Lydia Robb
CYSE 200T
November 16, 2025
Professor Duvall

The Human Factor in Cybersecurity

BLUF:

As CISO, I would allocate limited cybersecurity funds with 40% to human centered training, 40% to core cybersecurity technologies, and 20% to governance, monitoring, and incident response. This balance reflects research showing that human behavior, insider opportunity, and organizational culture drive much of today's cyber risk, and that technical safeguards must work hand-in-hand with informed, vigilant employees.

Human Behavior and Organizational Culture as Primary Risk Factors

The readings make clear that humans, not just machines, are central to both vulnerability and defense. White-collar cybercrime often occurs when trusted employees misuse legitimate access or rationalize unethical behavior within occupational roles. Additionally, routine activity theory highlights that capable guardianship includes employee awareness and responsiveness, not only technical controls. For these reasons, 40% of the budget goes toward training, culture, and insider risk awareness, including role-based instruction, ethical decision making reinforcement, phishing simulations, and leadership driven security messaging. These investments reduce both accidental and intentional human driven cyber incidents while strengthening the organization's overall security posture.

Technical Controls and Infrastructure Hardening

Technology remains essential for limiting the opportunities and impact of cyber threats, particularly when paired with informed human behavior. Another 40% of the budget supports technical safeguards such as identity and access management, endpoint protection, and network segmentation. These controls directly reduce the chance of data misuse or unauthorized system access, especially in roles with elevated opportunity for white-collar cybercrime. Resilience focused investments like redundancy, environmental safeguards, and disaster recovery capabilities ensure continuity when inevitable failures or incidents occur. The data center model illustrates how robust physical and operational design helps organizations withstand cyber or infrastructure disruptions.

Governance, Monitoring, and Incident Response Integration

The final 20% supports the organizational glue needed to ensure training and technology work cohesively. Governance provides clear policies, risk assessments, and internal controls grounded in an understanding of how cybercrime and workplace behavior intersect. Monitoring tools and

behavioral analytics strengthen detection of suspicious activity, while incident response planning ensures rapid containment and recovery when breaches occur. These practices align with research emphasizing that both cyber and white-collar offenses rely on weak oversight and inadequate guardianship. Effective governance and response capabilities maximize the value of both human focused and technical investments.

Conclusion:

Balancing limited cybersecurity funds requires recognizing that modern threats are sociotechnical, stemming from both system vulnerabilities and organizational behavior. By splitting the majority of resources evenly between people and technology, and dedicating a focused portion to governance and response, organizations create reinforcing layers of defense. This approach reflects the core insight of the readings: cybersecurity is not merely an IT function but a human centered, organization wide responsibility that integrates training, controls, and strong oversight.

References

Payne, B. K. (2018). *White-collar cybercrime: White-collar crime, cybercrime, or both?* Criminology, Criminal Justice, Law & Society, 19(3), 16–32.

Payne, B. K., & Hadzhidimova, L. (n.d.). *Cybersecurity and criminal justice: Exploring the intersections.* International Journal of Criminal Justice Sciences.