John Heath

November 11, 2025

The Human Factors in Cybersecurity

BLUF: Human factors in Cybersecurity are equally important to the software and hardware that support all cybersecurity systems. Because of this, organizations must carefully allocate funds to employee cybersecurity training, as well as to support their systems with up to date technology.

Human Factors

Human factors in cybersecurity are an overlooked aspect of securing systems. While software and hardware play a major role in cybersecurity, most security breaches are caused by human error. For example, phishing attacks are considered social engineering attacks because they manipulate human psychology. Attackers mimic authority, tease curiosity, ignite a sense of urgency or fear, or take advantage of trust in order to breach systems. They do this because it's much easier to exploit the human mind than it is to exploit security systems. Additionally, the untrained human mind is even easier to exploit. Without updated, consistent training on attacks like phishing, vishing, or scareware, even sensible people become easy targets for cyber attacks.

Allocation Funds to Cybersecurity

As a CISO, it is important to incorporate a plan for an organization's security budget. Regardless of the overall budget for cybersecurity, this budget based on percentages is a viable plan to ensure up to date technology, well trained employees, and money for incidentals.

25% of the entire security budget should go towards hardware. It is important to have secure servers, hardware security modules, high powered computers/computer chips, and on sight access controls such as locks that require proof of ID to enter. An additional 35% of the

security budget would go to software such as firewalls, cloud and network security tools, and encryption tools. While human error does account for the majority of security breaches, hardware and software are the backbone of cybersecurity. Without top notch technology, any security system would struggle to operate.

20% of the cybersecurity budget should go towards employee training, awareness, and testing. By utilizing Cost/Benefit analysis, it is evident that 20% of the cybersecurity budget would lead to better cybersecurity practices organization-wide while maximizing cost efficiency.

Lastly, the final 20% of the budget would go to incidentals and miscellaneous costs like security audits, cybersecurity insurance, SWOT analysis, or NIST compliance.

Conclusion

As a CISO, developing a budget that can support an organizations entire cybersecurity infrastructure, employees included, is a crucial aspect to ensuring true security for online systems.

References

CISA. “Avoiding Social Engineering and Phishing Attacks.” *Cybersecurity and Infrastructure Security Agency CISA*, CISA, 1 Feb. 2021, www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks.