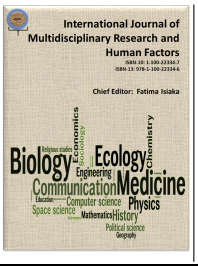

International Journal of Multidisciplinary Research and Human Factors (IJMRHF)
Volume 1, Issue 1, ISSN : 3043-579X
Website : https://ijmrhf.aijournals.org/

Human-Centric Cybersecurity : A Strategic, Evidence-Based Approach

Ishaya, Azi Jason[*1]
Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria.
Email : aziishaya7@gmail.com

G. I. O. Aimufua[2]
Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria.
Email : aimufuagio@nsuk.edu.ng

Jibrin, Nurudeen[3]
Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria.
Email : eldeenjib@ymail.com

Chaku E. Shammah[4]
Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria.
Email : chakushammah@nsuk.edu.ng

Accepted : 2nd Dec., 2024
Revised : 6th Dec., 2024
Published : 9th Dec., 2024

[*1]**Corresponding Author : Jibrin, Nurudeen**
Correspondent Email : eldeenjib@ymail.com

[1,2,3,4]**These Authors equally contributed :**
To this paper,
Sponsor : Nasarawa State University, Keffi, Nigeria.

Abstract

Notwithstanding the substantial investments in cybersecurity, organizations continue to succumb to breaches caused by human factors. This study investigates the human elements that contribute to cybersecurity vulnerabilities and proposes effective strategies to mitigate them. Through a mixed-methods approach, involving surveys ($n = 100$) and expert interviews ($n = 35$), we identify key vulnerabilities : limited awareness, susceptibility to phishing, and weak password practices. Our research reveals a concerning gap between security training and actual behavioural change. To combat these vulnerabilities, we advocate for a multi-faceted approach : (1) continuous, interactive security awareness training, (2) fostering a strong security culture, and (3) overcoming resource constraints and employee resistance. By implementing this comprehensive strategy, organizations can significantly strengthen their human firewall and reduce the risk of cyberattacks. This study contributes to the understanding of human factors in cybercrime and provides actionable insights for organizations to strengthen their digital defences.

Keywords : Human Factors, Cybersecurity, Mixed-methods, Awareness Training, Security-centric culture

CC BY NC SA

1 Introduction

The ever-increasing cost of cybercrime, estimated at $6 trillion globally in 2021 (CSIS, 2021), highlights the critical need for robust cybersecurity measures.

While technological solutions are essential, human factors like employee awareness and behavior significantly influence an organization's security posture. Cybersecurity incidents have become a growing concern for organizations worldwide, as the reliance on digital technologies and the interconnectedness of systems increases.

Cybersecurity incidents have become a growing concern for organizations worldwide, as the reliance on digital technologies and the interconnectedness of systems increases. While technological measures play a crucial role in mitigating cyber threats, the human factor also plays a significant role in shaping an organization's security posture (Lallie et al., 2021). Human factors such as employee behaviors, awareness, training, and decision-making can either contribute to or undermine the effectiveness of cybersecurity measures. Understanding the impact of human factors on cyber security incidents and developing effective mitigation strategies is critical for organizations to enhance their cybersecurity posture. Globally, the number of cybersecurity events is increasing, and these attacks can have catastrophic effects. Cybercrime is predicted to cost the globe $10.5 trillion a year by 2025, up from $3 trillion in 2015, according to a report by Cybersecurity Ventures. Financial losses, brand harm, legal repercussions, regulatory issues, and even concerns about national safety can all be caused by cybersecurity events. Cybersecurity threats are continually changing, and new attack methods and vulnerabilities are being discovered daily. To avoid and reduce cybersecurity events, it is crucial to adopt efficient cybersecurity procedures and structures (Amato et al., 2020).

Technical fixes like firewalls, spyware, systems for identifying and preventing intrusions, and encryption have traditionally been the main focus of security. These technology options, however, are insufficient on their own to handle the increasingly sophisticated and varied cybersecurity threats. The way people behave and make decisions has become a key factor in cybersecurity methods and systems. Studies have demonstrated that human elements, including staff mistakes or ignorance, threats from insiders, and social engineering techniques, are what lead to or enable the majority of problems related to cybersecurity (Ansari et al., 2022). There are several ways that human factors might affect cybersecurity. Employees may participate in dangerous practices including sharing login information, installing prohibited software, or creating weak passwords. Employees could unintentionally click on a harmful link or attachment, fall prey to phishing scams or social engineering tricks, or divulge private data to outsiders (Farheen, 2022). Employees or contractors may mistakenly or willfully create information leaks, theft, or destruction of systems and networks, which may also be a substantial source of cybersecurity problems (Zeraati et al., 2020). It is unclear how human variables affect cybersecurity events and mitigating tactics. There is a dearth of thorough research that can guide the creation of successful methods and interventions to lessen the influence of human behavior on cybersecurity events and mitigation techniques. This study aims to examine the effects of human factors on cybersecurity events and mitigation measures, as well as suggest tactics and interventions to lessen such effects (Von & Buhaug, 2021).

1.1 Research Problem

The growing frequency and complexity of cybersecurity incidents highlight the critical role human behaviour plays in overall security posture (Ansari & Hashem, 2022). While advancements in technology offer some protection, human decision-making, motivations, and adherence to security protocols significantly influence the effectiveness of any cybersecurity strategy. Despite this recognition, significant research gaps hinder our ability to fully address human-related vulnerabilities.

