Morgan Brown
CYSE 200T
April 6, 2025
Professor Duvall

Budgeting of Cybersecurity

BLUF: As CISO, I would allocate 30% of company funding to training, 60% to cybersecurity technologies and systems, and the remaining 10% to emergencies and updating and renovating outdated programs.

Importance of Functional Cyber Systems and Technology

The efficiency of technology and cyber systems should always be the key priority in a cybersecurity-based company or program. The quality of these systems and technologies should be operative, up-to-date, and appropriately monitored. The individuals tasked with working with these systems should be able to assure they meet the required standards, by passing and completing prior training. This technological importance led us to the decision that cyber systems and technology should receive the most funding.

Importance of Training

Cybersecurity Awareness is vital when working with technological programs and systems. The individuals tasked to oversee these systems can be just as much of a risk factor as they can be a security factor. Adequate training will benefit the security and effectiveness of technology systems, assuring that employees have been conditioned and are certified to work with the technology assigned to them.

Even given adequate training, employee dishonesty is always possible and can lead to cyber risks and mishaps. To defend against these human errors, a portion of the training process should demonstrate what to do and who to contact if another employee

is caught committing workplace deviance. In addition, certified employees should be taught how to detect human errors and defense measures to eliminate faults caused by the event.

All in all, training is vital to the success and safety of our cyber systems, leading us to give it the second most amount of our funding.

Updates and Renovations

Despite the company's newer stature and use of mostly modernized technology and systems, there will come a time when they need to be updated, which could be quite costly. Additionally, the company's physical or technical structures may require renovations, which could vary in cost. Ultimately, we decided that training and cyber systems should be the priority in funding, and updates and renovations would have the remaining funds for when necessary.

Possible Emergencies

The possibility of company emergencies could vary and come at unexpected times. Putting the utmost trust in our systems and employees, we bargained that emergency funding be shared with updates and renovations, assuming that though possible, are least likely to occur under our forcefully structured company.

Conclusion

All in all, allocating funds within Cybersecurity is crucial to the overall success of a company. With that being said, we believe that our funding should divided as such: 60% to cybersecurity systems and technology, 30% to training operations, and 10% to updates/renovations and emergencies.