Bryce Staples
November 16,2025

The Human Factors in Cybersecurity

With a limited cybersecurity budget, the most effective strategy is to balance investments between target employee training and essential security technologies that prioritize identity security, threat detection, and human-focused awareness programs to reduce human error and ensure rapid response to attacks.

How would we balance the tradeoff of training and additional cybersecurity technology?

A good balance between training and cybersecurity technology starts with recognizing that none of neither can stand alone. Technology reduces the number of threats that reach employees, while training helps reduce the likelihood that human error turns those threats into incidents. With a limited budget, the most effective approach is to fund core security technologies such as multi-factor authentication and automated patching because they directly reduce the attack surface and provide visibility into threats. Once these are in place, the remaining budget should be invested in targeted, continuous human-focused training, including regular phishing simulations.

How can we allocate our limited funds?

To allocate our limited funds, we could divide the funds in a way that strengthens both the technical defenses and the human element, but since most cyber incidents involve a combination of system weaknesses and human error. An effective allocation would be investing most of our budget in our core security technology that reduces the attack surface and detects threats early. Then we should use the remaining budget to strengthen the human side of security because people are still the most targeted vulnerability.

Conclusion

Balancing limited cybersecurity funds requires us to recognize that strong security depends on both effective technology and well-trained people. However, technology alone cannot prevent incidents if employees are unprepared to recognize or respond to suspicious activity. By investing most of our budget in essential security technologies and dedicating the remaining funds to continuous and targeted training. This balanced approach strengthens defense, reduces human error, and ensures a more resilient response to evolving cyber threats.