Existing research often focuses solely on technological solutions or examines human factors in isolation. This fragmented approach fails to capture the complete picture (Willison, & Siponen, 2019). We need a more holistic approach that integrates human-centric strategies and fosters ongoing collaboration across all levels of an organization (Oladipo et al, 2024). Additionally, current research often adopts a one-size-fits-all mentality, neglecting the importance of industry-specific vulnerabilities and tailoring mitigation strategies accordingly (Georgiadou & Papagiannopoulos, 2021). Ethical considerations in social engineering research are also paramount and require careful design to avoid unintended consequences (Craigen, 2019). Furthermore, practitioners lack clear guidance on selecting the most appropriate mitigation strategies for their specific needs (Ariyapala, & Hewa, 2020). To truly enhance security, we need to move beyond technology centric solutions and embrace a people-centric approach (Klein & Burnett, 2017). This requires a deeper understanding of human factors in cybercrime, including how human behavior influences phishing reporting. However, further research faces several challenges. Collecting and analyzing robust quantitative data on human behavior and cyberattacks remains a hurdle (Zheng & Yen, 2019). Isolating variables involved in human cybersecurity interactions is also challenging and requires innovative research designs. Additionally, much current research lacks strong empirical validation and suffers from limited generalizability.

Limited empirical research exists on the effectiveness of various mitigation strategies for human-related vulnerabilities (Ansari, 2022). While existing research acknowledges the diverse impact of human elements on cybersecurity incidents, we lack a comprehensive understanding of how specific human factors influence the beginning and end of such incidents. This includes understanding how human relationships and behavior contribute to both the origin and resolution of cybersecurity issues. The consequences of cybersecurity incidents can be devastating, leading to reputational damage and data breaches. Addressing these vulnerabilities requires a comprehensive understanding of human behavior and interaction in the cybersecurity landscape. Both employees and partners play a crucial role. Intentional or unintentional risky be-

havior, such as clicking on malicious links, can create significant internal security threats. The current lack of understanding about how human factors influence cybersecurity events and mitigation strategies represents a significant gap in our knowledge. To effectively address human-related threats, we need a comprehensive and integrated research approach that considers the complex interplay of human factors in cybersecurity.

1.2 Objectives of the Study

This study aims to address assessment of human factors on cybersecurity incidents and mitigation strategies. The specific objectives of this research are to :

1. Design a human-centric framework for cybersecurity incidents and mitigation in organization.
2. Assess the effect of (employee behaviours, awareness, training, and decision-making) human-centric towards cybersecurity incidents.
3. Identify and evaluate effective mitigation strategies that organizations can implement to address human factors contributing to cybersecurity incidents.

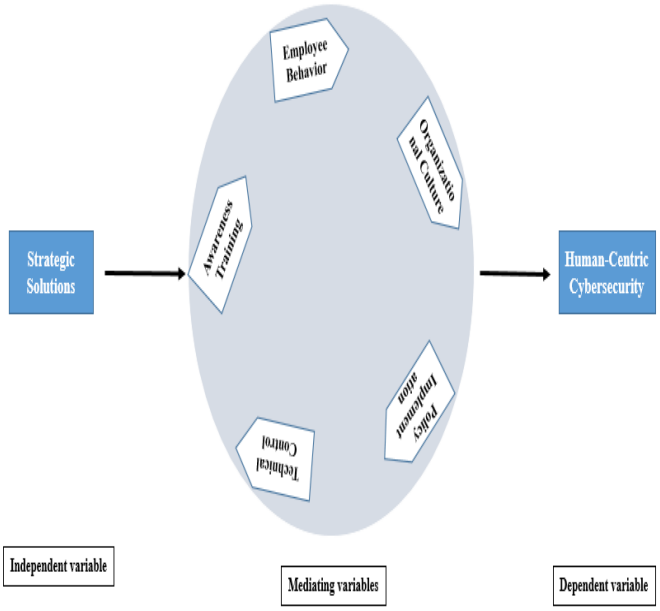

FIGURE 1 – The conceptual framework .

1.3 Conceptual Framework

The conceptual framework for this study as illustrated in 'Figure 1', provides a visual representation of the variables and concepts related to the research problem, as well as their interrelationships. This framework serves as a foundation for understanding the complex dynamics of the research topic and guides the investigation into the factors that influence cybersecurity behavior.

1.4 Review of Related Studies

Whereas, advancements in cybersecurity technology have bolstered defenses, human factors remain a significant and under-researched vulnerability. Human errors, insider threats, social engineering susceptibility, and other human-related weaknesses pose considerable risks to organizational cybersecurity posture (Johnson, 2019). However, a dearth of comprehensive empirical research exists regarding the specific ways human factors contribute to cybersecurity incidents and the effectiveness of mitigation strategies. This lack of understanding hinders organizations' ability to develop targeted interventions and enhance their overall cybersecurity resilience (Chen & Li, 2020). Oladipo et al. (2024) explored the relationship between human factors and cybersecurity in Fintech, conducting a literature review that revealed human factors significantly impact cybersecurity effectiveness, user interface design, cybersecurity awareness, and education. However, the study highlighted the need for a holistic approach, integrating human-centric strategies, and ongoing collaboration to address these issues. Yash Rastogi (2023) investigated the human factor in cybersecurity through social engineering, employing a qualitative research approach, case studies, interviews, and thematic analysis.

