**Project One:**

**Fundamental Concepts of Legal and Human Factors**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

April 14, 2024

**Security Awareness Training Case Study**

1. Identify security gaps or opportunities in training related to **human factors**. Describe the impact associated with not addressing each gap or opportunity to individuals and the organization.

A security gap at Fizz Cola is that the frequency of mandatory security awareness training is currently undefined. I will set mandatory security training bi-annually because according to Tan Soon Chew (2023) “at four months after initial training, employees are still able to spot phishing emails, but after six months, they start to forget what they have learned.” Another security gap is the audience of the training is undefined. The security awareness training should be made mandatory for all employees. Not addressing this security gap would leave training to be conducted at random times which may be too frequent or too long. Security training all employees helps gain the support of every individual at the company who then become security advocates who are motivated to comply with the policies and are more careful to avoid security breaches (Kim & Solomon, 2023, pg. 307). The areas the training should focus on are common attacks such as phishing, weak passwords, and installing rogue software that are most used by attackers as well as any specific attacks that have been happening to the company. For example, Fizz Cola has been seeing phishing emails that resulted in malware being installed on their systems. The training should have a strong focus on phishing attacks to help employees become more aware and spot any phishing attempts. Not implementing common attacks or relevant attacks used would make the training useless and wouldn’t help improve any security changes in the organization. Areas of the awareness training that are missing are the “requirements and expectations of the organization’s security policies” (Kim & Solomon, 2023, pg. 307). Making this clear to employees will help them comply with security controls if they know the policy states it. Another area where the awareness training is missing is explaining the penalty or each security violation. This will help motivate employees to be more aware of causing a human error if they know there is a possibility of losing their jobs as a penalty.

1. Identify security gaps or opportunities in training related to **legal factors**. Describe the impact associated with not addressing each gap or opportunity to individuals and the organization. *Note:* You do not need to quote specific laws here; focus on the concepts.

A security gap at Fizz Cola related to legal factors is ensuring the organization is responsible for protecting the property and any personal or private data they handle. Various laws such as CIPA/FERPA, FISMA, SOX, HIPAA, GLBA, and PCI DSS require organizations to use security controls to protect private and confidential data (Kim & Solomon, 2023, pg. 11). Not following these laws can lead to severe legal action being taken on the organization causing risk in reputation, financial stability, and long-term sustainability. A security opportunity in training related to legal factors is inclusion. Mandating the training for all employees, the training must be made available, legible, and appropriate for people of different backgrounds, cultures, and ethnicities. For example, the training must be available in different languages and not discriminate against any race, gender, religion, or disability. Tailoring the security training to support diversity and inclusion will help make everyone feel included and avoid potential legal factors.

1. Explain why a **proactive security mind-set** is beneficial for all levels of the organization. Provide examples that support your explanation.

Having a proactive security mind-set is beneficial for all levels of the organization because it helps employees to be prepared, resilient, and aware of security threats. Having a proactive mind-set to security, employees at every level can identify potential risks, implement preventive measures, and respond swiftly to security incidents before they escalate. Taking a proactive approach at all levels also increases the entire organization’s ability to protect assets, data, and comply with regulatory requirements. A proactive mind-set also reduces the chance of having human error causing a leak or attack on the organization. For example, if Fizz Cola conducts regular security audits and tests to identify weaknesses in its IT systems, then they can identify vulnerabilities, can implement patches, conduct updates, and add additional security controls to strengthen its defenses and mitigate the risk of attacks. It is always better to be prepared than to be caught off guard. Meaning being prepared can help avoid the amount of damage caused from an attack compared to being caught off guard and suffering from damage that is not recoverable or able to be fixed.

**Reference**

Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. https://openpage ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST3209 3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1