**A Day as a Chief Information Security Officer**

Antonio E. SantiagoFigueroa

Old Dominion University

CYSE 200T

Professor Haghnegahdar

November 8, 2024

Both training and new technologies are critical in protecting our assets. However, in this write up I will explain why I think training is more important at the end of the day. Without any training, the technologies we have are useless.

Before even beginning to spend any money, we must evaluate our current situation to see what we are lacking in. Are employees following basic policy regarding security? What is the level of awareness within the staff on cybersecurity? Do we know what our most common threats are? If the most basic policies, which are normally the most important, then what reason do we have to even invest in new technologies.

Training does much more than simply teach employees about policies. It promotes an environment where cybersecurity is at the forehead of employees’ thoughts, some simple mistake that might have been done in the past in ignorance will now be recognized and avoided. If someone is not sure if its ok to do something they will be more likely to ask instead of doing it. Humans are often the weak link in security due to things like phishing emails or not safely handling sensitive information. It also has a high return on investment as training is very cheap and significantly reduces the likelihood of attacks.

Once training has been properly addressed, we can start thinking about introducing new technologies. We should analyze in what ways our organization has historically been attacked and seek technologies to address those vectors of attack. The protection of sensitive data should also be prioritized. If current technologies are outdated, we can also think about upgrading those. With new technologies comes the added burden of having to train staff on how to operate these new systems which is something that cannot be forgotten. I think my allocation if I were a Chief Information Security Officer would be 65% to training and 35% to new technologies.

In conclusion, both training and new technologies are important but since without training new technologies are useless, I would have to prioritize training. Investments in technology should be geared towards targeting gaps in security that current technology doesn’t address. This balance creates a strong security layer that makes full use of all staff and implemented technologies while staying mindful of a non-infinite budget.

References

Alam, F. (n.d.). Four ways to embrace emerging tech with Cyber. Retrieved from https://www.ey.com/en\_us/insights/emerging-technologies/four-ways-to-embrace-emerging-tech-with-cyber

CybSafe. (2023). 7 reasons why security awareness training is important in 2023. Retrieved from https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/

Prümmer, J. (2023). A systematic review of current cybersecurity training methods. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404823004959

Robb, D. (2023). How security awareness training is evolving. Retrieved from https://www.shrm.org/topics-tools/news/technology/how-security-awareness-training-is-evolving