Alexandria Proctor

Professor Duvall

CYSE 200t

4 March 2025

The Human Factor in Cybersecurity

BLUF: As a Chief Information Security Officer with a limited budget, I would prioritize a balanced approach between employee training and investing in necessary cybersecurity technology. While technology can help detect and stop threats, well-trained employees are the first line of defense against most cyber attacks.

Understanding the Threat

Cyber threats are becoming more advanced every day, and humans are often the weakest link. Phishing emails, weak passwords, and accidental clicks on dangerous links are some of the most common ways hackers gain access to systems. If employees don’t know how to spot these risks, even the best cybersecurity tools may not be enough to protect the organization.

Why Training Matters

Training employees on how to recognize and respond to cyber threats is one of the most cost-effective ways to improve security. With regular workshops, short online courses, and practice drills, staff can become more aware and cautious. This helps prevent common mistakes and lowers the chance of successful attacks. Since training usually costs less than advanced technology, it's a smart investment for tight budgets.

The Role of Cybersecurity Technology

While training is important, technology still plays a big role in defending the system. Basic cybersecurity tools like firewalls, antivirus software, and multi-factor authentication should be funded and maintained. I would focus on affordable but effective tools that provide strong protection without using too much of the budget. These tools work behind the scenes to block threats that people might not catch.

Finding the Balance

To balance the budget, I would allocate around 60% to employee training and 40% to cybersecurity tools. This allows me to build a strong culture of cyber safety while also protecting the system with reliable technology. I would also reassess this balance regularly, making adjustments based on new threats or company growth.

Conclusion

In the end, both people and technology are needed to keep a workplace safe from cyber threats. As Chief Information Security Officer, my job is to use the budget wisely. By focusing on employee training and smart technology choices, I can create a secure environment without overspending. The best defense is one that combines smart tools with smarter people.