Cybercrime: Evolution, Impact, and Mitigation

Student's Name or Students' Names

Department Affiliation, University Affiliation

Course Number: Course Name

Instructor's Name

Assignment Due Date

Cybercrime: Evolution, Impact, and Mitigation

Today, the advancement in technology has led to various types of crimes. Criminals use technological devices and techniques to carry out their activities. Cybercrime is a criminal activity where a networked device or a computer is used to execute illegal activities. Cybercriminals may target individuals or organizations, access their data illegally, commit fraud, steal their identity, or breach privacy (Sobers, 2021). These actions are carried out to jeopardize a company or an individual due to personal or political reasons. Individuals, businesses, and governments have experienced countless losses due to cybercrime. In this paper, there will be a review of the evolution, impact, and mitigation of cybercrime.

It is argued that for cybercrime to survive, then it must evolve. Cybercrime has evolved from the traditional phone phreaking, which began in the 1970s, to the modern hacking system. Phone phreaking was a practice that exploited the vulnerability of the telecommunication network. It was aimed at making calls free of charge or reducing call rates. With the development of computer networks, cybercriminals have advanced to other ways of carrying out their activities (Gillespie, 2019). The first cybercrime was in 1988 when Robert Morris released the Morris worm. Morris was charged for violating the Computer Fraud and Abuse Act in 1989 (Pavlik, 2017). Since then, worms have been used to carry out denial-of-service (DoS) attacks on a large scale. The pre-2000 cybercrime was characterized by a single criminal manipulating a computer network. Besides, post-2000 cybercrime focuses on using a computer to interfere with network uses for financial profit. Many consumers have been forced to adopt cybersecurity measures to curb cybercrime. In this case, cybercriminals had to be innovative to continue with their activities.

A successful cybercrime has adverse impacts on an individual or organization. The implications of cybercrime include financial loss, theft of essential information and data, denial of

services, and loss of consumers' confidence and trust. Every year, the government and society lose billions of dollars to cybercrime (Kuklytė, 2017). Various sectors in society experience such economic impacts of cybercrime. For instance, piracy affects the software, music, and entertainment industries. Also, cybercriminals have robbed copyright holders of their rights, leading to severe financial losses in the industry. Businesses have been compelled to employ cybersecurity strategies. In this case, companies must update their software constantly and hire IT experts, which is often costly.

Modern business operators should develop countermeasures against hackers seeking to commit cybercrimes. The first step of protecting data is through the identification of risks. An organization should carry out a full risk assessment to understand the interests of the cybercriminals and resolve the issues immediately (Geetha et al., 2020). Businesses should also find out individuals who may be interested in capturing their data. Besides, finding network systems' vulnerabilities is essential in developing strategies to mitigate the catastrophic effects of cybercrime. Vulnerabilities can be identified by carrying out a penetration test to detect intrusion. Finally, the potential risks identified should be prioritized and resolved as soon as possible.

In conclusion, cybercrime is a global threat to institutions, organizations, and individuals, causing adverse effects. The effects include loss of customers' trust for business, loss of data, and loss of money. The rapid technological changes have led to advanced ways of cybercrime. As technology advances, the perpetrators devise new ways to cope with the change. The perpetrators explore private and public sector vulnerabilities and utilize them to accomplish the crime. Although it is difficult to eradicate cybercrime, taking countermeasures and prioritizing vulnerabilities can help mitigate the adverse effects of a cybersecurity breach. Therefore, having mitigation procedures in place enables timely actions to prevent the worst from occurring.

References

Geetha, S., Kumar, P. D., Velan, G. S., Ali, D. S., & Kanya, N. (2020). Big data analysis - cybercrime detection in social network. *Journal of Advanced Research in Dynamical and Control Systems, 12*(SP4), 147–152. https://doi.org/10.5373/jardcs/v12sp4/20201476

Gillespie, A. A. (2019). *Cybercrime: Key issues and debates*. Routledge.

Kuklytė, J. (2017). Challenges and vulnerabilities of analyzing cybercrime costs. *European Journal of Business Science and Technology, 3*(2). https://doi.org/10.11118/ejobsat.v3i2.105

Pavlik, K. (2017). Cybercrime, hacking, and legislation. *Journal of Cybersecurity Research 2*(1), 13–16. https://doi.org/10.19030/jcr.v2i1.9966

Sobers, R. (2021, March 16). *134 cybersecurity statistics and trends for 2021*. Inside Out Security. https://www.varonis.com/blog/cybersecurity-statistics/

WritingElites.net

The Custom Writing Experts

Need an Original, High-Quality, Plagiarism-Free Essay Like This One?

Order Now
