Jhayla Battle

Write Up - The Human Factor in Cybersecurity

As Chief Information Security Officer (CISO), balancing a limited budget between cybersecurity technology and employee training is a critical decision. While advanced technologies like firewalls, intrusion detection systems, and endpoint protection are essential, they are only as effective as the people who use them. Human error remains one of the largest contributors to cyber threats, often through phishing attacks, weak passwords, or unintentional data leaks.

I would allocate approximately 60% of the budget to robust cybersecurity tools and 40% to continuous employee training. The investment in technology ensures baseline protection, automates threat detection, and provides rapid response capabilities. However, regular, scenario-based training empowers employees to recognize and respond to cyber threats proactively.

Furthermore, fostering a strong security culture reduces risks from social engineering attacks and insider threats. This balanced approach not only strengthens technical defenses but also transforms employees into the organization’s first line of defense, maximizing security impact within budget constraints.