

Zack Fok

CYSE 200T

November 10th, 2024

Balancing a Cybersecurity Budget

With a limited budget, I would focus more on training employees and then spend what's left on essential security tools. This way, we're not just relying on technology, but also helping people spot and avoid threats.

1. Make Training a Priority

In today's world, Cybersecurity is one of the biggest threats. According to the article on Cybersecurity and Criminal Justice, "Cybersecurity has been described as the biggest threat facing financial institutions (McGee, 2016; Reuters, 2017), the federal government (Boyd, 2016), corporations (Moritz and Burg, 2015), and investors (Winn, 2017). It seems to be well accepted that cybersecurity is a growing threat that must be addressed." (Payne 2). In cybersecurity, people are often the easiest targets in cyber attacks, so training is essential. No matter how good our security tools are, they can't protect us from human mistakes, like falling for phishing emails. Regular training sessions could teach everyone to recognize common threats and react safely. This would reduce our overall risk and make the whole team a stronger first line of defense.

2. Invest in Key Security Tools

With the remaining budget, I'd pick security tools that directly address our biggest vulnerabilities—like antivirus software, firewalls, and threat detection. According to the article

Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes, “science, computer engineering, electrical engineering, and information technology. Research from these disciplines has been useful for developing computer hardware and software that enhances the security of various technological devices.” (Payne 2). While it would be nice to have the latest and greatest technology, covering the basics effectively will have the most impact. Tools that monitor for unusual activity or block known threats can add a solid layer of protection without blowing the budget.

3. Continuous Improvement and Evaluation

As cyber threats constantly evolve, it's important to review our training program and security tools regularly. I'd look for low-cost or free options to keep employees up-to-date on the latest threats and ensure that our security tools are still relevant. This way, we get the best of both worlds without overspending.