Brandon Johnson

CYSE 200T

November 10, 2024

The Human Factor in Cybersecurity

As a Chief Information Security Officer with a limited budget, balancing the allocation of funds between cybersecurity technology and training is crucial for maintaining an effective security posture. In today's threat landscape, both human factors and technical vulnerabilities contribute to cyber risks, so a strategic approach is necessary to maximize the impact of available resources. First, investing in training and awareness programs is essential because human error is often the weakest link in security. A significant portion of cyber threats, such as phishing and social engineering attacks, exploit this vulnerability. I would allocate about 40 to 50 percent of the budget to educating employees on security best practices. This would include phishing simulations to help staff recognize malicious emails, role-specific trainings and general awareness programs that reinforce the importance of security. In addition, incident response training would ensure that employees know how to report suspicious activities and respond effectively in the event of an attack. Since human mistakes are often responsible for breaches, investing in employee education can significantly reduce the likelihood of security incidents.

At the same time, cybersecurity technology is indispensable for defending against more sophisticated threats. While training helps mitigate human error, technology provides automated defenses that can quickly detect and block attacks. I would allocate another 40 to 50 percent of the budget to technology investments, focusing on tools that provide broad protection and complement the training efforts. Key technologies would include endpoint protection, which helps detect and respond to threats on individual devices, and email security solutions that filter out phishing attempts before they reach users. Multi-factor authentication would also be a priority, as it adds an extra layer of security, even if user credentials are compromised. Additionally, investing in firewalls and intrusion detection systems would help protect the network perimeter, offering an early line of defense against external threats. While prevention is critical, having an effective incident response plan is equally important. With the remaining 10 percent of the budget, I would focus on establishing a robust monitoring system and incident response protocols. This would include setting up 24/7 monitoring, either through an in-house team or outsourced service, to quickly detect and respond to potential threats. Regularly updating the incident response plan ensures the organization is prepared for various types of attacks, and investing in threat intelligence tools would help stay ahead of emerging risks.

In conclusion, balancing training and technology is key to building a strong cybersecurity defense within a limited budget. By focusing on training to reduce human error, technology to block and detect threats, and a solid incident response plan to mitigate damage when attacks do occur, the organization can create a more resilient and proactive security strategy. This integrated approach ensures that both people and technology work together to reduce risks and protect sensitive data.

Works Cited:

Verizon Data Breach Investigations Report (DBIR). Verizon, 2023, www.verizon.com/business/resources/reports/dbir.

National Cyber Security Centre (NCSC). "Incident Management." *NCSC*, 2024, www.ncsc.gov.uk/guidance/incident-management.