Human Factors: A CISO's Response to Human Error & Threats

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

April 4, 2025

Assignment:

You are the Chief Information Security Officer. You are aware of different points of view regarding human contribution to cyber threats. Realizing that you have a limited budget (the amount is unimportant):

1. How would you balance the tradeoff of training and additional cybersecurity technology? In other words, how would you allocate your limited funds?
2. How would a Chief Information Security Officer (CISO) balance the tradeoff of training and additional cybersecurity technology?

Human Factors: A CISO's Response to Human Error & Threats

As the Chief Information Security Officer (CISO), balancing the tradeoff between training and additional cybersecurity technology with a limited budget requires a prudent and strategic approach that maximizes security while addressing cyber threats' human and technical aspects. The NIST Cybersecurity Framework (CSF) provides an excellent guide (Nieles, Dempsey, & Yan Pilli, 2017; NIST, 2018). It emphasizes a risk-based and cost-effective approach across its five core functions: Identify, Protect, Detect, Respond, and Recover (Paulsen & Toth, 2016). I would start by leveraging the framework's Framework Core and Implementation Tiers to assess our cybersecurity posture and prioritize spending.

Risk-Based Assessment

First, I will prioritize a risk-based assessment of the company's cybersecurity posture. The assessment would help identify our organization's critical assets, threats, and vulnerabilities. I would analyze past incidents, current threat intelligence, and the organization's specific attack vectors. The analysis would provide a framework profile, comparing our "Current" state to a "Target" state, which would help me identify gaps where training or technology could have the most impact. Training is essential because human error causes over 65% of cybersecurity data breaches (HNS, 2024; Verizon Business, 2024). However, the technological framework must take higher priority and precedence than employee training because detecting, preventing, and responding to sophisticated attacks is essential, and humans alone cannot handle them.

Training & Continual Education

I will allocate about 40% of the company's budget to training and awareness programs. The training sessions will be routine, continuous education tailored to different roles within the

company. For example, general employees handling sensitive data would get phishing simulations and social engineering defense/awareness training, while IT staff participate in technical training on secure configurations and incident response (Cichonski, Millar, Grance, & Scarfone, 2012). The goal is to reduce preventable mistakes—like clicking malicious links or misconfiguring systems—which are cost-effective to address through education rather than cleaning them up after a breach. I would also invest in metrics to measure training effectiveness, like reduced incident rates, to ensure the allocated money for training is well spent and effective. Accurate metrics are also essential when explaining the need to invest in cybersecurity programs and procedures for upper management and stakeholders.

Cybersecurity Technology

The remaining 60% will go toward selective cybersecurity technology. I would focus on solutions that address our highest risks and integrate them well with our existing systems, streamlining the commissioning process while reducing costs for the company. For example, if ransomware is a top threat, I would prioritize endpoint detection and response (EDR) tools and robust backups instead of a niche AI-driven gadget or software/hardware application. I would also direct the company towards scalable, multi-function platforms—like a next-gen firewall with intrusion prevention—over single-purpose tools to help "future-proof" software and hardware by extending their commissioned life within the network. Lastly, if funds are allowed, I will reserve a small portion for emerging tech pilots in Research and Development (R&D) to stay ahead of evolving threats.

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Recommendations of the National Institute of Standards and Technology (NIS). *Computer Security Incident Handling Guide*, August.

HNS. (2024, May 2). *2024 Data Breach Investigations Report: Most breaches involve a non-malicious human element*. Retrieved from Help Net Security (HNS): https://www.helpnetsecurity.com/2024/05/02/verizon-2024-data-breach-investigations-report-dbir/

Nieles, M., Dempsey, K., & Yan Pilli, V. (2017). An Introduction to Information Security. *Computer Security, NIST Special Publication 800-12 Revision 1*, 101.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Gaithersburg, MD: U.S. Department of Commerce.

Paulsen, C., & Toth, P. (2016). Small Business Information Security: The Fundamentals. *National Institute of Standards and Technology (NIST 7621 Revision 1)*, 54.

Verizon Business. (2024, May 1). *2024 Data Breach Investigations Report*. Retrieved from Verizon Business: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf