THE IMPACT OF CYBERCRIME AWARENESS TRAINING AMONG EMPLOYEES IN CORPORATES FOR BETTER INFORMATION MANAGEMENT

Ruben Roy, Loyola Institute of Business Administration, Chennai
Joseph Francis J., Loyola Institute of Business Administration, Chennai

ABSTRACT

Cybersecurity is becoming an increasingly important issue in today's business world. The more digital the world becomes, greater becomes the threat of cyberattacks. Businesses are exposed to various cyber threats such as phishing scams and ransomware. IT companies are particularly vulnerable because they handle sensitive data and rely heavily on technology. Hence, the need to implement effective cyber security techniques for protection of self and clientele arises. Multi-factor authentication, encryption, firewalls and penetration testing are some of the most effective cybersecurity methods IT organizations employ to protect their data, systems, and networks from cyber threats. But for better protection, employee training might be needed. This paper deals with whether training all employees throughout the organization will help in the long run.

Keywords: Cyber security, Cyber-attacks, Information security management, Cybercrime awareness.

INTRODUCTION

Today's world relies heavily on electronic technology, and protecting that data from cyberattacks is difficult. The purpose of cyberattacks is to cause financial damage to businesses. In some cases, cyberattacks may have military or political objectives. Some of these damages are: PC viruses, knowledge breaks, data delivery services (DDS), and other attack vectors. To this end, different organizations use different solutions to prevent damage from cyberattacks. Cybersecurity follows real-time information on the latest IT data. So far, researchers around the world have proposed various methods to prevent cyberattacks and mitigate damage. Some methods are in the operational stage, while others are in the research stage Katrakazas et al. (2020). The purpose of this study is to collect and comprehensively review advances in proposed cybersecurity standards and examine the challenges, weaknesses, and strengths of proposed methodologies. Currently, most of the economic, commercial, cultural, social, and governmental activities and interactions between countries at all levels, including individuals, NGOs, governments, and government agencies, take place in cyberspace (Aghajani and Ghadimi 2018). Critical and sensitive infrastructure and systems are either part of cyberspace itself or are controlled, managed and used through this space Figure 1. The most important and sensitive information was transmitted or essentially formed in this space (Akhavan-Hejazi and Mohsenian-Rad, 2018). Most media activity is moved to this space, most financial transactions are conducted through this space, and the majority of citizens' time and activity is spent interacting in this space.

Fundamental Concepts

Citation Information: Roy, R., & Francis, J.J. (2023). The impact of cybercrime awareness training among employees in corporates for better information management. *Academy of Marketing Studies Journal, 27*(S5), 1-6.

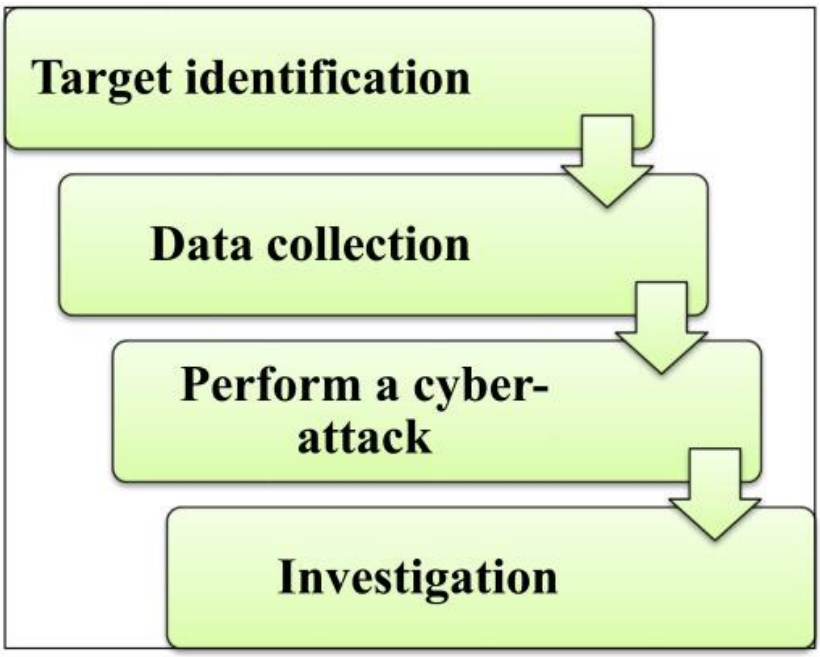

FIGURE 1
THE CYBER ATTACK PROCESS

In general, a distinction can be made between cyber-crime, cyber-warfare, and cyber-attacks. Fig. 2 and Table 1 describe the distinction between cyber-crime, cyber-warfare, and cyber-attack that defines the conceptual distinction between them Hart et al. (2020).

