Name: Huong Quach

Date: 06/22/25

The Human Factor

BLUF

A balance between technical controls and human training is necessary for effective cybersecurity. My approach as a CISO with limited funding would be to invest in high-impact technologies sparingly while concentrating on creating a robust human defense layer.

Humans in Cyberspace

The biggest weakness in an organization's cybersecurity architecture is frequently its workforce (What Is Security Architecture?, 2024). A large portion of security breaches are still caused by social engineering, phishing attempts, and straightforward errors like using weak passwords. Human error can undermine the efficacy of even the most sophisticated equipment. Consequently, I would allocate a significant amount of my meager resources to security awareness training. To keep staff members up to date on new risks, this would involve regular phishing simulations, required security courses, and recurring refresher training. By empowering staff members to take an active role in the organization's defense, training lowers the possibility that attacks will be effective (Social Engineering - the “Human Factor,” n.d.).

Technology Investments

Technology is crucial for automating defenses, identifying threats, and enforcing security standards, while training addresses human vulnerabilities. I would use the remaining funds to purchase specific cybersecurity solutions that offer the best value in terms of protection. To help stop typical attack vectors before they even reach users, this would comprise next-generation firewalls, email security filters, intrusion detection and prevention systems (IDPS), and endpoint protection solutions (Microsoft, 2024). Additionally, a relatively inexpensive, high-impact security strategy that directly lowers credential-based assaults would be to adopt multi-factor authentication (MFA) throughout the whole enterprise (IBM, 2023).

Budget Allocation

As CISO, I would prefer human training over technology and strive for a roughly 60/40 mix. This balance represents my opinion that human error is still the primary cause of the majority of security issues. We can greatly minimize attack surfaces and enable our technology investments to perform as planned by developing a watchful, security-conscious staff. By guaranteeing that staff members adhere to standard practices and are aware of potential risks, high-quality training increases the value of the technology used.

Conclusion

Cybersecurity is first and foremost a human issue, not just a technological one. As a CISO with little money, I would place a high priority on thorough security training and make calculated investments in crucial cybersecurity equipment (Cisco, 2025). This combined strategy

maximizes security results within a limited budget by addressing both technical and human vulnerabilities.

References

Cisco. (2025, March). What Is a CISO? Chief Information Security Officer. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-ciso.html

IBM. (2023, April 19). Intrusion Detection System. IBM. https://www.ibm.com/think/topics/intrusion-detection-system

Microsoft. (2024). What is: Multifactor Authentication. Support.microsoft.com. https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

Social Engineering - the “Human Factor.” (n.d.). Federal Office for Information Security. https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html

What Is Security Architecture? (2024). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-security-architecture