iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83521

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Impact Factors predicted of Cyber Security Awareness Breaching Information Technology Privacy in Organization

Anas A. Nicola
Faculty of Telecommunication, Engineering and Space Technology, Future University, Khartoum, Republic of the Sudan

Abstract: ***The present paper focuses on Cyber Security Awareness Campaigns, and aims to identify key factors regarding security which may lead them to failing to appropriately change people's behavior. The increasing recognition of human susceptibility to cyber threats highlights the imperative for integrating human factors into cybersecurity. The research explores the diversity of definitions across cybersecurity literature, revealing a significant discrepancy that hampers interdisciplinary understanding and the effective incorporation of human factors practices. In particular, our work considers these challenges from Different attitude of employs in the time of duty, a Psychology perspective and self-security awareness present a biggest challenge. However, as we believe that understanding how people perceive risks is critical to creating effective awareness campaigns. Changing behavior requires more than providing information about risks and reactive behaviors - firstly, people must be able to understand and apply the advice, and secondly, they must be motivated and willing to do. we extract essential components for an awareness campaign as well as factors which can lead to a campaign's success or failure. Finally, the research focusing to the peoples which can be able to understand and concern the risk of variabilities, enhancing its defenses against human-centric vulnerabilities emphasizing the critical role in mitigating human errors and human-induced problems in cybersecurity.***
Keywords: Cybersecurity, Ergonomics, Human Error, Human Factors, Human Performance, Technology.

I. INTRODUCTION

The significance of human factors in cybersecurity is increasingly recognized as researchers and industry experts acknowledge the susceptibility of individuals to psychological and cognitive exploitation by malicious entities. This elements as a threat vector, on par with technical vulnerabilities recognition of human [1,2]. The human factor refers to security decisions made by users as well as system administrators. In fact, the IBM Security Services 2014 Cyber Security Intelligence Index [6] states that 95% of all the investigated security accidents were largely due to human errors. Such errors include mis-configuration, poor patch management as well as the use of weak and repeated usernames and passwords [3]. Researchers have put a considerable amount of research effort to understand and model the human behavior within the cybersecurity context [4,5]. However, the frequency of today's cyber-attacks suggests that malicious entities are still computer systems. Therefore, we making use of the human vulnerability to jeopardize the security of nowadays need to make use of our knowledge and understanding of the human behavior to design and evaluate the security of computer systems, taking into consideration the uncertainties of the human factor. According to the Human Factors and Ergonomics Society [6], human factors is a scientific discipline devoted to understanding human interactions within systems, products, and devices that employ theory, principles, data, and design techniques to optimize human performance, behavior, and safety. Even though human factors engineering has existed before software, network, and cybersecurity engineering, there is a lack of human factors courses in cybersecurity curricula [7]. Each panelist brings a different research perspective, human work experience, and expertise in human factors in cybersecurity. The following are potential questions for the panelists:

1) How important are organization developing human factors in cybersecurity self-awareness?
2) What barriers prevent industry or organization from realizing the significance of human factors in cybersecurity?
3) What challenges will organization and industry face when integrating human factors courses into the curricula?
4) What is the best approach to train cybersecurity professionals on human factors?
5) What are the benefits of leveraging human factors practices in cybersecurity operations?

The main objective of this study is to investigate how human actions and errors contribute to cybersecurity risks. This study will focus on the various ways in which individuals, employees and end users, inadvertently introduce vulnerabilities in secure systems by examining real cyber incidents, the aim of this study is to identify the most common types of human error and the cognitive,

psychological and organizational factors affecting them [8]. By defining the scope in this direction, the study ensures a comprehensive study of human error across different sectors and organizational levels, so that targeted strategies can be developed will be reduced adapted to various circumstances [9].

