Policies/Strategies Regarding the economic impact of Cybercrime

Karan Mudaliar

CYSE 425W

Prof. Lora Pitman

11 October 2022

As the world is shifting rapidly towards technology, it is experiencing more cybercrime daily. Cybercrime indicates the illegal incident that took place online, including the help of electronic devices such as computers, laptops, phones, and wearable devices. Financial gain is the biggest interest of a cybercriminal. To achieve this, they try to steal other people's personal information, financial statements, debit card numbers, and other sensitive information which they can use later to transfer money to themselves. This paper will discuss how some of the policies/strategies can be used to avoid or to overcome the economic impact of cybercrime; what group of people are mainly impacted by this crime, and what is the standard of the policies/strategies within the national cybersecurity policy. With the growth of technology involvement in our lives, it is crucial to understand the economic impact of cybercrime.

The first policy that will be discussed here is the host integrity protection policies; this was introduced to limit the attackers from completely taking over the system integrity in situations like network-based attacks. The HIPP continuously monitors any changes or unusual activity in the host's environment and makes sure that everything is in its good state following the policy.

Second policy, data breach notification, due to this policy, all businesses are obligated to inform their customers and their employees about the suspected thefts of confidential information such as personal data and company's financial data. It was developed to help the victim entities and its clients by including the authorities to investigate the incident and possibly catch the attackers in a timely manner. Businesses are legally responsible for notifying the security breaches of data to everyone who has been involved in it.

Lastly, we will be addressing some of the cybersecurity strategies that can help improve the security of entities. This will cover how a strategy can be developed to clearly instruct the objectives, aim, and main concerns of the businesses, circulate and bring attention of everyone about the importance of the cybersecurity issues. We will discuss how to provide dedicated focus on prioritizing assets and purposes, constantly evaluating vulnerabilities and creating well-designed plans to reduce any vulnerabilities.

To conclude, we will go over some of the main points that we discussed earlier in this paper. Staying up to date on security and cybersecurity literacy can and will prevent cybercrime. Businesses should understand the importance of training their employees about the company computer usage policy. It could possibly save hefty amounts of money that would cost in the process of recovering the lost data and in the restoration after the cyber-attack. In total, it is every technology user's responsibility to stay aware about cyber risk and should educate themselves on how to protect their personal information.

.

REFERENCES

Li, Ninghui, Ziqing Mao, and Hong Chen. "Host Integrity Protection Through Usable Non-discretionary Access Control." (2006).https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/bibtex_archive/2006-38.pdf

Karyda, Maria, and Lilian Mitrou. "Data Breach Notification: Issues and Challenges for Security Management." *MCIS* (2016): 60.https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1060&context=mcis2016

“National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation’s Posture.” (2009, March 10). U.S. Government Accountability Office. https://www.gao.gov/products/gao-09-432t