Kelsie Sharp

Professor Kirkpatrick

CYSE 200

November 17, 2024

As an organization, how can we organize our standards of cybersecurity to include training and additional resources while staying within our budget?

Humans and Cyber

Although, when most people think of cyber-security they think of cyber threats and computers. Sometimes, the average person can forget that the reason these cyber- threats exist is because of humans. Humans can threaten security in a multitude of ways, often by accident or error. To prevent this, it is important that an organization spends quality time and money on training their employees on how to properly secure their information. Another way to protect from human threats is the implementation of additional cybersecurity technology. The big issue being many companies do not know how to budget this out.

Identify

When thinking about what we can do to mitigate human threats we must first Identify those Those specific threats. Human threats can be caused by accidents, negligence, or self-motivation. Accidents can include things like clicking on the wrong link and downloading malware. Negligence could be sharing passwords using bad passwords or using the same password over and over. Being intentionally trying to infiltrate an organization system for self-interest purposes like stealing money or information. Now that we know the things that we need to look out for we can invest in proper security measures that best meet our needs.

Training

When talking about employee training, most companies will hire a third-party organization to conduct the training. But if you have your own cybersecurity team it may be more cost-effective to keep the training within the company, if they are good (Mindanao, 2023). To estimate the value of the training simply add the cost of the organization or employees you are using to conduct the training and the hourly pay of those receiving the training and compare that to the potential loss you could fall victim to due to negligence (Mindanao, 2023). Once you know your potential loss, you can decide the price you would be willing to pay to prevent that loss through employee training and other forms of mitigation. There are some factors you should consider when deciding if you should spend money and time on employee training. For one, at least 90% of data breaches are caused by human error (Hofman, 2024). Not to mention the sheer amount of money you could be potentially saving due to training. Also, through this training your data and information can be safe from manipulation.

Other Forms of Cyber Security

On top of employe training it is imperative that you have other forms of security protecting you from both outside threats and threats within the organization. This is because you must remember that not all infiltrations are accidental. As for additional cybersecurity mitigations you have a plethora of options. You could use biometrics, firewalls, two step verification, cameras, physical security, monitoring, etc. Honestly, the possibilities for mitigating are as numerous as the possibilities for cyber-attacks. What types of mitigation you should invest in depend on the company or organization’s individual needs. But in general, always use strong passwords, do not share passwords, use two step authentication, and limit access on all systems to a need-to-know basis, etc. (Mindanao, 2023). All these things are cheap to do. Like determining the value of employee training, you must weigh the cost of mitigation against the potential cost of a cyber infiltration. Whether it is worth it can seem like a tough decision to make if you are not aware of the potential threats, so it is important that before deciding how much you are willing to pay, you see your risk. This way you can decide how much you are willing to risk, and the question of paying is simple.

Conclusion

In conclusion, mitigating your cybersecurity risk can get extremely expensive, especially if your just throwing random things at the issue. So, it is important to know the individualized risks and needs of an organization. This way you can optimize your spending to be the most effective. Humans are the root cause of all cybersecurity issues, and this is why employee training is extremely important. Its crucial to remember that employees have the power and access to cause severe damage intentionally and unintentionally. This is why its important to both train your employees and put other security measures in place as well.

Works Cited

Mindanao, K. (2023, November 22). *How much does security awareness training cost (& is it worth it?)*. Intelligent Technical Solutions. https://www.itsasap.com/blog/cost-security-awareness-training

Hofmann, S. (2024, January 18). *Is Security Awareness training worth the cost?* CyberPilot. https://www.cyberpilot.io/cyberpilot-blog/is-security-awareness-training-worth-the-cost

Mindanao, K. (2023a, July 28). *10 tips for cybersecurity on a budget [updated in 2023]*. Intelligent Technical Solutions. https://www.itsasap.com/blog/tips-cybersecurity-budget