JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

The Human Factor in Cybersecurity: Addressing the Risks of Insider Threats

Hewa Majeed Zangana[1*], Zina Bibo Sallow [2], Marwan Omar [3]
[1] IT Dept., Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq
[2] Computer System Department, Ararat Technical Private Institute, Kurdistan Region - Iraq
[3] Illinois Institute of Technology
[1*] hewa.zangana@dpu.edu.krd

Keywords:
Cybersecurity; Human Factors; Insider Threats; Organizational Culture; Training and Awareness

Abstract

In the rapidly evolving landscape of cybersecurity, the human element remains one of the most critical and complex factors to manage. Insider threats, whether originating from malicious intent or inadvertent actions, pose significant risks to organizational security. This paper explores the multifaceted nature of insider threats, examining the motivations and behaviors that drive individuals to compromise systems. By analyzing case studies and current research, we identify key vulnerabilities and the role of organizational culture in mitigating these risks. Furthermore, we propose comprehensive strategies for detecting, preventing, and responding to insider threats, emphasizing the importance of continuous education, robust access controls, and advanced monitoring technologies. This paper aims to provide a holistic understanding of the human factor in cybersecurity and offers practical solutions to address the pervasive challenge of insider threats.

1.INTRODUCTION

In the contemporary digital age, cybersecurity has emerged as a paramount concern for organizations worldwide. While technological advancements have fortified defenses against external threats, the human element within organizations continues to present a significant vulnerability. Insider threats—security risks posed by individuals within the organization—can be especially pernicious due to their access to sensitive information and systems. These threats can stem from both malicious intent and unintentional actions, making them complex to address effectively.

Research highlights that insider threats account for a substantial proportion of security incidents, emphasizing the need for a nuanced understanding and comprehensive strategies to mitigate these risks [1], [2]. The motivations behind insider threats are varied, including financial gain, personal grievances, and coercion, while unintentional threats often arise from human errors, lack of awareness, and inadequate training [3], [4].

The challenge of addressing insider threats is further complicated by the dynamic and multifaceted nature of human behavior. Studies indicate that a combination of psychological, social, and organizational factors influence insider actions, necessitating a holistic approach to cybersecurity that incorporates human factors [5], [6]. For instance, organizational culture, employee engagement, and stress levels significantly impact the likelihood of insider threats, highlighting the need for organizations to foster a security-conscious culture [7], [8].

This paper aims to explore the human factors contributing to insider threats and propose strategies to mitigate these risks. By examining case studies and current research, we identify key vulnerabilities and the role of organizational culture in addressing insider threats. We also discuss the importance of

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

continuous education, robust access controls, and advanced monitoring technologies in creating a resilient cybersecurity posture [9], [10].

Understanding and mitigating insider threats require a multidisciplinary approach that integrates insights from psychology, sociology, and cybersecurity. By leveraging a comprehensive framework, organizations can better detect, prevent, and respond to insider threats, thereby enhancing their overall security and resilience [11], [12].

This study seeks to explore the human factors contributing to insider threats in cybersecurity, focusing on the motivations and behaviors that increase organizational risks. It aims to evaluate the critical role of organizational culture in mitigating such threats, with an emphasis on fostering security awareness and employee engagement. Additionally, the research intends to develop a comprehensive framework for detecting, preventing, and responding to insider threats by combining technological advancements with human-centric strategies. Finally, the proposed framework will be empirically validated to assess its effectiveness in reducing cybersecurity incidents and enhancing organizational resilience.

In the following sections, we delve deeper into the nature of insider threats, examining both intentional and unintentional risks. We then propose a set of best practices and technological solutions designed to address these challenges, drawing on the latest research and practical case studies to illustrate effective strategies for mitigating insider threats in cybersecurity.

2.LITERATURE REVIEW

2.1 Insider Threats in Cybersecurity

Insider threats pose a significant challenge to cybersecurity due to their inherent complexity and the high level of access that insiders often possess. [1] emphasize the need for robust techniques and countermeasures to prevent insider threats, highlighting that these threats can originate from both malicious intent and unintentional actions. Similarly, [9] provide a comprehensive survey on detecting and preventing cyber insider threats, underscoring the importance of advanced monitoring and preventive measures.

