Short Research Paper #2

Zyron Sumulong

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

May 28, 2023

The purpose of this security policy will provide a foundation that outlines the corporation's approach to information security. The objective of this security policy is to protect information assets, mitigate risks and vulnerabilities, and enable incident response and recovery. The five significant issues that are addressed within this security policy are information classification, security awareness training, access control, encryption, and security incident management.

Information classification refers to the process of categorizing and labeling information based on its potential impact on the corporation's security. As the corporation handles enormous amounts of information, not all information has the same classification. Significantly, each information asset is assessed on the impact it can have if compromised. In doing so, the appropriate security controls can be implemented to safeguard the different kinds of classifications within each data. Businesses are informing which information must be protected with high priority, thereby deciding where to spend the information security budgets (Simplilearn, 2023). This benefits the corporation by optimizing risk and resources. Within reviewing information classification, employees will have the knowledge of how to handle, access, store, transmit and dispose of different types of information.

85% of data breaches are caused by human error, that's why we often hear that humans are the "weakest link" in security (Tessian, 2022). This statistic highlights the importance of creating an effective security awareness program to educate individuals on cybersecurity. Security awareness training can address the various security incidents that can occur throughout the corporation. This will promote a culture centered around cybersecurity to protect information assets and prevent security incidents. Employees will learn the best cybersecurity practices for keeping information secure. Implementing an effective training program will reduce any cyber risks, thus meaning fewer financial losses to the corporation.

Access control encompasses the two key elements of authentication and authorization, to protect systems from unauthorized access. Authentication refers to the verification of the identity of an individual. While authorization refers to the process of verifying what data the individual can access. When authentication is successful, access control systems can then authenticate and grant access to the individual via password, pin, encryption, keys, smartcards, and fingerprints to the resource they're looking to gain access to (Premier IT Solution, 2021). Administrators assign specific user roles and permissions to employees depending on what information they are authorized to access. Access control is a valuable security technique that can be used to regulate who or what can view or use any given resource (Premier IT Solution, 2021).

Encryption is a security measure that protects sensitive data from unauthorized access. Encryption protects sensitive data by using an encryption key that transforms plaintext (readable data) into ciphertext (unreadable data) using algorithms. The ciphertext is then converted to plaintext with a decryption key. Satori Cyber (2022), states that the best practice for data protection requires encryption of data at rest and in motion. Encryption at rest refers to a type of encryption for data when it is being stored in a system. While encryption in motion refers to the process of encrypting data while it is being transferred over a network between two devices.

Security incident management is crucial for any potential security breach within the corporation. As it outlines how to prepare, identify, manage, analyze, and recover from any security threat. By creating an incident response team, Lord (2022) states that they can analyze the incident to determine its scope, assess damages, and develop a mitigation plan. If a security incident is to occur, the corporation will have the knowledge and resources to minimize the impact of the incident and protect the corporation's reputation.

The security policy serves as a foundation for the corporation's commitment to information security, and expectations for employees and provides a guideline for information security. It will create a cybersecurity-conscious environment within the organization and help protect sensitive data, assets, and operations. The implementation of

this security policy will result in improved data security, increased user awareness, and a decrease in security incidents.

References

Lord, N. (2022, December 28). *What is Security Incident Management? The Cybersecurity Incident Management Process, Examples, Best Practices, and More*. Digital Guardian. https://www.digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process-examples-best

Premier IT Solution. (2021). The Important Of Access Control. *Premier IT Solution*. https://premieritsolution.co.uk/the-important-of-access-control/

Satori Cyber. (2022, December 5). *Data Security Policy: Why It's Important & How to Make It Great*. Satori. https://satoricyber.com/data-security/data-security-policy-why-its-important-and-how-to-make-it-great/

Simplilearn. (2023). Information Classification in Information Security. *Simplilearn.com*. https://www.simplilearn.com/information-classification-article

Tessian. (2022, March 29). *The Psychology of Human Error 2020 - Tessian*. https://www.tessian.com/research/the-psychology-of-human-error/