The Human Factor in Cybersecurity

Addressing that tradeoff, with a limited budget, involves striking a balance to develop both the human and technological aspects of cybersecurity. In this setting of CISO, my approach toward the availed resources would focus on maximizing the impact, considering further the effectiveness of user education and the role that advanced technologies will play in protecting the organization.

Training vs. Technology

- **Training**: According to Witkowski et al. (2017), human factors are usually the weakest link in an organization's security posture. Most cyber incidents result from human errors, such as falling for phishing scams or poor password choices, hence the very essential need for constant user training. The effective training programs should be comprehensive, including basic security awareness, but also covering more specialized topics in recognizing social engineering attacks, safe handling of sensitive data, and best practices of using technology securely.

Investment in training pays long-term dividends because it creates a culture of security awareness. Additionally, employees educated in cybersecurity best practices can often avert incidents that otherwise would require high-priced technology investment. Training allows the human resource to form the first line of defense against cyber-attacks, hence potentially reducing incidents and easing burdens on security technology.

- **Cybersecurity Technology**: The ever-sophisticating nature of cyber threats on the other side justifies the fact that technology plays an essential role in any security strategy. Performing continuous monitoring of the networks, threat detection, and response to

breaches, these tools and systems are significant during the defense from advanced persistent threats, malware, ransomware, and other complex forms of attack (Witkowski et al., 2017). At the same time, technology itself cannot offer complete protection, especially when end-users are not thoroughly trained to use it efficiently.

Budget Use Strategy

In such a limited budget, the best strategy will be to try to allocate such that at least cybersecurity is obtained through education and technology. I would do the following for this allocation strategy:

- **Train First**: Most of my budget would go into training users, specifically high-value targets: executives, system administrators, and employees with sensitive information. The training programs should be continuous, with periodic refreshers to address evolving threats. The NIST guidelines suggest focusing on both general awareness and specific role-based training (Witkowski et al., 2017). Since human error is often the leading cause of security breaches, a well-informed workforce can significantly reduce risk, making this investment crucial.
- **Targeted Technology Investments**: The remaining resources will be invested in cybersecurity technologies that are most critical for organizational needs. This will include the implementation of EDR systems, firewalls, and MFA solutions. These tools give very strong protections from common threats and work synergistically with employee training. For instance, while training can effectively enable the users to identify phishing, MFA can limit the effects in case a user's credentials are compromised. Witkowski et al. (2017) note that integrating technology with human behavior is critical towards developing a resilient security posture.

- **Continuous Improvement**: Training programs and cybersecurity technologies need to continuously be assessed against emerging threats for their effectiveness and updated. Both feedback from employees and hard data about security incidents help further tune training content and give insights into technology investments. Since the dynamic nature of cybersecurity threats, one needs to adapt to that reality with both human and technological defenses.

Conclusion

In short, where technology makes a very important contribution to an organization's asset protection, human behavior is typically one of the largest cyber-vulnerabilities. For this reason, a CISO would want to first focus investment on training-especially high-risk users-and second, focus on a core set of security technologies that enhance the overall cybersecurity strategy. Addressing these two areas in balance allows an organization to achieve more holistic, effective security while working with a relatively constrained budget.

References

Witkowski, Dave, et al. “Cybersecurity – the Human Factor.” *Deloitte Consulting LLP*, csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf.