Diane Gilzow

CYSE 200T

April 6, 2025

Professor Duvall

The Human Factor in Cybersecurity

BLUF: Cybersecurity is often composed of using technical measures that prevent cyberattacks and data breaches. These measures are often handled by human users that often require proper training and awareness. With a limited budget, there needs to be a balance between user training and implementing additional cybersecurity technology.

Humans vs. Technology

Cybersecurity technology and technological defenses are valuable resources to help secure sensitive, confidential data. Having robust and up-to-date cyber defense implementations in place can help protect against a wide range of threats, such as malware or an unauthorized user attempting to access confidential data. To handle confidential data, users are often trained on how to properly handle security protocols and how to be aware of such threats. However, with a limited budget, it can be difficult to balance between user training and cybersecurity technology, though there should be a focus on the root cause of the majority of security incidents: Human behavior. Human behavior has been shown to be the weakest link when it comes to cybersecurity. Even with robust security systems in place, it is ultimately users who interact with and manage these systems, and one simple mistake can lead to a catastrophic incident. According to an article, “...over 90% of successful breaches worldwide starting with a phishing email” (Cyberbitsetc.org). The quote shows just how much of a role human psychology plays in cybersecurity and how cybercriminals can exploit psychology for malicious purposes. Simply deceiving an individual into giving away sensitive information can lead to more damage than an attacker brute forcing their way into an organization’s internal network.

What Resources Should be Prioritized?

Since it is shown that humans are a primary vulnerability in cybersecurity, user training should be a priority in order to minimize the risk of breaches and the likelihood of human error. The budget would focus on investing in user training first, and then eventually allocate the remaining funds for implementing additional cybersecurity measures. By investing in user training first, employees can develop awareness to recognize and respond to common cybersecurity threats, especially when it comes to phishing emails because of how frequent they occur and how effective they can be. Once user training is in place, the remaining funds can be used to strengthen technological defenses, such as implementing firewalls, intrusion detection systems, and purchasing anti-malware software. With this strategy in mind, it will help address the root cause of many cybersecurity incidents while also focusing on investing and improving on cybersecurity technology. This can help create a balance between the two and ultimately secure a good cybersecurity structure within an organization.

Conclusion

Overall, user training and cybersecurity technology are both important factors to consider when implementing security measures. However, everything begins with the user, and users need to make sure that they are aware of certain threats and vulnerabilities within an organization and how important it is to handle confidential data. Therefore, prioritizing user training ensures that employees understand the risks they face and how their actions can impact the security of an organization while ensuring that technological measures are implemented to complement and enhance these efforts.

References

Capone, J. (2018, May 25). Capone - the impact of human behavior on security. https://docs.google.com/document/d/1J3v_V167mktbGVynbtHW8yHXW9onjaBzVASo-behDfY/edit?tab=t.0

Cyberbitsetc. (n.d.). *Cyberbitsetc - why is cyber security about human behavior?*. Cyberbitsetc.org. https://docs.google.com/document/d/1QplIrfcKlmkSOuKt9i0Kte72kYrukFeCm1wj9DxpnGU/edit?tab=t.0