Balancing the Budget for my Company

Camillia Epps

Charles E. Kirkpatrick

CYSE-200

23 March 2024

BLUFF

In my role as Chief Information Security Officer (CISO), I have the responsibility of protecting our organization's digital assets among a continually shifting landscape of cyber threats, all within the constraints of a tight budget. To effectively manage this, I utilize a deliberate resource allocation strategy that weighs the benefits of investing in comprehensive training initiatives against acquiring fundamental cybersecurity technologies.

Training Programs

As the Chief Information Security Officer (CISO), the critical importance of allocating funds to user training programs. These programs are crucial for teaching my employees the skills and knowledge they need to deal with the always-changing dangers of the internet. I am putting money into training, so my team learns how to stay safe online and handle security issues well. This approach helps put a stop to the risk of breaches caused by human error, enhancing my organization's overall cybersecurity resilience.

Incident Response Planning

As the Chief Information Security Officer (CISO), Investing in incident response planning is crucial for a CISO. It ensures my organization can quickly and effectively handle security issues. By making my plans better and practicing drills, I can make sure there's less damage or problems. Doing drills often helps me get better at responding and fixing any problems. This approach makes my cybersecurity stronger and lessens the impact of potential threats. Organizations should create a policy that states who is designated to report incidents and how the incidents should be reported. Requirements, categories, and timeframes for reporting incidents to US-CERT are on the US-CERT website. (Cichonski et al., 2012)

Security Awareness and Phishing

As the Chief Information Security Officer (CISO) making our security awareness program better is important, especially for fighting against phishing attacks. Phishing is a deceptive tactic used by cybercriminals to trick individuals into divulging sensitive information such as passwords or financial details. For instance, an employee might receive an email seemingly from their bank, urging them to click a link and verify their account details. However, the link leads to a fake website designed to steal their login credentials. By educating employees about such tactics and conducting phishing simulation exercises, we can help them to recognize and report suspicious emails and stop them from falling victim to such scams. It is critical to raise and maintain phishing awareness among employees with regular security training, maximizing the odds they recognize attacks. Simulated phishing exercises put users' knowledge to the test and show what types of attacks they are most likely to fall for so security teams can update training programs accordingly. (How to defend against phishing as a service and phishing kits, 2024)

Regulatory Compliance and Governance

As the Chief Information Security Officer (CISO), prioritizing compliance with regulations like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) is essential. These standards will be how we handle personal and payment data, ensuring it's kept secure. For instance, GDPR requires obtaining consent before using customers' personal information for marketing purposes. Using money for things like making data safe and controlling who can access it helps us keep our customers happy and follow the rules, which keeps our reputation safe.

Improvement and Innovation

As the Chief Information Security Officer (CISO), it's important to always make things better and find new ways to protect our data. This means looking into new tech and ways to deal with changing threats. For example, putting money into finding the newest security tools can really help make our defenses stronger. By doing this and putting resources into research, we can stay ahead of problems and keep our systems safe from hackers trying to break in.

Conclusion

As CISO, allocating budget is important for protecting our organization's digital assets from threats. We need to invest in training, tech, and plans to stay safe. By focusing on security awareness and making things better over time, we reduce risks. It's important to use our budget wisely to tackle cybersecurity challenges and keep our organization secure in the long run.

References

European Union. (n.d.). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

KnowBe4. (2024). Security Awareness Training | KnowBe4. https://www.knowbe4.com/

National Institute of Standards and Technology. (n.d.). NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology. (n.d.). NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.ipd.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 6). Computer security incident handling guide. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/pubs/sp/800/61/r2/final

PCI Security Standards Council. (2023, September 25). https://www.pcisecuritystandards.org/

TechTarget. (2024, March 20). How to defend against phishing as a service and phishing kits. https://www.techtarget.com/searchSecurity/tip/How-to-defend-against-phishing-a.

https://www.techtarget.com/searchSecurity/tip/How-to-defend-against-phishing-as-a-service-and-phishing