Name: Alexander Turnsek

Date: 11/12/2023

Cybersecurity Training Over Technology Investments

Given budget constraints, cybersecurity training for employees should take priority over investments in additional technology because humans are the weakest link in defenses; an aware, alert workforce is essential for adapting to constantly shifting threats.

Prioritize Training Over New Technology

When dealing with budget constraints, my priority would be spending on cybersecurity training and education for employees rather than investing in additional technology. Advanced security tools and systems can provide significant protection, but humans are still the weakest link in any organization's cyber defenses. "Humans can intentionally or unintentionally undermine any cybersecurity measure" (Legrand, 2022) "Regular cybersecurity awareness training can greatly improve employee vigilance and resilience against phishing, social engineering, and other common attack vectors that target people rather than systems.

Focus Technology Spending on Foundational Controls

Regarding technology, I would focus on optimizing and maximizing the usage of existing security solutions before acquiring new tools. Shoring up foundational security controls like multifactor authentication, endpoint detection and response, network monitoring, and regular patching and upgrades should be prioritized. This approach is more cost-effective than purchasing add-ons that provide limited additional protection.

Tailor Training to Employee Roles

Within the training budget, I would allocate funds toward role-based education so that employees in different functions get training tailored to the specific risks they face. For instance, secure coding practices would be emphasized in training for software developers, while human resources personnel would learn to identify social engineering attempts in job applications. Conducting phishing simulations and short security refreshers at regular intervals can be an economical way to keep security at the forefront of everyone's mind.

Conclusion

In conclusion, while a robust cybersecurity program includes both technological defenses and an educated workforce, training is the most effective use of limited resources. An aware, alert workforce that can adapt to new risks is essential. With the right training program, employees can become an invaluable line of defense against constantly shifting cyber threats.

References

Legrand, J. (2022, January 27). *Humans and Cybersecurity— The Weakest Link or the Best Defense?* Www.Isaca.org. Retrieved November 12, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/humans-and-cybersecurity-the-weakest-link-or-the-best-defense