Olivia Woodward

CYSE 200T

Professor Kirkpatrick

11/12/23

Budgeting Cybersecurity

This write-up anticipates how a Chief Information Security Officer would go about budgeting its cybersecurity technology with limited funds.

Budgeting Training

In class, it is always emphasized that training can mitigate one of the most dominant causes for data breaches in companies: employee error. Phishing emails, outside-of-work influences, or simply forgetting to hide one's badge can all lead to this. With proper training, a company cuts out a big portion of risk. However, funding training is tricky. Firstly, who is going to be paid to train employees? Does the company hire more people specifically for training, or will they use senior employees who know the ropes? Will they use special training applications or use presentations? There are many factors, and for the stress it takes off of risk management, I (personally) would put 15%-25% of our budget towards training. It is a large chunk, but because of its significance in deterring data breaches, I believe it is worth the money.

Budgeting Additional Assets

I saved the other 75% for additional resources because these resources include any other type of risk prevention: encryption, firewalls, monitoring systems, authentication, etc. While training is important, it can only support so much. That’s why we need these other tools to further help us. If our company were to only have training that wouldn’t make up for unsecure systems, no backup servers, physical securities, and more.

Conclusion

Overall, I believe additional assets are more important than training simply because they cover more bases. In the same breath, I can agree that training significantly reduces the number one cause of data breaches which is employee error. However, when it comes to real life businesses, I believe they should fund their cybersecurity assets gradually and then analyze what applies to their business specifically.