Neesha Currier

CYSE-200
Balancing Training and Cybersecurity Technology Investments
3/21/2026

Bottom Line Up Front (BLUF)

With a limited cybersecurity budget, I would balance spending between employee training and cybersecurity technology, with a slightly greater focus on training. Human error is one of the leading causes of cyber incidents, so improving employee awareness can reduce many risks before they occur. At the same time, cybersecurity technology is still necessary to detect and respond to threats that cannot be prevented through training alone.

Introduction

Organizations face constant cybersecurity threats, many of which are caused or influenced by human behavior. Employees may unintentionally create vulnerabilities through actions such as clicking phishing links, using weak passwords, or mishandling sensitive data. As a Chief Information Security Officer (CISO) with a limited budget, it is important to carefully decide how to allocate resources between employee training and cybersecurity technology to reduce overall risk.

Importance of Employee Training

Employee training is one of the most effective ways to reduce cybersecurity risks because many attacks target human behavior. Phishing attacks, social engineering, and poor security practices are common entry points for cybercriminals. By investing in regular training programs, organizations can teach employees how to recognize suspicious emails, create strong passwords, and follow proper security procedures.

Training is also cost-effective because it helps prevent incidents before they happen. A well-trained workforce can act as the first line of defense against cyber threats. Reducing human error can significantly lower the chances of data breaches and system compromises (Stallings & Brown, 2018).

Role of Cybersecurity Technology

While training is important, cybersecurity technology is still necessary to protect systems and data. Tools such as firewalls, intrusion detection systems, endpoint protection, and multi-factor authentication help organizations detect and respond to threats that employees may not notice.

Technology also provides automated protection and monitoring, which is critical in today's fast-paced threat environment. Even well-trained employees can make mistakes, so having strong technical controls in place helps reduce the impact of those errors.

Balancing the Budget

If I had to allocate a limited budget, I would prioritize employee training slightly more than technology, while still maintaining a balanced approach. For example, I might allocate around 60% of the budget to training and 40% to technology.

My reasoning is that many cyber threats rely on human error, so addressing the human factor can prevent a large number of attacks before they begin. At the same time, technology is still necessary to provide backup protection and detect threats that cannot be avoided through training alone.

This balanced approach ensures that both prevention and detection are addressed, which is important for building a strong cybersecurity posture.

Conclusion

Balancing employee training and cybersecurity technology is essential for managing cyber risks, especially with a limited budget. While both areas are important, investing slightly more in training helps reduce human-related vulnerabilities, which are a major cause of cyber incidents. At the same time, cybersecurity technology provides critical protection and monitoring capabilities. By combining both approaches, organizations can create a more effective and well-rounded cybersecurity strategy.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.