2.2 Human Factors Influencing Cybersecurity

Understanding the human factors in cybersecurity is crucial for mitigating insider threats. [13] discuss various human factors that influence cybersecurity, noting that human behavior, organizational culture, and individual differences play pivotal roles. The significance of human factors is further reinforced by [3], who evaluate the cybersecurity capacity of the industrial workforce, pointing out that human errors and lack of awareness are common contributors to security breaches.

2.3 The Role of Organizational Culture

[11] introduce a cyber-security culture framework for detecting insider threats, stressing the role of organizational culture in promoting security awareness and behavior. [5] adopt a socio-technical approach to derive cybersecurity risks from human and organizational factors, illustrating how organizational practices and employee engagement impact cybersecurity.

2.4 Unintentional Insider Threats

Unintentional insider threats, often stemming from human errors, are a significant concern in cybersecurity. [10] address the unintentional insider threat, emphasizing the need for comprehensive education and awareness programs. [14] propose frameworks to understand and counteract unintentional risks, advocating for a human-centric approach to enhance cybersecurity resilience.

2.5 Technological and Methodological Approaches

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

Various technological and methodological approaches have been proposed to mitigate insider threats. [15] model the effects of insider threats on complex systems, suggesting that simulation can be a valuable tool for understanding and mitigating these risks. [6] leverage an integrated methodological approach to human factors in cybersecurity, combining insights from psychology, sociology, and technology to develop effective countermeasures.

2.6 Case Studies and Practical Applications

Case studies provide valuable insights into the real-world application of cybersecurity strategies. [16] examine security threats to critical infrastructure, highlighting the human factor as a key vulnerability. [7] explore the drivers of insider threats through case studies, identifying common patterns and effective mitigation strategies. Similarly, [17] develops an unintentional insider threat assessment framework for healthcare cybersecurity, demonstrating the practical application of theoretical models. [5] provides insights into mitigation strategies for DoD cybersecurity risks posed by insider threats through a phenomenological study.

2.7 Comprehensive Strategies for Mitigation

To address the multifaceted nature of insider threats, comprehensive strategies are essential. [1] advocate for a combination of technological solutions and human-centric approaches. [17] provides a common-sense guide to mitigating insider threats, offering practical recommendations for organizations. These strategies are complemented by [18], who emphasizes the importance of addressing human factors in cybersecurity leadership. [8], [19] highlight the importance of addressing human factors such as stress, burnout, and security fatigue to enhance cybersecurity resilience.

2.8 Techniques and Countermeasures for Insider Threats

Advanced technological solutions have been extensively studied as a means to detect and prevent insider threats. [20] discuss the integration of AI-driven analytics and real-time threat detection systems in their comprehensive review on redefining security with cyber AI. These advanced solutions enhance an organization's ability to identify potential insider threats early and respond promptly, thereby significantly reducing the risk of data breaches and unauthorized access.

2.9 Threats to Specific Systems

In the context of specific threats, smartphone security poses unique challenges due to the high volume of personal and sensitive data they contain. [21] highlight the various threats, attacks, and mitigation strategies related to smartphone security. Their research emphasizes the critical need for robust security measures tailored to mobile devices, which are increasingly becoming targets for insider threats due to their widespread use in both personal and professional settings.

2.10 Human-Centric Approaches to Cybersecurity

A significant shift in cybersecurity research is the movement from viewing humans as the problem to recognizing them as part of the solution. [22] advocate for a 'human-as-solution' mindset in cybersecurity, emphasizing the potential of leveraging human factors to enhance security measures. Their research argues that understanding human behavior and motivations can lead to more effective cybersecurity strategies and foster a culture where individuals are actively involved in protecting organizational assets.

