Formulating the Right Security Policy

CYSE 300 – Professor Kovacic

Brandon Creech

Old Dominion University

Formulating the Right Security Policy

When it comes to safeguarding sensitive data within an organization, organizations have to be wary of the vulnerabilities that exist that can potentially expose it to malicious threats. An important objective of operating in an organization is having a security infrastructure built around preparedness and efficiency. Because of this, security policies are necessary to protect the sensitive data that exists and addresses issues within cybersecurity that can help the organization achieve optimal security. This brief research paper will provide an overview of a designed security policy that addresses five important security policy issues, leading to an optimal corporate information system.

The first important issue that will be addressed in the security policy is data breach response. A data breach attack on an organization can be deadly when action is not taking fast enough, and it is even worse when there is a lack of preparedness for such an attack. That is why developing a data breach response plan can mitigate this issue, where the organization will be promptly ready for an attack and respond swiftly and efficiently when it does happen. Procedures such as “breach notification, steps for containment and eradication, and preventing future incidents” outlined by Tori Thurmond can result in a lessened impact of a data breach (Thurmond 2024).

Another important issue to address would be cybersecurity awareness training. The training can best be defined as the functionality of the whole organization and that employees are the best asset to security (Richardson). When employees are put into the field of cybersecurity, they are expected to be able to adequately provide security and understand what to do in key situations, especially with cyberattacks. If an employee were to lack the understanding of what to do and how to properly prevent cyberattacks, it can lead to more problems. Providing efficient

awareness training such as how to monitor for signs of weakness in security infrastructure and ensuring that everything in the systems is up to date can prevent the inevitable.

Mismanagement in an organization can lead them to being more susceptible to a cyberattack. They are less likely to be prepared for one when everything is not in order and changes in the infrastructure are not tracked. Similar to the Security Awareness and Training Policy listed by Adsero Security, understanding what changes are made and by who can lead the employees to better understanding what was the potential cause of a cyberattack and then they can rollback on it. Implementing a policy that combats this issue can help teach employees to "recognize changes in technology that impact security and the organization (Adsero Security).

The last two important security policies that would be worth combating are ensuring security controls are handed to the right people and backing up data. Cyberattacks are not always external but sometimes it can happen within the organization, which is why it is important that security controls are handed to authorized IT employees. It also lessens the chances that an inadequate employee with low experience causes a mistake in the security systems. These kinds of duties should be paired along with ensuring that sensitive data is constantly being backed up in case of emergencies or natural disasters that will shut down infrastructure. Commvault recommends that it is a good idea to supplement this by having two copies of data, one that is easily accessible such as in the workplace and on a cloud service where no matter what happens, the data will still remain there (Commvault).

In conclusion, designing a security policy for the corporate information system based on these five important issues will prove effective in defending sensitive information against cyberattacks. The security policy will need to address: responding to a data breach, providing adequate security training to employees, tracking changes in security infrastructure, proper

security controls, and frequent data backups. With the constant loom of cyberattacks on the rise, it is important for the organization to face the most common issues that weakens them the most, which will in turn help strengthen their corporate information system.

References (APA)

Thurmond, T. (2024b, February 6). *15 Information Security Policies Every Business Should Have*. KirkpatrickPrice. https://kirkpatrickprice.com/blog/15-must-have-information-security-policies/

Richardson, R. (n.d.). *Cybersecurity Training for Employees: Best Practices to Follow - Tech Heads Inc.* Cybersecurity Training for Employees: Best Practices to Follow - Tech Heads Inc. https://blog.techheads.com/cybersecurity-training-for-employees-best-practices-to-follow

10 Must Have IT Security Policies for Every Organization. Adsero Security. (2024, January 23). https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/

What Is Backup Policy? Definition, Benefits & Solutions. Metallic. (n.d.). https://metallic.io/knowledge-center/glossary/backup-policy