Journal of Advances and Scholarly Researches in Allied Education
Vol. 21, Issue No. 5, July-2024, ISSN 2230-7540

Employee Awareness and Attitudes Towards Cybersecurity Technologies

Jayanthi Pankajakshan[1]*, Dr. Ruchi Maheshwari Bangur[2]

[1] Research Scholar, Banasthali Vidyapith, Radha Kishnpura, Rajasthan, India

Email: vtanwar@gmail.com

[2] Supervisor, Department of Commerce and Management, Banasthali Vidyapith, Radha Kishnpura, Rajasthan, India

Abstract - This study explores employee awareness and attitudes towards cybersecurity technologies. As organizations strive to improve their cybersecurity measures, the human element remains a critical yet often overlooked factor. This research investigates the correlation between employee awareness and the adoption of emerging cybersecurity technologies, the impact of these technologies on cybersecurity incident rates, and the relationship between employee satisfaction and cybersecurity awareness. A qualitative exploration approach was employed, utilizing data from peer-reviewed publications, technology conference proceedings, and industry reports. Surveys of cybersecurity experts and organizational executives were conducted to identify recurring themes and concerns. The findings reveal that increased employee awareness significantly enhances the effectiveness of cybersecurity measures and reduces security incidents. Furthermore, the study highlights the necessity of continuous training and education for employees to maintain a robust cybersecurity posture. The research also emphasizes the importance of integrating cybersecurity technologies into daily operations to enhance their efficacy. This comprehensive examination aims to assist organizations in developing resilient cybersecurity strategies that address both technological and human factors.

Keywords: Cybersecurity, Employee Awareness, Cybersecurity Technologies, Cybersecurity Incidents, Employee Satisfaction, Information Security, Cyber Threats

- X -

INTRODUCTION

Improving the current information security architecture has received a lot of attention in the battle to shield organizations from data theft and cybercrime(Hadlington, 2018). the emphasis on technological remedies for Cyber Security often ignores the fact that staff participation and awareness of the systems' benefits are necessary for them to be successful. The realization that humans are often the weakest link in the cyber security chain has drawn criticism from a number of academics. Organizations may become more vulnerable to security vulnerabilities as a result of factors such as dangerous cyber security behaviors, ignorance, misdirected attention, and passive involvement.

Understanding Cybersecurity Threats

A standard is defined as the best possible situation with a lower limit on attainment. It also refers to the technical requirements that a service facility must follow in order to provide service users with the greatest possible function, purpose, or profit from the services. Several global groups, consortia, and organizations play a crucial part in the creation of standards. Standards are described as papers that specify requirements, practices, and principles with the goal of guaranteeing the security, consistency, and dependability of goods, services, and systems, according to www.standards.org.au. Furthermore, according to the definition given by the ISO/IEC, standards are papers or guidelines that are created based on a broad consensus and approved by a legal body. They serve as models, samples, or guidelines that assist achieve the best possible outcomes in a certain situation(Taherdoost, 2022). A standard takes into account resource and technological constraints, realistically satisfies user needs, and complies with verification criteria.

Cybersecurity mishaps are often brought on by ignorance or human mistake. Over 8.5 billion records were compromised in 2019, accounting for more than 200 percent of the total quantity lost in 2018. Insider errors were mostly to fault, according to IBM's X-Force Threat Intelligence Index 2020. According to 34% of firms surveyed for the Ernst & Young Global Security of Information Survey 2018–19, phishing and careless/unaware staff are the largest cybersecurity vulnerabilities. The password "123456" was used by 23.2 million victim accounts globally, according to research conducted by the National Cyber Security Centre (NCSC) in the United

Kingdom. Some of the largest cybersecurity breaches in recent years have been linked to spear phishing and phishing emails, according to an Annual Cybersecurity Report which was released(Hong & Furnell, 2021). Therefore, one of the most essential ways to safeguard consumers at home and in organizations from dangers is to promote cybersecurity practices. It is true that in order to provide a safe cyber environment, both the technical and human components of information security must be addressed at the same time. The relationship between intentions as well as habits gives rise to motivated behaviors.

