The Human Factor in Cybersecurity

By: Austin McCarty

If I were a Chief Information Security Officer (CISO) with a limited budget, I would prioritize balancing investments between employee training and technology to effectively reduce cyber risks. Strengthening both personnel and systems is essential, as most security incidents arise from a combination of human error and technical vulnerabilities.

I would allocate approximately 50 percent of the budget to cybersecurity technologies that minimize human mistakes, such as single sign-on (SSO), endpoint protection tools, and multifactor authentication. These solutions automate secure practices, reducing the likelihood of insider misuse and errors. Additional measures, including email filters, privilege controls, and device management, further limit opportunities for attacks before they reach employees.

Around 30 percent of the budget would be dedicated to employee training. Even the most advanced tools are ineffective if users lack awareness of current cyber threats. Short, role-specific sessions and phishing simulations would equip employees to identify scams, report suspicious activities, and safeguard data. Building a strong culture of awareness ensures employees act as active defenders rather than liabilities.

The final 20 percent would fund detection and response efforts, such as security monitoring and incident response plans. These ensure the organization can quickly identify and contain any attack that happens. Which will help play a major role in finding the problems within the systems before they hopefully even happen.

In short, I'd invest first in technology to reduce risk, then in training to strengthen human judgment, and finally in detection to catch what remains. This approach with my budget I believe maximizes protection while staying within a limited budget.