Southern New Hampshire University

Project One: “Security Awareness Training”

Written By: Max Navarrette

Course: CYB-200-J9875 Cybersecurity Foundations 24EW4

Professor: Robert Brickan

Southern New Hampshire University

CYB 200 Project One Scenario One

Fizza Cola, a popular soda manufacturer, is an international leader in soda production. The company has also been instrumental in developing a lot of the most recent technology used in the bottling industry. However, given the financial growth Fizza Cola has recently experienced, there have been growing concerns surrounding minor security incidents. Recently, Fizza Cola has experienced phishing emails that have resulted in malware being installed onto computer workstations. Executives are most concerned with trade secrets and copyright infringement laws dealing with intellectual property. The executives have already implemented new technology (hardware) to help combat cyber threats in general, and they now want to invest in making their employee training more robust. As part of the information security team, you are being asked to evaluate the organization's approach to cybersecurity awareness and training. The executives have provided the following list of questions and concerns:

- The frequency of mandatory security awareness training is currently undefined.
- The audience of the training is currently undefined.
- What are the most important areas to focus on in the security awareness training?
- What areas of the awareness training are missing that, if present, would help limit the security issues the company is currently experiencing?

Southern New Hampshire University

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.

The absence of a defined frequency for security awareness training at Fizza Cola represents a critical human factor gap. Employees' abilities to identify and respond to cyber threats hinge on regular and comprehensive training or reminders along with condensed charts to help remind staff of the organization of what to look out for when identifying cyber threats to maintain a basic security posture. For instance, the increasing sophistication of phishing attacks requires the staff to at least recognize subtle cues, such as slight inconsistencies in email addresses or unexpected requests for sensitive information (Kim & Solomon, 2023a, pp. 72–113). Without this knowledge, employees might fall victim to such scams and, due to a lack of understanding of the protocols for reporting potential breaches, exacerbate the security incident by failing to alert the IT department promptly. Moreover, by not specifying the audience for the training, Fizza Cola misses the opportunity to tailor the training content to the needs of different departments. A one-size-fits-all approach may not adequately address the specific vulnerabilities each department faces. For example, the marketing team should be educated on the risks associated with social media interactions and brand impersonation. At the same time, the research and development department should be made aware of the dangers of industrial espionage and the importance of protecting trade secrets (Kim & Solomon, 2023b, pp. 414-430). A robust training program should incorporate simulations and scenario-based exercises that reflect real-world threats. These hands-on experiences can be far more effective than traditional lecture-based training in preparing employees to recognize and react to cybersecurity incidents. For instance, simulated phishing exercises can train employees to scrutinize emails critically and test their reflexes in reporting potential threats. Such practical training can solidify the theoretical knowledge imparted during training sessions and lead to an organization-wide, more resilient security posture. Fizza Cola's security awareness program must be strategically designed to include regular, role-specific training incorporating interactive and practical elements to combat the evolving threat landscape effectively. Additionally, it should establish clear protocols for reporting and responding to security incidents, emphasizing the collective responsibility of all employees to uphold the organization's cybersecurity (Levin et al., 2007).

2. 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.

Fizza Cola's cybersecurity training program exhibits significant gaps in legal education, which could leave the company vulnerable to non-compliance with data protection and intellectual property laws. Comprehensive training should convey the critical nature of observing legal standards, emphasizing protecting sensitive data as a legal obligation with severe consequences for non-compliance (Levin et al., 2007). The training should detail specific legal frameworks such as the General Data Protection Regulation (GDPR) in the European Union, which imposes hefty fines for violations, and the U.S. Defend Trade Secrets Act (DTSA), which provides remedies for the theft of trade secrets. Using case studies like the Target data breach of 2013, which resulted in a $18.5 million settlement with several states (Kim & Solomon, 2023a, pp. 72–113), can demonstrate the direct impact of legal non-compliance on a company's finances and reputation. These case studies should be complemented with scenarios that employees might encounter, such as handling requests for sensitive data without proper authorization, to illustrate the importance of legal compliance in their roles.