The last ten years have seen an exponential rise in the number of different security incidents, including malware attacks, unauthorized access, denial of service (DoS) attacks, zero-day attacks, data breaches, social engineering or phishing, and more, due to the rapidly growing prominence for information technology to recent decades. The security community recorded less than 50 million unique malware executables in 2010. This estimated figure more than quadrupled to almost 100 million in 2012. Based on AV-TEST figures, the security sector discovered more than 900 million malicious executables in 2019—a figure that continues to grow. Businesses and individuals may suffer large financial losses as a consequence of cybercrime and network assaults. For instance, estimates show that the average cost of a data breach is USD 3.9 million in the US and USD 8.19 million worldwide, and that cybercrime damages the global economy USD 400 billion annually(Ahsan et al., 2022). The security community predicts that throughout the next five years, there will be almost four times as many data breached. Consequently, in order to reduce further losses, companies need to develop and execute a thorough cybersecurity plan.

As this study is being conducted, billions of people worldwide are being impacted by the coronavirus pandemic, which is causing an unprecedented amount of turmoil in the globe Systematically understanding cybersecurity economics: A survey(Kianpour et al., 2021). We have been impacted by this significant occurrence not only in the real world but also online. Events like elections, Olympics, and wars swiftly find their way online, and enemies may use these worldwide occurrences to target individuals, groups, and governments. The cybersecurity domain's decision-makers have paused to consider these developments. Furthermore, researchers studying cybersecurity economics are working to create a consensus on the necessity of safe, long-lasting hyperconnected digital societies through raising awareness, forming solid multi-stakeholder alliances, and enacting significant structural adjustments in important areas of institutional operations.

Every member of society is impacted by the pervasive need for healthcare. The healthcare industry must exchange very sensitive and private information with patients, medical professionals, and other organizations while also gathering and preserving it. Technology advancements force HealthCare Systems (HCS) to change. The shift in healthcare from hospital-based, specialty-focused methods to dispersed, patient-centered care has been made easier by the digitization of health records, and this shift is universally acknowledged as necessary and inevitable. Breach of HCS cybersecurity exposing patient data or personal information would have a detrimental effect on patients as well as the healthcare facility, perhaps resulting in fatalities(Offner et al., 2020). The danger of ransomware attacks, device hacking, and loss of private medical information associated with cybersecurity is always increasing for the healthcare industry. Because personal information is so valuable, stolen health data are worth more than records of any other business. When they are sold on the darkweb, they may be used to finance illegal behavior and make identity theft, extortion, blackmail, and even murder possible.

The number of physical objects linked to the Internet has increased exponentially as a result of the Internet of Things (IoT) revolution. The Internet of Things (IoT) and other linked data technologies, or cyber-physical systems (CPS), are thriving because they improve operating systems and current infrastructure. There are many advantages that CPS may provide to businesses, governments, and people. But protecting these systems separately has proved to be very difficult. The cost and danger of possible assaults will increase as long as time- and safety-critical uses of CPS are implemented continuously. Cyberattackers are increasingly interested in CPS, such as smart grids, as they are essential parts of safety-critical infrastructures. As an example, hackers compromised the electric grid's control system in Ukraine, resulting in a power outage that affected over 230,000 people. In the absence of effective security safeguards, an attacker may be able to gain access to a CPS and do harm from a distance by sometimes employing devices linked to the Internet as entry points(Walker-Roberts et al., 2020).

