The Human Factor In Cybersecurity

Jonathan Roeseler

Undergraduate Cybersecurity Student, Old Dominion University

CYSE200T: Cybersecurity, Technology & Society

Professor Kirkpatrick

12 November 2023

BLUF:

This writeup regarding the human factor in cybersecurity will introduce the reader to the issue of limited budgets and its impact on the cyber world.

Cybersecurity Training & Systems

An organization's cybersecurity systems have to keep pace with the modern world, in other words, the new becomes the old pretty quickly. As a result, keeping systems up to date is one of the biggest concerns a company should have when considering its cybersecurity needs. Secondly, training employees to know how to work the devices on your network is crucial. Even if you have the best systems in the world, a bad employee could ruin everything and end up in a breach, lost data, etc. To add on, human errors are usually the result of network breaches (Morris).

Trade Offs in a Limited Budget

In the position of limited funds, and having to make a decision in which to allocate the budget, first and foremost, a CISO should try to limit or get rid of any dependencies on legacy systems. Such systems are no longer updated, easier to exploit, and harder or even impossible to fix if something breaks. In order to keep costs low, a CISO should try to have the most recent and current devices on "internet-facing" devices. This would enhance security tremendously. Finally, and overall, probably the most important factor in cybersecurity, would be employee-training. As stated previously, humans are the weakest link in cybersecurity. Because of this, training and making sure employees know how to work specific systems, what to do in certain situations, and to look out for common threats (tailgating, phishing emails), would be crucial to staying in business.

Conclusion

Cybersecurity is generally more reliant on those who are working the systems then the systems themselves. Consequently, employee-training is, in most cases, more important than upgrading systems, especially when there is a limited budget in place.

References

Morris, Monica. “8 Common Ways Hackers Break into Computer Systems.” *IT Services*, 28 Jan. 2023, www.sdtek.net/8-common-ways-hackers-break-into-computer-systems