Ava McLaughlin

CYSE 200T

April 5, 2025

The Human Factor in Cybersecurity

BLUF: Employees need proper training to prevent cyberattacks effectively; however, the cost of training, along with implementing other essential cybersecurity measures, can become overwhelming quickly. As Chief Information Security Officer, I would allocate my limited funds by consulting CISA and the CPGs, finding a balance between training and cybersecurity essentials, and experimenting with potential AI solutions.

CISA & the CPGs

Mr. David Price, a representative of CISA (Cybersecurity and Infrastructure Security Agency), explained that the agency developed Cross-Sector Cybersecurity Performance Goals (CPGs) to serve as a baseline for implementing cybersecurity practices. CPGs are especially effective for small to medium-sized businesses due to their prioritization of cost-effective solutions. Cost, impact, and ease of implementation are factors used to prioritize which goals to address first, which would be extremely helpful in determining how to allocate resources effectively. CPGs currently address five of the six core activities of the NIST Framework, including Identify, Protect, Detect, Respond, and Recover (Cybersecurity performance goals). CISA even offers free evaluations to help businesses assess their cybersecurity frameworks, allowing me to redirect the funds I would have spent on assessments toward other priorities like training, essential cybersecurity tools, and potential AI solutions.

Balancing Training & Cybersecurity Essentials

Despite the focus on technology, human psychology plays a crucial role in Cybersecurity; in fact, out "of the 9 areas of the psycho-technological matrix of cybersecurity threats, only 3 do not involve human psychology" (Why Is Cyber Security). People are often the greatest threat in security systems because human errors, like falling for phishing attacks, using weak passwords, or accidentally revealing sensitive information, can escape even the most advanced technological defenses; training is essential for this reason and should be considered just as important as technological defenses. As CISO, I would prioritize training practices alongside essential cyber defenses, such as firewalls, intrusion detection systems, and multi-factor authentication, ensuring that both are equally emphasized.

Potential AI Solutions

AI has proven to be valuable in some areas like automation, as well as threat detection and response. Workplace deviance is becoming more prevalent, likely due to advanced cyber threats that enable attackers to stay anonymous; this has created a demand for Zero-Trust policies. By integrating AI into systems, access to sensitive information can be limited to fewer employees, and security processes can be automated, reducing human error and strengthening overall protection (Capone, 2018). According to an article by Balbix, there are five top benefits of AI in Cybersecurity, such as improved threat intelligence, faster incident response times, better vulnerability management, more accurate breach risk predictions, and automated recommendations (Goodman, 2025). Not only is AI efficient, it's also cost-effective, as "organizations with extensive use of security AI and automation demonstrated the highest cost savings comparatively, with an average cost of a data breach at $3.60 million, which was USD 1.76 million less and a 39.3% difference compared to no use" (Vazquez, 2023).

References

Capone, J. (2018, May 25). The impact of human behavior on security. https://docs.google.com/document/d/1J3v_V167mktbGVynbtHW8yHXW9onjaBzVASo-behDfY/edit?tab=t.0

Cybersecurity performance goals (cpgs): CISA. *Cybersecurity and Infrastructure Security Agency CISA.* (n.d.). https://www.cisa.gov/cybersecurity-performance-goals-cpgs

Goodman, C. (2025, January 16). Artificial Intelligence in Cybersecurity. *Balbix.* https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

Vazquez, I. (2023, September 21). Economic impact of automation and artificial intelligence. *WatchGuard Blog*. https://www.watchguard.com/wgrd-news/blog/economic-impact-automation-and-artificial-intelligence

Why Is Cyber Security About Human Behavior? *Cyberbitsetc.org.* (n.d.). https://docs.google.com/document/d/1QplIrfcKlmkSOuKt9i0Kte72kYrukFeCm1wj9DxpnGU/edit?tab=t.0