II. RELATED WORK

Human error is widely recognized as one of the most important causes of cybersecurity issues. understanding can lead to serious vulnerabilities in an organization's network [10]. cybersecurity policies have staggered [11]. Understanding these psychological factors is essential to developing more effective human-centered security strategies that manage and mitigate the risks associated with human behavior in cybersecurity situations [12]. Cybersecurity strategies and policies provide structured approaches to protecting information systems, and many emerging traditions and models have shaped how organizations approach security notable example is the zero-trust model, which assumes that any entity, internal or external to an organization, can be trusted by default, requiring rigorous authentication with each access request and the National Institute of Standards and Technology (NIST) as well [13]. training and awareness programs can reduce the probability of human error in the short term, more research is needed to assess the long-term sustainability and feasibility of these improvements' changes in the impact of evolving threats, an area worthy of further investigation [14].

Table 1. lists the main approaches to cybersecurity management used in various industries, and highlights their limitations and specific application areas. This includes traditional methods like phishing awareness training and password policies, which are expensive but face challenges like user sensitivity, compliance issues etc.

TABLE 1 . Summary of Current Cybersecurity METHODS, LIMITATIONS, AND APPLICATION AREAS

Method	Limitations	Application Area
Phishing Awareness Training	- Users still susceptible to sophisticated phishing attacks.	Government
Password Policies (Complexity, MFA) -	Users tend to reuse or simplify passwords, leading to weak security despite guidelines. MFA may be difficult to implement for non-technical users.	Corporate networks - Personal accounts – E-commerce platforms
Zero Trust Architecture	- Complex for large organizations.	Large enterprises - Government institutions - Cloud services
Security Information and Event Management (SIEM)	High volume of alerts can lead to alert fatigue for security teams. Expensive to implement and manage.	Large enterprises
User Behavior Analytics (UBA)	Privacy concerns due to tracking user actions. - Requires large amounts of data to identify anomalies accurately.	Cyber defense agencies Large organizations
Artificial Intelligence (AI) for Threat Detection	AI systems can be vulnerable to adversarial attacks (i.e., tricking AI with subtle input modifications).	Critical infrastructure Security monitoring platforms
Regular Patching and Software Updates	Users often delay updates, leaving systems vulnerable. - Compatibility issues may arise with certain systems.	All sectors - Software development environments - Personal devices

III. METHODOLOGY

This study uses mixed methods, combining quantitative and qualitative research methods to provide a comprehensive understanding of the role of human error in cybersecurity incidents, ensuring research intensive and comprehensive Quantitative data will be collected through structured surveys to assess the frequency and types of human errors found in organizations. Table 2. Shows the main criteria used in the research methodology for studying human-related cybersecurity. It shows measurable factors, such as human error types, phishing error rates, and the effectiveness of cybersecurity training, along with their corresponding unit measures [15].

Table 2. Key Parameters And Unit Measures For Human-Centric Cybersecurity Methodology

Parameter	Description	Unit of Measure
Human Error Types	Common categories of human errors in cyber incidents (e.g., phishing, misconfigurations).	Frequency (number of occurrences)
Phishing Error Rate	Percentage of users who fall for phishing attacks.	Percentage (%)
Password Mismanagement Instances	Count of weak, reused, or improperly managed passwords.	Frequency (number of instances)
Error Frequency by Sector	Frequency of human errors in specific sectors	Frequency per sector
Incident Recovery Time	Time taken to recover from a human-error-induced cybersecurity incident.	Hours/Days

A. Human Factors in Cybersecurity

A main issue of human factors within cybersecurity is the current state that it is actively used within cybersecurity. Moreover, of the research that does exist, its scope is often limited [16], or ambiguous and varied, or only acknowledges the concept of human factors in passing [17]. Cybersecurity encompasses both the practice of safe online behaviors (e.g. scanning downloaded files) and the use of tools and resources to achieve it (e.g. anti-virus, firewalls). Therefore, at its core, all behavior related to addressing or causing cybersecurity issues require some level of human input.

B. Results

This section aims to elucidate how human factors are conceptualized in cybersecurity non activated with self-awareness in the organization, that let us offering comprehensive insights into reflects the various behavior s of human factors existing. While this list is not all-inclusive, it demonstrates the complexity of understanding what human factors mean in cybersecurity. After exploring define human factors in their activity routine work time. In addition, the mentoring behavior taken Monitoring employees during official working hours at a rate of 8 hours per day, 6 days a week, for a duration of one-month, total hours equal 192 HRS. Table 3. Figure 1, Table 2 Figure 2, has been explained behavior indicator.

Table 3. Results of Direct Observations **:**Behavioral Indicator

	Behavioral Indicator	Repetition	Percentage
Employees with self-awareness	Failure to secure the computer during working hours when leaving the office	80	60%
	Using unsecured personal storage devices	70	50%
	Downloading files from the internet on the work device and opening unknown links	82	55%
	Exchanging passwords verbally among colleagues along with sharing the use of a computer with each other without privacy	40	20%
	The employee's belief that the IT department is responsible for protecting devices in case of any damage or data theft.	65	45%

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

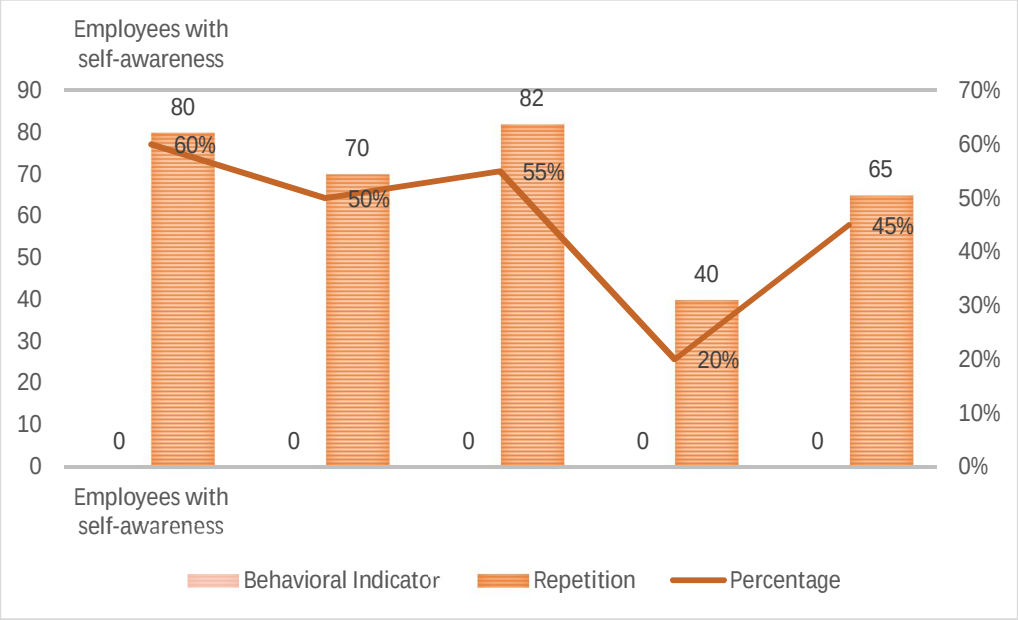


Figure 1. Employees with self-awareness

Results of Direct Observations :Behavioral Indicator

	Behavioral Indicator	Repetition	Percentage
Employees without self-awareness	Failure to secure the computer during working hours when leaving the office	90	70%
	Using unsecured personal storage devices	93	71%
	Downloading files from the internet on the work device and opening unknown links	95	94%
	Exchanging passwords verbally among colleagues along with sharing the use of a computer with each other without privacy	80	60%
	The employee's belief that the IT department is responsible for protecting devices in case of any damage or data theft.	95	98%