Attitudes and Perceptions of Cybersecurity Technologies

Government demands for comprehensive cybersecurity regulations have increased in tandem with the rise in civilian hack risk in recent years(Snider et al., 2021). These demands reached their zenith with the assaults on the Colonial Pipeline as well as SolarWinds in 2021, when the US government's lack of access to cybersecurity data in vital businesses severely jeopardized the economic and national security of the nation. Following these assaults, legislators and the general public showed renewed support for legislation than would require private companies to disclose cyberattacks, furthering a long-standing legislative trend. For instance, more than 280 legislation and resolutions pertaining to cybersecurity were submitted by 40 United States states and territories in 2020. In Israel and Europe, a comparable trend has occurred.

The goal of the study was to ascertain how students felt about social media site cybersecurity and personal privacy, as well as their understanding of these topics. In the context of this research, social media is defined as electronic communication platforms (such social networking and microblogging websites) that allow users to establish online communities for the purpose of exchanging ideas, information, and private messages. The capacity to manage one's personal information so that only those the owner wants to access it is known as privacy, as is "freedom from unauthorized intrusion."

This involves managing who can access what content on social media as well as controlling what content is visible defines digital literacy as falling into three categories: 1) locating and consuming digital material; 2) producing digital content; and 3) sharing or conveying it (p. 5–6). The concept of digital literacy should, according to the authors, include a fourth category: raising knowledge of privacy and security concerns and available defenses. In that regard, summer class participants at a large institution in western Pennsylvania were given a paper-based questionnaire(Bhatnagar & Pry, 2020). In order to expand the sample size, a paper-based survey was used instead of an online one.

In a variety of contexts and among the general public, people are often seen as the weakest link in the cybersecurity (CS) chain(Debb & Mcclellan, 2021). Psychological aspects are often the subject of research, such as the relationship between personality type and conscientiousness1,2 or the interaction between formal training and cognitive top-down decision making to increase adherence to best practices that take into account both human and computer elements. Furthermore, in order to get a better understanding of how and to what degree actual conduct reflects expressed opinions, there has been an increasing amount of interest in examining the gap between people's statements and actions. Examining the factors that lead to these views is crucial because they are closely related to how people see their susceptibility to computer-related hazards.

In the last several decades, information technology (IT) has advanced quickly. While the digital transformation of healthcare facilities has opened up new avenues for quality improvement, it has also presented challenges, including managing electronic patient records, illness records, family history information, and sensitive patient data. Studies on cybersecurity awareness among healthcare workers are worthwhile since they handle sensitive data and often lack the technical IT know-how to do it correctly and in accordance with best practices for application security. In actuality, healthcare workers must devote themselves entirely to fulfilling their primary duty of providing patient care. Their main worries are not information security best practices or IT expertise(Nunes et al., 2021). New behaviors and attitudes about the reality on individual and societal health are brought to the forefront by the creation of new social models of the interaction between the patient and the healthcare practitioner, which are based on trust. In other words, medical information and data bolsters the trust of medical practitioners while also boosting patient knowledge and awareness of their condition.

Human mistake is to blame for half of the cybersecurity breaches linked to regular handling of private electronic data and technological ramifications. Prior efforts to tackle this problem have often focused on the technological or physical fixes. Unfortunately, as more and more cybersecurity-related events are being reported worldwide, it is becoming clear that algorithms, systems, and procedures by themselves are unable to maintain the security of digital systems. According to a recent analysis, for example, cybersecurity-related mishaps were estimated to have cost the world economy almost $600 billion USD in 2018.

Research has begun to move toward comprehending the different human elements that impact cybersecurity since it has become more clear that the human side of cybersecurity offers as big of a danger as the technological component(Jeong et al., 2019). Thus far, research has shown that a person's attitude and behavior toward cybersecurity are mostly determined by their cultural background, innate personality traits including gender and age, and their own demographic characteristics. To properly comprehend the influence of these human variables on cybersecurity, new methodologies are needed due to their extremely subjective and complicated character. Still, the bulk of research on cybersecurity and human factors is dominated by a technological perspective. This emphasizes the necessity for a comprehensive examination of cybersecurity that takes into account the multifaceted and multidisciplinary character of the rapidly developing area.

