International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-11 Issue-11 November-2024 www.ijarets.org

CYBERSECURITY THROUGH EMPLOYEE EYES: ATTITUDES, CHALLENGES AND OPPORTUNITIES

Husneara Sheikh

Research Scholar, School of Technology and Computer Science

Glocal University, Mirzapur Pole, Saharanpur (U. P.) India.

Prof. (Dr.) Lalit Kumar Khatri

Research Supervisor, School of Technology and Computer Science

Glocal University, Mirzapur Pole, Saharanpur (U.P) 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 Technologies, Cybersecurity Incidents, Employee Satisfaction, Information Security, Cyber Threats, Cybersecurity, Employee Awareness.

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. 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 hyper connected digital societies through raising awareness, forming solid multi-stakeholder alliances, and enacting significant structural adjustments in important areas of institutional operations.

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).

LITERATURE REVIEW

(Zwilling et al., 2023) 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.

(Daengsi et al., 2023) 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.

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

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

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.

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 organizational 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 organizational 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.2022.323028

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/CIC48465.2019.0004

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/10.1080/02684527.2020.1752 459

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/10.1080/08874417.2020.1712