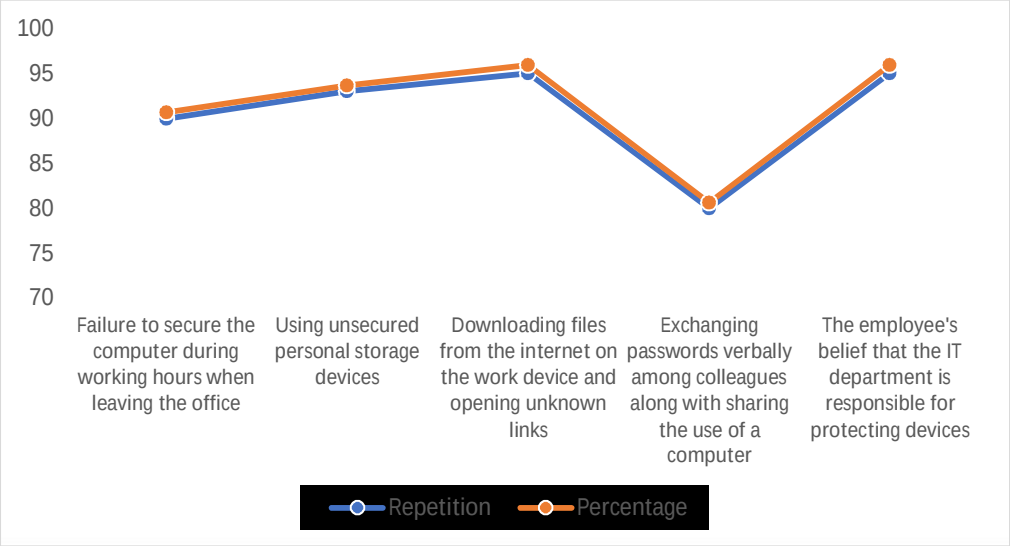


Figure 2. Employees without self-awareness

C. Discussion

human factors influenced cybersecurity in organization. The overall findings were that factors identified system and unknowingly clicking fraud emails and links due to limited knowledge and skills in cybersecurity. Table 1 and Table 2 shown Human Error Types. The results explained the percentage of behavior indicator of self-awareness, self without awareness. percentage of the breaching variabilities increasing from 70% to 85% with self-awareness. And without self-awareness reached to 95 %.How ever the variabilities of the total employees shown higher result attack indicator within different levels of the employee in different sectors. Figure 3 and Figure 4 shown the result details .

