CYSE200T: Write Up

The Human Factor in Cybersecurity

Taylor Reel

Strengthening Defenses: Training, Testing, and Technology for Limited Budgets

In today's ever-growing society, cyber threats take on not just a technical problem, but a human problem. As a Chief Information Security Officer (CISO) with a limited budget, deciding how to allocate funds between training for employees and cybersecurity technology becomes a challenging task. While advanced tools are important, research shows that human error remains the root cause of most breaches or threats. Due to this, major priority should lie in strengthening human awareness, validate defenses, and ensure that the technology used is effective.

The Harvard Business Review article, *"*The Best Cybersecurity Investment You Can Make Is Better Training*"* makes a clear argument for this: "…even the most sophisticated tools can't protect an organization if employees fall for phishing scams or use weak passwords" (Huang, 2017). Advanced technology can stop certain attacks, but human behavior determines whether those controls fully succeed. Roughly forty percent of the budget should be allocated towards training and awareness programs in order to reinforce employees' ability to recognize and respond to cyber threats. The programs would include role-based cybersecurity training, simulated exercises, and learning programs that measure improvement over time. These directives would reduce risk by addressing one of the most common entry points for attackers, careless or uninformed users.

Although training would help substantially, it alone is not enough to completely reduce cyber risks. Another crucial aspect to eliminating this would be to ensure that our defenses are

actually working as intended. According to an article written by Stacey Ornitz, “How cybersecurity leaders are optimizing their budgets in 2025,” organizations waste money on tools that are either poorly configured or fail to address real attacks (Cymulate, 2025). To avoid this issue, twenty percent of the budget should be used towards regular system evaluations and exposure testing. This would include mock cyberattacks, ranking vulnerability by urgency, and put towards tools that give clear feedback on which security measures are truly making a difference. Continuous testing like this would help ensure that all money spent from the budget is backed by evidence of security improvement.

The last twenty percent of the budget should go towards investments in core detection and response software. Endpoint detection and response software (EDR) specifically has proven to be a very effective way to identify and contain threats before they spread. According to the IBM webpage, “Studies estimate that as many as 90% of successful cyberattacks and 70% of successful data breaches originate at endpoint devices” (IBM, n.d.). These statistics show how critical is it to secure all devices, servers, networks, and other access points that employees use on a daily basis. In addition to EDR, this portion of the budget should also support secure logging systems and basic managed detection services. These tools are essential for quickly spotting and responding to breaches, but they must be scaled accordingly. A smaller system that security personnel fully understands is much more valuable thana larger, more complex one that employees have trouble managing. By focusing this part of the budget on practical, well-managed detection tools, the organization can build a strong second line of defense that quickly identifies threats and limits damage before it spreads.

In conclusion, with a limited cybersecurity budget, the best approach is to prioritize employee training, support it with regular testing, and invest in practical detection tools. This

strategy reduces risk, ensures defenses work, and helps the organization stay ahead of potential threats.

References

Disparte, D., & Furlow, C. (2017, May 16). *The Best Cybersecurity Investment You Can Make is better training*. Harvard Business Review. https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

Ibm. (2025, September 16). *What is endpoint detection and response (EDR)?*. IBM. https://www.ibm.com/think/topics/edr

Ornitz, S. (2025, June 3). *Optimizing cybersecurity budgets in 2025: A strategic guide*. Cymulate. https://cymulate.com/blog/cybersecurity-budget-optimization/?utm_source=chatgpt.com