

Isaiah Browne

CYSE 200T

November 9, 2024

The Human Factor in Cybersecurity

BLUF:

Finding the right balance between buying more cybersecurity technology and giving workers cybersecurity training is often hard, especially when money is tight. It is important for them to know what role they play in reducing online threats, especially since people are often the main cause of many breaches.

Training would be my first priority and would receive 40% of my budget. An additional safeguard against human mistake, the greatest danger to cybersecurity, is human error itself. It is crucial to train personnel to identify risks, adhere to best practices, and be watchful in order to avoid breaches. This should be your first priority since it represents the risk mitigation budget item that is likely to be the most costly. After that, a sizable chunk would go toward foundational technologies that offer comprehensive security. Things like MFA, firewalls, and endpoint security would all play an influence. These solutions can scale with the organization's growth and assist minimize threats that circumvent human defenses.

Conclusion:

The plan is to use training to deal with the most common weakness, which is human mistake, while also making sure I have the right technology to spot and stop threats that might get through. By finding a balance between these two areas, I'm making a full defense that uses both human awareness and automation. This plan gives us the best chance of avoiding a breach and limits the damage if one does happen, all while keeping within our budget.