

Sean Shreve

15APR2026

CYSE 200T

Professor Duvall

Write-Up: The Human Factor in Cybersecurity

BLUF: Balancing cybersecurity training and technology is critical. Prioritizing user training will provide the greatest return on investment because human behavior remains one of the largest vulnerabilities in cybersecurity. While security technologies are essential, their effectiveness depends heavily on how well users understand and follow proper security practices. A tight budget will limit overall capabilities, but the correct effort in a prioritized scheme will narrow the gaps.

The Human Factor

Many cyber threats exploit human weaknesses rather than purely technical flaws. Phishing, social engineering, and poor password habits are all examples of attacks that rely on user error. Cybercrime often occurs because of vulnerable targets and a lack of effective guardianship, which directly ties user behavior and awareness. Industry data supports this, showing that human error contributes to as much as 95% of cybersecurity breaches (Coker, 2025). Even the most advanced security systems can have vulnerabilities exploited if users are not properly trained. The human factor must be kept in mind as the fundamental and unavoidable reality of cybersecurity.

Balancing Technology and Training

Although training should be prioritized, cybersecurity technology still plays a critical role

in a defense in depth strategy. Firewalls, intrusion detection systems, and multifactor authentication are staple tools that provide necessary layers of protection that reduce risk. Implementing these technologies haphazardly are nearly as risky as not including them in the first place. Without proper training, workplace confusion can lead to resistance, misuse, or users attempting to bypass security controls. Clear communication, hands on training, and ongoing support are essential to ensure that employees understand the purpose of these technologies and use them correctly. Baseline technology should be established first with a specific employee comfort level achieved. Once that has occurred, more serious technological upgrades can be implemented with scaled training.

Allocation Strategy

With limited funds, I would allocate a slightly larger portion of the budget toward training initiatives while still maintaining essential security technologies. This would include regular phishing simulations, short and focused training sessions, and continuous awareness programs. At the same time, I would invest in core technologies that support access control and monitoring. I would have to keep focus on staple, baseline level of technology as mentioned before. This approach supports both the human and technical aspects of cybersecurity are addressed, reducing overall organizational risk.

Conclusion: My approach recognizes that cybersecurity is not a technical issue by itself, but a human one. The workforce must be well informed and supported with effective tools and training. Once the force is trained, then the technology can scale in more capabilities without causing much frustration. This can be supported with a limited budget and provides the best strategy for mitigating modern cyber threats.

References

Coker, J. (2025). *95% of data breaches tied to human error in 2024*. Infosecurity Magazine.

<https://www.infosecurity-magazine.com/news/data-breaches-human-error/>