**CYB 200 Project One**

Douglas Few

Southern New Hampshire University

December 5th, 2020

**Human Factors**

The first item on the list of concerns presented by the executives is the fact that the frequency of mandatory security awareness training is currently undefined. This needs to be addressed by making the training sessions scheduled more regularly. If the training sessions are being held once a month, employees will be more likely to be mindful of security awareness. This goes hand in hand with the second concern brought up by the executives, which is the undefined audience of the security training. According to Touchstone Security, 95% of all cybersecurity incidents are caused by human error (Touchstone, 2020). For this reason, every single employee in the company should be required to have at least a basic understanding of security protocols, and employees with higher privileges should be required to undergo more in-depth training depending on their privileges.

**Legal Factors**

The executives express concerns regarding intellectual properties and trade secrets. Considering the company’s recent strides in bottling technology advancement, the phishing emails and malware pose a significant threat to the company’s patents and copyrights (PhishProtection, 2020). If the malware happens to sabotage one of the bottling facilities, this could also pose a significant health risk to our customers, leading to legal battles and costly settlements. The biggest thing we need to focus on is teaching our employees about the dangers of phishing emails. We should also be emphasizing the importance of regularly scanning computers for viruses and malware.

**Proactive Security Mind-Set**

Being proactive at every level of the organization is important because every level is affected in one way or another by these kinds of threats. Even a laborer working in a bottling facility can be made aware of the risks related to sabotage and malfunctions concerning equipment. If said equipment were to malfunction, it could cause significant damage to

company property as well as injure an employee, which the company could be liable for (Tucker,2020). For this reason, we need to stress the importance of reporting any irregularities. Employees that work in marketing, advertising, and sales all have access to sensitive information that could prove harmful to the company if it were released, so these employees need to be more aware of threats like phishing emails that could lead to the installation of malware onto company computers.

References

PhishProtection. (2020, March 19). Phishing Awareness – Important Things That Every Employee Needs To Know In An Organization. Retrieved December 05, 2020, from https://www.phishprotection.com/content/phishing-awareness-training/phishing-awareness/

Touchstone. (2020, July 29). 5 Benefits of Security Awareness Training. Retrieved December 05, 2020, from https://touchstonesecurity.com/security-training/

Tucker, J. (2020). Workplace Injuries Due to Faulty Equipment - Who Is Liable? Retrieved December 05, 2020, from https://www.hg.org/legal-articles/workplace-injuries-due-to-faulty-equipment-who-is-liable-48843