Emmanuel Asare

CYSE 200

Cybersecurity Information Security Officer Budget

As a Chief information security officer, my goal is to ensure that the security and privacy of an organization's information and assets is secure. To accomplish this I will need to balance the tradeoff between training and additional technology for cybersecurity. I will need to focus on multiple aspects of an organization's risk assessment profile and resources.

Why is employee training important?

Due to the limited budget, cybersecurity training will be important for employees because they are easily targeted by potential hackers. According to the article "What makes businesses a target for cybercrime". "Employees are often the biggest threat to the security of your company–that is due to the inadequate employee training in best practices (Leonidas, 2018). Since most employees do not know basic cybersecurity they surf the web without being cautious of what they are doing this can lead them to downloading malicious software to computers. They can be subjected to scam and phishing emails where they can also potentially download and also send out personal information to attackers. Due to this I will ensure that employees are trained to reduce cyber attacks. Training will include security awareness, making sure they are using secured passwords and also changing passwords every 30-60 days. They can also be trained on phishing and get emails about security tips.

How will I emphasize the importance of cybersecurity technology?

With cybersecurity technology I will make sure I implement security controls. Employees will get access to not all aspects of a company's device but only certain things that they need

based on their job. For example, front desk workers will have access to low level permissions needed to help with basic questions and people on the highest rank of the organization like the CEO and etc will have the most control over things like budget, data, etc. I will also make sure firewalls are implemented. With firewalls I can monitor all traffic in the company's network so that if an unauthorized person gets access to the company's network I can block it and remove it. I'll also buy intrusion detection systems to monitor the company's network for malicious activity. According to Techtarget "AN IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use their IDS logs as part of the documentation to show that they are meeting certain compliance requirements (What is an intrusion Detection System(IDS)? Definition from SearchSecurity, 2021)". I'll also implement the use of antivirus like Norton 360 or McAfee. This will be the basic level of security I would use to prevent threats. How I would allocate the limited budget will be based on the organization's most risks and prioritize cybersecurity measures that will potentially address the risks and allocate resources for such risks. Which can mean either investing in training employees or investing more in technology.

Conclusion

   In conclusion my job as a cybersecurity information security officer will require the need to make decisions on either focusing on employee training or additional cybersecurity technology. Even though additional cybersecurity technology is good you still need to make sure employees are trained with the basics of cybersecurity in order to ensure the company is safe. It's much more efficient for employees to follow cyber policies than having employees who don't have a clue on policies and having to go back and spend money on potential payments in order to fix a

leak in a company's security system. The need for employee training is important but additional

technology can assist in making sure your company is in a safer position.

Works Cited

Leonidas, M. (2018, June 29). *What Makes Businesses a Target for Cyber Crime | NIC IT Partner*. NIC IT Solutions. https://www.nicitpartner.com/makes-businesses-target-cybercrime/

What is an intrusion detection system (IDS)? Definition from SearchSecurity. (2021, October 1). Security. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system