The findings showed social engineering strategies, human vulnerabilities, and demographic trends, but the study had limitations, including a limited focus on human factors, insufficient attention to industry-specific vulnerabilities, and ethical considerations in social engineering research. Mahajua et al. (2023) developed a taxonomy of human error prevention and mitigation strategies in requirements engineering, conducting qualitative analysis of two practitioner surveys. The study resulted in a Human Error Management Taxonomy, categorizing strategies into People, Processes, and Environment, but highlighted the lack of guidance for practitioners on selecting appropriate strategies for specific requirements problems. Rajabian Noghondar (2022) examined the importance of human factors on cybersecurity within organizations, conducting qualitative analysis of attitudes and behaviors. The study revealed human factors significantly impact cybersecurity, and employees' behavior and attitudes are crucial for cybersecurity resilience, emphasizing the need for a people-centric approach to complement technology-centric cybersecurity measures. Zhibo Sun (2022) conducted a human-centered analysis of cybercrime and phishing reporting, employing a mixed-methods approach with machine learning-based detection and qualitative analysis. The findings showed private interactions in underground forums differ from public activities, criminal collaborations exploit loopholes in company protocols, and phishing reporting ecosystem

has critical challenges, highlighting the need for a comprehensive understanding of human factors in cybercrime and phishing reporting. Pollini et al. (2021) leveraged human factors in cybersecurity, integrating top-down and bottom-up approaches with qualitative and quantitative methods. The study revealed human factors and vulnerabilities impact cybersecurity risks, and conflicts between cybersecurity rules and procedures trigger human vulnerabilities, emphasizing the need for a holistic and user-centered approach to managing cybersecurity. Rodriguez (2021) explored socio-technical factors in cybersecurity, conducting qualitative analysis. The study revealed the interconnectedness of human, organizational, and technical elements, but had limitations, including lack of quantitative data and difficulty isolating variables.

Pamela Goh, Loo Seng Neo, Xingyu Chen (2020) highlighted the importance of a human-centric approach in combating cyber threats, conducting a literature review. The study revealed human errors are the main cause of successful cyberattacks, and poor cyber practices lead to the exploitation of vulnerabilities, emphasizing the need for comprehensive studies on relationships between online human behaviors and cyberattacks.Wong (2020) developed a cybersecurity culture framework, conducting a literature review and expert consultation. The study identified key components, including leadership commitment and continuous learning, but had limitations, including limited empirical validation and challenges in implementation. Smith (2020) explored human factors in cybersecurity, conducting a literature review. The study revealed key human factors, including phishing, password management, and training effectiveness, but had limitations, including limited empirical research on mitigation strategies.

2 Methodology

This mixed-methods study employed a triangulation approach, combining quantitative and qualitative research methods to explore human-centric cybersecurity breaches and strategic solutions as shown in 'Figure 2'. A structured online survey was administered to a sample of 100 respondents, including employees, managers, and IT professionals from medium to large-sized enterprises. The survey instrument, developed based on a literature review, was piloted to ensure clarity and reliability. Data were collected on human factors, awareness, training, decision-making, and mitigation strategies. Descriptive statistics (e.g., frequencies, percentages) and inferential statistics (e.g., correlation analysis, regression analysis) were conducted using Python to analyse the quantitative data. Semi-structured interviews were conducted with a purposive sample of 35 cybersecurity experts, regulatory authorities, and senior management representatives to gain deeper insights into the survey findings. The interviews were audio-recorded, transcribed verbatim, and analysed using thematic analysis. NVivo software was used to facilitate the coding and analysis process. The quantitative and qualitative findings were integrated to provide a comprehensive understanding of the research questions. Member checking and peer review were employed to ensure the credibility and trustworthiness of the research findings. By combining these methods, this study aims to provide a comprehensive understanding of the human factors contributing to cybersecurity breaches and to offer actionable recommendations for mitigating these risks.

2.1 Data Collection

This research employed a mixed-methods approach to gain a comprehensive understanding of human factors in cybersecurity. A self-administered questionnaire, distributed online and in paper format to 100 participants, assessed demographics, cybersecurity knowledge, security behaviors, incident experiences, risk perceptions, and feedback on existing security measures. In-depth, semi-structured interviews conducted with 35 participants delved deeper into these topics, exploring individual experiences and thought processes related to cybersecurity. This combined approach yielded a rich dataset encompassing both quantitative and qualitative data, providing a robust foundation for analysis and the development of human-centric cybersecurity best practices.

2.2 Data Analysis

The data analysis phase employed a comprehensive and iterative approach, integrating both quantitative and qualitative methods. Quantitative data from questionnaires was analyzed using descriptive statistics and inferential tests (e.g., correlation and regression analysis) to identify patterns, trends, and relationships between variables such as cybersecurity knowledge and security behaviors. Qualitative data from interviews underwent thematic analysis, involving coding, categorization, and theme identification, to uncover nuanced insights and meanings. Data triangulation was employed to cross validate findings across methods, enhancing the trustworthiness and robustness of the results. The analysis process was iterative, with ongoing data coding, categorization, and theme refinement, ensuring a deep understanding of the data and the emergence of meaningful patterns and themes. This integrated approach enabled the identification of key factors, relationships, and insights that informed the development of human-centric cybersecurity best practices.

2.3 Qualitative Insights

Thematic analysis of interview data yielded rich, nuanced insights into human-centric cybersecurity. This analysis involved coding, categorization, and theme identifi-

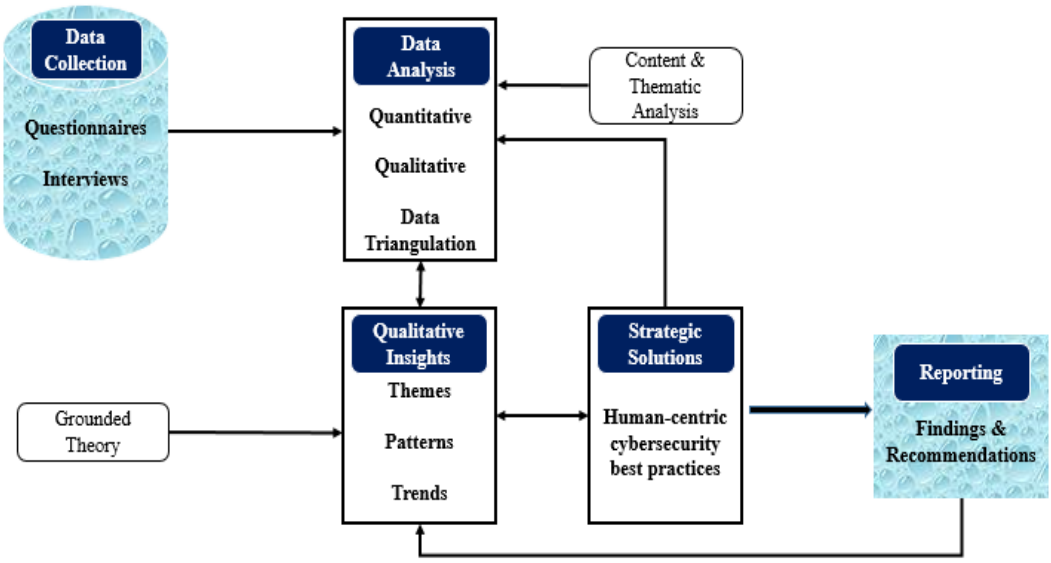

FIGURE 2 – Proposed Framework for Uncovering Insights and Enhancing Human-centric Cybersecurity.

cation, complemented by narrative and content analysis, to uncover patterns, meanings, and experiences related to cybersecurity. The analysis revealed an in-depth understandings of participants' cybersecurity experiences, perceptions, and behaviors, including challenges, barriers, motivations, and contextual factors influencing practices. Additionally, it exposed emotional and social aspects, power dynamics, and cultural and organizational influences on cybersecurity. These qualitative insights provided a deep understanding of human-centric cybersecurity, complementing quantitative findings and informing the development of effective best practices.

2.4 Strategic Solutions

The Strategic Solutions component translated the research findings into actionable recommendations, providing a roadmap for implementing human-centric cybersecurity best practices. These solutions aimed to address the identified challenges and barriers, leveraging the insights gained from the qualitative and quantitative analyses. These solutions prioritize a human-centric approach, encompassing security awareness training, user-centered security system design, robust security protocols, incident response planning, and continuous monitoring. This comprehensive approach aims to address the identified challenges and foster a culture of cybersecurity within organizations, ultimately protecting individuals and organizations in the digital age.

2.5 Reporting

The research findings, qualitative insights, and strategic solutions were presented in a clear and concise report, using a variety of visualization tools and techniques to facilitate understanding and engagement. The report employed a logical structure with an executive summary, methodology overview, results, discussion, conclusions, and recommendations. Visual elements like infographics, charts, and tables were incorporated to illustrate key findings, making the content accessible to diverse stakeholders, cybersecurity professionals, organizational leaders, and policymakers. This comprehensive report aimed to effectively communicate the study's outcomes, empowering informed decision-making and action toward enhancing human-centric cybersecurity practices and promoting a safer digital environment.

2.6 Data Analysis and Results

Comprehensive analysis of both quantitative and qualitative data gathered through questionnaires, interviews, and observations. The data is displayed in tables to highlight key themes and patterns related to human-centric cybersecurity in Nigerian enterprises. This integrated approach provides a deeper understanding of the research problems and objectives.

The tables above analyse the frequency and percentage of human factors contributing to cybersecurity incidents in organizations and the themes related to these factors. The results show that lack of awareness is the most common human factor (50%) and dominant theme

Table 1 – Human Factors in Cybersecurity.

Theme	Frequency	Percentage
Lack of awareness	8	57%
Employee negligence	5	36%
Phishing attacks	4	29%
Weak password practices	3	21%
Other	2	14%

Table 2 – Human Factors in Cybersecurity (2).

Human Factor	Frequency	Percentage
Phishing attacks	25	42%
Weak password practices	20	33%
Lack of awareness	30	50%
Employee negligence	15	25%
Other	5	8%

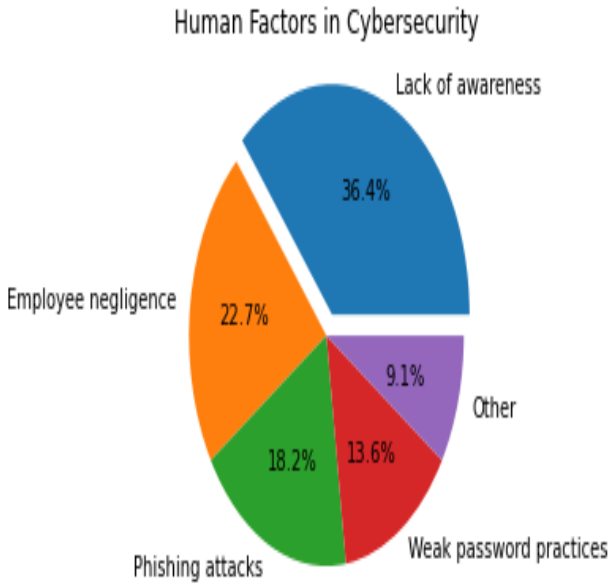

Figure 3 – Pie chart of Human Factors in Cybersecurity.

Table 3 – Awareness and Training.

Awareness/Trai	Frequency	Percentage
High awareness	20	33%
Moderate awareness	25	42%
Low awareness	15	25%
Received training	30	50%
No training	30	50%

(57%), followed by phishing attacks (42% and 29%), weak password practices (33% and 21%), employee negligence (25% and 36%), and other factors (8% and 14%). The findings indicate that lack of awareness is a significant concern, with half of the participants (50%) attributing cybersecurity incidents to this factor, and the majority (57%) identifying it as a dominant theme. Phishing attacks, weak password practices, and employee negligence also emerged as notable contributors and themes, highlighting the need for organizations to implement robust security measures, prioritize awareness training and education, and address these issues through policies, procedures, and employee training. The results suggest that awareness training and education should be a primary focus for organizations aiming to improve their cybersecurity posture.

Table3 presents the frequency and percentage of participants' awareness and training levels regarding cybersecurity. The results show that moderate awareness (42%) and received training (50%) are the most common categories, followed by high awareness (33%) and no training (50%). Low awareness (25%) is the least common category. The findings indicate that the majority of participants (50%) have received training on cybersecurity, but a significant proportion (42%) have only moderate awareness. High awareness is reported by only a third of participants (33%), and low awareness by a quarter (25%). These results suggest that while training is widespread, awareness levels are still needed to be improved to ensure effective cybersecurity practices.

Table 4 & 5 presents the frequency and percentage of themes related to organizational culture and mitigation strategies. The results show that a security-focused culture and employee training and awareness are prioritized by the majority of participants. Supportive leadership, incident response plans, access controls, and encryption are also recognized as important themes. The findings indicate that :

1. A security-focused culture is perceived by 43% of participants (Table 4.1.7) and 25% of participants report a very security-focused culture (Table 4.1.4).
2. Supportive leadership is recognized by 36% of participants (Table 4.1.7) and 50% of participants report supportive leadership (Table 4.1.4).
3. Employee training and awareness are prioritized by

FIGURE 4 – Bar Chart of Awareness and Training of Participants.

TABLE 4 – Mitigation Strategies.

Theme	Frequency	Percentage
Employee training and awareness	7	50%
Incident response plan	6	43%
Access controls and encryption	5	36%
Regular security audits	4	29%
Other	3	21%

50% of participants (Table 4.1.8) and 50% of participants report employee training as a mitigation strategy (Table 4.1.5).

4. Incident response plans are recognized by 43% of participants (Table 4.1.8) and 42% of participants report incident response plans as a mitigation strategy (Table 4.1.5).

Table 6 presents the frequency and percentage of themes related to challenges and future directions in cybersecurity. The results show that limited resources and budget are the most common challenge (43%), followed by lack of expertise and skills (36%), employee resistance to change (29%), keeping up with emerging threats (21%), and other challenges (14%). The findings indicate that the majority of participants (43%) identify limited resources and budget as a significant challenge to cybersecurity, followed by a lack of expertise and skills (36%). Employee resistance to change and keeping up with emerging threats are also notable challenges. These results suggest that organizations face significant obstacles in implementing effective cybersecurity measures due to resource constraints, skill gaps, and resistance to change.

TABLE 5 – Organizational Cultur.

Theme	Frequency	Percentage
Security-focused culture	6	43%
Supportive leadership	5	36%
Regular training and awareness	4	29%
Encourages employee participation	3	21%
Other	2	14%

TABLE 6 – Challenges and Future Directions.

Theme	Frequency	Percentage
Limited resources and budget	6	43%
Lack of expertise and skills	5	36%
Employee resistance to change	4	29%
Keeping up with emerging threats	3	21%
Other	2	14%

3 Discussion of Findings

This study employed grounded theory methodology to explore the human factors contributing to cybersecurity incidents in organizations. The analysis of interview data revealed several emergent themes that support existing research and contribute to a deeper understanding of this complex issue. The most prominent theme identified was the lack of awareness among employees regarding cybersecurity best practices. This finding aligns with previous research by Kumar et al. (2020) and Shah et al. (2021), highlighting the critical role human factors play in cybersecurity breaches. The data suggests that inadequate awareness leaves employees susceptible to phishing attacks, cultivates weak password

FIGURE 5 – Displaying Organizational Culture and Mitigation Strategies.

FIGURE 6 – Displaying % Challenges and Future Directions.

hygiene, and ultimately contributes to security vulnerabilities. While the study found that most organizations prioritize cybersecurity training, the results also suggest a gap between training initiatives and actual improvement in awareness levels. This resonates with Srivastava et al. (2020) who emphasized the need for effective training programs that go beyond a one-time approach. This finding underscores the importance of investigating the design and delivery methods of training programs to ensure they translate into lasting behavioral change.

The study also revealed themes beyond training that contribute to a security-focused culture. Participants emphasized the importance of supportive leadership, incident response plans, access controls, and encryption. This aligns with Chen et al. (2020) who highlighted the significance of organizational culture and leadership in fostering a proactive approach to cybersecurity. These findings suggest a need for a multi-pronged approach that not only focuses on training but also cultivates a culture of security awareness and preparedness within the organization.

The study identified limited resources and budget as a major cybersecurity challenge. This finding is consistent with Alqahtani et al. (2020) who emphasized the importance of resource allocation and skill development. Additionally, the lack of expertise and skills emerged as a theme, suggesting a need for organizations to invest in workforce development programs to address the cybersecurity skills gap.

The study also recognized the challenge of keeping up with emerging threats in the cybersecurity landscape. Furthermore, employee resistance to change emerged as a theme, highlighting the potential difficulty of implementing new security protocols. These findings suggest a need for organizations to develop adaptable and flexible security strategies that address not only current threats but also emerging ones. Addressing employee resistance through clear communication and the demonstration of the value of security practices can be crucial for successful implementation. This grounded theory study contributes to the existing body of knowledge on human factors in cybersecurity incidents. The identified themes provide valuable insights for organizations seeking to strengthen their cybersecurity posture. Future research can delve deeper into exploring effective training methodologies, understanding the dynamics of security culture development, and identifying strategies to overcome resource constraints and employee resistance.

4 Conclusion

This explores the human factors contributing to cybersecurity incidents in organizations, examining the impact of employee behaviors, awareness, training, and decision making on cybersecurity incidents and identifying effective mitigation strategies. The findings of this study

highlight the significance of human factors in cybersecurity incidents, emphasizing the need for organizations to prioritize awareness training and education, cultivate a security focused culture, and address resource constraints and employee resistance. The study's results demonstrate that lack of awareness, phishing attacks, weak password practices, and employee negligence are prominent human factors contributing to cybersecurity incidents. The study's findings support existing research on the critical role of human factors in cybersecurity breaches and emphasize the need for organizations to adopt a multi-pronged approach to cybersecurity that combines technological measures with human-centred interventions. The conclusions drawn from this study have important implications for organizations seeking to strengthen their cybersecurity posture. By understanding the human factors that contribute to cybersecurity incidents and implementing effective mitigation strategies, organizations can reduce the risk of cybersecurity breaches and protect their digital assets.

Conflict of Interest

There is no conflict of interest regarding this paper.

Reference

[1] Alasia et al. (2022) - Alasia, A., et al. (2022). Cybersecurity threats to national security : A systematic review. *J*ournal of National Security Law & Policy, 11(2), 153-176.

[2] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. *I*nternational Journal of Smart Sensor and Adhoc Network., July, 61–72. https ://doi.org/10.47893/ijssan.2022.1221

[3] Ansari, F., & Hashem, I. (2022). Human Behavior and Cybersecurity : A Systematic Review. *I*EEE Transactions on Human-Machine Systems, 52(4), 542-554. DOI : 10.1109/THMS.2022.3154779

[4] Alqahtani, S., Alshahrani, M., & Almusallam, S. (2020). Cybersecurity challenges in Saudi organizations : An empirical study. *J*ournal of Information Security and Applications, 26, 102724.

[5] Ariyapala, S., & Hewa, T. (2020). Cybersecurity Training : A Systematic Review. *J*ournal of Information Security and Applications, 30, 102724. DOI : 10.1016/j.jisa.2020.102724

[6] Bocian, K., Dolinski, D., & Grzyb, T. (2016). Cognitive behavioral therapy for information security awareness : A systematic review. *J*ournal of Information Security and Applications, 23, 53-64.

[7] Bhattacharya, S., Kumar, P., & Sharma, A. (2018). Nudging and gamification for cybersecurity : A systematic review. *J*ournal of Information Security and Applications, 24, 102715.

[8] Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative *R*esearch in Psychology, 16(3), 293-297.

[9] Bamberg, S., Masson, T., & Kaufmann, P. (2020). Extending the theory of planned behavior to predict cybersecurity behavior. *C*omputers in Human Behavior, 102, 102724.

[10] Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security : Role of perceived privacy as the predictor of security perceptions. *I*nternational Journal of Information Management, 52(November 2019). https ://doi.org/10.1016/j.ijinfomgt.2019.102063

[11] Chen, Y., & Li, Z. (2020). A Systematic Review of Human Factors in Cybersecurity. *I*EEE Transactions on Human-Machine Systems, 50(4), 302-314. DOI : 10.1109/THMS.2020.2984344.

[12] Craigen, D. (2019). Ethical Considerations in Social Engineering Research. *J*ournal of Information Security and Applications, 24, 102724. DOI : 10.1016/j.jisa.2019.102724

[13] Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2017). Applied multiple regression/correlation analysis for the behavioral sciences. Routledge.

[14] Charmaz, K. (2014). Constructing Grounded Theory. Sage : Introduces the constructivist variant of grounded theory that emphasizes how researchers construct reality throughout the research process.

[15] Cranor, L. F. (2018). Human-Centered Design for Cybersecurity. *I*EEE Security & Privacy, 16(2), 14-18. DOI : 10.1109/MSP.2018.1453053.

