Jahmire Whitehurst 11/14/2024

The Best Balance of Funding for Training and Technology

BLUF:The balance of training and cybersecurity technologies is a 60:40 ratio of new training to cybersecurity technologies. This paper is the reasoning behind my allocation of the funds.

The Importance of Employee Training

“Cybersecurity awareness training for employees helps you minimize your risks stemming from the human element. No technology solution can help you stop all cyber attacks and data breach vectors, after all”(Center for Internet Security, n.d.). Cybersecurity training is one of the most important topics in an organization and should definitely be taken into account. Even the most sophisticated technology that could stop any cybersecurity attack would need a good amount of employee training. Malicious attacks like social engineering, phishing, and insider attacks all can be minimized or even avoided with adequate employee training. Social engineering uses people to infiltrate systems. This can be done by sharing passwords to attackers on accident or on purpose, intimidation to download malicious files, or something as simple as a request for help with a malicious intent. Phishing deceives people into thinking that the site they are trying to enter is real when in fact it has a malicious intent. Insider attacks use employees to infiltrate an organization's systems. Unauthorized access can be acquired on accident or on purpose. To conclude, social engineering and all its subfields can be minimized if not avoided with proper employee training.

The Importance of Cybersecurity Technology

The right technology can be vital in protecting major cybersecurity assets. Older technologies have more vulnerabilities to malware and are never a good idea to use for important information. Newer technologies do not have as many vulnerabilities and can process more information faster. “use automation and machine learning to help identify and respond to cybersecurity events. These technologies can analyze large amounts of data and identify patterns and anomalies that may indicate a potential threat,”(Guttula, 2022). This shows that technology can make the amount of work easier on humans. Furthermore, the use of user friendly interfaces can make the use of advanced technology self explanatory and minimize training. Technology does not stop here though with the use of advanced systems comes biometric technology and multi factor authentication. Multi factor authentication makes it very difficult for unauthorized users to get into systems even with the password. Biometrics are even more protection to multi factor authentication that require retina scans, iris scans, or fingerprints to get into a system.

Conclusion

Throughout my analysis the importance of training has been emphasized leading me to understand the importance of training. This has also been proven for a few reasons technology can be highly advanced but training will always be needed no matter what. Then a large part of malware social engineering is based on human error. Technology rarely makes mistakes and it is usually the person that programmed that computer that made an error. All of these factors lead to the balance of 60:40 of funds with a majority in training and minority in technology.

References

- CIS. (n.d.) *Why Employee Cyber Security Awareness Training is Important*. Center for Internet Security. https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important
- Kim.D. (2023). *Fundamentals of Information Systems Security. Jones and Bartlett Learning. 10.17226/6457.*
- Guttula. S.V. (2022,December 25). The importance of advanced technology in cybersecurity. Linkedin. https://www.linkedin.com/pulse/importance-advanced-technology-cybersecurity-venkata#:~:text=By%20providing%20individuals%20with%20the,safe%20online%20environment%20for%20everyone.