Impact of Positive Attitudes on Cybersecurity Practices

Cyberspace is defined as the non-physical, interactive environment of information flow as well as communication between networks and computer systems by the International Telecommunication Union (ITU). To put it another way, it is a worldwide realm made up of interconnected networks of software and storage-related information technology infrastructure. Organizations and governments have used the non-physical realm to go from managing a specialized network to a sophisticated, decentralized, linked system throughout time. This has hampered security efforts by increasing the number of attack spots. With more devices linked, the realm of interdependent networks has gotten harder to secure, making organizations more vulnerable to cybersecurity incidents that might cause them to lose a lot of money and damage their brand(Onumo et al., 2021).

The need to create the essential security and privacy measures will only increase due to the internet's rapid global growth and the resulting increase in connection among people, businesses, and finance. However, one of the frequent problems with their cybersecurity assurance is people's improper online activity. Because of the many errors people make online, some research has even called humans the main cybersecurity weak link. Simple errors like intentionally using a pen drive infected with malware, accepting dubious email attachments (which may even include executable file types), or simply clicking a malicious phishing link posted to social network groups out of greed are examples of some of these faults.

Additionally, in order to help organizations, institutions, security practitioners, and researchers identify users who are more vulnerable to inadequate and dangerous security practices, it is imperative to comprehend how the individual differences of internet users influence their cybersecurity behaviors(Fatokun et al., 2019). Owing to their exploratory style of learning, tertiary institution students are a group of intelligent people who often utilize the internet. These pupils have reportedly been shown to be susceptible to cyberthreats, notwithstanding the research. Additionally, research has shown that students at postsecondary institutions tend to have comparable age groups, genders, and educational backgrounds. This suggests that studying these aspects in relation to cybersecurity practices would be fair.

Cyberattacks can have devastating repercussions. Hacks or data breaches have the ability to seriously harm an organization's finances or reputation and erode public confidence in the targeted company. Additionally, even individual user data is not secure, and the wider effects of hacks pose a risk to national security. In addition to technological fixes, end-user cybersecurity training is receiving more attention. There are many different strategies available, such as large-scale but ineffective awareness campaigns; challenge-based learning, where participants take on multiple tasks in particular domains; capture the flag events, where participants must secure their own flag or file as well as capture those of others; or video games on a table.

Introducing a serious game is an alternative strategy(Van Steen & Deeleman, 2021). A serious game is different from a conventional game in that its main objective is not to amuse or provide pleasure. Serious games, on the other hand, are designed to help players learn. In addition to having this instructional objective, they may be planned as activities with set dates, times, and regulations. Through interactive aspects that may be explored alone or with others, serious games can be used to instruct or educate an audience. When it comes to improving knowledge and cognitive abilities, serious games may be more beneficial than traditional teaching methods.

Every aspect of our life is surrounded by information technology (IT). Technology has quickly emerged as the keystone for the advancement of several vital fields, including company administration, healthcare, transportation, and education. To enhance services and preserve their competitive advantages, both public and commercial institutions have embraced technology to linked their vital resources to the internet. Governmental organizations and commercial businesses must safeguard their IT infrastructure as well as data. They have become more fixated on technological security solutions, ignoring the reality that people, procedures, and technology work together to provide successful security(Alkhazi et al., 2022a). Consequently, Security issues have been regularly reported by huge enterprises that have made significant investments in robust security solutions.

LITERATURE REVIEW

(Daengsi et al., 2022)Three stages made up the study: the first phishing assault, the knowledge transfer using a mixed-approach, and the second phishing attempt with a different content. Employee cybersecurity awareness has increased, according to data validation and interpretation of the findings. Employees who clicked on the phishing email fell off by 71.5%. Consequently, other companies and other sectors/industries might use this strategy to improve cybersecurity. Additionally, it was shown that, within the Thai cybersecurity ecosystem, gender significantly influenced cybersecurity knowledge, as Thai female workers had a greater degree of cybersecurity awareness.

