The Human Factor in Cybersecurity

Arielle C. Chapman

School of Cybersecurity, Old Dominion University

CYSE200T

Mr. Charles E. Kirkpatrick

November 12, 2023

In navigating the challenges of limited cybersecurity budget, my approach as CISO involves prioritizing staffing to attract and retain skilled professionals, investing in firewalls, MFA, and outsourced services to enhance our technological defenses, and, emphasizing that employee training mitigates human error. This all will reinforce our comprehensive and balanced cybersecurity standing.

A Balanced and Strategic Gameplan

Effective cybersecurity requires a combination of trained-personnel and technological defenses; however, they cannot always be fleshed out to their fullest capability in the business world. With a limited budget, I as Chief Information Security Officer (CISO) would be required to assess the most valuable assets to our company. Using risk assessment, we can begin laying out which defenses we need to prioritize. I'd allocate my limited funds in accordance with the following priorities:

Staffing

Clearly, cybersecurity pays well. In order to hire and keep quality professional who will not make costly mistakes, you must pay them competitively.

Firewalls & MFA

Simply, if hackers cannot penetrate our systems, our data is protected. I'd secure our assets with firewalls, antiviruses, access control systems, intrusion prevention systems, and other methods to keep unvalidated users out. Additionally, I'd use MFA. This secures the profile end. While passwords are easily hackable, MFA means that they cannot validate who they claim to be.

Outsourcing

I'd say this category goes hand in hand with the previous one. I'd recommend outsourcing what we can to businesses that focus solely on that specific trade. That way, there security for it is likely to be much more advance. Much more of their budget is free to go towards it.

Employee Training/Awareness

Human error has been and remains a significant fault point in cybersecurity. Should our company invest in quality training to understand online and physical security, we may prevent scams from allowing infiltration into the data.