

Michael Everett

Course: CYSE 200T

Date: April 6, 2025

Professor Duvall

Balancing Human Training and Technology in Cybersecurity

BLUF: With a limited budget, I would prioritize a balanced investment in both cybersecurity training and technology, with a greater emphasis on human factors. While technology provides essential tools for defense, the human element remains the most vulnerable and potentially the strongest link in the cybersecurity chain.

Introduction

As the Chief Information Security Officer, I am constantly navigating the challenge of optimizing cybersecurity strategies within the budget. This is often centered around whether to gather more resources toward technologies or toward employee training. A well-rounded strategy that addresses both human behavior and technological defense is key to a strong security system.

Weak Points in Human Elements

Most cyber incidents can be traced back to human error whether through phishing scams, weak passwords, or social engineering. According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches involved the human element (Verizon, 2023). This statistic underscores the importance of security awareness training. Effective training programs not only educate employees on identifying threats but also foster a culture of security mindfulness. For example, periodic phishing simulations can help staff recognize real-world attacks, reducing successful breaches over time.

Technology as a Force

While humans are a key vulnerability, technology is a necessary line of defense. Tools such as endpoint detection and response, firewalls, intrusion detection systems (IDS), and multi-factor authentication provide critical safeguards. However, these tools are only effective when properly used and managed often by trained humans. Therefore, I

would allocate approximately 60% of the budget toward training and 40% toward technology. This ratio allows for a solid investment in technical defenses while ensuring that the people operating them are not the weakest link.

Conclusion

Cybersecurity is not solely a technology problem it's also a human one. An organization's defenses are only as strong as its people. By emphasizing training, supported by technological tools, we can build a security culture that mitigates risks effectively even on a limited budget.

References

Verizon. (2023). 2023 Data Breach Investigations Report. Retrieved from <https://www.verizon.com/business/resources/reports/dbir/>