The Human Factor in Cybersecurity

Name: Caitlene Baer

BLUF

Companies need to determine appropriate worker security training budgets compared to contemporary security technology investments while working with restricted financial resources. Modern cyber protection systems based on technology platforms stop most cyber breaches by addressing human errors. Both security measures provide complete protection against cyberattacks when organizations make investments into these systems.

Introduction

The protection of computer systems now demands business-wide attention because it has become crucial for operational success. The size of an organization does not determine their risk from sophisticated and high-volume cyberattacks. Operational continuity alongside trust depends on maintaining data confidentiality, integrity, and availability because ransomware attacks and insider threats remain constant threats. According to Kim and Solomon, organizations need proper people preparedness and process readiness to supplement technology infrastructure in achieving cybersecurity success. The Chief Information Security Officer (CISO) needs to make deliberate trade-off decisions since limited funding should be allocated towards protection strategies that offer maximum protection and enduring value.

Human Error and the Importance of Training

Rapid security technology innovation has not eliminated human error from its role as the primary cause of security incidents. System exposure mostly takes place when employees either follow malicious links, keep weak login passwords, or misuse sensitive business data. According to Kim and Solomon, strong security measures become vulnerable to persons who lack awareness or experience in security training.

Organizations should conduct complete employee training sessions to lower this risk factor. The organization runs security awareness courses on a regular basis as well as conducts simulated phishing campaigns to train employees about policies through scenario-based incident response exercises. People develop better capabilities to identify possible security threats during training and learn suitable responses when they occur. The NIST Cybersecurity Framework integrates “awareness and training” as a fundamental element within its Protect function. Personnel with adequate knowledge function as human security controls to detect dangerous activities and report security

risks while upholding security policies. Training enabled by policies and clear procedures minimizes the potential of mistakes, which could endanger system security.

The Role of Cybersecurity Technology

The defense of internal vulnerabilities depends on training, while technology safeguards organizations against external threats along with automated attacks. To create multiple barriers of defense, organizations need to deploy firewalls along with endpoint protection platforms as well as intrusion detection and prevention systems (IDPS), encryption methods, and multi-factor authentication systems. The combination of several security measures through defense-in-depth strategies represents the only effective way for organizations to achieve full protection, according to Kim and Solomon.

The NIST Cybersecurity Framework establishes technical measures as essential components for the Detect and Protect and Respond functions. An organization's capacity to discover and handle cyberattacks in real-time becomes stronger due to the implementation of continuous monitoring tools alongside access control systems supported by automated alert systems. Public and private companies that require strong protection can implement AI-based threat detection and cloud access security brokers and endpoint detection and response platforms despite having smaller security team numbers.

Budget Allocation Strategy

A restricted cybersecurity budget should allocate funding in the following way due to cyber threats' technical and human aspects:

- Cybersecurity technologies receive 55% of the budget allocation, while firewalls, endpoint security, DLP systems, and intrusion detection tools are included. The organization obtains a strong base for recognizing and stopping unauthorized behavior from this investment.
- A budget of 45% should be allocated to implement training and awareness programs that deliver employee training and leadership instruction with phishing exercises and compliance updates. These initiatives transform each member of staff into wired participants within the community of cybersecurity.

The return on investment will be optimized by utilizing cost-free materials delivered by NIST and CISA and the SANS Institute together with other non-profit and government entities. The tools provide training improvement capabilities that do not require additional expenses.

Conclusion

The implementation of cybersecurity requires technologies together with human behavior interventions. Human actions play an important role in causing security

incidents; thus, organizations must allocate equivalent resources to their training efforts. The CISO role requires me to implement a security plan that equally values advanced technical limitations and workforce education enhancement. By following the advice of Kim and Solomon as well as NIST Cybersecurity Framework best practices, my approach will combine the usage of technology with a workforce that receives proper training. Organizations that dedicate resources to their staff and technological infrastructure will perform better at stopping**,** observing, and reacting to sophisticated cyber dangers in today's world.

References

Kim, D., & Solomon, M. (2023). *Fundamentals of information systems security* (4th ed.).

Jones & Bartlett Learning. https://www.jblearning.com/catalog/productdetails/9781284220735?srsltid=AfmBOopl_07g95PqkY1F13sfotA6ofwGb8fEo-rSysZvbNBc2Cqpv2mq
NIST. (2023). *Cybersecurity Framework*. National Institute of Standards and Technology. (CSF 2.0) https://www.nist.gov/cyberframework