Is Cybersecurity Training Practical or Not?

Bhawnish Sharma
Old Dominion University

Is cybersecurity training practical or not?

Bhawnish Sharma

Old Dominion University

12/15/2022

Introduction

With technology growing, there has been an increase in cybercrime. Because of this, private and public sectors face global problems, i.e., phishing, security breaches, and identity theft. With cybersecurity software available on the internet, anyone can access it. As technology advances, cybersecurity experts must answer the tough question of, "is cybersecurity training practical or not"?

By studying how people interact and collaborate with technology, cybersecurity experts can better understand how the human factor plays into the practicality of cybersecurity training. Threat actors are getting smarter by finding innovative ways to exploit networks. Furthermore, they do this by monitoring behaviors through people's online activities. For example, by using social engineering, they can obtain sensitive information online. Threat actors use this method by deceiving users into giving them account information and access to their network. A 2015 report by IBM highlights that the human factor accounts for 95% of cybersecurity incidents. This is caused by inconsiderate work practices, ignorance, poor software patching, malicious software codes, unsecured network connections, and inadequate communication surrounding sensitive information (Gyunka & Christiana, 2017).

Methods

For my research, I began to look through the ODU library database. I started by reading multiple articles daily to gain better knowledge about my topic. I was assisted by the writing center and the ODU Liberian, Ms. Dorothy.

Other resources I used were the ACM library, google Scholar articles, and IEEE Xplore. For my research, I wanted to narrow down my topics, so I looked for specific keywords such as "cybersecurity," "training," "effective," "human factors," "training," "hacking," and "phishing"

on these online databases. After several days of research, I was able to narrow down my topic, focusing on case studies done within cybersecurity and businesses.

Literature review

Researchers have conducted many experiments to explore the impact training has on cybersecurity behaviors. I have presented two case studies. These studies are done in a business. Their findings help us understand the effectiveness of training. I am interested in whether the training was effective for the organization.

Case one is a research paper titled "the positive outcomes of information security awareness training in companies." This research study involves 2900 employees within a Turkish company. They aimed to see whether password security training would be practical. This research was carried out over 12 months. Case two is a research paper titled "A Real-World Study on Employees' Susceptibility to Phishing Attacks." In this article, the researcher conducted a case study on an Italian company. With 191 employees, the primary purpose was to reduce phishing attacks on their company by giving training.

Training effective

Eminagaoglu, Ucar, and Eren (2009) explored the effectiveness of security training. They indicated that the purpose of security training is to avoid any factors that could lead to any hack on the company. Their main goal was to have users employ a secure password. It is human nature that we reuse our passwords, especially given how many we must remember. They wanted to educate all the employees about having strong passwords on their accounts.

Each employee in the business was given proper password training and security awareness. They add additional steps like posters on office walls, surveys, and quizzes.

The study was conducted within one year. After receiving the training, they were asked to create a password for their Microsoft Active directory. The IT team used multiple tools like a dictionary attack, brute force, and L0phtcrack LC5 to crack the password. Just before the project was initiated, they could break 98.8% of the password of the employees in 24 hours. After six months of training and security awareness campaigns, they could crack 87.8% of the password of the employees in 24 hours. Twelve months after the project, they could break 63.6% of the password of the employees in 24 hours. The authors concluded that education and awareness are among the best and most effective tools for reducing the risks associated with information security. Users should be enabled with much more efficient and effective (in terms of time, money, and impact) awareness materials such as posters, brochures, animated movies, animated electronic messages, and online quizzes with prizes. (Eminağaoğlu, Uçar , &Eren ,2009)

Training ineffective

Paci and De Bona (2020) explored how cyber-attacks on businesses and other organizations are one of the most significant issues they face. These companies are primarily targeted through exploiting emails and phishing techniques. This study showed no significant effect of the employees' demographic data on susceptibility to phishing. Furthermore, employees perceived embedded training as highly effective. However, it did not reduce their susceptibility to phishing (De Bona & Paci, 2020).

They performed two phases in this experiment by conducting a research study on an Italian company. In the first phase, the 191 employees involved were sent a phishing email to change their password. In the email participants received, the IT team attached a fake direct link that led them to a phishing website that stole data. Overall, 31.4% of the employees clicked on that link (i.e., 65

out of 191), and 23.5% submitted their usernames and passwords to the phishing website. In phase two, they selected 45 employees who were part of phase 1. The selected employees were caught in a phishing attack. After receiving proper training, a week later, they received a new phishing email regarding the pay slip. The employees were given the instruction that due to a technical issue, there might be errors in their holidays and leave hours reported in last month's pay slip. A direct URL link guided the user to the HR payroll department in that email. Employees who fell victim were slightly higher than those in the first phase: 24.4% versus 23.56%. (De Bona & Paci, 2020). According to the authors, training was not effective. They also believed that the participants did not read the training manual properly. This training failed because the scientists did not consider the human factor in their study.