2.11 Influence of Human Factors in Specific Domains

The impact of human factors on cybersecurity varies across different sectors. [23] provide a systematic review of how human factors influence cybersecurity within healthcare organizations. Their

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

study highlights the unique challenges and requirements of the healthcare sector, where human factors such as stress and workload significantly affect security practices and susceptibility to threats. This research underscores the need for tailored approaches to address these specific challenges and improve overall cybersecurity in healthcare settings.

2.12 Future Directions and Challenges

The dynamic nature of cybersecurity necessitates continuous adaptation and innovation. [12] discuss the evolving landscape of social engineering and insider threats, calling for ongoing research and development. [24], [25] advocate for a dynamic systems approach to understanding human factors in cybersecurity, highlighting the need for interdisciplinary collaboration and adaptive strategies.

In summary, the literature underscores the complexity of insider threats and the critical role of human factors in cybersecurity. By integrating insights from various disciplines and adopting a holistic approach, organizations can enhance their resilience against insider threats and safeguard their digital assets.

3.METHOD

This section outlines the methodology used to investigate and address insider threats in cybersecurity, emphasizing the human factor. The approach integrates both qualitative and quantitative methods to provide a comprehensive understanding of the issue and propose effective mitigation strategies.

3.1 Research Design

The research employs a mixed-methods approach, combining quantitative data analysis with qualitative insights to explore the human factors contributing to insider threats in cybersecurity. This approach allows for a holistic understanding of the problem and the development of robust countermeasures.

3.2 Data Collection

Data collection involved two primary sources:

1. **Surveys and Questionnaires**: Surveys were distributed to employees across various industries to gather data on cybersecurity awareness, behaviors, and attitudes. The survey included questions related to:
    - Awareness of cybersecurity policies and procedures
    - Frequency of cybersecurity training
    - Personal experiences with cybersecurity incidents
    - Perceptions of organizational cybersecurity culture
2. **Interviews and Focus Groups**: In-depth interviews and focus groups were conducted with cybersecurity professionals, IT managers, and employees. These sessions aimed to gain deeper insights into:
    - The effectiveness of current cybersecurity measures
    - Challenges faced in implementing cybersecurity protocols
    - Suggestions for improving cybersecurity practices and policies

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

3.3 Sample Population

The study targeted a diverse sample population, including:

- Employees from various sectors (e.g., finance, healthcare, government)
- Cybersecurity professionals and IT managers
- Participants from different organizational levels (e.g., executives, middle management, frontline employees)

The sample size consisted of 300 survey respondents and 30 interview and focus group participants, ensuring a wide range of perspectives and experiences.

3.4 Data Analysis

The data analysis involved the following steps:

1. **Quantitative Analysis**: Survey data were analyzed using statistical methods to identify patterns and correlations. Key metrics included:
    - Frequency of cybersecurity incidents
    - Levels of cybersecurity awareness and training
    - Perceived effectiveness of cybersecurity measures
2. **Qualitative Analysis**: Interview and focus group transcripts were analyzed using thematic analysis. This involved coding the data to identify recurring themes and insights related to human factors and insider threats. The themes were then grouped into broader categories for further analysis.

3.5 Framework Development

Based on the data analysis, a framework for mitigating insider threats was developed. This framework incorporates best practices from the literature and insights gained from the qualitative and quantitative data. The framework consists of the following components:

1. **Awareness and Training Programs**: Regular and comprehensive training sessions to enhance employees' cybersecurity awareness and skills.
2. **Policy and Procedure Enhancement**: Updating and reinforcing cybersecurity policies to address common vulnerabilities and insider threats.
3. **Technological Solutions**: Implementing advanced monitoring and detection tools to identify and mitigate insider threats.
4. **Organizational Culture**: Fostering a cybersecurity-centric organizational culture that promotes vigilance and responsibility among employees.
5. **Continuous Evaluation and Improvement**: Regularly assessing the effectiveness of cybersecurity measures and making necessary adjustments based on feedback and new threats.

3.6 Validation

To validate the proposed framework, a pilot study was conducted within a selected organization. The pilot study involved implementing the framework components and monitoring their impact on

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

cybersecurity incidents and employee behavior over six months. Feedback from participants and incident reports were used to refine the framework further.

3.7 Ethical Considerations

The research adhered to ethical guidelines to ensure the confidentiality and anonymity of participants. Informed consent was obtained from all participants, and data were stored securely to prevent unauthorized access. The study also received approval from the relevant institutional review board.

By employing a comprehensive and multidisciplinary approach, this study aims to provide actionable insights and practical strategies for addressing insider threats in cybersecurity, with a focus on human factors.

4.RESULTS AND DISCUSSION

This section presents the findings from the mixed-methods study, integrating quantitative data from surveys and qualitative insights from interviews and focus groups. The results are discussed in relation to existing literature and the proposed framework for mitigating insider threats.

4.1 Quantitative Results

4.1.1 Survey Findings

The survey data were analyzed to identify key patterns and correlations related to insider threats and human factors in cybersecurity. The main findings are as follows:

1. **Cybersecurity Awareness and Training**:
    - **Awareness Levels**: Approximately 65% of respondents indicated a moderate to high awareness of cybersecurity policies and procedures within their organizations.
    - **Training Frequency**: Only 40% of respondents reported receiving regular cybersecurity training (at least once per year).
    - **Perceived Effectiveness**: 55% of respondents believed that their organization's cybersecurity training programs were effective in raising awareness and improving security practices.
2. **Incidence of Insider Threats**:
    - **Reported Incidents**: 30% of respondents reported experiencing or being aware of at least one insider threat incident in their organization within the past year.
    - **Types of Insider Threats**: The most common types of insider threats reported were unintentional errors (45%), followed by malicious actions (35%) and social engineering attacks (20%).
3. **Organizational Culture and Behavior**:
    - **Supportive Culture**: 60% of respondents felt that their organization promoted a culture of cybersecurity, encouraging employees to report suspicious activities and follow security protocols.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

- **Behavioral Compliance**: Despite high awareness levels, only 50% of respondents consistently adhered to cybersecurity policies and procedures.

4.1.2 Statistical Analysis

A correlation analysis was conducted to explore the relationships between various factors:

- **Training and Awareness**: A strong positive correlation (r = 0.72) was found between the frequency of cybersecurity training and the level of awareness among employees.
- **Awareness and Compliance**: There was a moderate positive correlation (r = 0.58) between awareness levels and behavioral compliance with cybersecurity policies.
- **Organizational Culture and Incident Reduction**: Organizations with a supportive cybersecurity culture reported fewer insider threat incidents, with a negative correlation (r = -0.65) between culture scores and incident reports.

4.2 Qualitative Results

The qualitative data from interviews and focus groups provided deeper insights into the challenges and solutions related to insider threats:

1. **Challenges in Implementing Cybersecurity Measures**:
    - **Resource Constraints**: Many participants highlighted the lack of resources (time, budget, personnel) as a major barrier to effective cybersecurity implementation.
    - **Employee Engagement**: Engaging employees and maintaining their interest in cybersecurity training was a common challenge. Participants suggested that traditional training methods often failed to capture employees' attention.
2. **Effective Practices and Recommendations**:
    - **Interactive Training**: Participants recommended more interactive and engaging training methods, such as simulations and gamification, to improve employee participation and retention of information.
    - **Regular Updates and Communication**: Continuous communication and regular updates about new threats and best practices were deemed crucial for maintaining a high level of cybersecurity awareness.
    - **Leadership Involvement**: The involvement of top management in promoting cybersecurity culture was seen as essential. Leadership commitment to cybersecurity was associated with better compliance and fewer incidents.
3. **Technological Solutions**:
    - **Advanced Monitoring Tools**: The use of advanced monitoring and detection tools, such as AI-driven analytics and real-time threat detection systems, was highlighted as effective in identifying potential insider threats.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

- **Access Controls**: Implementing strict access controls and regular audits of user permissions were recommended to minimize the risk of unauthorized access and data breaches.

