Tyler Henson
11/16/2025

“Allocating Funds”

When allocating funds for our company, I believe 70% of the money should go to additional cybersecurity technology and 30% should go to employee training.

Cybersecurity Technology

New cybersecurity technology should take 70% of the money because new technology is very expensive and often times requires multiple pieces of equipment in order to work, For example, firewalls, endpoint protections, vulnerability scanners, encryption tools, and intrusion detection and prevention systems all have to be in good condition in order to work properly and do their jobs. This costs a lot of money which is why 70% of the budget for cybersecurity should go to technology.

Employee Training

Employee training is a vital part of cybersecurity especially for large companies that are big targets for criminals. Thus, a company should implement a comprehensive cybersecurity training program that includes onboarding new employees, having regular training sessions, and continuous reinforcement through methods like phishing simulations and policy updates. This does not cost as much money as the new technology which is why it should only take 30% of the budget.

Conclusion

In conclusion, new cybersecurity technology should take 70% of the cybersecurity budget while employee training should only take around 30% of the budget. This is because new technology is incredibly expensive and it all has to be bought in order for the department to function properly and efficiently. However, employee training does not take as much and therefore does not require as much money.

“References”

NordLayer. (2024, August 7). *10 steps to train employees on cybersecurity*.

@NordLayer; NordLayer.

https://nordlayer.com/blog/training-employees-on-cyber-security/