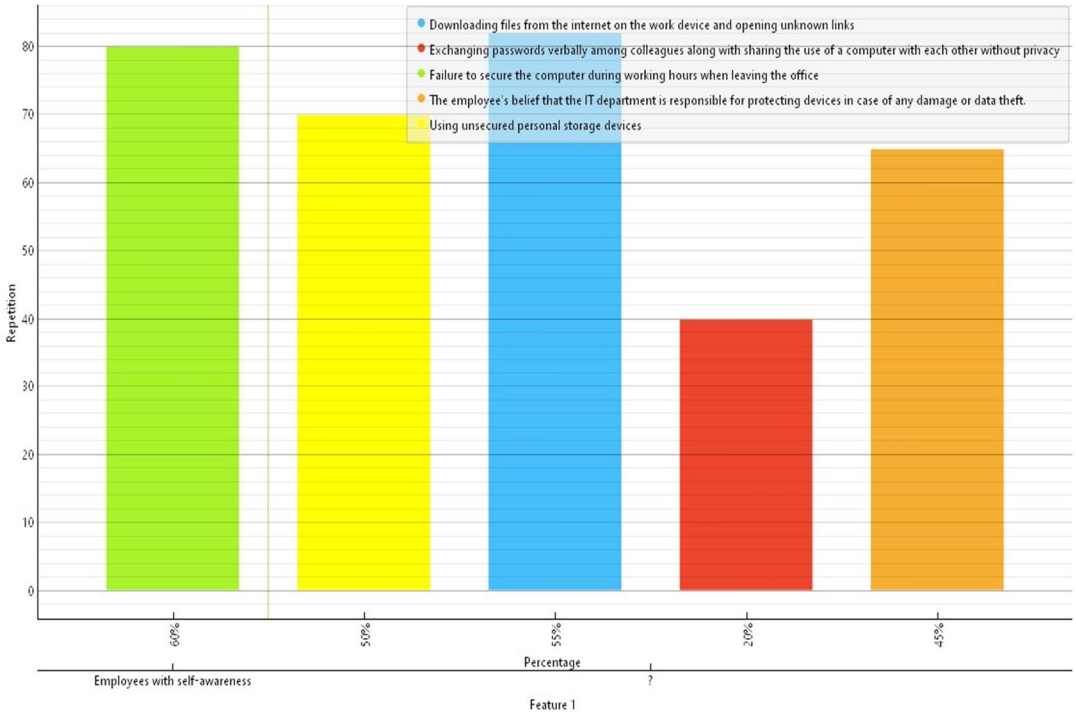


Figure 3. Explained the percentage characteristics of the Results of behavior indicator Attacks.

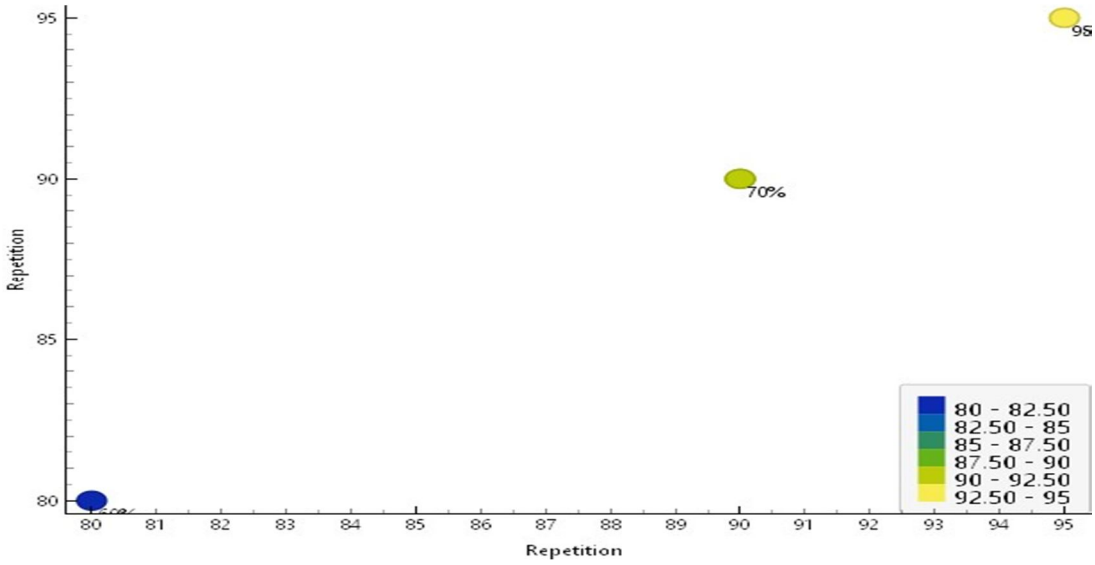


Figure 4. provided randomly percentage breaching awareness of the variabilities Attack

