Thomas Roeseler

CYSE 200T

Professor Charlie Kirkpatrick

November 20, 2022

The Human Factor in Cybersecurity

Training employees in cybersecurity is very important because employees or users are the weakest link in cybersecurity measures. Many cybersecurity attacks are preventable, so making sure your employees are knowledgeable in cybersecurity and them being able to report suspicious activity in your company's systems is important because they can help prevent cybersecurity attacks. The most common data breaches occur because of employee error, they have access to important systems and data which makes them more of a target for hackers. You want to have the good and updated technology for your company, but it doesn't do any good if you don't have any knowledgeable, trained employees. Consistently updating your technology is important because it lowers security risks.

Employee training

The training that you use for your employees must be effective and there should be regular training sessions to make sure your employees are knowledgeable with cybersecurity and will be able to identify suspicious activity. There should be a good percentage of your budget that you use for training your employees. Some money will be spent for new technology, but there must be enough money spent on effective training. The amount of money spent on training is how much will afford effective cybersecurity training for your employees. The remaining amount will be spent on additional cybersecurity technology. "It's vital for each employee's level of understanding about cybersecurity issues before starting any new initiative from scratch so that everyone knows where they stand technologically speaking when it comes time for them to allocate resources toward improving security measures within their organization through increased awareness levels regarding threats posed by hackers/malicious actors online,

(Renteria 2022).” Employees should know about cybersecurity and how it relates to their position and what they do. They shouldn’t just learn about cybersecurity, it should be about how it relates to their job.

Most data breaches happen because of human error. These data breaches are preventable, so that is why training your employees in cybersecurity is very important. The more the employees are educated and trained with cybersecurity knowledge, the more likely they’d be able to identify and prevent any suspicious activity on the company’s systems or networks. “A security threat cannot be avoided or reported if it is not recognized, (Author 2021).” If employees are not trained and knowledgeable, then they will be less likely to recognize a security threat in the company’s systems.

Conclusion

Since your employees are the weakest link in cybersecurity, it is important to have them trained well and because attacks are preventable, a good percentage of the limited budget would go towards training the employees instead of spending it on more cybersecurity technology. There will be money spent on additional cybersecurity technology, but in order for that technology to be useful, the training will come first. Educating employees about cybersecurity benefits the company because they will be more likely to identify and react accordingly with training and knowledge about cybersecurity. Another important aspect of training your employees in cybersecurity is to train them in a way that it affects their position.

References

Author, C. (2021, October 8). *Cybersecurity training for employees: What you need to know*. Cybint. https://www.cybintsolutions.com/cybersecurity-training-for-employees-what-you-need-to-know/#:~:text=Knowledge%20of%20cybersecurity%20and%20information%20technology%20is%20extremely,recognized%21%20This%20seems%20obvious%20but%20you%E2%80%99d%20be%20surprised.

Renteria, L. G. P. (2022, October 28). *The importance of training your employees in Cybersecurity*. LinkedIn. https://www.linkedin.com/pulse/importance-training-your-employees-cybersecurity-pedroza-renteria/