Nathan Milnes

The Human Factor in Cybersecurity

BLUF: As a Chief Information Security Officer (CISO) with a limited budget, it would be crucial to carefully think about how to allocate resources to maximize the efficiency of your company's cybersecurity measures. Balancing your budget and the tradeoff between training and actual technology would be crucial for building a robust defense.

Human error is a common factor in cyber security breaches, so providing employees with concise, effective, and regular training could potentially cost very little to the company but act as another layer of defense. It is reported that 95% of cyber security breaches are primarily caused by human error and they tend to cost their company $3.33 million per breach. (Threatcop Article) If the company was to have a group of the cybersecurity analyists each dedicate one day a month to company training through a powerpoint presentation or hands-on training, that training would be essentially free since you're already paying the employees to be there. This training would include phishing, physical security, and the importance of security updates on workstations. If training was conducted in this way, it would allow to company to invest heavily into cyber technology in order to secure the company's data. The company could then use said funds to hire outside entities for security audits and penetration testing, as well as invest in the most up-to-date software and hardware.

By balancing the company's time and money in technology and training this approach aims to create a layered defense that addresses numerous aspects of cyber security. Regular assessments and realocation of funds and time would be key to staying on top of emerging threats.

References:

Sara Abraham (March 10th, 2022) Top 5 Cybersecurity breaches due to human error

https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/