Junhee Lee

April 15, 2026

CYSE 200T

Professor Duvall

The Human Factor in Cybersecurity

BLUF:

Given limited resources, my cybersecurity strategy would prioritize workforce training and targeted technology investments aligned with the NIST Cybersecurity Framework. The goal is to mitigate the most relevant and probable threats to the agency by developing a security-aware culture while strategically deploying technology that enhances detection, protection, and response capabilities where human vigilance is insufficient

NIST Aligned Risk Management

The NIST Cybersecurity Framework provides a structured approach emphasizing the functions of Identify, Protect, Detect, Respond, and Recover. To maximize limited resources, my agency would start by identifying our highest risk assets and most likely attacks through regular risk assessments. This ensures funding supports controls addressing the most relevant and realistic threats such as phishing, credential theft, and endpoint vulnerabilities rather than less probable or highly advanced attacks unlikely to target our environment. By grounding budget allocation in the NIST CSF, we ensure that spending decisions align with federal standards and measurable risk reduction outcomes.

Allocation of Funds

With the threat landscape mapped, my funding allocation would follow a 60/40 split between training/human factors and technology investments. Over half of the budget would support continuous employee training programs emphasizing phishing awareness, safe password practices, and incident reporting. Human error remains a leading factor in breaches, and empowering staff reduces the likelihood of successful social engineering and insider threats.

Training must extend beyond annual compliance modules, and it should be an evolving program integrated into daily operations. Simulated phishing exercises, role-based security briefings, and engaging awareness campaigns reinforce good cyber practices. By making a culture where security is everyone's responsibility, the organization reduces reliance on technical barriers alone. This shift also fulfills the NIST CSF's Identify and Protect categories by ensuring personnel actively recognize and mitigate threats in real time.

The remaining funds would be invested in technology that directly complements human defenses such as multi-factor authentication, endpoint detection and response solutions, network segmentation, and automated patch management. These tools mitigate risks that cannot depend on user behavior alone. Integrating such technology under the NIST "Protect" and "Detect" functions ensures rapid identification and containment of emerging threats.

Regular performance reviews and incident response simulations would gauge the effectiveness of both training and technology. NIST's guidance leads this approach by emphasizing continuous improvement and feedback. Metrics such as click rates on phishing simulations, system patch latency, and time to detect incidents would inform the reallocation of funds and refinement of priorities for each fiscal cycle. This model ensures that investments respond to shifting threats and organizational changes while maintaining compliance and audit readiness.

Conclusion:

Under NIST guidance and budget constraints, a balanced cybersecurity strategy emphasizes well-trained personnel and well-placed technologies focused on the most likely threats. By investing more heavily in human factors, our largest risk and first line of defense while reinforcing them with critical, targeted technologies, the agency can achieve measurable improvements in resilience and compliance without unnecessary spending. The true power of this approach lies not in how much we spend, but in how intelligently we align our spending with NIST principles and evolving threats.