CYSE 200T Write-Up: “The Human Factor”

Herald Anacta

School of Cybersecurity, Old Dominion University

CYSE 200T: Cybersecurity, Technology, and Society

Mr. Charlie E. Kirkpatrick

November 20, 2022

Herald Anacta

November 20, 2022

The Human Factor

Human contributions to the world of Cybersecurity play a vital role in preventing cyber threats. It can be argued that human presence and participation in any realm of technology is very important. In the same manner, making sure that technology is always current, and up to date is always a top priority. In this week's article, we were presented with a scenario in which you must allocate a budget between human training or additional technology. Now, if I were to put my Chief Information Officer hat, I would say that it should be an even 50/50 split between additional human training and additional technology. Both are equally important and therefore should both be given equal emphasis, attention, and in this case, equal funding.

How to Budget?

We all wish we have unlimited funds. If this is the case, tech companies won't have to worry about allocating resources. However, the reality is that companies have finite resources to distribute and budget. Before the start of each fiscal year, tech companies should plan and make a blueprint on how to evenly give funding to all its departments. Any sort of new business initiative adopted across a CISO's company must be assessed and have a security budget applied to it, if applicable, to ensure that the company and its new customers remain secure (Krishnan).

Training or Technology?

Man, or Machine? I say both. Ensuring that all employees receive adequate training will ensure that human errors will be limited to a minimum. Keeping everyone up to date with the current information about Cyber technologies will help mitigate the risk of people making the wrong decisions because they do not have any idea of what is going on. In the same vein, investing in additional and newer cybersecurity technologies will put the company in a better position to thwart potential cyber attackers. Making sure that both hardware and software are always updated and have the proper personnel to look after them is a good 1-2 punch to protect a company from cyber-attacks. Strengthening people's education in security/cybersecurity inside organizations represents an important step in consolidating a concrete distinction in the protection of data assets (Cano).

Conclusion

The limitation of funding should not force a company to choose between proper human training or additional technology. They both are equally important, are both vital cogs to a company's success in combating modern day cyber threats.

References

Krishnan, Ashwin. (2022). Cybersecurity Budget Breakdown and Best Practices. Techtarget.com, https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices. Accessed 18 November 2022

Cano, Jeimy (2019). The Human Factor in Information Security. Isaca.org, https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security. Accessed 19 November 2022