Madison Brown

Balancing Training and Technology in Cybersecurity Budgeting

When you have a limited budget in cybersecurity, it's important to spend money on both employee training and security technology because both are needed to keep an organization safe.

Why Training Matters

Most cyber-attacks happen because people make mistakes, like clicking on phishing emails or using weak passwords. These simple errors create openings that hackers can easily exploit. Training employees helps them understand these risks and learn how to avoid them in their daily work. If the people who work for you know what to look for, they can stop many threats before they cause harm. Training builds awareness and makes employees an important line of defense in cybersecurity. (CIS Security, 2022)

Why Technology Matters

Technology is vital for cybersecurity because cyber threats are becoming more advanced and frequent. By 2025, new technologies like AI and the Internet of Things will bring new risks. Cybercriminals will use AI to create smarter attacks that can change quickly and avoid detection. More connected devices also mean more ways for hackers to break in. Security tools like firewalls and constant monitoring help protect against these attacks all day, every day. (Science News Today, 2025)

How I Would Split the Budget

Since most cyberattacks happen because of human error, I would allocate most of the budget towards training employees. Educating staff on how to recognize threats like phishing and weak passwords helps prevent many attacks before they even start. However, it’s still important to invest in essential cybersecurity technologies to protect the network from threats that employees might not detect. This approach balances the biggest vulnerability, human error, while also using technology to cover gaps. Regularly evaluating and updating both training and technology ensures the organization adapts to new threats and makes the best use of limited resources.

Conclusion

In short, a Chief Information Security Officer must carefully balance limited resources to protect against cyber threats. Training employees is vital because many attacks start with simple human mistakes. At the same time, investing in security technology helps stop sophisticated threats that humans alone can’t catch. Focusing too much on one and not enough on the other leaves the organization vulnerable. Regularly updating both training and technology keeps defenses strong as new risks emerge. This balance builds a safer, more resilient organization that truly values and protects its critical information.

References

CIS Security. (2022). Why employee cybersecurity awareness training is important. Retrieved from https://www.cisecurity.org/blog/why-employee-cybersecurity-awareness-training-is-important/

Science News Today. (2025). Why cybersecurity will be more important than ever in 2025. Retrieved November 15, 2025, from https://www.sciencenewstoday.org/why-cybersecurity-will-be-more-important-than-ever-in-2025