Cyber-Security Policy

Brandon J. Tenn

Cyber-Security Policy

 Keeping up to date with software is not something that should be over looked. Each new patch will fix issues and possible exploitations in the software. Some of these issues can be just the vulnerabilities that a hacker needs to perform a cyber-attack.

Having strong passwords is a must for everyone working in the company. Since many cybercriminals have various methods to crack weak passwords, such as dictionary words and brute force attacks. With better and more security centric passwords, hackers would find it very difficult crack passwords and acquire employees’ credentials. In addition, changing passwords every three months is a requirement.

Arguably, the most important thing to have in the information systems policy is training regarding cyber security awareness. If this is not prioritized, then this will be a huge risk to security. An outsider can gain access to the server though one out of the many employees who are not being vigilant against phishing emails and ransomware attacks. In this regard, training is paramount!

There also has to be measures in place to mitigate damages and enforce stringent access after a breach has occurred as this will help to ensure that the damage caused can be keep at an absolute minimum. Immediate actions that should be performed are reporting to supervisors, reporting to upper management, and finding out what type of sensitive data was accessed and/or stolen.

There has to be rules regarding workstation safety. This should definitely include actions such as always logging out when leaving work desk for any period of time. Practicing this will help prevent insider threat where hackers pay or convince someone from the company to give them access to their account or give the credentials of other employees when they are not paying attention their workstations.

References

Ameen, N., Tarhini, A., Shah, M., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, 106531.

Photopoulos, C. (2008). Managing Catastrophic Loss of Sensitive Data [electronic Resource].