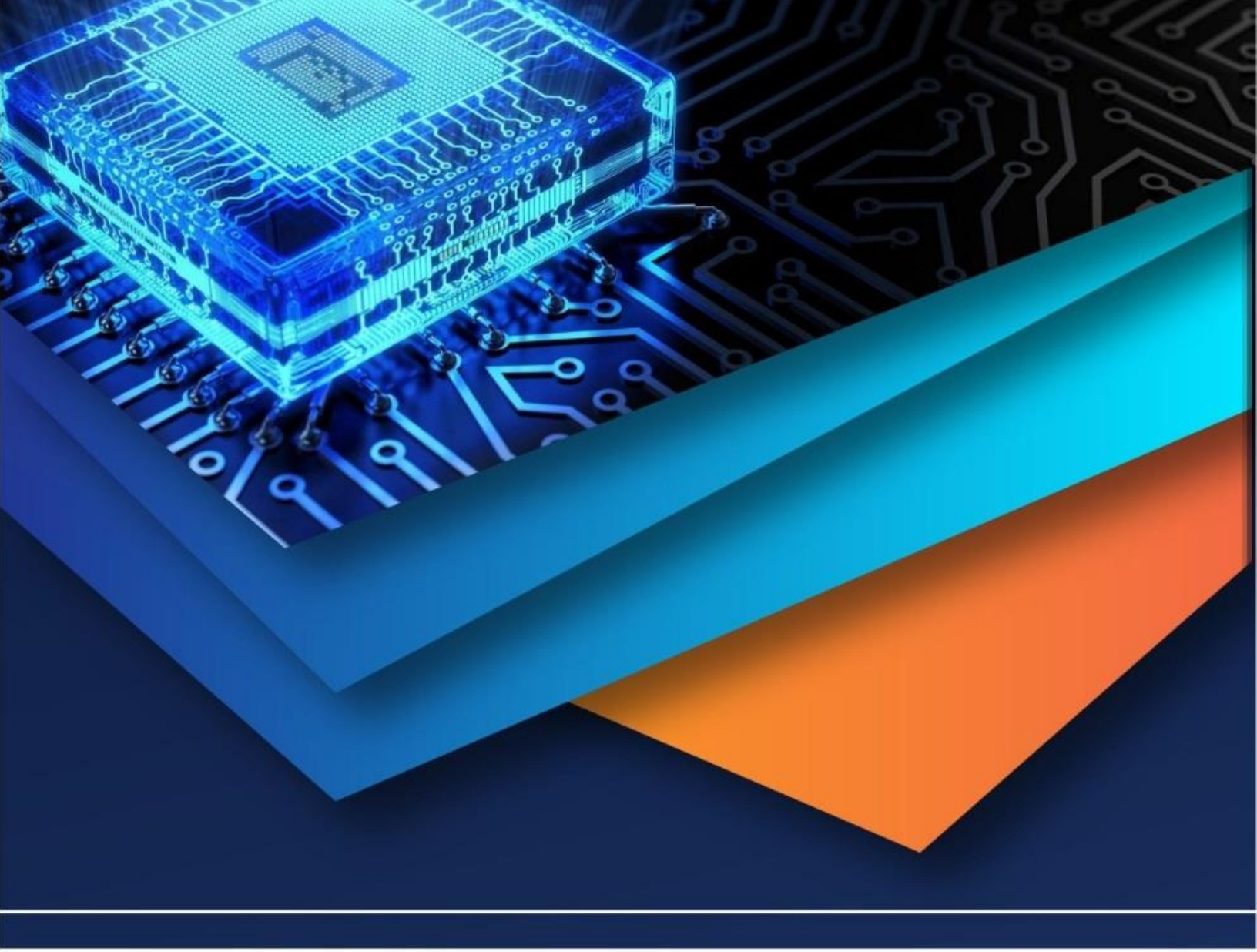
IV. CONCLUSION

The study gives elucidation of human factors within cybersecurity emerges as a critical area for scholarly inquiry, given its profound implications for the efficacy of mitigative strategies against human-induced vulnerabilities. and provide overall conceptual frameworks of the antecedents of employees' cybersecurity behavior. In so doing, we emphasize both end-users of cybersecurity in organizations and employees focused specifically on cybersecurity work. We provide an expansive agenda for future organizational science research on cybersecurity The engagement of human factors practitioners, predicated on a unified understanding of human factors, is indispensable. Therefore, the cybersecurity domain must achieve consensus on these definitions to bolster its defensive capabilities against the multifaceted challenges posed by human elements. researcher in this study gives highlight for the number of breaching attacks inside organization. researcher take this awareness happened routinely inside organization for to assist the Information technology department activate the rules and policy for how the employee developing to protect attack.