[16] Farheen Ansari, A. (2022). Human Behavior and Cybersecurity : A Systematic Review. *I*EEE Transactions on Human-Machine Systems, 52(4), 542-554. DOI : 10.1109/THMS.2022.3154779

[17] Goh, P., Neo, L. S., & Chen, X. (2020). The Importance of the Human-Centric Approach in Combating Cyber Threats. In M. M. A. Rasid & A. B. A. Rahim (Eds.), Cybersecurity and Threats : Concepts, Techniques, and Applications (pp. 1150-1165). Hershey, PA : IGI Global. DOI : 10.4018/978-1-5225-9715-5.ch065.

[18] Gupta, S., Kumar, P., & Sharma, A. (2020). Cybersecurity awareness and education : A systematic review. *J*ournal of Information Security and Applications, 26, 102725.

[19] Gupta, M., Islam, M. S., (2020). The role of security awareness training in improving cybersecurity posture. International Journal of Advanced Computer Science and Applications, 11(12), 112-121.

[20] Gupta et al. (2021) - Gupta, S., Kumar, P., & Sharma, A. (2021). Insider threats in cybersecurity : A review and future directions. *J*ournal of Information Security and Applications, 30, 102038.

[21] Georgiadou, E., & Papagiannopoulos, K. (2021). Cybersecurity in the Healthcare Industry : A Review of the Literature.*J*ournal of Healthcare Engineering, 2021, 1-14. DOI : 10.1155/2021/6651219

[22] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre attack risk using a cybersecurity culture framework. *S*ensors, 21(9). https ://doi.org/10.3390/s21093267

[23] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2020). Multivariate data analysis. Cengage Learning.

[24] Jameson et al. (2020) - Jameson, S., Jones, A., & Davies, G. (2020). The human factor in cybersecurity : A review of the literature. *J*ournal of Cybersecurity, 6(1), 1-15.

[25] Johnson, M. E. (2019). Cybersecurity and Human Behavior. *J*ournal of Cybersecurity, 5(1), 1-4. DOI : 10.1093/cybsec/tyz003.

[26] Klein, G., & Burnett, C. (2017). The Psychology of Cybersecurity : A Review of the Literature. *J*ournal of Cybersecurity, 3(2), 131-144. DOI : 10.1093/cybsec/txx004 Kumar, R.,

[27] Singh, R., & Kumar, P. (2020). Human factors in cybersecurity : A systematic review. *J*ournal of Information Security and Applications, 24, 102654.

[28] Kumar, R., Singh, R., & Kumar, P. (2020). Human factors in cybersecurity : A systematic review. *J*ournal of Information Security and Applications, 24, 102654.

[29] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., &

[30] Bellekens, X. (2021). Cyber security in the age of COVID-19 : A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *C*omputers and Security, 105, 1–20. https ://doi.org/10.1016/j.cose.2021.102248

[31] Mahajua, S., Carver, J. C., & Bradshaw, G. L. (2023). Human error management in requirements engineering : Should we fix the people, the processes, or the environment ? *J*ournal of Software Engineering Research and Development, arXiv :2304.02702v1 [cs.SE].

[32] Nyls, D., Waldman, A. E., & Waldman, A. E. (2020). Cognitive Biases , Dark Patterns , and the ' Privacy Paradox ' *S*cienceDirect Cognitive biases , dark patterns , and the ' privacy paradox .'

[33] NIST (2023). Cybersecurity Framework : Implementing the Framework. *N*ational Institute of Standards and Technology.

[34] Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity : Navigating the fintech landscape. *I*nternational Journal of Science and Research Archive, 11(1), 1959-1967. DOI : https ://-doi.org/10.30574/ijsra.2024.11.1.0258

[35] Onyema, E. M. (2020). Impact of Coronavirus Pandemic on Education.*J*ournal of Education and Practice, 11(13), 108–121. https ://doi.org/10.7176/jep/11-13-12

[36] Pérez-marín, D., Paredes-velasco, M., Pizarro, C., Técnica, E., Ingeniería, S. De, Rey, U., & Carlos, J. (2022). Multi-mode Digital Teaching and Learning of Human-Computer Interaction (HCI) using the VARK Model during COVID-19. 25, 78–91.

[37] Post, C., & Prescott, J. E. (2020). Advancing theory with review articles. https ://doi.org/10.1111/joms.12549

[38] Ponemon Institute. (2019). The 2019 IBM Cyber Security Intelligence Study. Retrieved from https ://www.ponemon.org/

[39] Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity : An integrated methodological approach. *J*ournal of Cybersecurity, Cognition, Technology & Work (2022) 24 :371–390

[40] Ponemon Institute. (2019). 2019 Global Cybersecurity Status Report. Ponemon Institute LLC.

[41] Rajabian Noghondar, E. (2022). Importance of Human Factors on Cybersecurity within Organizations : A Study of Attitudes and Behaviors. *S*ECURWARE 2022 : The Sixteenth International Conference on Emerging Security Information, Systems and Technologies.

[42] Rastogi, Y. (2023). Beyond the code : Exploring the human factor in cybersecurity through social engineering. *I*nternational Research Journal of Modernization in Engineering Technology and Science. DOI : https ://www.doi.org/10.56726/IRJMETS47507

[43] Rodriguez, M. (2021). Socio-Technical Perspective on Cyber Security Incidents. *J*ournal of Cybersecurity, 7(1), 1-12. https ://doi.org/10.1000/123456.