Cyber Threats

The main cyberattack methods are denial of service, logic bombs, exploit tools, sniffers, Trojan horses, viruses, worms, spam, and botnets. Denial of service prevents authorized users from accessing the system and vice versa. In fact, at some point, the attacker will start sending various messages to the targeted computer, blocking the flow of legitimate data. This prevents the system from using the internet or communicating with other systems; Le Nguyen & Golman, (2021). Another method, called Pervasive Denial of Service, attacks from many distributed systems simultaneously rather than launching an attack from a single source. Worms are often used to spread across multiple computers and attack targets. Exploit tools are publicly available that can detect and infiltrate network vulnerabilities of varying skill levels. A logic bomb is another type of attack in which a programmer enters code into a program and the program automatically performs destructive activities when certain events occur (Li et al., 2021). Sniffers are also programs that sniff routed information and look for specific information, such as passwords, by examining every packet in the data stream Jamal et al. (2021). Trojans hide malicious code and generally look like useful programs that users can quickly run. In addition, viruses infect system files, which are usually executable programs, and place their copies in these files. Loading infected files into memory executes versions of them, allowing the virus to infect other files. Unlike worms, viruses require human intervention to spread. Worms, on the other hand, are autonomous system programs that regenerate themselves by copying from one computer to another on a network (Aziz and Amtul, 2019). Finally, botnets are networks of infected remote control systems used to distribute malware, coordinate attacks, spam, and steal messages. Botnets are usually secretly installed on a targeted computer to allow unauthorized users to remotely control the targeted system to achieve their malicious goals. Botnets are also known as electronic soldiers (Kharlamova et al., 2021).

Citation Information: Roy, R., & Francis, J.J. (2023). The impact of cybercrime awareness training among employees in corporates for better information management. *Academy of Marketing Studies Journal, 27*(S5), 1-6.

Cyber Security Methods Used For It Firms

Multi-factor authentication (MFA): One of the most effective ways to prevent unauthorized access to your IT systems is to use MFA. This method requires the user to provide multiple forms of ID. B. Passwords and fingerprints before access to the system is granted.

Encryption: Encryption is the process of converting data into an unreadable form that makes it difficult for hackers to steal or access sensitive information. IT companies should use encryption to protect data at rest and in transit.

Firewall: A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on defined security rules. Firewalls can prevent unauthorized access to your network and detect and block malicious traffic.

Regular Software Updates

IT organizations must regularly update all software, including operating systems and applications, to address vulnerabilities and prevent cyberattacks.

Employee Training

IT companies should educate their employees on cybersecurity best practices such as detecting phishing emails and creating strong passwords. Also, employees should be trained to report security incidents to the IT department.

Penetration Test

IT companies should conduct regular penetration tests to identify system and network vulnerabilities. Penetration testing simulates cyberattacks to test the effectiveness of an IT organization's cybersecurity measures.

Incident Response Plan

IT organizations should develop an incident response plan so that they can respond quickly and effectively to cyberattacks. Your incident response plan should includeprocedures for detecting, containing, and mitigating cyberattacks.

Citation Information: Roy, R., & Francis, J.J. (2023). The impact of cybercrime awareness training among employees in corporates for better information management. *Academy of Marketing Studies Journal, 27*(S5), 1-6.