Furthermore, training should cover the processes for reporting and responding to potential breaches, referencing protocols mandated by laws like the Health Insurance Portability and Accountability Act (HIPAA), which requires prompt notification of breaches affecting healthcare information. Lastly, the training should encourage understanding the global legal landscape, as cyber threats do not respect geographic boundaries. Discussions about the extraterritorial implications of laws like GDPR and how they apply to multinational corporations can prepare Fizza Cola's employees to handle data responsibly across jurisdictions. Fizza Cola's employee training should blend legal theory, case study analysis, and practical exercises that build a robust understanding of the legal aspects of information security, ensuring compliance and mitigating the risk of legal entanglements.

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

A proactive security mindset is crucial for safeguarding an organization against cyber threats. This approach involves anticipating potential security incidents and establishing preventative measures. At the operational level, fostering a culture of vigilance where employees actively report suspicious behavior can significantly reduce the risk of successful attacks. Benzel et al. (n.d.) advocate for employee empowerment as a critical defense against cyber threats. For instance, training initiatives that simulate phishing scenarios can effectively prepare employees to recognize and respond to such threats, thereby reinforcing the company's human firewall. Mid-level managers play a pivotal role in implementing proactive security measures. They must ensure that their teams adhere to best practices, such as applying patches and updates to mitigate known vulnerabilities often exploited by attackers (Kim & Solomon, 2023a, pp. 72–113). Regular security audits and risk assessments can also help identify potential weaknesses before adversaries exploit them. At the executive level, a proactive mindset means prioritizing cybersecurity in strategic planning and resource allocation. Leaders must advocate for sufficient budgeting to adopt advanced security technologies, such as machine learning algorithms that detect anomalous patterns indicative of a breach (Navarrette, n.d., pp. 1–17).

Additionally, executives must ensure the organization maintains an updated incident response plan, which could include conducting tabletop exercises to simulate a cyber crisis management (Kim & Solomon, 2023b, pp. 414–430). Cross-department collaboration is also vital in a proactive security strategy. Information sharing between departments can lead to quicker identification of threats and a more coordinated response. For example, the IT department could work with human resources to tailor security training that addresses the specific needs of different employee groups. A proactive security approach extends to the organization's supply chain. Ensuring suppliers and partners adhere to strict security standards can prevent breaches that originate outside the organization but have internal consequences (Kim & Solomon, 2023a, pp. 72–113). A proactive security mindset at all organizational levels, encompassing front-line employees, management, and executives, is fundamental in building a resilient cyber defense. This collective approach ensures that cybersecurity is not just an IT issue but a strategic priority that aligns with the organization's broader objectives.

References:

University, S. N. H. (n.d.). *CIA Triad and Fundamental Security Design Principles* (pp. 1–3). SNHU. Retrieved March 14, 2024, from https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/22533,-1/

Benzel, T. V., Irvine, C. E., Levin, T. E., Bhaskara, G., Nguyen, T. D., & Clark, P. C. (n.d.). *Design principles for security* (pp. 1–28). Secure Core. https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/21566. Secure Core Technical Report | ISI-TR-605 | NPS-CS-05-010 .

Kim, D., & Solomon, M. (2023a). *Fundamentals of information systems security* (4th ed., pp. 1–574). Jones & Bartlett Learning. Chapter 3: Risks, Threats, and Vulnerabilities pp.72-113.

Kim, D., & Solomon, M. (2023b). *Fundamentals of information systems security* (4th ed., pp. 1–574). Jones & Bartlett Learning. Chapter 13: Information Security Standards pp. 414-430.

Levin, T. E., Irvine, C. E., Benzel, T. V., Bhaskara, G., Clark, P. C., & Nguyen, T. D. (2007). *Design principles and guidelines for security* (pp. 1–34). NAVAL POSTGRADUATE SCHOOL . https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/21566. Technical Report: NPS-CS-0 7-0 14, ISI-TR-6 48.

Navarrette, M. A. (n.d.). *Cybersecurity Playbook* (SNHU Edition, pp. 1–17). Template Provided by: Sothern New Hampshire University Professor: Robert Brickan Course: CYB-200-J9875 Cybersecurity Foundations 24EW4.