REFERENCES

[1] Nobles, C. (2022, March). The Dunning-Kruger Effect around human factors in cybersecurity, Top Cyber News Magazine https://www.linkedin.com/company/topcybernews/
[2] Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: a scoping review. In The 12th International Conference on Advances in Information Technology (pp. 1-11).
[3] G. T. Services. Ibm security services 2014 cyber security intelligence index. Technical report, 2014.
[4] B. Schneier. The psychology of security. In Progress in Cryptology - AFRICACRYPT 2008, volume 5023 of Lecture Notes in Computer Science, pages 50–79. Springer Berlin Heidelberg, 2008.
[5] R. West. The psychology of security. Communications of the ACM, 51(4):34–40, 2008.
[6] Human Factors and Ergonomics Society. n.d. What are human factors and ergonomics? https://www.hfes.org/About- HFES/What-is-Human-Factors-and-Ergonomics.
[7] Security. (March 2022). Top Cyber News Magazine. Retrieved July 1, 2022 from https://www.linkedin.com/company/topcybernews/
[8] K. Jadhav, S. Haggag, and H. Haggag, "Diving deep into human centric issues within cyber security," in Joint 4th International Workshop on Experience with SQuaRE Series and Its Future Direction and 1st Asia-Pacific Software Engineering and Diversity, Equity, and Inclusion Workshop (IWESQ 2022+ APSEDEI 2022), Tokyo, Japan, 2022, pp. 60–68.
[9] Corman, "The Human Element in Cybersecurity–Bridging the Gap Between Technology and Human Behaviour," 2023.
[10] Wang, P. Zheng, Y. Yin, A. Shih, and L. Wang, "Toward human-centric smart manufacturing: A human-cyber-physical systems (HCPS) perspective," Journal of Manufacturing Systems, vol. 63, pp. 471–490, 2022.
[11] R. Rohan et al., "Enhancing Cybersecurity Resilience: A Comprehensive Analysis of Human Factors and Security Practices Aligned with the NIST Cybersecurity Framework," in Proc. 13th Int. Conf. Advances in Information Technology, 2023, pp. 1–16.
[12] L. Bishop, "The employee experience in cybersecurity and how to mitigate risk," Ph.D. dissertation, Cardiff University, Cardiff, U.K., 2023.
[13] Smith and K. Patel, "Building Cyber Resilience through Security Culture: The Role of Human Factors in Machine Learning Environments," ACM Transactions on Cyber-Physical Systems, vol. 6, no. 3, pp. 1-22, 2023.
[14] N. Poehlmann et al., "The organizational cybersecurity success factors: an exhaustive literature review," in Advances in Security, Networks, and Internet of Things: Proc. SAM'20, ICWN'20, ICOMP'20, ESCS'20, 2021, pp. 377–395.

[15] N. M. A. Chisty, P. R. Baddam, and R. Amin, "Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity," Engineering International, vol. 10, no. 2, pp. 69–84, 2022.
[16] Heather Young, Tony van Vliet, Josine van de Ven, Steven Jol, and Carlijn Broekman. 2017. Understanding Human Factors in Cyber Security as a Dynamic System. In International Conference on Applied Human Factors and Ergonomics. Springer, 244ś254.
[17] Alex Vieane, Gregory Funke, Robert Gutzwiller, Vincent Mancuso, Ben Sawyer, and Christopher Wickens. 2016. Addressing human factors gaps in cyber defense. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 60. SAGE Publications Sage CA: Los Angeles, CA, 770ś773.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY