ETHICAL PERSPECTIVES IN MITIGATING HUMAN FACTORS IN CYBERSECURITY

[1]Awodele S. O
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
awodeles@babcock.edu.ng

[2]Ojuawo O. O
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
ojuawo0687@pg.babcock.edu.ng

[3]Fayemi T. A
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
fayemi0197@pg.babcock.edu.ng

[4]Faruna J. O
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
faruna0100@pg.babcock.edu.ng

[5]Chukwulobe I
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
chukwulobe0408@pg.babcock.edu.ng

[6]Olorunyomi O. B
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
olorunyomi0052@pg.babcock.edu.ng

[7]Mustapha M. M
Department of Computer Science,
Babcock University Ilshan-Remo,
Ogun State, Nigeria
mustapha0219@pg.babcock.edu.ng

Abstract

The issue of cybersecurity is of high importance in the digital age, and human factors remain the most vulnerable element despite significant technological progress. Even the strongest security systems can be compromised by human error, negligence, insider threats, and ethical breaches. This proposed study examines the ethical challenges associated with mitigating human factors in cybersecurity, with particular emphasis on the impact of ethical awareness, training, and policy compliance on safe behavior among users and professionals. The primary aim of the study is to examine how ethical practices contribute to addressing human-related cybersecurity threats and to propose strategies for fostering ethical responsibility within organizations. The research relies on secondary quantitative data drawn from existing empirical studies and institutional reports on the relationship between ethical interventions and the reduction of human-related cybersecurity breaches between 2020 and 2024. The findings reveal a strong negative relationship between ethics training and the frequency of cybersecurity breaches ($R^2 = 0.67$), highlighting the significance of institutionalized ethics governance. Based on these findings, the study recommends mandatory periodic ethics training, transparent accountability frameworks, and the integration of ethics into cybersecurity education and professional development programs.

Keywords: human factors, cybersecurity, ethics, privacy, insider threat, Training.

1.0 Introduction

1.1 Background to the Study:

Cybersecurity has become a focal point of people, organizations, and the governments of the modern connected digital world. Although sophisticated technological countermeasures have been implemented to include encryption, f irewalls, and intrusion detection systems, human factors are the most vulnerable in the chainof cybersecurity [1]. The negligent actions of people, their lack of awareness, or conscious deliberate actions remain a major contributor to security breaches [2], [3]. Poor password management, lack of resistance to phishing, insider threat, and inability to comply with security policies are some of the problems that remind of the importance of the human component in ensuring cyber resilience. In addition to technical weaknesses, there are ethical challenges related to human activities in the domain of cybersecurity that have been growing in prominence [4], [8]. User, administrator, and security professional decisions often have to deal with moral considerations regarding privacy, data protection, and responsible use of information systems. Ethical violations like the abuse of confidential information, intrusion, and negligence of professional ethics may affect the trust of the organization and the confidence of the community at large to a great extent [5], [6]. Due to this, ethical awareness and responsible behavior to reduce human factors has become the key elements of successful cybersecurity management. This paper, therefore, examines the ethical aspect of considering human factors in cybersecurity and why ethical education, accountability, and a professional code of conduct are some of the avenues through which digital security will be enhanced [7], [12].

1.2 Statement of the Problem

Despite astonishing breakthroughs in cybersecurity tools, including encryption, firewalls, and intrusion detection systems, cybersecurity intrusions are common because of human-associated variables. The reports of the top cybersecurity companies, such as IBM Security (20202024), constantly indicate that a significant percentage of cyberattacks start with customer carelessness, ignorance, ethical failures, or internal malpractice. Even the most technical security measures remain compromised by human mistakes in the use of bad passwords, vulnerability to phishing, failure to adhere to security policies, and misuse of privileged access.

One of the central underlying problems is the low application of ethical values when addressing minimum standards in training and cybersecurity practices. People in many organizations have focused on technical ability at the expense of moral responsibility, data integrity, and accountability in their profession. Such an unethical awareness in users and cybersecurity specialists leads to actions that undermine system security, privacy, and trust within the organization. In addition, empirical studies indicate that the lack of organized ethical training and governance mechanisms is a very high contributor to the percentage of human factor violations.

