Name: Chris Coleman

Date: March 21st, 2024

The Head of the Table

BLUF

Finding a balance between hiring cybersecurity experts and purchasing technology is essential in the innovative field of cybersecurity resource management. The study explores the complex choices involved in directing limited funds toward improving technological defenses and human skills. By carefully examining the benefits and drawbacks of each strategy, this research aims to provide insightful guidance on how best to allocate resources to minimize cyberthreats and strengthen organizational cybersecurity.

Introduction

As the organization's Chief Information Security Officer (CISO), it is my responsibility to make sure that, despite my limited resources, the cybersecurity posture of the company is strong. To weigh the advantages and disadvantages of investing in cybersecurity technology with employee training, I would place a higher priority on a well-rounded strategy that takes both factors into account.

The Strategy

Before anything else, I would set aside a couple of thousand dollars for thorough cybersecurity training for each employee. The main objectives of this training would be to enlighten staff members about popular cyber threats, teach them best practices for managing sensitive data, and offer direction on recognizing and preventing possible security problems. By funding training, we enable staff members to take on the role of active cyber defenders, decreasing the possibility that human mistakes would result in breaches of security. At the same time, I would set aside money to invest in fundamental cybersecurity technologies that safeguard our network and data. Purchasing reliable device protection solutions,

firewalls, intrusion detection systems, and encryption tools are a few examples of how to do this. These solutions will help reduce the dangers of malware, unauthorized access, and data breaches while acting as the first line of defense against external threats.

Conclusion

Overall, we can fortify our organization's defenses against new cyber threats while making the best use of our limited budget by implementing a balanced approach that combines staff training with strategic investments in cybersecurity technology. This strategy recognizes the vital role that technological advancements and human factors play in protecting the digital assets of our company and lowering cybersecurity risks.

References

Reid, J. (2023, August 9). *The human factor in cybersecurity: Crowe LLP*. Crowe. https://www.crowe.com/insights/the-human-factor-in-

cybersecurity#:~:text=Some%20of%20the%20most%20common,comes%20to%20operational%20security%20measures.

Hamayun, M. (2023, November 23). *The importance of the human factor in cyber security*. Check Point Blog. https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/