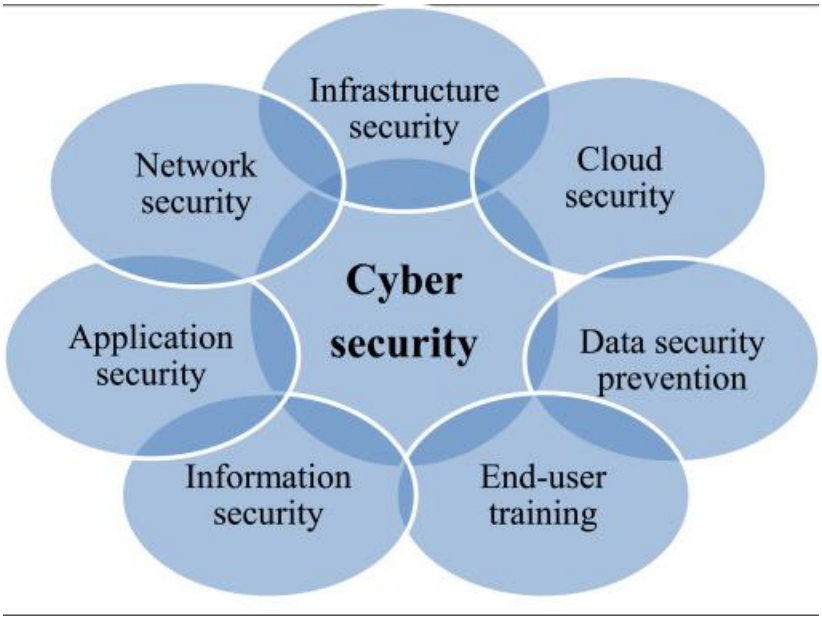

FIGURE 2
DIFFERENT ELEMENTS OF CYBER SECURITY

LITERATURE REVIEW

According to a Ponemon Institute study 2019, the most effective corporate cybersecurity measures include implementing firewalls, encrypting sensitive data, and performing regular software updates. The survey found that 64% of organizations affected by a data breach do not have a formal cybersecurity strategy. Additionally, the study found that organizations with a cybersecurity strategy are more likely to detect and respond to cyberthreats quickly and effectively Figure 2.

Another study by Accenture (2019) found that investing in cybersecurity measures can reduce the cost of cybercrime by up to 70%. The study also found that organizations that adopted a proactive cybersecurity approach had a greater impact in reducing cyber threats than those that took reactive measures. A study by Kaspersky (2020) found that cybersecurity threats increased during the COVID-19 pandemic, with phishing scams being the most common. The study found that 73% of businesses had suffered a phishing attack in the last 12 months. The study also found that companies that educate their employees about cybersecurity practices have lower success rates for phishing attacks Khan et al. (2020).

Cybercrime is projected to cost businesses $6 trillion annually by 2025, according to a study by Cyber security Ventures (2021). The research highlights that the most effective cybersecurity strategies include a mix of technical solutions such as firewalls and encryption, along with non-technical solutions such as: B. Employee Training and Implementation of Incident Response Plans gain. A Gartner study (2021) predicts that by 2025, 60% of organizations will be using cloud-based security solutions. The study assumes that organizations assume that all users, devices, and networks are potentially compromised and require rigorous verification before being granted access to sensitive data or systems. Researching trust security. It also emphasizes the importance of implementing a model.

A study (2020) conducted by Awad and Al-Zoubi examined the level of cybercrime awareness among Jordanian university students. The survey found that the majority of students had a low awareness of cybercrime and were unfamiliar with the various types of cybercrime. The study recommends that educational institutions include a cybercrime awareness program in their curricula to improve students' knowledge and awareness of cybercrime.

Citation Information: Roy, R., & Francis, J.J. (2023). The impact of cybercrime awareness training among employees in corporates for better information management. *Academy of Marketing Studies Journal, 27*(S5), 1-6.

Another study by Kim et al. (2020) examined cybercrime awareness levels among seniors in South Korea. The survey found that seniors have lower levels of cybercrime awareness compared to younger generations. The study recommends that governments and related organizations provide cybercrime awareness programs specifically targeted at older adults.

A 2019 study conducted by Alsajjan and Alashoor examined the level of awareness of cybercrime among Saudi citizens. The survey found that the majority of respondents had a low awareness of cybercrime and its potential impact. The study recommends that the Saudi government implement cybercrime awareness programs targeting different age groups and socioeconomic backgrounds. A study conducted by examined the level of awareness of cybercrime among medical students in Saudi Arabia. The survey found that the majority of medical students have moderate cybercrime awareness. However, the study also found that students lacked knowledge of the laws and regulations related to cybercrime. The study recommends including cybercrime education in medical school curricula Sakhnini et al. (2021).

METHODOLOGY

Conduct employee surveys in corporate environments that measure employee awareness levels of various types of cybercrime.

TalentLMS and Kenna Security created a 7-question quiz to find out how much your employees know or don't know about basic cybersecurity principles. Respondents ranged in age from 18-54 and worked in various industries in the United States. They all use computers for most of their work, with 43% working in the office and 57% working from home Figure 3.

