7-2 Project Three: Service Level Agreement Requirement Recommendations

Joshua Merren

Southern New Hampshire University

CYB-260-11229 Legal and Human Factors of Cyb C-3

Professor Jimmy Harvey

18 June 2024

Implementing a standard of regular security audits and assessments is crucial for proactively identifying and addressing vulnerabilities within the organization's IT infrastructure. This standard involves conducting regular security audits and assessments to proactively identify and address vulnerabilities within the organization's IT infrastructure. Establishing this standard is essential because it allows the organization to evaluate the effectiveness of existing security measures and identify areas of improvement. These audits will include thorough reviews of the systems and procedures related to data protection, access controls, and incident response capabilities. By routinely assessing the security landscape, the organization can avoid potential threats, including social engineering tactics that often exploit overlooked weaknesses. Additionally, these audits will help ensure that all security protocols are current and in line with industry best practices as outlined in CIS Control 20, Penetration Tests, and Red Team Exercises (Center for Internet Security, 2021). The aim is to create a resilient environment where security measures are continuously refined and reinforced, directly contributing to a robust defense mechanism against cyber threats. This proactive approach mitigates the risk of security breaches and aligns with regulatory compliance requirements, safeguarding the organization's reputation and operational integrity.

The organization will strengthen its defense against attacks by establishing detailed incident response and reporting procedures. This procedure provides employees with a clear and structured approach to follow when they suspect a social engineering attack. It provides instructions on reporting possible security incidents to the IT security team, along with essential details like what information needs to be supplied and how to keep track of

any proof of the attack. This is vital because a quick and organized response to suspected attacks can significantly reduce the potential damage. By having these procedures in place, the organization ensures that employees know exactly what to do and whom to contact, enhancing the speed and effectiveness of responding to security incidents. The procedure also aligns with CIS Control 19, Incident Response and Management, ensuring the organization is prepared to handle incidents promptly and efficiently (Center for Internet Security, 2021). A well-defined incident response procedure reinforces the importance of security within the organization and ensures compliance with security best practices.

A training program focusing on social engineering is necessary because these types of threats specifically target human vulnerabilities, often the weakest link in cybersecurity defenses. Social engineering attacks are designed to trick employees into giving away sensitive information or gaining unauthorized access, and they are becoming increasingly sophisticated. The training program will educate employees on the various forms of social engineering and teach them to be skeptical of unexpected requests for information or urgent demands. It will also encourage them to double-check the sources of suspicious messages. This training is crucial for preventing potential breaches if employees are unprepared. The program will include practical examples and simulations to ensure employees can apply what they have learned in real-world scenarios. Employees need to understand attackers' tactics and follow safe practices to better protect themselves and the organization from security threats.

The expected outcomes of implementing a targeted training program on social engineering are significant. Firstly, the program aims to reduce the number of security incidents related to social engineering by increasing employee awareness and preparedness. Employees trained to recognize the signs of social engineering attacks are less likely to fall victim to them. Secondly, the training will help to establish a proactive security culture where employees are encouraged to share their knowledge and experiences with their peers, further strengthening the organization's defenses. Another critical outcome is improving the organization's ability to respond quickly and effectively to threats, minimizing potential damages. Over time, this training will lead to heightened security awareness among employees, making the organization a more challenging target for cyberattacks. This proactive approach helps protect sensitive information and enhances the organization's reputation as a secure and responsible entity.

References

Center for Internet Security. (2021). CIS Controls, Version 8.

https://www.cisecurity.org/controls/v8/