(Aldawood & Skinner, 2019) This research draws attention to the difficulties and recurring problems that companies face when trying to build human knowledge defenses against social engineering assaults. A thorough assessment of the literature is offered along with an appraisal of current methodologies to support these claims. The results demonstrate that hackers are still effective in their evil activities of stealing sensitive data that is essential to enterprises, even in the face of cutting edge cyber security procedures and employees with advanced training.

(Zwilling et al., 2022)The correlations between cyber security awareness, knowledge, and behavior with protection tools are the main emphasis of this research, which is conducted among people generally and in Israel, Slovenia, Poland, and Turkey specifically. The findings indicate that while internet users are aware of cyber threats, they only take the bare minimum of precautions, which are often straightforward and widely available. The results of the research also demonstrate that, independent of respondent country or gender, more cyber knowledge is linked to a higher degree of cyber awareness.

(Gundu, 2019)The goal of this research is to provide a cybersecurity policy compliance reinforcement and incentive model that will aid in the advancement of knowledge transformation into beneficial cybersecurity practices. Both the deterrence theory as well as the idea of planned action are included into the model. The model was improved and validated via the use of expert review and action research. Thirty workers from a SME to South Africa participated in the extensive two-cycle action research study. The relationship between knowledge, incentives and penalties, and behavior was noted in the research. The research confirmed that having knowledge does not guarantee moral behavior. Only around 64% of behavioral intentions transformed into desired action after information dissemination programs. This revealed the connection between workers' fear of punishment or their attraction to money, which leads them to behave safely.

(Oluwaseun Abrahams et al., 2024) The study looks at the methods used by businesses to make sure that security policies and procedures are followed, with a focus on the importance of effective monitoring systems, transparent communication, and consequence control. The impact of effective accountability frameworks on overall cybersecurity posture is shown via the integration of case studies and real-world scenarios. Specifically, it focuses on maximizing employee participation and cultivating a responsibility culture. This study summarizes major results and highlights new developments in cybersecurity awareness and education initiatives. From developing a watchful and proactive workforce to strengthening defenses against new cyber threats, companies may benefit from the insights gained from this investigation.

(Huang & Pearlson, 2019)Beyond only the newest technology, organizational cybersecurity demands other things as well. Every employee in the business has to take steps to lower risk in order to make it secure. It is especially the duty of leaders to comprehend, mold, and harmonize the attitudes, values, and beliefs of the whole company with overarching security objectives. Managers must find workable ways to handle the human aspect of cybersecurity. This study presents a model that characterizes the elements that go into creating an organizational cybersecurity culture as well as how it can be quantified. These elements are shown in a case study of a "culture of data protection" established by Liberty Mutual's financial services executives. This will assist managers in comprehending and implementing suggestions to establish a better developed cyber security culture inside their company.

(Pósa & Grossklags, 2022)Students who have work experience are more conscious of the cyber-security dangers that come with working remotely, and a larger percentage of them are aware of the designated person they can get in touch with in case of an emergency. We address an area that has seen little study attention up to this point by presenting organizational security measures via the eyes of workers with little job experience. We provide suggestions for both remote study and work situations, particularly in cases where the results of our survey and those found in the research literature survey disagree.

(Alkhazi et al., 2022b) According to our research, all approaches contribute equally to knowledge growth. On the other hand, the attitudes of users are more affected when the same message is delivered over many channels. However, text-based and game-based training formats outperformed their counterparts in terms of behavioral change. Furthermore, the intervention technique affected the workers' propensity to participate in future awareness programs and self-education activities. These results have significant ramifications since ISA programs have to be created in a manner that encourages staff members to adopt security procedures in their day-to-day operations and has a positive mental impact on them.