4.3 Discussion

The findings from this study align with existing literature on the importance of human factors in cybersecurity. [1] emphasize the need for robust countermeasures against insider threats, which is supported by our findings that highlight the significance of regular training and a supportive organizational culture. The positive correlation between training frequency and awareness levels underscores the importance of continuous education, as noted by [9], [13].

The study also corroborates the insights of [10], who address the challenge of unintentional insider threats. Our findings reveal that unintentional errors are a common type of insider threat, suggesting the need for more engaging and effective training programs to reduce these incidents. [14] advocate for human-centric approaches, which are reflected in the recommendations for interactive training and leadership involvement.

The role of organizational culture, as discussed by [11], is evident in our results, which show that a supportive culture correlates with fewer insider threat incidents. This highlights the importance of fostering a cybersecurity-centric culture, as proposed by [5].

4.4 Framework Validation and Implications

The proposed framework, validated through a pilot study, demonstrates practical applicability in mitigating insider threats. By integrating awareness and training programs, policy enhancements, technological solutions, and fostering a supportive culture, organizations can effectively address both intentional and unintentional insider threats. The framework's success in the pilot study suggests its potential for broader implementation and scalability across different industries.

In summary, this study provides a comprehensive understanding of insider threats and the human factors influencing cybersecurity. The findings underscore the need for continuous education, leadership involvement, and advanced technological solutions to enhance organizational resilience against insider threats. Future research should explore the long-term impact of these strategies and the evolving nature of insider threats in the rapidly changing cybersecurity landscape.

5.CONCLUSION

The study aimed to investigate the human factors contributing to cybersecurity risks, with a specific focus on insider threats, and to develop a comprehensive framework to mitigate these risks. The research findings underscore the critical role that human factors play in the cybersecurity landscape, highlighting both the challenges and effective strategies for addressing insider threats.

One of the key findings is the importance of regular cybersecurity training and awareness programs. The study revealed a strong positive correlation between the frequency of cybersecurity training and the level of awareness among employees. This suggests that continuous education is crucial for maintaining high awareness and compliance with cybersecurity policies. Organizations that invest in regular and interactive training programs are better equipped to mitigate insider threats by ensuring their employees are well-informed and vigilant.

The research also highlighted the significant impact of organizational culture on cybersecurity. A supportive culture that promotes security awareness and encourages employees to report suspicious activities is associated with fewer insider threat incidents. This finding aligns with previous studies emphasizing the need for a cybersecurity-centric culture within organizations. Leadership commitment to cybersecurity plays a pivotal role in fostering such a culture, as it influences employee behavior and compliance with security protocols.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 3, Nomor 2, January 2025, Page 76-85
DOI: https://doi.org/10.58602/jics.v3i2.37

Technological solutions, such as advanced monitoring tools and strict access controls, were identified as effective measures for detecting and preventing insider threats. The integration of AI-driven analytics and real-time threat detection systems enhances an organization's ability to identify potential insider threats early and respond promptly. Regular audits of user permissions and implementing stringent access controls further reduce the risk of unauthorized access and data breaches.

The proposed framework, validated through a pilot study, demonstrates practical applicability in mitigating insider threats. By integrating awareness and training programs, policy enhancements, technological solutions, and fostering a supportive culture, organizations can effectively address both intentional and unintentional insider threats. The framework's success in the pilot study suggests its potential for broader implementation and scalability across different industries.

In conclusion, this study provides a comprehensive understanding of insider threats and the human factors influencing cybersecurity. The findings underscore the need for continuous education, leadership involvement, and advanced technological solutions to enhance organizational resilience against insider threats. Future research should explore the long-term impact of these strategies and the evolving nature of insider threats in the rapidly changing cybersecurity landscape.

6.REFERENCES

[1] R. A. Alsowail and T. Al-Shehari, "Techniques and countermeasures for preventing insider threats," *PeerJ Comput Sci*, vol. 8, p. e938, 2022.

