Michonda Ramsey

Lida Hagh

CYSE 200T

November 8th, 2024

The Human Factor in Cybersecurity

Introduction

In the world of technology, and cybersecurity, human behavior has been considerably the weakest in security protocols. As society become more dependent on technology, cyber threats and hackers have made users an easier target for all types of cybercrimes. Many procedures have been implemented in businesses, companies, and organizations to combat the growing threats. As cybercriminals evolve, more companies are leaning towards appointing Chief Information Security Officers to close the security gaps within their corporation.

What is a Chief Information Security Officer, and why are they important.

To understand the process of how the different security measures and protocols are put in place to keep the security risk low, we must first understand who responsibility it falls under. While most small business and companies cannot afford the luxury of having a destinated person assigned to protecting their private information and secrets, the ones who do usually give all obligations over to what is to be called a Chief information officer (CISO). “The CISO is a strategic level position, responsible for ensuring that the information assets and IT systems are protected and secure, and that such protection is in line with the strategic direction of the organization.” (Hooper, V., & McKissack, J. (2016). In my opinion, CISOs are critical to ensuring that data is safeguarded and protected from internal and external forces that intend to bring harm to a company.

Strategies to achieve security balance

If I were put in the position of a CISO, there are many strategies I would employ to create a seamless balance of security within an organization. The initial step I would take would be ensuring all employees are full trained on company policies surrounding cyber threats and first line of defenses. This would be the most cost-effective portion as employees are already included in the company overhead and would cheaper to train verse adding advanced technology. It would also push security awareness among the organization ensuring no one person is allowing external threats to slip through the cracks. Regular assessments would need to be applied to measure the effectiveness of the trainings and verify if the knowledge learned in being retained. For threat detection, cloud-based services could be leveraged for security services. This would be a particle solution as it would free the bandwidth of the servers for on-site performance. I would lastly deploy a robust monitoring system to for constant supervising of all the data and information on the companies’ devices. This would be the costliest portion of my security plan, but in the end, it would save the company money by preventing even more costly data breaches. With each aspect of my plan tied into one another its s simple approach to balance out a simple security proposal.

Conclusion

In conclusion when examining the faults of systems against cyber threats, there are many factors to consider. There will never be a such thing as a perfect solution because cyber criminals are transforming right in front of our eyes. At some point int the future, there will be nothing remaining that is free of technology, and as long as that is a growing factor Chief Information Security Officers will be vital to the protection of modern technology.

References

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585-591. https://doi.org/10.1016/j.bushor.2016.07.004