RESEARCH GAP

All of the study points to different elements of employee knowledge and attitudes toward cybersecurity technology, but there are still unanswered questions. While a number of studies concentrate on the significance of corporate culture, gender factors, and the efficacy of training programs, the long-term durability of these training benefits and the ongoing development of cybersecurity threats get less attention. Furthermore, there is a dearth of thorough research on how these tactics might be integrated into various organizational and cultural settings, as well as the unique difficulties small and medium-sized businesses (SMEs) have in maintaining high cybersecurity awareness. It is also yet unclear how human behavior and technology developments interact, particularly in distant work settings. Developing more resilient cybersecurity strategies requires a more comprehensive strategy that incorporates these components and takes into account the changing nature of workforce behavior and cybersecurity threats.

METHODOLOGY

Research Design

The study will use a qualitative exploration research approach to examine how businesses adopt new cybersecurity solutions. Data will be gathered via a methodical examination of technology, conference proceedings, peer-reviewed publications, cybersecurity news sources, and more. To address frequent issues with technology integration, surveys of cybersecurity experts and executives of organizations will be undertaken. Recurring themes and concerns will be found via thematic analysis. Data will be gathered using feedback forms, pre- and post-session surveys, and engagement metrics in workshops and knowledge-sharing events in order to increase awareness among stakeholders within the company. The report intends to assist businesses in strengthening their cybersecurity posture by offering a comprehensive overview on emerging trends in cybersecurity.

Research Objectives

- Correlation between Cybersecurity Awareness and Adoption of Emerging Technologies.
- Impact of Emerging Technology Adoption on Cybersecurity Incident Rates.
- Relationship Between Employee Satisfaction and Cybersecurity Awareness.

Study Area

This research aims to investigate employee awareness of and attitudes about cybersecurity technology in the workplace. In order to determine how much participants' self-confidence, independence, and capacity to accomplish both personal and professional objectives are increased by continuous peer-reviewed publications, conference proceedings, industry reports on academic databases, online cybersecurity news websites, a multi-site research will be conducted. Data from various demographic groups may be gathered to get a knowledge of cybersecurity technologies and employee awareness in general and particular scenarios. Through an examination of these procedures, the research hopes to provide insight on how educators and legislators may create inclusive policies and settings that encourage Employee Awareness, that will eventually improve personal cybersecurity across a variety of devices.

Hypothesis

H1: Correlation between Cybersecurity Awareness and Technology Adoption.

H2: Impact of Emerging Technology Adoption on Cybersecurity Incidents.

H3: Relationship Between Employee Satisfaction and Cybersecurity Awareness.

Sampling Technique

A stratified random sample approach would be suitable to investigate the effectiveness of employee knowledge of and attitudes toward cybersecurity technology. This strategy guarantees a fair representation of the various demographic groups, including people of various ages, educational backgrounds, and degrees of community involvement and cybersecurity technology proficiency. The research has a higher chance of obtaining a representative and balanced sample if the population is divided into many relevant strata and individuals are then randomly selected from each. This strategy covers employee knowledge and cybersecurity attitudes and experiences across a variety of demographic groupings, leading to more accurate and broadly relevant outcomes.

Sample Design

The Simple Random Sampling approach was used to survey 280 financial departments in total for this investigation.

DATA COLLECTION

The knowledge and attitudes of employees concerning cybersecurity technologies will be examined using a quantitative method approach. Quantitative information on staff awareness, participant attitudes, and cybersecurity will be gathered using structured surveys with Likert scale questions. Employee awareness, new cybersecurity technologies, and people's attitudes will all be evaluated by these surveys. With the use of these methods, one will be able to comprehend the link between growing cybersecurity dangers, employee awareness, and evolving cybersecurity technologies.

TOOLS AND TECHNIQUES FOR DATA ANALYSIS

Tools

The AMOS (Analysis of Moment Structures) program and the Statistical Package for the Social Sciences (SPSS) will be used for data analysis in this research.

