Isaiah Seaborn

Professor Duvall

CYSE 200T

6 April 2025

BLUF (Bottom Line Up Front)

As CISO with limited resources, I would prioritize cybersecurity training slightly more than technology, dedicating 60% of the budget to improving human awareness and 40% to essential technical defenses. This balance reduces risk from both human error and system vulnerabilities.

Introduction

In today's evolving threat landscape, organizations face cyber risks from both technical vulnerabilities and human error. As Chief Information Security Officer (CISO) with a limited budget, it is critical to balance investments in cybersecurity training and technology. The most effective strategy is to focus slightly more on human factors while still maintaining core technical defenses.

Investing in Human Awareness

Human error continues to be a leading cause of cybersecurity incidents. In fact, 74% of breaches involve the human element, such as phishing, social engineering, or misuse of credentials (Verizon, 2023). To address this, 60% of the budget should be allocated to employee training. Effective programs include simulated phishing attacks, role-based education, and regular testing to assess progress. A well-trained workforce significantly lowers the risk of successful attacks.

Smart Technology Spending

While human training is critical, technology still plays an essential role. With the remaining 40% of the budget, organizations should implement affordable, high-impact tools. Multi-Factor Authentication (MFA), Endpoint Detection and Response (EDR), and automated patch management are proven methods to reduce vulnerabilities and respond quickly to threats (NIST, 2022). These tools create a layered defense system that complements employee awareness.

Conclusion

In conclusion, the best approach is a balanced one. Training empowers employees to recognize and respond to threats, while smart technology investments guard against technical vulnerabilities. This strategy maximizes security impact within a limited budget.

References

National Institute of Standards and Technology (NIST). (2022). *Cybersecurity Framework*. https://www.nist.gov/cyberframework

Verizon. (2023). *2023 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/