Adeline Harris

Write-up: The Human Factor in Cybersecurity

As the Chief Information Officer (CISO) of a company, it is my responsibility to protect our company's digital assets against evolving sophisticated cyber threats. However, I must undertake this task within the constraints of my limited budget, where every expense must be properly priortized and justified. In my role I must decide how best to manage our resources: invest in employee training or acquire more cybersecurity technology. This write-up will examine the decisions and compromises involved in finding the right balance between these two critical aspects of cybersecurity defense.

Tradeoff in Cybersecurity

A tradeoff, in general, entails compromising one thing for another. Within a company, there already exists a tradeoff between investing in employee's training and implementing cybersecurity technology during the strategic decision-making process where funds or resources are to be allocated. With limited funds, this process tends to be complex. Investing in these two aspects is important to enhancing the company's security posture. Employee training, on one hand, involves creating awareness on best practices, threats, attack vectors, and methods, as well as incident response, to prepare them to recognize and mitigate risks. Cybersecurity technology, on the other hand, involves purchasing and implementing various applications, hardware tools for detecting, protecting and responding to threats. The tradeoff arises from the need to effectively balance these two, considering the factor of limited budget and the threat environment. Finding a balance is crucial for strengthening a company's cybersecurity posture.

In today's interconnected digital age companies are made constant targets for cyber threats ranging from social engineering, malware attack on systems to ransomware and data breaches. To protect the company's confidential information both employee training and implementing cyber technology solutions must be prioritized.

Employee Training is essential for a robust cybersecurity posture. Employees represent the weakest security link, thus ensuring their training stands as the first line of defense against attacks. Such training aids them in identifying and mitigating risk before they lead to damage. These programs equip employees with the necessary knowledge and skills to recognize phishing attempts, social engineering tactics, and follow cybersecurity best practices. Additionally, it promotes a culture of cybersecurity awareness, wherein employees grasp the importance of employing strong passwords, securing their devices and promptly reporting any unusual activities. Through continuous training, companies can empower their employees to proactively protect their assets.

Cyber Technology - While employee training is essential, it does not provide complete protection against cyberattacks. Deploying advanced technology solutions such as VPNs, firewalls, and intrusion detection systems, continually monitors, detects and responds in real-time to mitigate risks. Additionally, encryption which secures confidential data and multi-factor authentication add another layer of security. (Elve8me, n.d.) (Marvin, 2024) (NCC DATA, n.d.)

Allocation Decision

Managing security with limited funds poses a challenge for a company, as it hinders investment in training programs or additional cybersecurity technologies due to financial constraints. Creating successful training programs can be expensive, involving costs such as hiring trainers and acquiring materials. Maintaining regular training may also prove difficult in the long term. Acquiring and implementing cybersecurity technologies can be similarly costly, encompassing expenses such as hardware purchase, licensing fees, and upkeep. Investing in new technologies becomes challenging with limited funds. As a CSIO with constrained resources, deciding how to allocate resources between training and additional cybersecurity technology is daunting. Prioritizing one over the other affects the security posture, potentially leaving the company vulnerable to threats or knowledge gaps that could lead to severe consequences. Several factors need consideration when allocating funds:

1. **Risk Assessment:** Evaluating the company's security posture and identifying weaknesses guides investment decisions based by focusing on high-risk and high-impact areas.

2. **Assessing competency and skills level of employees:** Evaluating their skills is crucial. If they lack security knowledge, investing training will be beneficial. Conversely, if they are proficient, investing in additional technology may be preferable.
3. **Monitoring Emerging threats and Tool Availability:** Keeping up with new threats and technology is essential. Investing in advanced tools can enhance security. Additionally, estimating the cost of these tools is imperative.

Based on risk assessment and identifying areas with high risks, a portion of the funds will be allocated where they are needed most urgently to address them. A significant portion will be allocated to training employees tailored to their roles and responsibilities and utilize cost-effective technology solutions such as cloud-based, which offers operational benefits at lower cost. Additionally, outsource other security functions.

(SenseOn, n.d.) (Ryerse, 2023)

In conclusion, balancing investment between employee training and cybersecurity technology is crucial, as both are vital for enhancing the cybersecurity posture of a company. To effectively manage the limited funds, it is important to evaluate employee skills, conduct thorough risk assessments, and prioritize investments. As CISOs, it is important to maximize cybersecurity investments to reduce risks and protect the company's assets in a threatening environment.

References

Elve8me. (n.d.).

Marvin, M. (2024, January 24). *A CISO's Guide to Balancing Cybersecurity and Productivity*. Portnox. Retrieved April 5, 2024, from https://www.portnox.com/blog/security-trends/a-cisos-guide-to-balancing-cybersecurity-and-productivity/

NCC DATA. (n.d.). Wikipedia. Retrieved April 5, 2024, from https://www.linkedin.com/pulse/best-ways-use-technology-prevent-cybersecurity-attack-ncc-data/

Ryerse, J. (2023, October 18). *Cybersecurity Budget: Tips for Effective Allocation*. ConnectWise. Retrieved April 5, 2024, from https://www.connectwise.com/blog/cybersecurity/cybersecurity-budget-planning

SenseOn. (n.d.). Wikipedia. Retrieved April 5, 2024, from https://www.linkedin.com/pulse/how-much-should-business-spend-cybersecurity-senseon-tech/