Name: Jestina Hill

Date: 11/10/2024

Enhancing Cybersecurity Spending

Investing the same amount of money in both cybersecurity tools and training for employees will make cybersecurity work better even if money is tight. By improving technology defenses and encouraging employees to find and deal with risks, these strategies will reduce both internal and external weaknesses.

Importance of Cybersecurity Technology

Because of the extent to which people today are dependent on technology, cybersecurity has become more difficult to achieve (*Why Is Cybersecurity Important | Cybersecurity | CompTIA*, n.d.). This is because safeguarding sensitive information has become an even more important concern than it was in the past. Investing in cybersecurity technology not only helps protect against assaults, but it also helps provide a key first line of defense against cyber dangers. Organizations and society as a whole can be negatively impacted by cyberthreats, which can range from personal data to financial transactions (Why Is Cybersecurity Important | Cybersecurity | CompTIA, n.d.). It is possible for organizations to benefit from the importance of cybersecurity by reducing the risks of data breaches, reputational damages, and financial losses. Devices, software, or processes that are designed to safeguard networks, assets, programs, and data against assaults, damage, or unauthorized access are the tools that they utilize (Valle, 2024).

The Significance of Employee Training

It is important to keep in mind that employees are the most valuable assets that a company have while you are considering whether your employees require training (8 Reasons for Employee Cybersecurity Training | PDQ, n.d.). Even if they got training a year ago, they might not know the most up-to-date information about cybersecurity because things are always changing (8 Reasons for Employee Cybersecurity Training | PDQ, no date). Setting up a regular training program for your staff will help them stay up to date on the latest cyber threats that are trying to get your private data. Educating employees about what to look for will also make them less likely to fall for a bad hacker's trick (8 Reasons for Employee Cybersecurity Training | PDQ, n.d.). They would know how dangerous it is to open questionable files, use weak or frequently used passwords, connect to public networks, and do other similar things (8 Reasons for Employee Cybersecurity Training | PDQ, n.d.).

Budget Allocation

Cyberattacks are getting more difficult and common, so companies need to make security a top priority (Birkeland, 2023). Businesses need a budget for protection that protects their digital assets well (Birkeland, 2023). Both could be used together to improve security, use of resources, and cyber protection. Risk assessment should rank threats by effect and likelihood (Birkeland, 2023). It puts important security holes at the top of the list to protect against major threats. It is important to train employees regularly on how to spot and fix hacking problems. By teaching individuals about safe internet practices, password management, and phishing scams (Birkeland, 2023). With limited resources, a 35% training and 65% technology strategy will improve security. Setting it up that way will help people get the training they need and reduce human error to avert cyber threats, strengthening technical defenses.

Conclusion

For a cybersecurity plan to work, you need both trained staff and software safeguards. A balanced budget that puts training and technology at the top of the list can help build a multi-layered defense, raise knowledge about cyberthreats, and encourage the use of technology. By focusing on both the technological and human aspects, organizations can build a strong and cost-effective security stance.

References

Birkeland, L. (2023, December 20). How To Tackle Budgetary Constraints In Cybersecurity: Effective Strategies. larsbirkeland.com. https://larsbirkeland.com/budgetary-constraints-in-cybersecurity/#:~:text=Key%20Takeaways%201%20Budgetary%20constraints%20impact%20the%20efficacy,compliance%20and%20reducing%20security%20risks%20within%20limited%20budgets.

Valle, N. (2024, September 23). Cybersecurity Tools: Types, Evaluation Methods and Implementation Tips. *Invgate*. https://blog.invgate.com/cybersecurity-tools#:~:text=Cybersecurity%20tools%20are%20software%2C%20devices%2C%20or%20processes%20designed,threats%2C%20while%20also%20preventing%20attacks%20and%20identifying%20vulnerabilities.

Why Is Cybersecurity Important | Cybersecurity | CompTIA. (n.d.). CompTIA. https://www.comptia.org/content/articles/why-is-cybersecurity-important

8 reasons for employee cybersecurity training | PDQ. (n.d.). https://www.pdq.com/blog/why-cybersecurity-trainings-are-important/