Policies/Strategies regarding the economic impact of cybercrime

Karan Mudaliar

CYSE 425W

Prof. Lora Pitman

4 December 2022

Technology plays a significant role in assisting us with most of our daily life tasks. A lot of individual and entity must give high importance to cybersecurity in order to limit any form of cyberattacks. Cyberattacks that are more frequent are identity theft, misusing personal data, and unlawfully accessing other people's information. As it is becoming difficult for individuals and businesses to dodge these cyberattacks, there have been multiple cybersecurity policies in use to help mitigate the impact of these cyberattacks, or even try to avoid these. Policies that will be discussed in this paper are confidential data policy, security awareness and training policy, and data breach notification law. Paper will focus on explaining the social implications of all three cybersecurity policies. Cybersecurity policies establish a certain behavior within technology users towards securing information properly and ensures the awareness of necessary steps in case of data breaches.

The development of confidential data policy took place to minimize the risk of compromising the confidentiality of the information. Businesses with the minimal control over tracking the information flow are benefiting from this policy. Its purpose is to track anyone who has access to someone else's personal data and monitor the use of those data (Kasperbauer, 2019).

There have been positive consequences since the introduction of confidential data policy. Businesses started to use two of the effective methods to handle and secure their company's data. First, data masking, it helps with limiting unauthorized access to the information. Mostly in the healthcare setting it was used to make the interpretation of personal information more difficult. Second method, applying litigation towards an individual in case of them getting caught misusing the data. Stricter civil laws have been executed to penalize the violators, by this action from the organizations present a great example for all others to be more careful when dealing with someone else's personal data and to only access them when it is required (Kasperbauer, 2019).

To discuss the cultural and subcultural influence on shaping the confidential data policy is that there have been many improvements in transparency of data flow. Such as who is sharing data, who is the receiver of that data, and what is the purpose of sharing the data. This policy also creates a standard between all the user's behaviors when accessing the data.

Next, security awareness and training policies, the rapid swift in the behavior of IT firms storing most of their data digitally are making them vulnerable to hackers and identity thieves. The security awareness & training policy was established to literate all the users who are authorized to access the sensitive data about how to protect their company's confidentiality and maintain the integrity of the information.

Assistance from the security awareness and training policy has impacted several individuals and organizations in a positive manner. Organizations having their employees properly trained on security awareness. This practice ensures that organizations are following the government's security law (Wlosinski, 2019). Security awareness training has become a backbone for an organization in providing various instructions on different levels of sensitive data protection, which eventually lessens the risk of an organization from being security breached. Security awareness training delivers detailed information about different types of vulnerabilities that a user should focus on on their personal devices and computer desktops. Once they get the knowledge of types of vulnerabilities, they can make their decision on how to process to handle the issue.

The cultural and subcultural influence of security awareness and training policies is that it has become a significant part in strengthening the organization's security and privacy policies. It arranges a standard mandatory process for all the new hires to go through the security training at the time of on boarding and also for current employees to have security training periodically. Through this training, the organization is able to clearly communicate to their employees about security and privacy threats, providing them with the right point of contact details that can be used by them at the time of a security breach and get assistance from them (Wlosinski, 2019). Businesses that are complying with this policy are receiving positive recognition and enhancing their reputation in the market.

Third policy, the data breach notification law; when a business gets their security breached, they are not only getting hurt financially but also leaving a negative impression on their reputation. In the past, businesses have attempted to keep their security breach information private in fear of losing their business completely. To handle this behavior of the businesses law enforcement has introduced data breach notifications law to obligate the businesses to report all and any security breaches to the law enforcement and each party whose information has been compromised (Laube & Böhme, 2016).

The impacts of data breach notification laws have been both negative and positive. The positive is that it requires firms to share information with individuals and authorities. Sharing any details with clients, it enhances the transparency of how their data has been protected and what type of investments do the firms make on securing the data. Sharing information with the authorities can help law enforcement in making their decision about the breach, declaring the final damages, and also stop the breach on time before losing all the data completely (Laube &

Böhme, 2016). On the other hand, a negative consequence is that companies are in danger of losing a future client due to not trusting them with handling their data.

Investments in security and utilization of security breach detective devices are clear examples of the cultural and subcultural influence of data breach notification law. Businesses have started to consider investing in their security systems to securely store data. Detective control is another move that is being made by businesses. It detects any security breach and alerts the firms about reporting it to the authorities. Due to this, authorities and impacted parties get notified in no time and help them secure other information that is still not being compromised.

In conclusion, as discussed above, the social factors, social consequences, and cultural subcultural influence of these policies, I would say these policies have enhanced the data security policies of many organizations. Starting from confidential data policy that has assisted the organizations with monitoring the flow of the data. Security awareness and training policies provide a clear understanding for employers and their employees regarding potential risk and threats to the company’s networks, systems, and devices. Lastly, data breach notifications are mainly supported by all victims of identity thefts. It requires an organization to report any security breach to all impacted victims and law enforcement. All three policies address and documents many organizations intention and approach towards the security of their data.

References

Kasperbauer, T. J. (2019). Protecting health privacy even when privacy is lost. *Journal of Medical Ethics*, *46*(11), 768–772. https://doi.org/10.1136/medethics-2019-105880

Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity, 2(1), 29–41. https://doi.org/10.1093/cybsec/tyw002*

Wlosinski, Larry. G. (2019). The Benefits of Information Security and Privacy Awareness Training Programs. *ISACA JOURNAL, 1. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs*