Dylan Shaver

Professor Duvall

CYSE 200T

April 1, 2025

# The Human Factor in Cybersecurity

**BLUF:** As a Chief Information Security Officer (CISO) with cybersecurity budget constraints, I would implement a balanced approach prioritizing employee training and security technologies to strengthen organization resilience against cyber threats. Focusing employee training on human factor errors will provide a maximum return on investment in risk reduction.

## Understanding the Human Threat Factor

Numerous studies have shown that human error accounts for the majority of cybersecurity incidents (Verizon, 2023). Employees often unintentionally open the door to cyber attackers by falling for phishing emails. While technology can mitigate some of these risks, it cannot replace human judgment. Therefore, the corporate culture must highlight the importance of employee cybersecurity training.

## Strategic Technology Investment

Technology plays a critical role in supporting human defenses. With limited funds, I would prioritize high-impact solutions. Tools such as encryption, endpoint detection and response (EDR), multi-factor authentication (MFA), and security information and event management (SIEM) platforms provide essential layers of protection (Smith & Lee, 2022). These technologies help detect threats in real-time, enforce access controls, and streamline incident response, all of which are critical in today's dynamic threat landscape.

## Finding the Balance: A 60/40 Approach

Given the tight budget, I would recommend allocating 60% of available funds to employee training and awareness efforts, with 40% allocated to technology investment.

- Training (60%): The human factor is most frequently the weakest point in cybersecurity. Even with the latest security tools, employees if not adequately trained, may inadvertently introduce vulnerabilities by using weak passwords, falling prey to a phishing scam, or improperly handling sensitive information. Investing 60% of the budget in training guarantees that employees, from the C-suite to the ground level, are locking down their online behaviors. Incorporating awareness campaigns, implementing mandatory security training exercises with phishing simulations and role-playing exercises would equip employees with the tools they need to recognize and respond to threats effectively.

- Cybersecurity Technology (40%): As important as human behavior is, you cannot ignore the necessity of effective cybersecurity technology. Purchasing key technologies that augment workforce training and block/monitor malicious traffic would be top priority. The emphasis would be on layered security, like firewalls and Intrusion Detection Prevention Systems (IDPS).

**Conclusion**

Effective cybersecurity requires a dual focus on people and technology. Training builds a proactive human defense layer, while technology fills in the gaps where human oversight may fail. A well-balanced strategy that incorporates education and reinforces it with essential tools allows organizations to build a cost-effective and resilient cybersecurity program, even with limited resources.

---

**References**

Smith, R., & Lee, J. (2022). *Cybersecurity strategy in resource-constrained environments*. Cyber Defense Press.

Verizon. (2023). *Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/