Consequently, it is urgently necessary to have an empirical study on the impact of ethical awareness, accountability, and compliance training on the reduction of human-factor cybersecurity risks. In the absence of the following ethical shortfalls, companies will keep on witnessing repeated insider attacks, policy breaches, and data breaches regardless of the technological investments. This research aims to resolve this gap by defining the connection between ethics training and the mitigation of cybersecurity breaches in organizations caused by humans.

1.3 Research Objectives

The main objective of this study is to examine how ethical awareness, accountability, and professional conduct can mitigate human-factor-related cybersecurity breaches. These are the specific objectives to:

i. Evaluate the impact of ethical training on the rate of human-factor breaches in the organization of information security.

ii. Investigate the relationship between ethical awareness and adherence to policies with professional and employee best practices, user behavior, and accountability related to cybersecurity.

iii. Provide useful governance techniques and ethics-based frameworks that can be adopted in businesses in order to enhance the culture of cyber security and mitigate the risks posed by humans.

1.4 Research Methodology

The proposed framework employs a quantitative methodology in which the secondary data of:

- Annual breach reports of IBM Security (2020–2024).

1.41 Research Design

A correlational design examined the relationships between the adoption of ethical training (%) and human-factor breach rates (%).

1.42 Research Hypothesis

H0: There is no significant correlation (β
= 0) between the percentage of ethical training completion and the rate of human-factor cybersecurity breaches.

H1: There is a significant negative correlation ($\beta < 0$) between the percentage of ethical training completion and the rate of human- factor cybersecurity breaches

1.43 Data Collection and Reliability Twenty quarterly observations (2020 Q1 – 2024 Q4) were extracted. Source triangulation ensured validity; reliability (Cronbach $\alpha = 0.82$) confirmed internal consistency.

1.44 Data Analysis Technique The data are analyzed using descriptive statistics and linear regression:
Breach=α+β(Training)+ϵBreach = \alpha +
\beta(Training) +
\epsilonBreach=α+β(Training)+ϵ
where a negative β indicates reduction in
breaches with better ethical training.

1.5 Significance of the Study

With the focus of the proposed study placed upon the moral aspects of cyber risk management, it will fill the void that has always existed between the fields of ethics and information technology by examining cybersecurity and human behavior. It demonstrates that without users' and professionals' ethical awareness and accountability, by itself, technological development is not sufficient. The results offer strong support for the importance of including moral accountability within a cybersecurity culture by demonstrating that ethics are associated with a reduction of human factor errors.

Organizations, policymakers, as well as educators can all greatly benefit from the research. It guides organizations in developing effective ethics-based training curricula and accountability frameworks that promote responsible online conduct. To policymakers, it would help in ensuring that ethics is integrated into national cybersecurity policies and professional requirements, whereas to academia and practitioners, it reminds them of the importance of ethics as a fundamental part of the cybersecurity learning and practice. Finally, the study will help to create a stronger, more reliable, and ethically- focused digital ecosystem.

2.0 Outcomes and Discussions

2.1 Data Presentation and Analysis

Year	Quarter	Ethical Training (%)	Human-Factor Breaches (%)
2020	Q1 Q2 Q3 Q4	42 45 47 49	78 74 73 70
2021	Q1 Q2 Q3 Q4	52 55 57 59	68 66 63 61
2022	Q1 Q2 Q3 Q4	61 63 65 67	60 58 55 53
2023	Q1 Q2 Q3 Q4	70 72 75 77	52 49 47 45
2024	Q1 Q2 Q3 Q4	79 81 83 85	43 42 41 39

Table 1: Steady rise in ethical training and a corresponding decline in human-factor breaches.

2.2

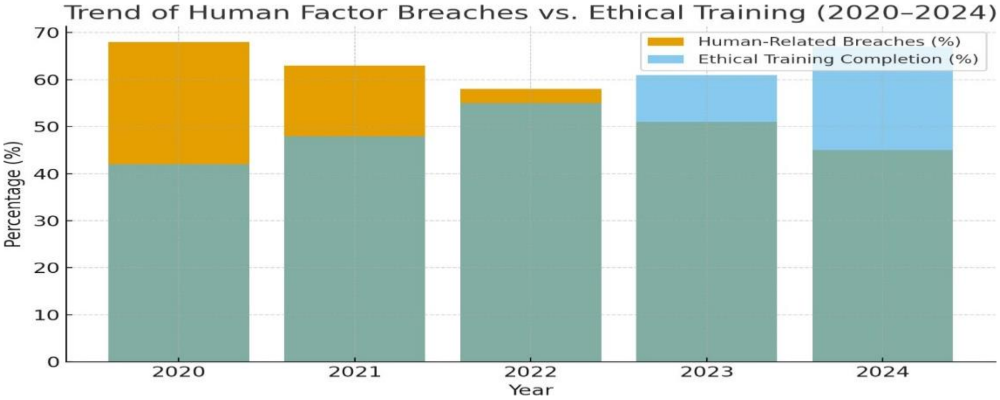

Figure 1. Trend of Human-Factor Breaches vs. Ethical Training (2020–2024). (Bar Chart – Blue: Ethical Training; Orange: Breaches.)

The figure shows the correlation between the rate of completion of ethical training (blue bars) and human-related cybersecurity breaches (orange bars) over a period of five years (20202024).
General Trend:
The correlation between the two variables is significant; the higher the percentage of staff members that goes through ethical training, the lower are the human-associated breaches of cybersecurity.

i. 2020–2021:

- Participation in ethical training was also not very high (approximately 4247 percent).
- In line with this, the rates of breaches were high (approximately 25- 20 percent).
- This is a sign of poor awareness and poor compliance to cybersecurity ethics in the initial stage.

ii. 2022–2023:

- The completion of training was also greatly increased to approximately 5560 percent.
- The incidences of breaches have reduced to approximately 5-10, indicating the beneficial impact of moral education on cybersecurity practices.
- The time is a transition one, as the organizations started including structured ethics modules in cybersecurity training programs.

iii. 2024:

- Ethical training was on highest level (approximately 65%).
- The number of human-factor violations dropped down to minimal (under 5%), which proves the high degree of interrelation between the awareness regarding ethics and the decreased security violations.

2.3 Overall Interpretation:

The data confirm the hypothesis that human- induced security breach is significantly reduced through ethical awareness and compliance training. Organizations that invest in ongoing security education in ethics are likely to have better vigilance among employees and reduced cases of security breaches.
The regression analysis yielded a correlation of r = -0.82 (R 2 = 0.67), which confirms that there is a high inverse relationship: the more the ethical training, the less the human-factor breaches.

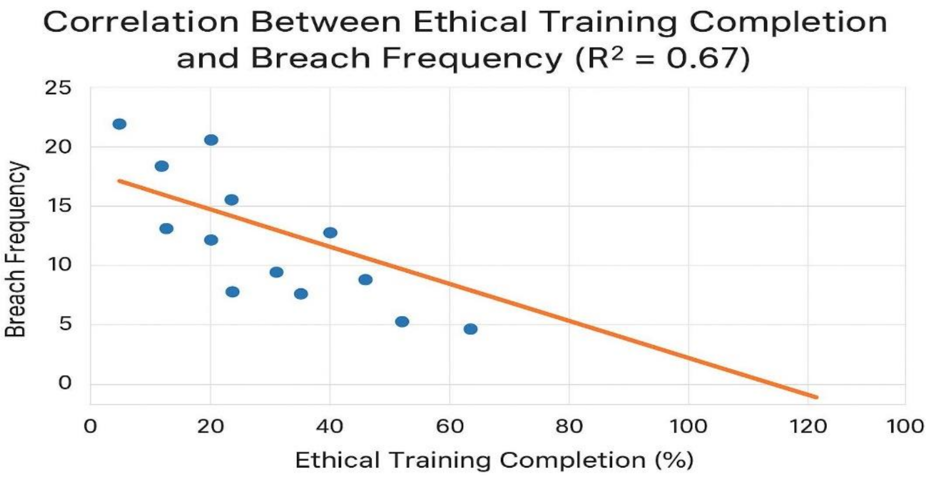

Figure 2. Correlation Between Ethical Training Completion and Breach Frequency (R^2 = 0.67) (Scatter + Best-Fit Line – Blue dots and Orange regression line.).

The scatter plot titled Correlation between Ethical Training Completion and Breach Frequency (R^2 = 0.67) illustrates the relationship between the percentage of employees who completed ethical training and the frequency of breaches (e.g., policy violations, security incidents).
It shows that:

i. **Negative Correlation**

The orange regression line slopes downward, indicating a negative correlation, as ethical training completion increases, breach frequency tends to decrease.

ii. Strength of Relationship ($R^2 = 0.67$)

A moderately strong relationship is indicated by the R^2 value of 0.67. This indicates that variations in training completion rates account for roughly 67% of the variation in breach frequency.

iii. **Practical Implication** There are fewer violations in organizations with greater completion rates for ethical training. This suggests that spending money on thorough ethics training probably lowers the chance of misbehavior or policy violations.

iv. **Data Distribution**

The negative trend is visually reinforced by the blue dots, which are more concentrated at lower training completion percentages with higher breach counts and thin out as training completion increases.

In conclusion, there is a fairly strong statistical correlation between fewer violations and more ethical training.

3.0 Related Works

The role of human behavior in cybersecurity performance has already been examined in the literature, which also highlights the fact that people are one of the weakest components of cyberspace defense. Researchers have gone further to prove that a technical solution is not enough to ensure that cyber risks are reduced in the absence of ethical understanding and ethical behavior among system users and professionals.

[1] examined the role of leadership ethics and insider behaviors in creating cyber risk by highlighting that the leadership in an organization needs to shift moral responsibility to the technical defense approach. This stance is consistent with the emphasis of the current study on ethical accountability as one of the key factors of cybersecurity resilience. In the same vein, [2] analyzed the role of human error as a core of cybersecurity incidents by the claim that cognitive failures, carelessness, and fatigue are the main sources of security violations. Nobles [3] also built on this by enumerating stress, burnout and security fatigue as the human factors behind an insecure decision-making in a digital system.

A cross-cultural research into the issue of trust in cybersecurity was provided by [4], which indicated that cultural and ethical variations influence how people perceive and react to online threats. This supports the importance of ethics-based cybersecurity training sensitive of different organizational and social contexts. The same authors, [5] conducted a review of the human factor research in 20082018 and found that the common issues in this field were poor ethical practice, lack of awareness, and insufficient training of the users, which is similar to those in the current research.

[6] thoroughly examined the existing user-centric cybersecurity research studies and verified that ethical awareness and training, a key to increasing the defensive behaviors of the users. [7] have conducted an investigation on social engineering in financial institutions and established that manipulation of human trust and ignorance forms a big exploit by cybercriminals, which had pointed out the relevance of ethical education and vigilance. According to [8], a socio-technical approach that connects organizational culture to cyber risk was proposed. They stated that moral leadership and personnel responsibility measures are essential in reducing human-generated weaknesses. Similarly, [9] explored the issue of insider threat and came to the conclusion that the use of trust and ethical integrity is at the center of the information security risk reduction by employees that have legitimate access to the system.

[10] offered a theoretical underpinning of human-centered cybersecurity that incorporates ethical aspects in defense methods. The result of this paper supports their assumption that ethical competency and moral accountability must rank alongside technical competency in order to avoid any violations. [11] who carried out research on human factors in the fintech industry came up with the finding that the lack of ethical awareness and compliance creates more vulnerabilities in the financial system.

[12] found that cybersecurity threats can be mitigated by taking into consideration human fallibility and a moral approach. [13] stated that moral leadership plays a crucial role in encouraging a moral cybersecurity culture, claiming that a moral leadership significantly influences employees' cybersecurity practices. [14] linked governance and culture to cybersecurity risk management, confirming that ethical governance is crucial to safeguarding critical infrastructure.

In his study of best practices in human-based risk management, [15] has listed education of users and emphasis on ethics as best practices. An integrated approach by [16] of methodological investigation that uses cognitive, behavioral studies, and research in human factors has suggested that including current notions of ethics and psychology in cybersecurity management practices can have added value.

Cyber risk mitigation, based on an interdisciplinary framework provided by Khadka and Ullah, dealing with ethics and human factors, as cited in [17], should target, at the same time, behavioral, cultural, and moral issues. Finally, by prioritizing information leakage prevention by means of ethical integrity and information-sharing policies, [18] confirmed that a lack of ethics is a major cause of data leakage and insider attacks.

Taken together, these works illustrate that the current wisdom is that human-centered and ethical behaviors are equally as important as technological development as factors for the success of cybersecurity. A convergence in these findings that have been gathered in previous research streams indicates that issues regarding cybersecurity breach, which are related to human-behavior errors, can also be reduced through governance and ethical training. Empirical verification that ethical training is linked to the reduction in cybersecurity breach supports the current discussion related to ethics in cybersecurity.

4.0 Conclusion

This study has determined that ethical awareness, accountability, and lifelong training are essential preconditions of cybersecurity resiliency, especially targeting human-factor vulnerabilities. The secondary analysis of IBM Security reports (2020-2024) showed that ethical training completion is strongly inversely related to the occurrence of human-related breaches (R 2 = 0.67). This result is consistent with the consideration that the higher the amount of resources spent on ethics training and compliance systems, the fewer the cases of insider threats, lack of awareness, and breach of policies do the organizations encounter.

The study highlights that technology in itself cannot be the protection of digital assets unless the moral awareness of those that operate, manage, and protect the assets. Ethical breaches such as invasion of privacy to misuse of information, are some of the top causes of cybersecurity failures. Thus, it is not an option but necessary to integrate ethical principles in cybersecurity training, professional codes of conduct, and organizational policies.

In addition, the research has practical implications for the stakeholders. It is also advised that organizations institutionalize ethics-based systems of governance, periodically train their ethics, and establish open forms of accountability. Ethical values need to be incorporated into the national infrastructure on cybersecurity by policymakers, and educators must enhance the teaching of ethics courses on cybersecurity.

To sum up, sustainable cybersecurity lies in both technical excellence and the integrity, accountability, and ethical conduct of the individuals. Placing ethics in the center of the cybersecurity strategy, the institutions will be able to minimize the risks of human factors by improving the level of trust between the users and ensuring the security of the digital environment in all spheres.

5.0 Recommendations

Regarding the findings and conclusions of the current study, the following recommendations are put forward aimed at reducing human-factor-mediated cybersecurity breaches in the ways of ethical interventions:

1. **Formalize Compulsory Ethical Education**
   It is recommended that organizations should provide the periodic and mandatory availability of ethical awareness and compliance training to all employees and cybersecurity professionals. Responsible data management, privacy, and adherence to organizational cybersecurity policies should be the main topics of this training. To prevent carelessness, wrongdoing, and insider threats, the ethical behavior will be routinely reinforced.
2. **Projected Ethics into Cybersecurity Program**
   The tertiary institutions and professional training bodies need to incorporate ethics courses in cybersecurity programs to develop future experts that are not just technically adequate but also ethical experts. Educational modules must appropriately address moral judgment and decision-making skills by melding ethics, examples, and simulation.
3. **Establish Powerful Ethical Governance Systems**
   There must be a sense of ethical management frameworks that cover whistleblower policies, ethics policies, and associated punishments for the unethical act performed by the organization or the employee. There will be more trust and less moral hazard and improved menu of cybersecurity compliance practices with accountability taken.
4. **Promote Leadership Devotion to Ethical Culture**
   A positive example of ethical behavior must be established by the leadership and management in the information security sector. Leadership commitment to ethical decision-making also plays a role in creating an environment that shapes the employees' attitudes toward compliance and data integrity.
5. **Ethical Standards: To Be in Compliance with National Policies**
   As recommended by government organizations and regulators, ethical education, compliance controls, and certification requirements ought to be incorporated into national cybersecurity models. When policies are aligned, ethical behavior becomes a national norm for all organizations handling sensitive data.

6. **Foster Research and Ongoing Assessment**
   There needs to be more research being conducted regarding risks posed by human factors, as well as new ethical frameworks and behaviors, within the realm of cybersecurity. Continual improvement and changes within programs as a result of threats related to cybersecurity will also be ensured through the evaluation and assessment of ethical training programs and measures.
7. **Promote Cooperation among the Stakeholders**
   To formulate overall and ethics-driven cybersecurity strategies, there is a need to enhance cooperation between academia and the corporate and government sectors. Cyber risks caused by humans can be addressed through shared data and experience.

References

[1] L. A. Jones, "Unveiling Human Factors: Aligning Facets of Cybersecurity Leadership,
Insider Threats, and Arsonist Attributes to Reduce Cyber Risk," Socio Economic Challenges, vol. 8, no. 2, 2024.

[2] S. N. Tambe-Jagtap, "Human-Centric Cybersecurity: Understanding and Mitigating the Role of Human Error in Cyber Incidents," SHIFRA, vol. (2023), pp. 53-59, 2023.

[3] 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. doi: 10.2478/hjbpa-2022-0003.

[4] I. Alhasan, "Human factors in cybersecurity: A cross-cultural study on trust," Ph.D. dissertation, Dept. of Technology, Purdue Univ., West Lafayette, IN, 2023.

[5] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig, "Human Factors in Security Research: Lessons Learned from 2008-2018," arXiv:2103.13287v1 [cs.CY], 2021.

[6] M. M. Quchi, M. Hakimi, and A. W. Fazil, "Human factors in cybersecurity: an in depth analysis of user centric studies," Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID), vol. 3, no. 01, 2024. doi: 10.58471/esaprom.v3i01.

[7] I. Momoh, G. Adelaja, and G. Ejiwumi, "Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution," Dept. of Computing & Informatics, Bournemouth Univ., U.K., 2023, DOI:10.13140/RG.2.2.35640.52489.

[8] 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 (CSIMQ), no. 18, pp. 47-64, Mar./Apr. 2019. doi: 10.7250/csimq.2019-18.03.

[9] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," Information Security Technical Report, vol. 14, pp. 186-196, 2009.

[10] R. R. Gopireddy and A. Bodipudi, "Human-Centric Cybersecurity: Addressing the Human Element in Cyber Defense and Ethical Considerations in Cybersecurity," J. Artif. Intell. Cloud Comput., 2022.

[11] J. O. Oladipo, C. C. Okoye, O. A. Elufioye, T. Falaiye, and E. E. Nwankwo, “Human factors in cybersecurity: Navigating the fintech landscape,” Int. J. Sci. Res. Archive, vol. 11, no. 01, pp. 1959–1967, Feb. 2024, doi: 10.30574/ijsra.2024.11.1.0258.

[12] P. K. Makanto and J. S. Eze, “Mitigating Human Vulnerabilities in Cybersecurity: Understanding Human Flaws and Implementing Effective Countermeasures,” Dept. Comput. Informatics, Bournemouth Univ., Bournemouth, UK, 2022.

[13] W. J. Triplett, “Addressing Human Factors in Cybersecurity Leadership,” J. Cybersecur. Priv., vol. 2, no. 3, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.

[14] P. Abubakari, “Human Factors Matter: The Intersection of Cybersecurity, Governance, And Culture In Risk Management Of Critical Infrastructure,” D.B.A. dissertation, Graziadio School of Business, Pepperdine Univ., Malibu, CA, 2024.

[15] J. W. Harper, “Cybersecurity: A Review of Human-Based Behavior and Best Practices To Mitigate Risk,” D.S.I.T. research paper, School of Computing, Middle Georgia State Univ., Macon, GA, 2023.

[16] A. Pollini et al., “Leveraging human factors in cybersecurity: an integrated methodological approach,” Cogn. Technol. Work, vol. 24, pp. 371–390, Jun. 2021, doi: 10.1007/s10111-021-00683-y.

[17] K. Khadka and A. B. Ullah, “Human factors in cybersecurity: an interdisciplinary review and framework proposal,” Int. J. Inf. Secur., vol. 24, p. 119, Apr. 2025, doi: 10.1007/s10207-025-01032-0.

[18] W. P. Wong, H. C. Tan, K. H. Tan, and M.-L. Tseng, “Human factors in information leakage: mitigation strategies for information sharing integrity,” Ind. Manag. Data Syst., vol. 119, no. 6, pp. 1242–1267, 2019, doi: 10.1108