[2] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," *Electronics (Basel)*, vol. 9, no. 9, p. 1460, 2020.

[3] U. D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2–35, 2019.

[4] J. R. Schoenherr, "Insider threats and individual differences: Intention and unintentional motivations," *IEEE Transactions on Technology and Society*, vol. 3, no. 3, pp. 175–184, 2022.

[5] T. R. McEvoy and S. J. Kowalski, "Deriving cyber security risks from human and organizational factors–a socio-technical approach," *Complex Systems Informatics and Modeling Quarterly*, no. 18, pp. 47–64, 2019.

[6] A. Pollini *et al.*, "Leveraging human factors in cybersecurity: an integrated methodological approach," *Cognition, Technology & Work*, vol. 24, no. 2, pp. 371–390, 2022.

[7] M. L. Green and P. Dozier, "Understanding Human Factors of Cybersecurity: Drivers of Insider Threats," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, 2023, pp. 111–116.

[8] C. Nobles, "Stress, burnout, and security fatigue in cybersecurity: A human factors problem," *HOLISTICA–Journal of Business and Public Administration*, vol. 13, no. 1, pp. 49–72, 2022.

[9] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1397–1417, 2018.

[10] M. Canham, C. Posey, and P. S. Bockelman, "Confronting information security's elephant, the unintentional insider threat," in *Augmented Cognition. Human Cognition and Behavior: 14th International Conference, AC 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22*, Springer, 2020, pp. 316–334.

[11] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting insider threat via a cyber-security culture framework," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 706–716, 2022.

[12] L. Kasowaki and O. Yusef, "The Human Factor in Cybersecurity: Addressing Social Engineering and Insider Threats," EasyChair, 2023.

Hewa Majeed Zangana: *Corresponding Author

[13] M. K. S. Alwaheidi[1], S. Islam, S. Papastergiou, and K. Kioskli, "Human Factors in Cybersecurity, Vol. 127, 2024, 187-193 AHFE," *Human Factors in Cybersecurity*, p. 187, 2024.
[14] N. Khan, R. J. Houghton, and S. Sharples, "Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks," *Cognition, Technology & Work*, vol. 24, no. 3, pp. 393–421, 2022.
[15] T. Baluta, L. Ramapantulu, Y. M. Teo, and E.-C. Chang, "Modeling the effects of insider threats on cybersecurity of complex systems," in *2017 Winter Simulation Conference (WSC)*, IEEE, 2017, pp. 4360–4371.
[16] I. Ghafir *et al.*, "Security threats to critical infrastructure: the human factor," *J Supercomput*, vol. 74, pp. 4986–5002, 2018.
[17] M. Theis *et al.*, "Common sense guide to mitigating insider threats," 2019.
[18] W. J. Triplett, "Addressing human factors in cybersecurity leadership," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 573–586, 2022.
[19] C. Nobles, "Botching human factors in cybersecurity in business organizations," *HOLISTICA–Journal of Business and Public Administration*, vol. 9, no. 3, pp. 71–88, 2018.
[20] M. Omar and H. M. Zangana, *Redefining Security With Cyber AI*. in Advances in Information Security, Privacy, and Ethics. IGI Global, 2024. doi: 10.4018/979-8-3693-6517-5.
[21] H. M. Zangana and M. Omar, "Threats, Attacks, and Mitigations of Smartphone Security," *Academic Journal of Nawroz University*, vol. 9, no. 4, pp. 324–332, 2020.
[22] V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset," *Int J Hum Comput Stud*, vol. 131, pp. 169–187, 2019.
[23] S. Nifakos *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, p. 5119, 2021.
[24] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an improved understanding of human factors in cybersecurity," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2019, pp. 338–345.
[25] H. Young, T. van Vliet, J. van de Ven, S. Jol, and C. Broekman, "Understanding human factors in cyber security as a dynamic system," in *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17– 21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA 8*, Springer, 2018, pp. 244–254.

Hewa Majeed Zangana: *Corresponding Author