Ronald W. Sudol III

SNHU CYB200

Project One

08/06/2023

**Security Awareness Training Case Study**

Fizz Cola is right to address security concerns not just from a hardware point of view but also from a security awareness point of view. Robust and well-defined security training coupled with cultivation of a proactive security mindset will promote a secure and efficient work environment free of unnecessary or unmitigated risk.

Human factors need to be considered when addressing security training. People are frequently busy at work, and they may not understand how their roles and responsibilities can directly affect a company’s overall level of security. By defining the frequency of mandatory security awareness training and keeping track of attendance, a company can ensure that employees are receiving training. By further defining the audiences for training sessions, a company can ensure that employees are receiving a level of security training appropriate for their position in the company.

Legal factors should also be considered. Security training is mandated under The Federal Information Security Management Act of 2002. “Agencies must train employees and any other users of their IT systems, including contractors, to make them aware of risks to the agency’s IT systems as well as making them aware of their duties to protect these systems”( Kim & Solomon, 2010). Security awareness at the user level can help protect trades secrets and sensitive information and as such is essential for adequate security compliance. Furthermore, The Sarbanes-Oxley Act of 2002 requires that “Financial reports, records, and data are accurately maintained”( Kim & Solomon, 2010). Breaches of financial systems and data can cause the integrity of that system to be drawn into question and affect a company’s compliance status.

A proactive security mindset promotes the overall security of a system or company. Many attacks rely on end user error or deception to breach basic security measures. By pre-emptively raising security awareness within an organization, the effectiveness of attacks like phishing are reduced proportionally to how well the end user can identify these attempts. Even small passive gestures like signs reminding users to lock workstations or brief security newsletter emails can help to promote security culture and keep end users on guard.

**CITATIONS:**

Kim, D., & Solomon, M. G. (2010). *Fundamentals of Information Systems Security*. https://openlibrary.org/books/OL25116284M/Fundamentals\_of\_information\_systems\_security

*A Taxonomy of Operational Cyber Security Risks Version 2*. (2014b, May 21). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91013