Write Up- The Human Factor in Cybersecurity

As Chief Information Security Officer (CISO), the responsibility of safeguarding our organization against cyber threats rests heavily on allocating our limited budget efficiently. The question of how to balance investments in training and cybersecurity technology is crucial for maintaining a strong defense posture. A balanced approach that combines strategic deployment of cybersecurity technologies with targeted investments in training would be the most successful given the limitations of a limited budget.

A crucial first step is funding cybersecurity awareness and training initiatives for staff members. This comprises routine training sessions catered to specific job functions, simulated phishing exercises, and workshops. It is justified by the fact that human mistake frequently plays a major role in security breaches. Strengthening our workforce's cybersecurity awareness and knowledge will help us drastically lower the likelihood of successful intrusions. Well-trained employees are more likely to identify phishing attempts, follow best security practices, and understand the importance of data protection. Investing in training can save a significant amount of money by lowering the frequency of incidents, making it a more cost-effective option than purchasing new equipment. Setting aside some money for the purchase, installation, and maintenance of necessary cybersecurity technologies. This entails making investments in reliable endpoint security systems, encryption tools, intrusion detection and prevention systems (IDPS), and security information and event management (SIEM) systems. Training by alone is insufficient to completely eliminate some dangers. Investing in technology adds another line of defense and assists in addressing vulnerabilities.

By improving our detection, reaction, and recovery from cyber disasters, advanced technologies help us minimize possible harm and disruption. By balancing investments in

training and cybersecurity technology, we can maximize the effectiveness of our cybersecurity efforts within the confines of a limited budget. This approach acknowledges the critical role of both human factors and technical solutions in safeguarding our organization against evolving cyber threats. Training empowers our workforce to become proactive defenders, while strategic technology investments augment our defensive capabilities.

Work Cited

"Redefining the Human Factor in Cybersecurity." *Daily English Global Blogkasperskycom*, www.kaspersky.com/blog/human-factor-360-report-2023/. Accessed 8 Apr. 2024.