

The Human Factor in Cybersecurity

Xavier Guiler

CYSE200T

3/22/24

For a balancing tradeoff between training and cybersecurity technology with a limited budget as a Chief Information Security Officer, I would maximize the effectiveness of both the aspects while ensuring that funds would be placed efficiently. We can allocate our funds strategically towards training programs and to enhance our cybersecurity technology to maximize security in the company.

Training

While cybersecurity technology is especially important, I would start by investing a larger portion of the budget into training as human error is one of the largest causes of data breaches. “Human error is inevitable, even in fields as thorough and technically efficient as cybersecurity” (Butaka 2021). By training employees, we give them education and awareness about the latest threats and the best practices to avoid these which are significant for preventing cyber threats. By giving regular training to employees about cybersecurity practices and safe internet usage, we can count on them as a layer of defense against potential cyber threats. Cybercriminals often target employees with tactics such as phishing, this leads to many other holes that this cybercriminal could use. Without the correct and proper training, employees are more likely to click on malicious links by accident which could leak sensitive data. Not only would this training ensure an enhanced and effective defense against threats but also it would create security awareness within the organization and whoever these employees teach these practices too as well.

Cybersecurity Technology

Secondly, I would portion the rest towards cybersecurity technology as having the right tools for these threats is just as important as the training is. These tools could include firewalls, intrusion

detection systems (IDS), and intrusion prevention systems (IPS). Levering these tools of IDS and IPS can allow more efficient and effective protection of specific but critical assets in the company. Depending on the company, technologies such as encryption, multi-factor authentication (MFA), and secure access controls could also ensure the safety of sensitive and critical data. By ensuring that our technology is up to date and the strongest it can be, we minimize potential threats, breaches, and ensure we stay ahead of the never-ending cyber threats.

In conclusion, by ensuring the balance between training and cybersecurity technology, we can ensure the protection of the company. I would prioritize education while leveraging cybersecurity technology to maximize the company's defenses. I believe this would maximize the effectiveness of the company's limited budget and the results of this process. By doing so, we can mitigate risks, and optimize the company's added resources towards a specific cause with less worry of human error.

References

Human error in Cyberspace. ISACA. (n.d.). <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-38/human-error-in-cyberspace>

Jayaraman, N. (2023, December 15). *IDS vs. IPS: Key difference and similarities best for Cybersecurity*. Cybersecurity Exchange. <https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/>