Brendan Marcelo
CY200T

# Strategic investments in Cybersecurity

Cybersecurity in continuously evolving, it is crucial for Chief Information Security Officers to make strategic investments that address both human and technical factors. This paper explores how CISOs can effectively balance their limited budgets by prioritizing comprehensive training programs, enhancing cyber hygiene practices, conducting vulnerability assessments, and investing in essential cybersecurity technologies.

## Intro

As a Chief Information Security Officer, it is essential to prioritize investments and manage a limited budget that address technical solutions and human factors. Investing in comprehensive training programs, augmenting employee cyber hygiene, conduct vulnerability assessments, implement essential technologies, and educational investments for employees.

## Employee Training

As a chief information security officer, it is vital to allocate a significant portion of the budget to develop and implement comprehensive cybersecurity training for all levels of employees. Cybersecurity awareness programs are comprehensive, long-term products that show your workforce how to spot security threats and potential attacks(Esecurityplanet, n.d.) By implementing this type of training, it offers an up to date dashboard of campaign and user activity without the box reporting, an intuitive administrative interface, and the ability to customize or cobrand the service(csooline.com)

Security awareness is an essential in any part of risk management strategy and helps raise awareness on password security, phishing attacks, and cyberthreats.

### Cyber Hygiene

Cyber hygiene is used to create a structured and intelligent environment that reduces the risks of external contamination without having consistently spend lots of IT efforts on these processes(Watts,2023). Cyber hygiene consists of monitoring systems and databases, managing user access systems, and adequate protection of important data. Allocating resources to promote strong password management, multi-factor authentication, and securing remote access policies is vital for cyber security hygiene.

### Vulnerability Assessments

Identifying security weakness and applications in systems and applications plays a big role in conducting vulnerability assessments.  More Saas (software as a service) customers now require regular vulnerability assessments, and having proof of security testing can also help you to generate more business(intruder,2023).

### Essential Technologies

Allocating funds for essential technologies that provide foundational security measures is a significant part in the budget. Technologies such as antivirus software, endpoint protection solutions, and endpoint detection response or EDR tools. EDR tools are used to protect devices from malware and unauthorized access. Tools such as firewalls, intrusion detection systems, and intrusion prevention systems to monitor and secure network against malicious activities. As well as implementing these tools into, it is also important to upgrade outdate software and minimize redundant software within your network. Keeping up with inventory of the network such as number of hosts to the location of network servers can also play a factor in strategically planning a budget.

## Employee Education

Another major part of the budget is to invest in proper certification programs for employees at every level. Cybersecurity is full of individuals who work together to keep your network infrastructure in tact, therefore a major investment is to make sure employees are trained to do so. This can be utilized by investing in certifications for employees such as any CompTIA certification that has to do with the sector of cybersecurity your company specializes in. Also raising awareness about common cyber threats, password security, data protection, and phishing attacks. Regular training sessions and simulated exercises about these topics are essential to better your employees and contribute to your budget as a chief financial officer.

## Conclusion

In conclusion, effective cybersecurity management requires a balanced approach that addresses both technical solutions and human factors. By investing in comprehensive training programs, enhancing cyber hygiene practices, conducting regular vulnerability assessments, and employing essential tech, organizations can strengthen security measures and mitigate the risk of cyber-attacks. Ongoing training and certification for employees plays an essential role in building a culture of cybersecurity awareness and readiness in the organization. Overall, a strategic allocation of resources to address technical and human aspects of cybersecurity is a key portion of an organizations budget.

## Works Cited

Madden, A. (2018, June 13). *Efficient deployment of Cybersecurity*. IT1. https://it1.com/efficient-deployment-of-cybersecurity/

Taylor, M. (2024, February 13). *The Benefits of a Virtual Chief Information Security Officer (vCISO)*. Secure Cyber Defense. https://securecyberdefense.com/the-benefits-of-a-virtual-chief-information-security-officer-vciso/#:~:text=A%20vCISO%20will%20conduct%20a

Intruder. (2023). *How To Perform A Vulnerability Assessment: A Step-by-Step Guide*. Www.intruder.io. https://www.intruder.io/guides/vulnerability-assessment-made-simple-a-step-by-step-guide

*Cyberhygiene program by ISSP*. (n.d.). ISSP Global. Retrieved March 25, 2024, from https://www.issp.com/cyberhygiene

Watts, S. (2023, October 31). *Cyber Hygiene: Concepts and Best Practices for Cybersecurity*. Splunk-Blogs. https://www.splunk.com/en_us/blog/learn/cyber-hygiene.html

*Cybersecurity Training | Best Cybersecurity Awareness Training*. (2020, March 10). ESecurityPlanet. https://www.esecurityplanet.com/products/cybersecurity-training/