Implementing effective Cybersecurity Investments

Nehemia Araia

Department of Cybersecurity, Old Dominion University

CYSE200T: 31563

Dr. Charles E. Kirkpatrick

March 31st, 2024

After reading this week's readings and various articles I have learned that it would be pretty challenging to balance training and additional cybersecurity technology with limited funds. I would approach this decision by making sure I have a good understanding of our organizations specific risks, vulnerabilities and current cybersecurity posture. Overall, I would make sure to make my decision as balanced as possible while incorporating what I feel is most important.

Continuous Evaluation and Adjustment

While keeping in mind that cyber threats are constantly evolving, it is crucial to continuously evaluate the effectiveness of both the technical and training side. Regular assessments, penetration testing, and incident response exercises will help identify areas for improvement and better future decision making. By considering these options organizations can identify vulnerabilities, improve preparedness, and most importantly mitigate the risk of cyber threats. As the Chief Information Security Officer, I would need to gain more insight and evaluate my options more as this will determine the strength of my security for my organization.

Employee Training and Technology

My two biggest priorities acknowledging that I have a limited budget would be essential cybersecurity technologies and employee training and awareness programs. I would still make sure to incorporate other components like risk assessment as an example but would mostly balance between the two I provided as they will be the most effective. For technology, next-generation firewalls, intrusion detection and prevention systems, and vulnerability management tools are all technologies that would provide the most value for my potential budget. Investing in these specific cybersecurity technologies will form a crucial layer of defense while also mitigating potential risks. For security training, it is no longer an event or an annual mandatory compliance checklist (Krishnan, 2022, p.1). People are often the weakest in cybersecurity defenses due to the lack of an effort in making sure everyone is trained properly. I choose this as a second priority because it is crucial to invest in this as employees should be able to recognize and mitigate cyber threats efficiently.

Conclusion

In conclusion, After reading this week's reading and gaining more knowledge through research and articles I have created a balanced and strong defensive strategy. I made sure to include what I felt like would benefit the company the most while maximizing the effectiveness of the options that I decided to choose with a limited budget.

References

Krishnan, A. (2022, September 1). *Cybersecurity budget breakdown and best practices: TechTarget*. Security. https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices

Harrington, D. (2023, October 26). *Cisos navigate budgets and business-cybersecurity*. ENHALO. https://enhalo.co/must-know-cyber/cisos-must-navigate-budgets-and-business-savvy-cybersecurity/