The Human Factory In Cyber Security

If a CISO is met with the challenge of limited resources when deciding where to allocate their cybersecurity foundations, several aspects must be considered. If there is a reliable physical or software based asset that leads to a more secure environment, then that should be prioritized. However, the importance of the human factor cannot be overlooked. Training and regular protocol updates are paramount and must be a part of any secure organization.

The Problem

In this hypothetical, the CISO of an organization is faced with the allocation of limited resources and must decide on what to prioritize when setting up the cybersecurity foundations. There are multiple things to consider when deciding what determines an organization's security. Why would the organization be attacked? What sensitive assets does the organization hold? What type of clientele do they work with? All of these variables play into the planning and preparation of a cybersecurity framework.

The Non-Human Factor.

Obviously, without hardware such as servers or databases, there is little to no need for a cybersecurity infrastructure. As a baseline, a secure database and basic firewall to limit and monitor traffic on the network should be implemented. Software such as a secure and reliable firewall is relatively inexpensive[1,2], so therefore its value is far above that of its actual price, making it a high priority. Things such as secure airlock doors and advanced security systems run a high bill at the benefit of relatively little baseline security, making them non-essential.

The Human Factor

The human factor in cybersecurity is arguably one of the most important components in a secure organization. If resources had to be allocated between devices, software, and personnel training, arguably 70% should go towards the training. The employees of an organization maintain a unique position of being the first and oftentimes last lines of defense against cyber attacks. Thorough training and planning must go into the preparation of any incidents like malware attacks, DDoS attacks, and phishing attempts. The value of such training is easy to overlook, as the benefits are not readily visible. However, the most common types of cyberattacks on organizations today are initiated through human contact. Phishing, spear phishing, and target brute force password attacks are extremely common ways individual employees can lead to an attack being successful on an organization and therefore, can be one of the biggest liabilities[3].

[1] *Network Firewall Price.* Fortinet.

[2] *Understanding Firewalls for home and small office use.* Lepide Blog.

[3] *15 common types of cyber attacks and how to mitigate them.* Robinson, P.

Conclusion

In conclusion, the benefits to training the human factor of a cybersecurity framework tower above those given by the software side. If faced with limited resources and a selection between upgrading hardware and training personnel is to be made, nine times out of ten, it's the better bet to go with the human aspect.

References

Markovic, I. (2023, December 13). What is the average cost of training a new employee?. eduMe.https://www.edume.com/blog/cost-of-training-a-new-employee#:~:text=According%20to%20the%20Association%20for,on%20training%20and%20development%20initiatives.

Network firewall price: Comparing security costs. Fortinet. (n.d.). https://www.fortinet.com/products/network-firewall-pricing#:~:text=Firewall%20Security%20Price,and%20%244%2C000%20for%20firewall%20hardware.

Robinson, P. (2024, February 8). 15 common types of cyber attacks and how to mitigate them. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

Understanding firewalls for home and small office use: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, April 4). https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use#:~:text=Firewalls%20do%20not%20guarantee%20that,run%20malware%20on%20your%20computer

GeeksforGeeks. (2023, February 22). Difference between authentication and

authorization. GeeksforGeeks

https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/

Google. (n.d.). What is the CIA triad_ definition, explanation, examples - techtarget.pdf.

Google Drive.
https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

Hashemi-Pour, C., & Wigmore, I. (2023, August 1). What is internet of things privacy (IOT privacy)?: Definition from TechTarget. IoT Agenda.
https://www.techtarget.com/iotagenda/definition/Internet-of-Things-privacy-IoT-privacy

Shea, S. (2022, August 11). What is Data Security? the ultimate guide. Security. https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know