Write up: the human factor in cybersecurity

Pamela Davis

03/21/26

If I were a Chief Information Security Officer with a limited budget, I would split resources between employee training and cybersecurity technology but lean slightly more toward training—about 60% training and 40% technology. The reason is that human behavior is often the weakest link in cybersecurity. Even the most advanced systems can fail if employees fall for phishing emails, reuse weak passwords, or mishandle sensitive data.

Investing in regular, practical training helps reduce these risks by teaching employees how to recognize threats and respond appropriately. For example, phishing simulations and short awareness modules can significantly lower the chances of successful attacks. Training also helps build a security-focused culture, which has long-term benefits beyond any single tool.

That said, technology is still essential. I would allocate funds to critical protections like firewalls, endpoint security, multi-factor authentication, and monitoring systems. These tools act as a safety net when human error does occur, helping detect and stop threats before they cause major damage.

Overall, my approach would focus on balance: training to prevent mistakes and technology from catching them when they happen. This layered strategy provides the most effective protection while making the best use of limited resources.