Ally Howard

11/12/2025

Bridging the Human Gap in Cyber Defense

With a limited budget, 60% should be prioritizing training over expensive technology because most breaches stem from human error. It is more important to focus funds on high impact, low-cost measures like learning how to use basic technology and automated updates. Once basic defenses are strong, 40% of the remaining funds should go to essential technology.

Effective Training

Training is a crucial factor in the workplace. It is important to prioritize people first, then inexpensive technology. Most breaches start from human action and error. Even the best technology can fail if workers do not understand the basic security measures and protocols. "While technical security controls like firewalls, email security, and endpoint protection provide layers of defense against cyber threats, no one technical solution can stop all cyber attacks. Information security awareness training provides tools, techniques, and best practices that SLTT employees can use to spot potential threats, take appropriate actions, and protect their organizations,"(Center for Internet Security, 2022). Training is an investment where a small spend on this prevents a likely larger loss in new technology. Regular training that is engaging can help create a well aware security culture of workers that reduces the most common risks in the cyber workforce.

Cybersecurity Technology

Remaining funds should go towards a cost effective, impactful technology like endpoint protection and updated automation. Technology provides tools to detect, prevent, and respond to threats but is also only effective as the people using it. "Detection and prevention go hand in hand—in order to prevent threats, you must be able to detect them in real time,”(Threat Detection and Threat Prevention: Tools and Tech, 2022). In this case, workers need to be able to work with basic technology before even putting it in the workplace for it to be compromised a lot quicker. This can strengthen the technical layer of defense and well trained users.

Conclusion

In this limited budget scenario, the most effective strategy is a balance that strengthens both the training for workers and technology. Mainly investing in training makes sure that workers become the first line of defense against human error which is the main cause of most breaches. At the same time, using the remaining funds on technology like the endpoint protection and authentication, builds a solid foundation that prevents and detects attacks of all kinds. By combining these two factors and effectively balancing them provides a strong workplace with educated workers and essential technology and security.

References

Center for Internet Security. (2022, June 22). *Why Employee Cybersecurity Awareness Training Is Important*. CIS. https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important

"Threat Detection and Threat Prevention: Tools and Tech." *Cynet*, 22 Aug. 2022, www.cynet.com/advanced-threat-protection/threat-detection-and-threat-prevention-tools-and-tech/.