Deandre Turner

Old Dominion University

CYSE 200T

Professor Chris Bowman

Budgeting and Distribution for Cybersecurity

BLUF

Budgeting for Cybersecurity should be flexible and change depending on the situation. We must use strategy to closely analyze and monitor the severity of is all. We should have a budget for system failures protocols, proper education, and back up alternatives.

The Complexity of Cyber Threats

As cybersecurity threats continue to grow more advanced and complex, businesses and institutions must prioritize and facilitate the implementation of strong cybersecurity measures. A major part of that effort involves carefully managing the budget to address these ongoing challenges. If I were placed in the role of Chief Information Security Officer (CISO), I would begin by assessing the current risks and establishing clear protocols and contingency plans. Cybersecurity is not a one-time issue, but “a series of interrelated, ongoing processes” that must be closely monitored at every phase of a system’s lifecycle (McSpaden & Appeaning, 2018, p. 1).

Awareness and Educational Access

With this understanding, budget allocation should be based on the most critical areas of cybersecurity. Because cyberattacks are complex and constantly changing, the budget must

remain flexible and adaptable to various scenarios. I believe that 50–60% of the budget should be dedicated to educating employees and staff about cybersecurity threats and proper digital behavior. Security breaches happen more often than most people assume, and many are caused by human errors such as clicking on malicious links or unknowingly sharing sensitive data. As the NCSL notes, employee behavior "can dramatically help or hinder an organization's overall cybersecurity efforts" (McSpaden & Appeaning, 2018, p. 8). Therefore, it is essential to prioritize awareness and emphasize the consequences of careless digital actions.

Technological Protocols and Investment

The remaining 40–50% of the budget should be used for cybersecurity technologies and protocols. This includes everything from intrusion detection systems and firewalls to data backups and breach simulations. Spending should be carefully monitored, and we should follow specific internal policies to ensure responsible use of funds. A portion of this around 25–30% should focus on backup systems and emergency protocols, especially for critical operational data. The remaining funds would be used for prevention, including reliable security software and firmware. According to Cymulate (2023), cybersecurity spending should be based on "a quantified, global and granular evaluation of each tool's efficacy" to reduce waste and improve performance.

Flexibility and Situational Awareness

In total, I would recommend a flexible model: 45% for education, 30% for backup and response protocols, and 25% for prevention tools. These percentages can shift depending on the situation. For instance, if employees receive a suspicious email asking for private information,

the organization should temporarily increase its education spending to 55–60% as a preventative measure. Once the threat is addressed, spending can return to its regular distribution.

Conclusion

Cybersecurity is both an individual and organizational responsibility that requires serious attention. Everyone must be aware of the risks, as even small mistakes can lead to major consequences. Therefore, budgets must be structured to cover all necessary areas education, emergency protocols, and prevention while remaining flexible to respond to emerging threats. With continuous monitoring and thoughtful analysis, CISOs can make the most of limited resources while minimizing security risks.

References:

1. Cymulate. (2023, February 2). *Cybersecurity budget optimization: How to get the most out of your cybersecurity spend.* https://cymulate.com/blog/cybersecurity-budget-optimization/

2. McSpaden, S., & Appeaning, M. (2018, January). *Budgeting for cybersecurity*. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/budgeting-for-cybersecurity.aspx