Security Awareness Training  
CYB 200 Cybersecurity Foundations

Wesley Kuzma

Southern New Hampshire University

Fizza Cola, a popular soda manufacturer, is concerned about the security education in the company since recently they experienced a threat via phishing emails that contained malware and were installed in the workstation computers. Fizza Cola acted and implemented a new and sophisticated technology to help them combat these types of threats, but even if they have the latest technology, Fizza Cola knows that if employees are not educated properly, cyber-attack will still be a regular issue.

As part of the information security team, my job is to educate and train the employees about cybersecurity awareness. First, identify the level of training in the company that will be the focus of quarterly speeches, including a general speech for the whole company. This will provide general knowledge to the audience and room meetings with each department can help them to concentrate on what kind of vulnerabilities they could be more exposed to.

Frizza Cola will need to create a familiar environment where everyone can get familiar with different members of the company, so a physical attack would be prevented since most of the members are familiar with each other. Knowing who you work with will create a much more secure workspace. Each time that any staff member leaves their workstation, it needs to be locked and any type of paperwork should be locked or put away.

Since the management level has privileged information within the company, they are more vulnerable to being hacked by a malicious user, for this, the management team will need to be monitoring their workstation to prevent a leak of information of any type. If any member of management is not at their office, the office should be closed and locked.

The Legal System is strict about data storage and usage, to prevent any problem, Frizza Cola will need to implement their policy at a zero-tolerance level, since if there is any issue that involves Frizza Cola and their customer data, the legal consequences are going to have a huge impact in the company. The legal system is in charge of making companies hold companies accountable for any data breach, which also enforces better methods to secure information in their networks. As technology progresses, companies need to implement more sophisticated equipment and training in the companies to step forward and lower their legal issues.

A proactive security mid-set will prevent many breaches or vulnerabilities within the company since employees can be more aware and mindful of the threats and their impact on the company. Always welcoming any employee with any question related to security will help Frizza Cola to reach a high level of security awareness, which will help us to prevent any legal issues or negative effects within the company. For example, using the scenario where Frizza Soda got phished by a malicious actor, the malicious actor could steal information about their employee, intellectual property, customers, or service which will end up affecting either their customers or products. All these can help Frizza Cola to achieve the fundamentals of CIA (Confidentiality, Integrity, and Availability).

Reference

Gaskell, A. (2021, September 28). Cyberchology: How the human factor affects cybersecurity - cybernews. https://cybernews.com/editorial/cyberchology-how-the-human-factor-affects-cybersecurity/