**Courtney Jones 04/06/2025**

**CYSE 200T Spring 2025**

**Fortifying the Human Firewall: A Balanced Cybersecurity Investment Strategy**

***BLUF***

Given a limited cybersecurity budget, the most effective approach to mitigating human-related cyber threats is to allocate funds strategically, prioritizing foundational and continuous security awareness training alongside targeted technology investments in areas offering the most significant risk reduction and automation.

**The Enduring Human Element**

The reality is that humans remain a significant vulnerability in any organization's cybersecurity posture (Verizon, 2024). Employees can inadvertently create pathways for cyber threats through social engineering attacks, accidental data leaks, or poor password hygiene (Verizon, 2024). Studies have consistently shown that many security breaches involve human error (IBM, 2023). While sophisticated cybersecurity technologies offer crucial layers of defense, they are often rendered ineffective if the human element is not adequately addressed (Proofpoint, 2023). Therefore, neglecting security awareness training favoring solely technological solutions is a short-sighted approach.

**A Balanced Allocation Strategy**

With a limited budget, my strategy would focus on a tiered approach, prioritizing foundational training and strategically deploying technology where it offers the greatest impact.

1. **Foundational and Continuous Security Awareness Training (Approximately 40% of Budget):**

This would be the cornerstone of my investment. A comprehensive program would include regular and engaging training modules covering topics like phishing awareness, password security, data handling best practices, and social engineering tactics (Verizon, 2024). This training should be delivered frequently and in digestible formats to maximize retention (NIST, 2018). The training would be delivered through various formats, including interactive modules, videos, and simulated attacks (Verizon, 2024; Proofpoint, 2023). Testing employees' susceptibility to phishing attempts through simulations is crucial for identifying vulnerabilities and reinforcing training (Proofpoint, 2023). Furthermore, establishing clear and accessible security policies and procedures ensures employees understand their responsibilities and have easy access to security guidelines (Verizon, 2024). Cultivating a culture of security awareness encourages employees to report suspicious activity without fear of reprisal (Verizon, 2024).

Reasoning: A well-trained workforce is a crucial first line of defense, significantly reducing the likelihood of successful social engineering attacks and accidental data breaches (Verizon, 2024). This proactive approach is often more cost-effective in the long run than solely relying on reactive technological solutions (Proofpoint, 2023). Organizations with strong security awareness programs often experience a lower incidence of security incidents (IBM, 2023).

2. **Targeted Technology Investments (Approximately 60% of Budget):**

While training is paramount, specific technologies are essential to augment human vigilance and automate threat detection and response. I would focus on implementing Multi-Factor Authentication (MFA) across all critical systems, as it adds a significant layer of security against unauthorized access, even if passwords are compromised (Verizon, 2024). Investing in Endpoint Detection and Response (EDR) systems provides real-time monitoring and analysis of endpoint activity, enabling rapid detection and response to threats that may bypass traditional antivirus solutions (Verizon, 2024). Robust Email Security Solutions with Advanced Threat Protection are crucial for identifying and blocking sophisticated phishing attempts and malicious attachments (Verizon, 2024). Finally, regularly scanning systems for known vulnerabilities using Vulnerability Management Tools allows for proactive patching and reduces the attack surface (Verizon, 2024; NIST, 2018).

Reasoning: These technologies provide critical automated defenses and enhance our ability to detect and respond to threats that may still slip through due to human error (Verizon, 2024). Prioritizing MFA and EDR offers significant risk reduction for the investment (Verizon, 2024). Combining human awareness with technological controls, a layered security approach offers the most robust defense (NIST, 2018).

**Conclusion**

In conclusion, a balanced approach prioritizing ongoing, effective security awareness training alongside strategic investments in key cybersecurity technologies represents the most prudent use of a limited budget (IBM, 2023; NIST, 2018; Proofpoint, 2023; Verizon, 2024). By "fortifying the human firewall" and implementing essential technological safeguards, we can significantly reduce our organization's susceptibility to human-related cyber threats and build a more resilient security posture (Verizon, 2024).

**References**

IBM. (2023). Cost of a Data Breach Report 2023. IBM Security. Retrieved from <https://www.ibm.com/reports/data-breach>

NIST. (2018). NIST Cybersecurity Framework. National Institute of Standards and Technology. Retrieved from <https://www.nist.gov/cyberframework>

Proofpoint. (2023). 2023 State of the Phish Report. Proofpoint. Retrieved from <https://assets-global.website-files.com/615d3b1833fa9330d4c96b6a/643d7471d2826f4534113baa_State%20of%20the%20Phish%202023%20SkyriverIT.pdf>

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon. Retrieved from

<https://www.verizon.com/business/resources/reports/dbir/>