International Journal of Science and Engineering Science Research
Volume 1 | Issue 2 | April-June 2025 | ISSN 3049-2793
Peer Reviewed (Referred Journal)

Cyber Awareness in The Digital Ecosystem

Dr. Shailesh Kumar Pathak

Assistant Professor, Department of Commerce, Rajashri Krishna Dutt PG College Jaunpur, Uttar Pradesh, India

Author Email: skpathak2512@gmail.com

Abstract

Technology is evolving at rapid scale and there by consumer adoption, but Awareness is not aligned to that speed. As individuals increasingly rely on digital platforms for communication, financial transactions, and various other activities, the risk of cyber threats has grown exponentially. Understanding and assessing individual preparedness to mitigate cyber risk is a multifaceted challenge that involves delving into an array of factors, cultivating awareness, and analyzing online behavior.

Factors influencing individual preparedness to tackle cyber risk are diverse and interconnected. One of the pivotal elements is technological literacy. In an era dominated by complex digital systems and sophisticated cyber threats, individuals with a higher level of technological literacy are better equipped to comprehend and respond to potential risks. This literacy encompasses not only the ability to navigate digital interfaces but also an understanding of fundamental cyber security principles. Factors such as educational background, professional training, and exposure to technology contribute significantly to an individual's technological literacy.

Moreover, socio-economic factors play a crucial role in shaping an individual's cyber risk preparedness. Disparities in access to technology, internet connectivity, and financial resources can create vulnerabilities, as individuals with limited access may be less aware of cyber threats or lack the means to implement robust security measures. Social and cultural factors also influence how individuals perceive and respond to cyber security issues. Attitudes towards privacy, trust in digital platforms, and the prevalence of cyber norms within a community all contribute to shaping an individual's approach to cyber risk mitigation.

Keywords

Cyber Security, Ecosystem, Awareness, Digital Fraud

Introduction

A critical aspect of awareness is understanding the Information leakage to unauthorized, the value of personal data and the potential consequences of its compromise. With the increasing digitization of personal information, individuals must recognize the significance of safeguarding their data from unauthorized access. Awareness campaigns that highlight real-world examples of cyber incidents and their repercussions can be instrumental in conveying the urgency of adopting proactive cyber security measures. The individuals who is using the technology and technology enabled services such as Software and application including mobile applications, it is a minimum requirement to understand purpose, what data is being accessed, what data is transmitted etc. They also expected to know the consequences of not understanding. Additionally, staying informed about the latest cyber security trends, emerging threats, and best practices is essential for individuals to adapt their defense strategies accordingly.

Online behavior serves as a direct reflection of an individual's cyber security preparedness. The way individuals engage with digital platforms, their adherence to security protocols, and their response to potential threats collectively contribute to their overall cyber risk posture. An analysis of online behavior involves scrutinizing aspects such as credential hygiene, adherence to software updates, and the cautiousness exercised while interacting with emails and other digital communications.

Individuals who prioritize strong, unique passwords, regularly update their software and applications, and exercise caution when clicking on links or downloading attachments are more likely to be resilient against cyber threats. On the contrary, risky online behavior, such as the reuse of passwords across multiple platforms, neglecting software updates, and falling victim to phishing attempts, significantly heightens the

2 security should be approached with a multi-stakeholder strategy that considers the needs of individuals, companies, and governments alike. This study is a great tool for scholars, practitioners, and policymakers in the area of sustainable development and cyber security to use when figuring out how to include cyber security into digitalization in a way that doesn't compromise security.

Edensor, Mehmet Emin et al., (2022) This study presents to what extent Kyrgyz- Turkish Manas University students are knowledgeable about cyber security in the distance education process. The survey was conducted with a sample of 517 students from all faculties of the university at the undergraduate, graduate, and PhD levels. Our research study shows that

although huge numbers of cyber attacks are occurring around the world, the students did not have any knowledge about cyber security and the effects of cyber attacks overall. An analysis of cyber security awareness was undertaken by asking questions focused on malicious software, password security, and social media security. Although we live in an age of technology where our entire lives are indexed to the internet through the distance education process, it has been determined that students have a weak cyber security awareness. It has been further concluded that cyber security education should be given to prevent the students from becoming a victim of cyber attacks, helping them to use the internet more effectively.

Foya, David. (2020) The study looked at the level of awareness and state of preparedness for organizations on cyber security. The main objective of the research was to determine the impact of cyber security awareness and preparedness of organizations on the security behaviors of employees. Research questions was what is the level of preparedness of organizations in response to cybercrime/attack. The study was significant as it brought out suggestions on critical issues identified on cyber security. The research adopted the qualitative approach as it sought to assess human behavior in relation to awareness. The inter poeticism philosophy was used as well as the multi case study research strategy. The researcher used interviews and questionnaires for data gathering. The major findings of the research where that the firms where ill prepared with regards to cyber security. Another major finding was that the employees where not really aware of the subject understood Resources are

dedicated to aspects of the business that authorities deem more important. The researcher recommended that the firms conduct more frequent security awareness programs so that this influences the security behaviour of employees in a positive way. It was also a recommendation that the firms invest in the requisite skill sets to effectively address cyber security issues.