Questionnaire

1. *Which of the following passwords would outsmart a hacking attack?*
2. *Which of the following file types have the potential to be harmful?*
3. *How does ransomware work?*
4. *USB Drives are harmless if you see but nit use the content: True or False?*
5. *If your laptop is password-protected then its files are safe even if device gets lost/stolen : True or False?*
6. *Which of the following actions are necessary to keep documents safe?*
7. *After receiving a suspicious mail from your CEO with a link, what would you do?*

RESULTS AND DISCUSSION

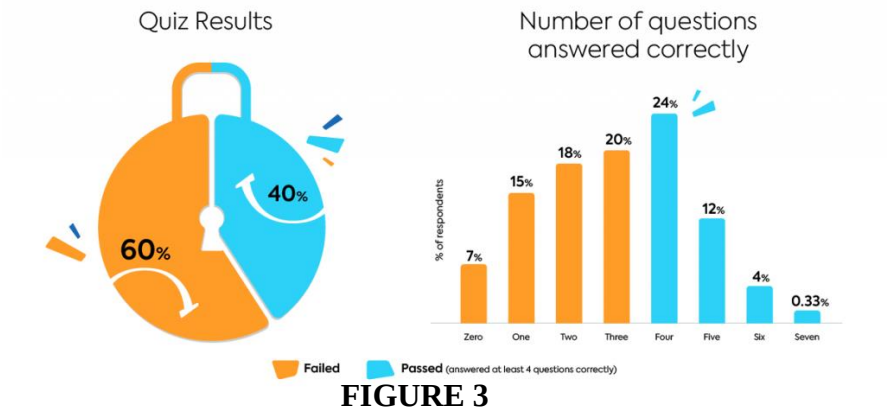

FIGURE 3
RESULTS OF QUESTIONNAIRE

Citation Information: Roy, R., & Francis, J.J. (2023). The impact of cybercrime awareness training among employees in corporates for better information management. *Academy of Marketing Studies Journal, 27*(S5), 1-6.

Respondents who answer 4 or more questions correctly are considered a pass, otherwise they are considered a fail. 60% of respondents failed the evaluation. In fact, 7% of the respondents answered all questions incorrectly, while less than 1% of respondents answered all 7 questions correctly while 61% of those trained answered fewer than 4 questions correctly. And of those who answered all seven questions incorrectly, 80% said they were trained.

CONCLUSION

Gathering conclusion from all the above, businesses should implement effective cyber security measures to protect against cyber threats. Research shows that the most effective cyber security measures for businesses include implementing firewalls, encrypting sensitive data, implementing regular software updates, and investing in proactive cyber security measures. Additionally, employee training and the implementation of an incident response plan are key elements of a comprehensive cyber security strategy. As cyber threats continue to evolve, organizations must stay abreast of the latest cyber security trends and strategies. The results of these quizzes show the average employee's limited knowledge of cyber security threats and best practices. Also, most employers provide some sort of training for their employees on the subject, but it is spotty and the return on investment is low.

REFERENCES

Aghajani, G., & Ghadimi, N. (2018). Multi-objective energy management in a micro-grid. *Energy Reports*, *4*, 218-225.

Akhavan-Hejazi, H., & Mohsenian-Rad, H. (2018). Power systems big data analytics: An assessment of paradigm shift barriers and prospects. Energy Reports, 4, 91-100.

Aziz, A. A., & Amtul, Z. (2019). Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. *Pharmacological Research*, *149*, 104471.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

Jamal, A. A., Majid, A. A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2021). A review on security analysis of cyber physical systems using Machine learning. *Materials Today: Procee*

Katrakazas, C., Theofilatos, A., Papastefanatos, G., Härri, J., & Antoniou, C. (2020). Cyber security and its impact on CAV safety: Overview, policy needs and challenges. *Advances in transport policy and planning*, 5, 73-94.

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, *148*, 105837.

Kharlamova, N., Hashemi, S., & Træholt, C. (2021). Data-driven approaches for cyber defense of battery energy storage systems. *Energy and AI*, *5*, 100095.

Kim, Y. S., Choi, M. K., Han, S. M., Lee, C., & Seong, P. H. (2020). Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP. *Annals of Nuclear Energy*, *149*, 107790.

Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries:'Law on the books' vs 'law in action'. *Computer law & security Review*, *40*, 105521.

Lee, C., Chae, Y. H., & Seong, P. H. (2021). Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs. *Annals of Nuclear Energy*, *158*, 108287.

Sakhnini, J., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2021). Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. *Physical Communication*, 47, 101394.

Received: 23-Mar-2023, Manuscript No. AMSJ-23-13376; **Editor assigned:** 24-Mar-2023, PreQC No. AMSJ-23-13376(PQ); **Reviewed:** 28-Apr-2023, QC No. AMSJ-23-13376; **Revised:** 20-May-2023, Manuscript No. AMSJ-23-13376(R); **Published:** 03-Jun-2023

Citation Information: Roy, R., & Francis, J.J. (2023). The impact of cybercrime awareness training among employees in corporates for better information management. *Academy of Marketing Studies Journal, 27*(S5), 1-6.