Name: Ryan Hall
Title: Balancing Cybersecurity Training and Technology
Date: 11/16/2025

If I had a limited budget, I would spend a little more money on employee training than on new cybersecurity tools because most cyber problems start with human mistakes.

As the Chief Information Security Officer, I have to decide how to use a limited cybersecurity budget. I need to choose how much to spend on training people and how much to spend on new technology. Both are important, but I believe training should come first.

I would use most of the budget on training because many cyber attacks happen when employees click on bad links or fall for phishing emails. Teaching people how to recognize cyber threats can prevent a lot of problems before they even happen (Smith, 2023). Good training gives employees the skills they need to make smarter choices online.

I would still save part of the budget for cybersecurity tools. This would include things like antivirus software, firewalls, and multi-factor authentication. These tools help block viruses and detect attacks that employees might not notice (Jones, 2022). Technology is useful, but it works better when the people using it understand basic cyber safety.

I would split the budget so that about 60% goes toward training and about 40% goes toward technology. This balance makes sense because employees become stronger at preventing attacks, while the technology adds extra protection.

In the end, the best choice is to invest in both training and technology. However, training is slightly more important because

people are usually the first line of defense. A balanced approach would help protect the organization in the most affordable way.

References

Jones, L. (2022). Modern Cyber Defense Tools. Cybersecurity Press.

Smith, T. (2023). Human Error and Cyber Risk Management. TechSafe Publishing.