Carlos Carey

Professor Kirkpatrick

The Human Factor in Cybersecurity

15 November 2022

The Impacts of Humans in the Cybersecurity Field

No matter how much you train someone on how to be secure, no human is perfect in being completely safe when it comes to the internet or the workplace. The other side of the argument can be that improperly trained employees may not fully utilize the technology they have access to.“The major human factor issue in cybersecurity is a lack of user awareness of cyber threats,” (*Impact of human vulnerabilities on cyber security*). If I were a Chief Information Security Officer and had a limited budget to spend between employee training and new technology, I would split it into sixty percent on training and forty percent on technology.

Why Sixty Percent Training

“The fact is, employees are often the primary targets for hackers looking to penetrate critical business systems,” (*The Importance of Cybersecurity Training).* Employees seem to be one of the weakest links of cyber security, as opening what seems to be a simple email could be the backdoor entrance someone needs to get into the system. An employee simply not following protocols (if there are any) could spiral into a disaster for any company. According to Townsened, it now takes companies on average 197 days to identify a breach of data security as it occurs and it can take up to another 69 days to contain it (2021, November 3). You could

have the very best and most modern technology money can buy, but it doesn't mean anything if your employees cannot fully utilize it for what it's worth.

Implementing something such as an awareness program for cybersecurity risks would benefit the overall work environment, and help employees be more aware of some basic and possibly more complex ways to not be vulnerable targets. Making sure employees are properly trained on how to use their programs can be a simple way to also mitigate the vulnerabilities they may encounter. Enforceable policies would help protect employees and minimize business risks as the policies would help remind employees to do things they may see as tedious and unnecessary that leave your company vulnerable. Finally, implement regular testing as employees who are trained, need to be tested. Testing employees helps the employee retain what they learn and it lets you, the employer, know that your employees are performing their tasks properly and meeting their requirements and expectations.

Why Forty Percent Technology

Technology continues to advance at a rapid pace, and so do the threats that we have to face. "The rapid development of technology is a testament to innovators, however, security lags severely," (*Top 10 Threats to Information Security*). Between companies having the technology with no educated individuals to use it and some failing to embrace the new technology to help protect their data, leaves them vulnerable to being taken advantage of by cybercriminals. Companies with ignorance of cybersecurity and technology tend to not make it far, and those who fail to implement the technology required tend to meet the same fate.

Implementing things such as simple encryption can help save a company legal troubles as sensitive information getting out is as much a cybersecurity issue as it is legal. Passwords are a thing of the past from what we have learned in class, biometric technology and using things such as retina scans could help keep the work environment more secure. Having access to more modern fitments of security will help your company as updating your systems allows it to recognize more threats, as it can only detect threats that it knows of. Having backups are critical in modern cybersecurity, you never know what someone can want, or manage to get access to. If all else fails you can have some peace of mind knowing your company's information is stowed away somewhere in an offshore backup where nobody can reach and manipulate it.

Conclusion

It is apparent that both technology protection and training are very important to cybersecurity, and that the training of your employees is more important than the technology your employees have access to. You can pay for the cream of the crop technology, but it won't be worth a dime if you don't have an employee who can properly utilize it to its full capacity. The impacts of humans in cybersecurity will continue to grow with the field, and with it the risks they pose to security as long as they are uneducated and informed of the risks that surround them. Luckily the field has taken note of the issues of uneducated people with cyber risks and has begun to implement programs to help mitigate their risk to the company, however, this is just the beginning.

Works Cited

Varughese, J. (2021, November 1). *Impact of human vulnerabilities on cyber security*. CybSafe. https://www.cybsafe.com/research/impact-of-human-vulnerabilities-on-cyber-security/

Townsened, C. (2021, November 3). *The Importance of Cybersecurity Training*. United States Cybersecurity Magazine. https://www.uscybersecurity.net/cybersecurity-training-important/

Top 10 Threats to Information Security. (2022, April 7). Georgetown University Online. https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology