The Human Factor In Cybersecurity

Tariq Sims

Old Dominion University

CYSE 200T

Professor Kirkland

11/12/2023

As the Chief Information security officer, I would balance the tradeoff of training and additional cybersecurity technology by doing a few things such as a “Risk Assessment,” by evaluating my organization’s potential threats and vulnerabilities as well as prioritizing cyber security measures based on the noticeable risks and use the limited resources on the more critical areas of focus. This will allow for improvement overall in my organization's cybersecurity. Secondly, I would invest in cybersecurity and awareness training programs for my employees this will allow a reduction in security issues. Thirdly, I could make a technology investment and invest in cost-effective technologies that will identify the vulnerabilities in my organization which can include things like anti-virus software, firewalls, and encryption tools. Lastly, I would encourage employee involvement to participate in cybersecurity measures, in which they can identify potential security threats and issues. These things can be a small investment into the company to not allow further security issues with cybersecurity.

Resources:

***Cybersecurity Risk Assessment | IT Governance USA*. (n.d.).**

https://www.itgovernanceusa.com/cyber-security-risk-assessments#:~:text=A%20cybersecurity%20risk%20assessment%20is,to%20information%20and%20information%20systems.

Synack. (n.d.). Get Out What You Put In (And More): Why You Should Invest in Employee Security Training. *Nasdaq*.

https://www.nasdaq.com/articles/get-out-what-you-put-in-and-more-why-you-should-invest-in-employee-security-training