Abraham Perez

November 12, 2023

The Human Factor in Cybersecurity

BLUF:

In this write-up, I will discuss the training methods needed for the usage of cybersecurity technology that is within budget. I will also be explaining what devices/technologies will be needed that are accessible with the remaining funds.

Training Employees-

Training employees is a valuable tool, especially in the cybersecurity field. The majority of it would be teaching employees the CIA Triad, that being Confidentiality, Integrity, and Availability. Confidentiality means protecting valuable information/data that shouldn't be accessed by the general public. Integrity means maintaining the status of information and making sure that no unauthorized modifications/tampering has been done. As well as Availability, in which employees, security personnel, etc. can access the information needed. There are also safety procedures when securing an employee's information. There are simple steps, such as having a secure password that isn't short and has special characters, avoiding spam/phishing emails, and even knowing what can and can't be accessed with their authorization.

Necessary Technology-

With the training out of the way, certain devices are needed to help ensure a company's security. One example would be Nmap, a tool that "scans networks and IT systems to identify existing security vulnerabilities" (Mutune, 2022). This tool can be easily accessible for the IT department and helps keep a step ahead from any attacks. Another device that can be used is a port scanner, which can see what ports are open/closed and make sure there aren't any unauthorized entries that come through the firewall. There are plenty of other tools/devices that can be used to help create a secure network, but it would all have to be within a company's budget.

Expectations vs. Reality (Conclusion)-

A company must be able to train their employees on how they can keep themselves secure as well as the company secure. There are also necessary devices that can help strengthen the security of said company. One would consider pushing more on the side of having more

technology than training, but realistically it can be the opposite. What matters most is having employees who are taught well and know what to do to reduce risk in a digital environment. Overall, the main takeaway from this is to keep your employees up to date on the “know-how” of cybersecurity and be able to ensure the safety of the digital environment that’s being used within monetary confines.

Works Cited

Mutune, G. (2022, December 31). *27 top cybersecurity tools for 2023*. CyberExperts.com. https://cyberexperts.com/cybersecurity-tools/