Bianca Perez

4/9/2023

The Human Factor

A Chief Information Security Officer ". . . is responsible for the overall security of an organization's information systems." (Watts, 2022). Though faced with a limited budget, means that an CISO has to challenge the tradeoff between training and cybersecurity technology. In this essay, I will discuss as a Chief Information Security Officer how I would allocate the budget towards training and cybersecurity technology while explaining my reasons for doing so.

The First Step

Initial recommendation: a Chief Information Security Officer (CISO) should evaluate the data of the technology, processes, security posture. By doing this, I will learn about the organization's state and improve the security. Once I gather the insights, I will also find what threats are facing the organization and the current security posture. The assessments will reveal where it's critical to devote the funds to, whether that is technology or training.

The User's Use of Technology

The Human Factor in cybersecurity ". . . [is] the weakest component for the security of any ICT infrastructure and implies the greatest risks and threats for a company or organization." (Team, 2022). Researchers have conducted 9 out 10 data breaches that are caused by users. Proving that users are the main cause for threats to occur. Therefore employee training is crucial

to any company to mitigate attacks and alleviate the probability of errors. In particular, having cybersecurity awareness training is the most efficient way to inform employees on how to strengthen the human element of the company's security. The training program can cover phishing, passwords, and social engineering to ensure a secure environment. Overall, most of the funds will go toward employee training as it's essential to have confidence that the workforce can face security challenges now and in the future.

Cybersecurity Technology

The remaining funds will go to cybersecurity technology that provides the best protection. For instance, a firewall security ". . . provides a set of related programs that prevent outsiders from accessing data on a private network." (Cybersecurity for Small Businesses, n.d.) A firewall also protects computers from malicious software and helps identify any rogue network traffic, a first line defense in any network security. Furthermore, it prevents hacking and promotes privacy for sensitive data. To leverage the firewall, I would use up-to-date antivirus software: Providing a security combination that works in unison. Ensuring the availability to easily disable or solve security threats. A next layer of protection I would ensure is an Intrusion Detection System (IDS), an application that oversees any hostile activity or any violations. The benefit of such a system is that it will notify an attack that might be taking place in real time. Which time is vital in these situations before any more damage occurs. Whenever the IDS targets any malicious activity, an Intrusion Prevention System (IPS) is a tool that takes action against it. This technology ensures that all traffic that enters the system obeys the policies that are stated by the organization. However, since there is a limited budget, the remaining resources should only be spent on the best protection for the employees to have full advantage.

Conclusion

In conclusion, the most important aspect to focus is on the human factor when it comes to the security of the organization. For humans will always make mistakes that could cost the company its data and safety. The remaining will go to the cybersecurity technology that should benefit the workforce. Overall, it is challenging to do a tradeoff with security but it's rewarding to solve any issues that come along.

References

Cybersecurity for Small Businesses. (n.d.). Federal Communications Commission. https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

Team, N. M. (2022, December 20). *Human Factors in Cybersecurity: Protect Yourself - Think Big. Think Big.* https://business.blogthinkbig.com/human-factors-in-cybersecurity/

Watts, S. (2022, November 22). *The CISO Role: What Does a Chief Information Security Officer Do?* Splunk-Blogs. https://www.splunk.com/en_us/blog/learn/chief-information-security-officer-ciso-role.html#:~:text=A%20CISO%20is%20responsible%20for,security%20teams%20at%20larger%20organizations