

Stephen Saintcyr

Kirkpatrick

CYSE200T

8 March 2025

### The Human Factor in Cybersecurity

If I were to get the position of a Chief Information Security Officer (CISO) with a limited finance plan to work with, I would try to achieve a reasonable compromise between investing in human resources and technology. For me, an organization's biggest risk in cybersecurity is not out of date software or if there are any missing devices that need attending to, most of the time it is people's negligence, phishing and exposure of data tend to lead to a lot of breaches. Mostly focusing on these issues leads to making employee training my top priority. I guess around 60% of the budget goes towards training and awareness. This includes conducting frequent phishing attempts and specific type training sessions for all major threat areas like HR and finance, and ever refreshing sessions for everyone for keeping security issues in focus. When employees understand the type of action to be taken when under threat, a lot of times, the attack can be stopped from happening. Also, creating a security responsibility culture among all employees is very helpful. The following 30% would cover central cybersecurity tools. Rather than the latest or most advanced tools, I would prioritize the basics such as multi-factor authentication (MFA), endpoint security, email filtering, firewalls, and patching. These are critical components to any

security system and are very cost-effective. The last 10% would be set aside for monitoring and evaluation. I think it is important to track how effective the training and tools are, so I'd use this portion for things like reviewing logs, running internal audits, and maybe even bringing in a third party now and then to get an outside perspective. At the end of the day, you can buy all the tech in the world, but if your team isn't prepared, it won't matter. That's why I'd lean more toward training people and backing them up with the right tools. That combination gives the most security for your funds.