Deja Brown

During this week's reading, you've been exposed to different points of view regarding human contribution to cyber threats. Now, put on your Chief Information Security Officer hat. Realizing that you have a limited budget (the amount is unimportant), how would you balance the tradeoff of training and additional cybersecurity technology? That is, how would you allocate your limited funds? Explain your reasoning.

From what I have learned balancing the trade off between training and additional cybersecurity technology is important, especially with a limited budget. This is and idea I'd how to approach it:
The first step would be conducting a risk assessment to identify any potential threats in the organization. This shines a light on the areas that need immediate attention.
Next, I'd suggest training. Human error is often the weakest link. With this I also would invest in basic security measures. Things like firewalls and security antivirus software can serve as protection.
The third step would be adding access/ authorization controls. Limiting certain sensitive information and data can reduce the risk of threats from within.
I would also recommend an incident response plan. It's important to be prepared to respond to any and all types of breaches. Along with this I would ensure that regular updates for the security and other systems will be checked. That would help identify vulnerabilities before they had the chance to be exploited.