In 2018 Dr. Nobles wrote a paper entitled "Botching Human Factors in Cybersecurity in Business Organizations." Dr. Nobles states that human errors cause most cyber-attacks. In a recent study, 80% of organizations said that security awareness training had reduced their staff's susceptibility to phishing attacks. (Daly, 2022). The U.S. and U.K. national-level cybersecurity policies listed human-related errors in cybersecurity as a significant degradation to national security (Nobles, 2018). They use social engineering as one of the methods to control IT-trained professionals. Another issue they introduce is "the difficulty in assessing and measuring fatigue, frustration, and cognitive exertion in cybersecurity, which might result in technical mistakes and increased risk" (Nobles, 2018). Despite the obstacles, this article also recommends ways to improve security training and cyber methods used in business. With all the training provided in the business industry, the rate of cybercrime is still increasing every year.

Lhan, Hewage, Nawaf, and Alkhalil (2021), published a paper entitled, "A Recent Comprehensive Study and a New Anatomy." They discuss threat actors and how to approach

people using different methods. The report also adds that security training in every business is essential. Focusing on training and preparing users for dealing with such attacks are critical elements to minimize the impact of phishing attacks (Alkhalil & Hewage, 2021). The researchers collected data from various countries about phishing. They found that the percentage of phishing attacks is rising yearly. According to researchers, security training is not stopping cybercrime.

A security awareness blog named "Security Awareness Training Statistics & Trends:2022 Edition." This website collects data on business companies and their effect on cybercrime. The data collected by this website indicate that the percentage of cyber-attacks is increasing yearly. No sattack in every company is significantly high because of human factors.

Discussion

In the literature review, security training and protection against cybercrime is one of the most prominent challenges organizations are still facing. **'***Is cybersecurity training practical or not?'.* Our professors' emphasis in school is that cyber security training will reduce cybercrime worldwide. However, according to my research, the percentage of cybercrime is rising yearly. Researchers forecast the global cost of cybercrime in 2019 to reach over 2 trillion dollars (Morgan, 2016). People are the key factor to either success or failure of information security management in organizations. Every security breach or security problem is associated with humans, not only with technology. Human factors are mainly responsible for this failure of cyber security in organizations.

Conclusion

The fact that human error is still a factor in cyber operations shows that current approaches to training cannot eliminate human error. Due to complex technology, some employees make mistakes that lead to severe business problems. Even in basic security training, experts recommend

that we change our passwords often to reduce the risk of security breaches. Whenever a company gets hacked, the information about the public is also at risk. Businesses need to start thinking differently. Instead of requiring more training, they might explore monitor employee actions and providing meaningful and timely feedback. If instance, they could introduce software that monitors employees' password creation and usage across multiple accounts. The best way to prevent cybercrime is to make our defense system more robust and innovative. We need to consider the human element first and often during our solutions. For example, will users trust a system that monitors their passwords across work and private accounts? How can we make AI feedback more effective? I am concerned that training, certifications, and security awareness campaigns continue with limited effectiveness.

Reference

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 1-23

Beyer, R. E., & Brummel, B. (2015). Implementing effective cyber security training for end users of computer networks. Society for Human Resource Management and Society for Industrial and Organizational Psychology, 1-22.

Daly, J. (2022, May 17). How effective is Security Awareness Training? usecure Blog. Retrieved October 29, 2022, from https://blog.usecure.io/does-security-awareness-training-work#:~:text=In%20a%20recent%20study%2C%2080,within%20the%20first%2012%20months.

De Bona, M., & Paci, F. (2020, August). A real world study on employees' susceptibility to phishing attacks. In Proceedings of the 15th International Conference on Availability, Reliability and Security 1-10

Eminağaoğlu, Mete, Erdem Uçar, and Şaban Eren. "The positive outcomes of information security awareness training in companies–A case study." information security technical report 14.4 (2009): 223-229.

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on HBGary. Computing & Information Systems, 21(2), 1-10

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. Interdisciplinary Journal of Contemporary Research in Business, 5(7), 329-354

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017, April). Use of phishing training to improve security warning compliance: evidence from a field experiment. In Proceedings of the hot topics in the science of security: symposium and boot camp, 52–61.