Alrobaian, Shouq et al., (2020) People are the weakest link in the cyber security chain when viewed in the context of technological advancement. People become vulnerable to trickery through contemporary technical developments such as social media platforms. Information accessibility and flow have increased rapidly and effectively; however, due to this increase, new electronic risks, or so-called cybercrime, such as phishing, scams, and hacking, lead to privacy breaches and hardware sabotage. Therefore, ensuring data privacy is vital, particularly in an educational institute where students constitute the large majority of users. Students or

trainees violate cyber security policies due to their lack of awareness about the cyber security environment and the consequences of cybercrime. This paper aims to assess the level of awareness of cyber security , users' activities, and user responses to cyber security issues. This paper collected data based on a distributed questionnaire among trainees in the Technical and Vocational Training Corporation (TVTC) to demonstrate the necessity of increasing user awareness and training. In this study, quantitative research techniques were utilized to analyze the responses from trainees using tests such as the Chi-Squared test. Proof of the reliability of the survey was provided using Cronbach's alpha test. This research identifies the deficiencies in cyber security awareness among TVTC trainees. After analyzing the gathered data, recommendations for tackling these shortcomings were offered, with the aim of enhancing trainees' decision-making skills regarding privacy and security using the Nudge model.

Alahmari Ph.D., Abdulmajeed (2020) Small and medium-sized enterprises (SMEs) have been encouraged to take advantage of any possible business opportunities by utilizing and adopting new-technologies such as cloud computing services, there is a huge misunderstanding of their cyber threats from the management perspective.

Underestimation of cyber security threats by SMEs leads to an increase in their vulnerabilities and risks, which unfortunately can become actual challenges to them and other related parties. The purpose of this paper is to provide a systematic literature review based on recently available evidence on cyber security risk management in SMEs in order to understand the current situation. The authors aim to reveal the role the SMEs' management is playing in addressing cyber security risks in recent years, as found in the literature, and to suggest avenues for further research. The paper follows a well-known method for conducting a systematic literature review. Starting with a keyword search and an assessment of fitness for this review, 15 papers out of 50 have been analysed by NVivo software according to bibliographical information, research design and findings. The review identified 5 major perspectives that play a key role in SMEs' cyber security risk management, which are threats, behaviours, practices, awareness, and decision-making respectively. Importantly, empirical research on cyber security risk management in SMEs is needed.

Alharbi, Talal et al., (2018) Information exchange has become increasingly faster and efficient through the use of recent technological advances, such as instant messaging and social media platforms. Consequently, access to information has become easier. However,

new types of cyber security threats that typically result in data loss and information misuse have emerged simultaneously. Therefore, maintaining data privacy in complex systems is important and necessary, particularly in organizations where the vast majority of individuals interacting with these systems is students. In most cases, students engage in data breaches and digital misconduct due to the lack of knowledge and awareness of cyber security and the consequences of cybercrime. The aim of this study was to investigate and evaluate the level of cyber security awareness and user compliance among undergraduate students at Majmaah University using a scientific questionnaire based on several safety factors for the use of the Internet. We quantitatively evaluated the knowledge of cybercrime and protection among students to show the need for user education, training, and awareness. In this study, we used a quantitative research methodology and conducted different statistical tests, such as ANOVA, Kaiser–Meyer–Olkin (KMO), and Bartlett's tests, to evaluate and analyze the hypotheses. Safety concerns for electronic emails, computer viruses, phishing.

REFERENCES

1. Goswami, Shankha & Sarkar, Shouvik & Gupta, Krishna & Mondal, Surajit. (2023). The role of cyber security in advancing sustainable digitalization: Opportunities and challenges. Journal of Decision Analytics and Intelligent Computing. 3. 270-285. 10.31181/jdaic10018122023g.

2. Erendor, Mehmet Emin & Yildirim, Merve. (2022). Cyber security Awareness in Online Education: A Case Study Analysis. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3171829.

3. Alahmari Ph.D., Abdulmajeed & Duncan, Bob. (2020). Cyber security Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 1-5. 10.1109/CyberSA49311.2020.9139638.

4. Nunes, Paulo & Antunes, Mario & Silva, Carina. (2011). Evaluating cyber security attitudes and behaviors in Portuguese healthcare institutions. Procedia Computer Science. 181. 173-181. 10.1016/j.procs.2021.01.118.

5. Wang, Keyong & Guo, Xiaoyue & Yang, Dequan. (2012). Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. Electronics. 11. 1659. 10.3390/electronics11101659.

6. Zwilling, Moti & Klien, Galit & Lesjak, Dusan & Wiechetek, Łukasz & Çetin, Fatih & Basım, H. Nejat. (2015). Cyber Security Awareness, Knowledge and