60. https://doi.org/10.1108/JFC-11-2017-0118

Raghavan, A. R. & Parthiban, L. (2014). The effect of cybercrime on a bank's finances. *International Journal of Current Research and Academic Review, 2*(2), 173-178.

Yadav, H. & Gour, S. (2014). Cyber attacks: An impact on economy to an organization. *International Journal of Information & Computation Technology, 4*(9), 937-940.