Information Security Systems and Threats

Ryan Woodard

Old Dominion University

Cyse 200T

Professor Christopher Bowman

04/23/2023

Introduction

Information security is a critical issue that organizations and individuals must pay close attention to in today's digital age. Cyber threats, cyberstalking, and cyber harassment are some of the key challenges that people face. The information security triad includes confidentiality, integrity, and availability. Authentication, multi-factor authentication, encryption, and backups are essential elements of information security systems. Firewalls and physical security are also necessary for protecting an organization's data. Phishing attacks are a common form of cyber threat that people face, and it is important to be aware of their dangers. Cyber stalking and harassment are key issues that people face, and they can cause long-lasting damage. In this essay, we will combine and revise the discussions on information security systems, cyber threats, and cyberstalking/cyber harassment to provide a comprehensive understanding of these issues.

Information Security Systems

Information security systems refer to the various measures organizations and individuals can take to protect their sensitive data from unauthorized access, use, disclosure, or destruction (Szczepaniuk et al., 2020). The information security triad includes confidentiality, integrity, and availability. Confidentiality ensures that information is only accessible to those authorized to view it. Integrity means ensuring that information is not altered or tampered with and serves its intended purpose. Availability refers to ensuring that those with the appropriate authorization can access information. Authentication is a critical element of information security systems, and it refers to the process of verifying that the person behind the computer screen is who they claim to be. Multi-factor authentication is a more secure method that uses two or more factors, such as something a person knows, something they have, or something they are, to verify their identity. Role-based

access control is another essential element of information security systems, and it involves assigning roles to users and then assigning access based on those roles.

Encryption is another critical element of information security systems. It involves converting information into a coded form during transmission or storage to ensure that only authorized individuals can access it (Hwang et al., 2021). Pretexting is a cybersecurity threat, and it involves a hacker calling an IT helpdesk and pretending to be an authorized user to gain access to sensitive information. Backups are important because they protect in case of a cybersecurity breach. A good backup plan should include where and what information is being stored, consistent backups, and storage of backup data different from where the primary data is stored. Firewalls are another essential element of information security systems, and they provide an additional layer of protection for an organization or company. They can operate as hardware, software, or both and filter packets based on a set of rules. Physical security is also important for protecting an organization's data, and it involves protecting the hardware and networking components that store and transmit information resources.

Cyber Threats

Cyber threats are malicious activities by cybercriminals to gain unauthorized access to sensitive information, steal data, or cause damage to an organization or individual (Kaloudi & Li, 2020). Phishing is a common form of cyber threat, and it involves sending a malicious email or text message from an anonymous domain to entice a person to click on a link. If a person clicks on the link, the hacker may install Malware on their device, access personal information, or carry out a ransomware attack. Phishing attacks are becoming more sophisticated, and attackers use social engineering tactics to exploit human curiosity, fear, and gullibility. Training and phishing awareness is essential to ensure that individuals can recognize a deceitful email or message and

know how to handle the situation. Changing passwords regularly, ensuring devices are up to date, and installing antivirus software are ways individuals and businesses can protect themselves from phishing attacks.

In addition to phishing attacks, there are other types of cyber threats that individuals and organizations should be aware of. Malware is a type of software designed to damage or disrupt computer systems, and it can be spread through email attachments, downloaded files, or malicious websites (Wagner et al., 2019). Ransomware is a type of Malware that encrypts files on a victim's device, making them inaccessible, and then demands payment in exchange for the decryption key. Distributed denial-of-service (DDoS) attacks are another type of cyber threat that involve overwhelming a target website or server with traffic, causing it to crash and become unavailable to users. To protect against these cyber threats, individuals and organizations should implement strong security measures, such as firewalls, antivirus software, and intrusion detection systems. Regularly updating software and systems, using strong passwords, and limiting access to sensitive information can also help to prevent cyber-attacks. Individuals and organizations must remain vigilant and stay informed about the latest cyber threats and security best practices to ensure their data and systems remain safe and secure.

Cyberstalking/cyber harassment

Cyber stalking and cyber harassment are malicious activities that involve using technology to harass, intimidate, or threaten an individual. Cyberstalking can involve unwanted communication, monitoring, or surveillance, and it can cause significant emotional distress for the victim (Stevens, Nurse, & Arief, 2021). Cyber harassment involves using technology to harass or bully an individual, and it can take many forms, including trolling, doxing, and revenge porn. The effects of cyberstalking and harassment can be devastating and long-lasting, and victims may

experience anxiety, depression, and even suicidal thoughts. Individuals need to take steps to protect themselves from cyberstalking and harassment, such as limiting the amount of personal information they share online, blocking or reporting any harassing or threatening messages, and seeking support from friends, family, or professionals if necessary.

Organizations also have a responsibility to protect their employees from cyberstalking and harassment. They can do this by establishing clear policies and procedures for dealing with these issues, providing training and awareness to employees, and taking appropriate action against perpetrators. In addition to the personal and emotional toll that cyberstalking and harassment can take on individuals, it can also have significant consequences for businesses and organizations. Cyberstalking and harassment can lead to lost productivity, decreased employee morale, and damage to the organization's reputation. It can also result in legal liability if the perpetrator is an employee or if the organization fails to take appropriate action to address the issue.

To prevent cyber stalking and harassment in the workplace, organizations should implement a zero-tolerance policy for such behavior and establish clear guidelines for reporting and addressing incidents. This includes training and awareness to employees on what constitutes cyberstalking and harassment, how to recognize it, and what steps to take if they experience or witness it. It is also important for organizations to have a clear and confidential reporting system in place and to take swift and appropriate action against any perpetrators. Information security, cyber threats, and cyberstalking/cyber harassment are critical issues that individuals and organizations must address in today's digital age. By implementing strong information security systems, raising awareness about cyber threats, and preventing and addressing cyberstalking and harassment, we can protect ourselves, our businesses, and our communities from harm.

Conclusion

In today's digital age, information security, cyber threats, and cyberstalking/cyber harassment are critical issues that individuals and organizations must pay close attention to. Information security systems such as authentication, encryption, backups, firewalls, and physical security are essential for protecting sensitive data. Cyber threats such as phishing attacks are becoming more sophisticated, and individuals and organizations must take steps to protect themselves from these malicious activities. Cyberstalking and harassment are also significant issues that can have long-lasting effects on victims, and individuals and organizations need to take appropriate steps to prevent and address these incidents. By being aware of these issues and implementing appropriate measures, individuals and organizations can better protect themselves and their sensitive information from cyber threats and attacks.

References

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. Computers & Security, 90, 101709.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345-356.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34.

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589.

Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367-376.