Identity Theft

Marie Madeleine Anita Bekono

Old dominion University

CYSE-300

Joe Kovacic

12/10/2023

Identity Theft

Cybersecurity is at the forefront of this issue, making securing digital assets a significant burden for businesses worldwide. Attackers are continuously devising new ways to overcome security measures, making it difficult for organizations to keep up. Businesses spent about $45 billion on cybersecurity in 2018 alone to combat these attacks, and this figure is anticipated to climb in the coming years. Cybersecurity is a comprehensive phrase that encompasses a wide range of strategies, tools, and procedures used to protect networks, devices, and software from internal and external threats. By establishing effective cybersecurity safeguards, businesses may limit the risks of data breaches, loss of valuable information, and reputational damage.

Identity theft has become a serious concern in today's digital age and is considered a cybercrime. This unlawful behavior comprises stealing or obtaining private information from individuals or organizations, such as credit card details, passwords, and social security numbers, in order to mimic the victim for financial gain. Using the stolen information, the perpetrator may create new accounts or get access to existing ones, defrauding the victim (Smith et al., 2019). Financial losses, credit rating harm, and reputational damage are just a few of the serious consequences of identity theft. It is critical to take vigilance and put in place the necessary protections to prevent personal information from falling into the wrong hands.

Among these measures include the use of strong passwords, the avoidance of disclosing sensitive information online, and the routine checking of financial accounts.

Users, fraudsters, and irate staff may be concerned about data security. To safeguard data, network security must be implemented using a combination of rules, hardware, processes, and software that can thwart internal and external threats. For example, routinely updating operating systems and browsers can significantly reduce vulnerabilities and protect against identity theft. To increase security, choose strong and unique passwords, as identity thieves typically use personal information to guess passwords (Abomhara, 2015). Encryption can also help with identity authentication and prevent illegal data access.

When utilizing the internet, it is critical to exercise caution, especially when connecting to public networks, because attackers may use that network to grab control of computers or phones. These fundamental network security concepts can dramatically reduce the likelihood of data breaches and ensure the security of sensitive data.

Identity theft has been a developing concern since the 1960s, with new methods emerging daily. TCP/IP's development in the mid-1970s was critical in data security. TCP/IP is a set of protocols and rules that allow various networks to connect to the internet. TCP/IP's governing rules allow interconnectivity and data exchange across streams by dropping packets into a postal system that connects the sender and recipient. As a result, it is now possible for

Many people to connect online. However, hackers who perpetrate identity theft can use the same network to access computers and personal devices. As a result, it is vital to be vigilant in protecting against cyber-attacks on devices and personal information.

Obtaining someone's personal information in order to commit fraud is a serious crime punishable by law. The Identity Theft and Assumption Deterrence Act makes identity theft a federal criminal in the United States. Under the legislation, identity thieves’ risk hefty penalties, including up to five years in jail for terrorism-related offenses and up to two years for more general or petty offenses (Jorgensen, 2017). The legislation serves as a deterrent to anyone thinking about committing identity theft and underscores the government's commitment to safeguarding individuals from potentially harmful situations. Individuals must safeguard their personal information and report any suspicious activity to authorities.

Identity theft is becoming increasingly common in today's digital world, and security specialists are critical to securing both individuals' and organizations' personal data. Controlling employee computer access is an effective protective step for identity theft. The risk of unauthorized access and potential data breaches can be greatly reduced by restricting access to only the programs necessary to execute certain tasks. This can be accomplished by putting in place access control measures such as password security, two-factor authentication, and biometric identity. Employee access should be limited, and security specialists should stay current on hardware, software, and operating system improvements (Kahn et al., 2016). Security measures are ensured using the most recent technologies to protect against the most recent cyber dangers, including identity theft. Hardware and software should also be updated on a regular basis to ensure that any security holes are addressed as soon as possible. By implementing these best practices, security professionals may help prevent identity theft and ensure the security of sensitive data.

To summarize, identity theft is one of the most common sources of financial loss in enterprises. If businesses want to prevent such crimes in today's world, when technology is fundamental to business activities, they must develop cutting-edge cybersecurity defenses. Companies must invest billions of dollars in cutting-edge technology to protect their clients' data and deter identity thieves from stealing personal information.

Businesses can avoid potential financial or reputational harm from a security breach by upgrading and investing in current technology. Businesses must recognize the significance of cybersecurity and take the necessary actions to protect themselves and their consumers.

References

Jorgensen, J. W. (2017). U.S. Patent No. 9,712,289. Washington, DC: U.S. Patent and Trademark Office.

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication, and Ethics in Society, 17(1), 42-60.

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security matter? Journal of Financial Services Research, 50(1), 121-159.

Abomhara, M. (2015). Cyber security and the Internet of things: vulnerabilities, threats, intruders, and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.