Elizabeth Howard

CYSE 200T

3/30/2025

Budget Allocation for Cybersecurity Preparedness

Based on the recent risk assessment and business impact analysis, a significant number of information security incidents occurred due to human factors. Therefore, there will be a budget shift allocating more funds for employee training and awareness. Overall, the company will redistribute funds to support the end user training first, our technology and tools second, and additional resources third.

End User training First

In the past we have allocated the largest percentage of funds to our technology and cybersecurity tools. The findings of the recent analysis have concluded that these tools are rendered useless if we do not consider the human factors and resources that are utilizing them. Therefore, going forward 70% of the budget will now be allocated toward the training each employee to secure, maintain confidentiality for, guard the integrity of and ensure availability for their own department's information and critical data. First, 20% of the funds will go toward articulate development and course curriculum for asynchronous training. Finally, 30% will go toward policy creation and the OneNote platform to store scenarios, best practices, protocols and SOPs for cybersecurity threats and incidents.

Technology and Tools

Our technology and cybersecurity tools will receive 20% of the overall budget funding. This will allow us to acquire a virus protection and firewall service for a fraction of the cost that we were paying before. This is because some of the monitoring and password maintenance will be in the hands of the end users. Thew new antivirus software will still provide the dame level of protection for the network.

Additional Resources

The final 10% of the budget will be set aside for the contingency fund. We will utilize this portion of the budget to pursue countermeasures int eh event of an attack. This can also be utilized to contract legal resources should the situation arise.

Conclusion

People are our most valuable resource. Therefore, we will allocate most of our budget to training our people to safeguard their departments informational assets. From now on the budget will serve employee training first, cybersecurity tools second, and any additional resources third.