Name: Samuel Woodruff

Date: 11/10/2024

The Human Factor of Cybersecurity

Cybersecurity is largely thought of as majorly technologically focused. While true, cybersecurity has an entire other aspect that is just as important - people. If I were a CISO with a limited budget, I would carefully allocate funds to address cybersecurity needs as well as the human factor because both are equally as important.

The Human Factor

People are one of the most important factors when it comes to cybersecurity. Companies can have all the cybersecurity technology in the world but will still have security breaches if their employees are not trained and knowledgeable. According to Kapersky, "...52% of businesses admit that employees are their biggest weakness in IT security..." (Kapersky, p. 1, 2024). That's a large number of companies admitting that employees may be the weakest link in cybersecurity. Actions like employees using unauthorized devices, not updating their devices regularly, and sharing sensitive data through unauthorized means all contribute to a higher likelihood for the next big security breach.

Employee Training and Education - 45%

If I were a CISO, I would allocate 45% of my limited budget towards employee training and education. People can either be one of cybersecurity's strongest or weakest tools. Countless security breaches have been found to be caused by employee malpractice or carelessness and it's important to have the funds to properly address this issue. With adequate funding, employees will be knowledgeable, responsible, and more sensitive to actions that may lead to security breaches. Education can be done through hands-on training, staff security meetings, regular audits to ensure policy is being followed, and mock-breaches to make sure employees are prepared.

Cybersecurity Programs and Technology - 55%

I would allocate 55% of my limited budget towards cybersecurity programs and technology. The business and its employees must have the tools available to effectively prepare, prevent, and recover for security

breaches. Having the most up-to-date software and technology can go a long way in helping prevent security breaches. Allocating slightly more funds to technology will ensure that employees are ready to address any threat that is presented.

Conclusion

The Human Factor of cybersecurity is majorly important. Businesses often point towards lack of employee training and education as one of the biggest contributing factors to security breaches. If in the role of CISO, I would allocate 45% to employee training and 55% to cybersecurity technology. This allocation of funds ensures that employees will be knowledgeable as well as have the tools necessary to address dynamic cybersecurity threats.

References

Kaspersky. (n.d.). *The human factor in IT security*. Kaspersky. Retrieved November 10, 2024, from https://www.kaspersky.com/blog/the-human-factor-in-it-security/