Writeup- The Human Factor in Cybersecurity

Collin Fitzgerald

CYSE 200T

4/6/2025

Introduction

As the Chief Information Security Officer, working with a budget that has been limited in funds, tentativeness to real issues is key. I would take an approach that achieves a balance between human training and cybersecurity technology on hand to mitigate any short or long term cyber threats. I would keep my priorities centered around impact and cost effectiveness to handle both short and long term issues my organization may face. With a good practice of allocating budget portions to effective preventive measures, my organization can display peak mission effectiveness without fear of cyber threats.

Human Training

I feel that with the large portion of cyber threats being at the hands of human error, I would stress regular training receiving approximately 40% of our allocated budget. I feel as though with an effective training regime, issues that are caused normally by human error can be mitigated as much as possible. These training regimes would not only be mandatory, but recurring to continue resilience to cyber tracks on the human level of my organization. The areas to keep my human counterparts within the organization effective at stopping cyber threats are focused into three groups. The first group being phishing awareness, as my human counterparts need to know what these attempts look like, and the process to resist and report them. The second area of focus is password management, which training can ensure password management is upheld and regularly instilled in day to day operations. The last area of focus I want to touch base on is incident response. Incident response is an area that the 40% portion of our budget will touch base on, ensuring human counterparts know the reporting process for any possible cyber threat and/or literal attack.

Cybersecurity Technology

I feel as though the importance of technology justifies the 60% allocation of our budget towards these assets. The automated security measures and deterrence it creates are something humans cannot achieve as effectively. Technology being a larger portion of the budget shows how strongly I believe in adding more layers to our organizations defense measures. The first area I want to focus the budget allocation on is antivirus software so that our devices are protected and monitored at all times. The second area I would like to focus this portion of the budget on is an array of firewalls, intrusion detection and prevention systems. Having these different measures in place is essential to protecting our organization's data within the networks we utilize. The last area of this budget portion I want to stress is encryption and decryption methods, so that we as an organization can ensure sensitive data is not at risk whether it be in transit or in storage. The overall priority of this 60% allocation is making sure our critical infrastructure is protected and free from risk of human error.

Conclusion

With a balance of human and technological aspects of security, while maintaining a limited budget, I believe as the CISO I will be able to implement and enact proper security procedures to protect my assigned organization as desired. By reducing human error with training regimes, and necessary tools in the cybersecurity realm, and long term or short term threats can be assured to not achieve their desired effects of any systems I oversee. The approach I am taking will be effective at maximizing available resources and achieving resilience alongside of protection.