Techniques

SEM Analysis

A statistical method known as structural equation modeling (SEM) analysis allows researchers to investigate intricate correlations between several variables at once. Structural equation modeling (SEM) employs both multiple regression and component analysis to evaluate the direct and indirect impacts of a theoretical model. Correlation hypothesis testing using both visible as well as latent (unobserved) variables is especially useful since it sheds light on the structural links underlying the data. The social sciences, behavioral research, and other domains where comprehending the connections among distinct categories is crucial often use social science methodology, or SEM. Through this method, model fit may also be evaluated to verify that the suggested theoretical model accurately reflects the data.

DISCUSSION

There is a definite correlation between employee knowledge and the overall effectiveness of organisational cybersecurity, as the presented theories demonstrate. A stronger organisational cybersecurity posture is positively correlated with increased employee understanding of developing cybersecurity technologies because better-informed staff are better able to identify and address possible threats, which lowers security incidents including vulnerabilities. This connection emphasises how crucial it is to provide workers with continual training and education so they not only know about the newest technology but also know how important it is for them to preserve security. Furthermore, knowledgeable staff members are much more likely to utilise cybersecurity technologies efficiently and incorporate them into their regular tasks, which greatly increases the technologies' efficacy. The belief that these technologies are advantageous and easy to use also plays a part in their efficient use, suggesting that user experience is critical to cybersecurity results. Therefore, improving organisational security and lowering risks requires funding extensive awareness campaigns and making sure cybersecurity technologies are seen as approachable and beneficial.

REFERENCE

1. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. https://doi.org/10.3390/jcp2030027
2. Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet*, *11*(3). https://doi.org/10.3390/fi11030073
3. Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022a). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*(December), 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286
4. Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022b). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286
5. Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal*, *18*(1), 48–58.
6. Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, *27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7
7. Debb, S. M., & Mcclellan, M. K. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 605–611. https://doi.org/10.1089/cyber.2021.0043
8. Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1). https://doi.org/10.1088/1742-6596/1339/1/012098
9. Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*, *May*, 94–102.
10. Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*(1), 269–281. https://doi.org/10.5281/zenodo.1467909
11. Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*. https://doi.org/10.1016/j.jisa.2020.102710
12. Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-Janua*, 6398–6407. https://doi.org/10.24251/hicss.2019.769
13. Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019*, 338–345. https://doi.org/10.1109/CIC48465.2019.00047
14. Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. *Sustainability (Switzerland)*, *13*(24). https://doi.org/10.3390/su132413677
15. Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, *181*(2019), 173–181. https://doi.org/10.1016/j.procs.2021.01.118
16. Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), 556–585. https://doi.org/10.1080/02684527.2020.1752459
17. Oluwaseun Abrahams, T., Ajoke Farayola, O., Kaggwa, S., Ugomma Uwaoma, P., Olanipekun Hassan, A., Onimisi Dawodu, S.,

& Author, C. (2024). Cybersecurity Awareness and Education Programs: a Review of Employee Engagement and Accountability. *Computer Science & IT Research Journal*, *5*(1), 100–119. https://doi.org/10.51594/csitrj.v5i.708

18. Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *ACM Transactions on Management Information Systems*, *12*(2). https://doi.org/10.1145/3424282
19. Pósa, T., & Grossklags, J. (2022). Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students. *Journal of Cybersecurity and Privacy*, *2*(3), 490–515. https://doi.org/10.3390/jcp2030025
20. Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1), 1–11. https://doi.org/10.1093/cybsec/tyab019
21. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*, *11*(14). https://doi.org/10.3390/electronics11142181
22. Van Steen, T., & Deeleman, J. R. A. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 593–598. https://doi.org/10.1089/cyber.2020.0526
23. Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: understanding security threats in the era of cyber-physical systems. *Journal of Supercomputing*, *76*(4), 2643–2664. https://doi.org/10.1007/s11227-019-03028-9
24. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Corresponding Author

Jayanthi Pankajakshan*

Research Scholar, Banasthali Vidyapith, Radha Kishnpura, Rajasthan, India

Email: vtanwar@gmail.com