Brandon Norton

CYSE 200T

April 6, 2025

Professor Duvall

A Fine Balance of Budgeting Training and Cybersecurity IT

BLUF: Budgeting for a comprehensive cybersecurity framework may be challenging, but with the correct management of resources and knowledge of your network/team, the limits are higher than you might think.

The Importance of Training

With 70% of data breaches being caused by the human element in 2023 (CybSafe, 2023), it’s clear that adequate training is the weakest link when it comes to comprehensive cybersecurity coverage. For training to be effective, however, everybody on the network must be on the same page; training must be mandatory for everyone. One untrained user or sysadmin could be the vulnerability that cripples your network. As a CISO of a large company, mandatory training will be a high priority of mine. Training doesn’t have to be a slog, however; there are methods and educational activities to make companywide training a fun and educational event. In addition to the training being mandatory, it also must be a repeatable event (annually) and consistently maintained.

The Cost of Training

Fortunately, training is significantly cheaper than purchasing licenses and additional hardware that could run the company tens of thousands of dollars. Assuming the company already has a functional cybersecurity team, these employees that are already on payroll can be utilized to develop a comprehensive training program. I would task them with finding our company’s vulnerabilities and incorporating that information into our training classes. Cost wise, we would only lose a few man-hours. The damage that we could prevent, however, is invaluable.

The Balance of Training and IT

Training may be important, but I wouldn’t put all my eggs into one basket, because maintaining modern cybersecurity technology is also important. My cybersecurity team needs to find the right balance of training and technology, which may be difficult to find as every company’s goals and priorities are different. Older systems (especially legacy systems) take significantly longer to secure and lock down; one missed configuration or patch day and your system could be left wide open for exploitation (Mukherjee, 2024).

Conclusion: Both training and modern cybersecurity technologies are important, however, technology is only as effective as the person using it. Untrained admins and users could unintentionally wreak havoc on a network simply because they are untrained; they don’t know what they don’t know. On the flip side, training can only carry you so far, because at a certain point, dated technology could become a vulnerability that takes a network down.

CybSafe. “7 Reasons Why Security Awareness Training Is Important in 2023.” *CybSafe*, 4 Apr. 2023, www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important. Accessed 6 Apr. 2025.

Mukherjee, Sourjesh. “Common Vulnerabilities in Legacy Systems and How to Mitigate Them | SecOps® Solution.” *Secopsolution.com*, 15 May 2024, www.secopsolution.com/blog/common-vulnerabilities-in-legacy-systems-and-how-to-mitigate-them. Accessed 6 Apr. 2025.