Brendo Pierce

CYSE 300 – Professor Kovacic

Spring 2023

Short Research Paper 2

System security policies have been relied on in multiple organizations in order to keep data and information of those companies protected. Despite the policies being put in place for employees and staff to follow to keep organizational information safe, there are still threats and malicious attacks that companies face. These protocols serve little help if the employees don't follow what is instructed, which is the main reason for companies to encounter threats in the first place (Ifinedo, 2014). This research paper will discuss the significance of information system security policies, and analyze the five most important information security system policy issues.

The first information system security issue is the access control, which is the staff in charge of who gets access to certain information and facilities. When an employee obtains access to sensitive information and manages to mess something up, then that's when the following issues occur most of the time.

Data protection is maintaining the confidentiality and privacy of sensitive information while adhering to privacy regulations. Data protection becomes an information system issue not only when the security is being compromised, but when staff don't comply with the protocols in ensuring its protection.

Cybersecurity is the protection against external threats such as cyberattacks to ensure information confidentiality, integrity, and availability (CIA). Similar to data protection, when staff do not follow the correct procedures to enable cybersecurity protocols, cybersecurity is weak in terms of protecting company information.

Risk management is being able to recognize and minimize potential and future information system security risks. Risk management becomes an issue when a company is potentially exposed to risks or weaknesses that could harm its data and information systems, and

those in charge do a poor job alerting the company of the weaknesses to proceed with the next protocol.

The last information system security issue is incident response. Incident response is having a plan established in order to minimize any damage or data lost/ stolen. Incident response teams rely on the staff that is in charge of the previous security issues above, meaning that for these employers to do their job correctly, the entire staff has to follow proper procedures correctly.

References

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management, 51*(1), 69-79.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.