Important Issues to Be Addressed In System Security Policies

Samantha Riggs

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

September 15, 2024

There are many factors that go into the creation and implementation of corporate information system security policies. These policies will ensure the security and confidentiality of sensitive information present within the system. Due to this, these policies must be carefully created by considering the different areas of a system's security that could potentially hold vulnerabilities.

The first issue to be addressed within a security policy is the need for management of security threats present in the organization. The main goal of an incident response policy should be to prevent cyberattacks before they happen. This also includes determining the organization's response to the incident so that any potential disruptions or cost is minimized. "An effective incident response plan to help cyber incident response teams detect and contain cyberthreats, restore affected systems and reduce lose revenue, regulatory fines and other costs." (Holdsworth, Kosinski 2024).

The next issue to be addressed is the management of an organization's data. Data protection is essential for any organization that holds any kind of sensitive data. In this policy it is important to consider the CIA Triad, which stands for confidentiality, integrity, and accessibility. A policy surrounding data protection should focus on the reduction of risk concerning the potential for a data breach.

The third issue, especially in today's rapidly changing technological environment, is the need for a remote access policy. With the rising number of employees who work remote from home it is important to consider the security of an employee's unsecured personal devices and network. An organization that utilizes remote work requires a policy that addresses these issues and helps ensure that their systems are kept safe from a data breach or other malicious attack.

When considering the organization as a whole, the issue of network security is presented. A policy that addresses this issue should “outline principles, procedures, and guidelines to enforce, manage, monitor, and maintain data security on a corporate network.” (Khachatryan 2024). An organization’s network security should be properly maintained in order to prevent or mitigate attacks.

The last issue that should be addressed when creating security policies is the need for security awareness and training among the employees of an organization. It is important for all employees, not just the ones involved with information technology, to be aware of and be able to address security concerns. The policy created in response should require security training in order to educate employees with knowledge of common security vulnerabilities and how to prevent easily avoidable attacks methods such as phishing.

References

Khachatryan A. (2024, April). *10 Information Security Policies Every Organization Should Implement.* Ekran. https://www.ekransystem.com/en/blog/information-security-policies

Holdsworth J., Kosinski M. (2024, August) *What is incident response?*. IBM. https://www.ibm.com/topics/incident-response