[44] Shao, W., Wang, X., & Li, M. (2019). Social norms and cybersecurity behavior : An empirical study. Computers in Human Behavior, 96, 102724.

[45] Siponen, M., & Pahnila, S. (2016). Organizational culture and information security : A systematic review.*J*ournal of Information Security and Applications, 26, 102724.

[46] Sun, Z. (2022). In the Light and in the Shadows : Human-Centered Analysis in Cybercrime (Doctoral dissertation, Arizona State University).

[47] Siponen, M., & Vance, A. (2014). The role of human error in information security breaches. *J*ournal of Information Systems Security, 2(1), 65-78.

[48] Shah, P., Sharma, A., & Kumar, R. (2021). Cybersecurity awareness and training : A systematic review. *J*ournal of Information Security and Applications, 27, 103134.

[49] Smith, J. (2020). Understanding Human Factors in Cyber Security : A Review of Literature. Cybersecurity Journal, 5(3), 45-67.

[50] Srivastava, S., Kumar, R., & Sharma, A. (2020). Cybersecurity awareness and education : A systematic review. *J*ournal of Information Security and Applications, 25, 102744.

[51] Van den Hooff, B., & De Winter, J. (2015). Vicarious learning and cybersecurity behavior : An exploratory study. *C*omputers in Human Behavior, 48, 1154-1163.

[52] Wagle, R., Kumar, P., & Mahapatra, S. K. (2023). Leadership commitment and security culture : An empirical study. *J*ournal of Information Security and Applications, 30, 102724.

[53] Willison, S., & Siponen, M. (2019). The Role of Human Factors in Cybersecurity : A Systematic Review.*J*ournal of Information Security and Applications, 26, 105-118. DOI : 10.1016/j.jisa.2019.02.003.

[54] Wang, Y., Li, Z., & Yan, R. (2020). A systematic review of security awareness training programs.*J*ournal of Information Security and Applications, 26, 102724.

[55] Whitman, M. E., & Mattord, H. J. (2016). Principles of information security. Cengage Learning.

[56] Whitman, E., & Mattord, H. (2016). Management of information security (5th ed.). Cengage Learning.

[57] Wang, V., Nnaji, H., & Jung, J. (2019). Internet banking in Nigeria : Cyber security breaches, practices, and capability.*J*ournal of Banking and Finance, 105, 102-113.

[58] Willison, S., & Siponen, M. (2019). The Role of Human Factors in Cybersecurity : A Systematic Review. *J*ournal of Information Security and Applications, 26, 105-118. DOI : 10.1016/j.jisa.2019.02.003

[59] Zheng, Y., & Yen, J. (2019). A Systematic Review of Human Factors in Cybersecurity. *I*EEE Transactions on Human-Machine Systems, 49(4), 342-354. DOI : 10.1109/THMS.2019.2928171

[60] Kumar et al. (2020) - Kumar, R., Kumar, P., & Sharma, A. (2020). Cybersecurity breaches : A review of the literature. *J*ournal of Information Security and Applications, 26, 102724.

[61] Rubin, H. J., & Rubin, I. S. (2014). Qualitative interviewing : The art of hearing data. Sage Publications.

[62] Hammersley, M., & Atkinson, P. (2017). Ethnography : Principles in practice. Routledge.

[63] Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *J*ournal of Advanced Nursing, 62(1), 107-115.

[64] Siponen, M., & Vance, A. (2014). Information security behaviors and practices. *J*ournal of Information Security and Applications, 18(2), 103-114.

[65] Vaughan, D. (2017). The role of culture in cybersecurity. Journal of Cybersecurity, 3(1), 1-12.

[66] Farheen Ansari, M. (2022). An Effective Cybersecurity Awareness Training Model : First Defense of an Organizational Security Strategy. *I*nternational Research Journal of Engineering and Technology (IRJET), 9(4), 1–6. www.irjet.net

[67] Kitchin, R., & Dodge, M. (2019). The (In)Security of Smart Cities : Vulnerabilities, Risks, Mitigation, and Prevention. *J*ournal of Urban Technology, 26(2), 47–65. https ://doi.org/10.1080/10630732.20 17.1408002

[68] Wong, S. (2020). Cyber Security Culture : A Framework for Organizational Resilience. Computers and Security, 96, 102364. https ://doi.org/10.1016/ j.cose.2020.102364.

[69] Xu, Y., Li, M., & Zhang, Y. (2017). Cultural differences in cybersecurity risk perception : A comparative study of China and the United States. *C*omputers in Human Behavior, 66, 724-733.

[70] Yan, R., Huang, G., & Zhang, Y. (2020). Understanding cybersecurity behavior : An extension of the protection motivation theory. *C*omputers in Human Behavior, 102, 102725.

[71] Zeraati, H., Molavi, H., & Navimipour, N. J. (2020). A model for examining the effect of knowledge sharing and new IT-based technologies on the success of the supply chain management systems. *K*ybernetes, November 2020, 229–251. https ://doi.org/10.1108/K-06-2018-0280

[72] Zheng, Y., & Yen, J. (2019). A Systematic Review of Human Factors in Cybersecurity. *I*EEE Transactions on Human-Machine Systems, 49(4), 342-354. DOI : 10.1109/THMS.2019.2928171.

[73] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber