Tgen Hampsher
CYSE 200T
April 1st, 2025
Professor Duvall

The Struggle of Deciding to Fix Human Versus Technological Vulnerabilities

BLUF: If I were the Chief Information Security Officer (CISO) with a limited budget to work with, I would emphasize a majority of the budget going towards training employees and cybersecurity personnel.

Benefits of Employee Training

Employee training can come in a wide variety of ways and represents many different methods. However, the overall definition I would use for describing employee training in cybersecurity would be the process of teaching employees how to practice good cyber-hygiene and adhere to company policies, standards, and guidelines to reduce the risk of human error by employees. From things such as showing employees how to connect to a VPN, how to create a unique password, and what federal regulations apply to the data being collected by the company, the goal is to teach employees as much as possible about what they are allowed to do within the company network and its data.

According to Krithi Thiyagarajan (2024) from the Cyber Resource Center, there are six main benefits that arise from proper employee training: The first benefit is that when employees learn how to detect common attack techniques like phishing, malicious links, and fake users, the risk of that threat being realized is reduced. Additionally, employee training can help ensure that employees are aware of the federal and state requirements that pertain to their company, which decreases the chance that a company will be found liable for an incident that occurs.

Furthermore, training helps make sure that employees who have access to sensitive information within the company know how to properly store, transport, and modify the data which lowers the chance of data breaches and leaks occurring. To continue, proper training of employees acts as an additional layer of defense, which overall boosts the security posture of the company. Even further, employee training helps ensure that employees know how to respond to incidents that occur, which enhances the response speed of a company to a realized threat. Lastly, employee training ultimately saves the company money by reducing the risk and impact of attacks.

Benefits of Additional Cyber Technology

The benefits from upgrading cyber technology such as newer operating systems, firewalls, VPN's and many other physical and digital technologies will always make a company more secure. The argument could easily be made to continue to enhance security through adding more layers to defend through greater technology. However, there eventually reaches a limit where too many upgrades and defense layers start to affect the usability for the end user, which causes frustration and still ultimately harms the company.

Human Errors Cause a Majority of Attacks

Although cybersecurity attacks involve using various technologies and attack methods, attacks in the last decade have shown to be caused in the majority by human errors rather than technological errors. In fact, Research from the World Economic Forum has found that roughly 95% of total global cyber incidents occur due to human error, according to Anna Zhadan (2022) from Cybernews. What this means is that rather than most attacks being successful due to the lack of defense technology found within companies, most attacks are succeeding due to cyber criminals using social engineering methods and exploiting human based mistakes in the

technology to infiltrate networks and conduct the full attack. For companies, this means that no matter how sophisticated and expensive their technology is, weakness in proper employee training will ultimately still lead to an attack occurring.

Conclusion

In conclusion, there is undoubtedly a need for both cyber technology and proper employee training to protect data. However, cyber criminals have shifted focus to exploiting the human errors of a company and their network rather than aspects of the technology itself. As a result, I would make sure that my company had a medium amount of defense technology in place, and afterwards I would focus my attention on more frequent and proper employee training, in hopes of eliminating as many human vulnerabilities as possible.

References

Thiyagarajan, K. (2024, June 3). *URS Cyber Resource Center*. URS Cyber Resource Center. https://www.cyberresourcecenter.com/blog/6-key-benefits-of-providing-cybersecurity-training-for-employees

Zhadan, A. (2022, January 12). *World Economic Forum finds that 95% of cybersecurity incidents occur due to human error*. CyberNews. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/