GJR Publication
OPEN ACCESS

Global Journal of Research in Engineering & Computer Sciences
ISSN: 2583-2727 (Online)
Volume 04| Issue 06 | Nov.-Dec. | 2024
Journal homepage: https://gjrpublication.com/gjrecs/

Review Article

Human-Centric Cybersecurity: Behavioral Insights and Strategic Approaches for Enhanced Awareness

[1]Livingston Sunday Aduku, [2]Sarafadeen Leye Lawal, [3]Muhammad Ahmad Baballe*

[1, 2, 3]Department of Mechatronics Engineering, Nigerian Defence Academy (NDA), Kaduna, Nigeria.

DOI: 10.5281/zenodo.14497164 **Submission Date:** 12 Nov. 2024 | **Published Date:** 15 Dec. 2024

***Corresponding author:** Muhammad Ahmad Baballe
Department of Mechatronics Engineering, Nigerian Defence Academy (NDA), Kaduna, Nigeria.
ORCID: 0000-0001-9441-7023

Abstract

Cyberthreats are advancing in sophistication, challenging the adequacy of traditional technical defenses. This paper explores the critical role of human behavior in cybersecurity vulnerabilities, emphasising the psychological and social factors that influence decision-making at individual and organisational levels. We present an innovative framework to enhance cybersecurity awareness, leveraging tailored user segmentation, interactive education strategies, and continuous assessments. The framework employs scalable technological tools, including e-learning platforms, mobile applications, and simulated environments. We discuss key organisational policies and national initiatives, emphasising the significance of public-private partnerships and regulatory integration. Practical recommendations for incorporating behavioral insights into cybersecurity strategies are provided, alongside future research directions in emerging technologies, behavioral analytics, and immersive education. By addressing human-centric vulnerabilities, this study aims to mitigate human error-driven incidents and fortify digital resilience across organisational and national domains.

Keywords: *Cybersecurity Awareness, Behavioral Cybersecurity, Interactive Education, Cybersecurity Policies, Cybersecurity Framework, Behavioral Insights.*

I. INTRODUCTION

In today's digitally interconnected world, the global digital economy is valued at over $14.5 trillion annually, highlighting cybersecurity's pivotal role in maintaining global stability. However, the projected $10.5 trillion annual cost of cybercrime by 2025 signals a pressing threat to organisations and individuals alike [1]. While technological advancements in cybersecurity offer significant defenses, human error persists as a primary vulnerability. Studies attribute nearly 88% of data breaches to user negligence or mistakes [2]. High-profile incidents, such as the Colonial Pipeline ransomware attack leading to fuel shortages across the United States and the SolarWinds breach, which compromised thousands of organisations globally, underscore the consequences of exploiting behavioral vulnerabilities [3, 4]. These events demonstrate that even the most robust technical defenses can falter when human awareness is inadequate.

Technical measures, including firewalls, encryption, and intrusion detection systems, remain vital in combating cyber threats. However, cybersecurity's weakest link is often the human element. Phishing attacks, weak passwords, and accidental data leaks frequently result from insufficient awareness or inadequate training. Addressing these vulnerabilities requires an in-depth understanding of the psychological, social, and cultural factors shaping human behavior. Organisations must cultivate a culture of cybersecurity awareness to mitigate the risks posed by human error effectively [5].

While human behavior's critical role in cybersecurity is widely acknowledged, current solutions often lack an integrated approach that combines behavioral insights with technical measures. Existing studies typically focus narrowly on either technological defenses or user education, creating a disconnect between these domains [6, 7]. This paper seeks to address

this gap by developing a holistic, user-centric framework that incorporates tailored user segmentation, interactive education strategies, and continuous assessments to enhance cybersecurity awareness. The overarching objective is to offer a scalable, evidence-based solution to mitigate human-related cybersecurity risks.

This study draws on theories from behavioral science, psychology, and sociology, integrating them with concepts from cybersecurity to form a robust theoretical foundation. This interdisciplinary framework provides a deeper understanding of how human factors influence cybersecurity practices and informs the development of strategic, actionable solutions.

This paper addresses the following key research questions:
1. How can tailored user segmentation address diverse cybersecurity awareness needs?
2. What interactive education strategies are most effective in engaging and educating users about cybersecurity?
3. How can continuous assessments ensure the sustained effectiveness of cybersecurity awareness programs?

The main key contributions of this study are as follows:

i. **Behavioral Insights**: An exploration of critical psychological and social factors affecting user behavior and their role in cybersecurity vulnerabilities.

ii. **Framework Development**: The design of a strategic, evidence-based framework tailored to diverse user groups to enhance cybersecurity education.

iii. **Policy Recommendations**: Guidance for embedding cybersecurity awareness into organisational and national strategies.

iv. **Future Research Directions**: Identification of gaps and opportunities for advancing research in behavioral cybersecurity.

II. LITERATURE REVIEW

This section provides a review of cybersecurity awareness programs, emphasising their evolution, the intersection with human behavior, and the critical gaps that necessitate this study. High-impact journals, industry reports, and case studies are examined to synthesise a holistic understanding of the domain. The review leverages reputable cybersecurity reports from ENISA, NIST, and Verizon for industry perspectives.

2.1 Overview of Cybersecurity Awareness Programs

Historical and Contemporary Initiatives

Cybersecurity awareness programs have evolved significantly over the past two decades. Early initiatives focused on distributing basic guidelines, such as ENISA's Awareness Raising Campaign (2010) [8], which emphasised simple and safe online behaviors. Over time, programs integrated technology-driven methods like gamification and real-time simulations.

Key insights from the literature include:

Gamified Platforms:

Trombino (2023) [9]: Demonstrated the efficacy of Hack The Box (HTB) in teaching secure software development to undergraduate students through gamified scenarios.

Pramod (2024) [10]: Highlighted the role of gamification in making cybersecurity education engaging, emphasising interactive platforms like cybersecurity escape rooms.

Chen et al. (2023) [11]: Found that gamified Information Security Education Systems (ISES) positively impacted users' information security awareness through emotional and cognitive pathways.

Case Examples from Industry and National Programs

A deeper understanding of program implementation can be derived from organizational and national case studies:

i) **Google's Security Training Program**: Uses real-time feedback during phishing simulations, resulting in a reported 40% reduction in successful phishing attempts (Google Security Report, 2023) [12].

ii) **UK National Cyber Security Centre (NCSC)**: Launched the "Cyber Aware" campaign targeting small businesses, focusing on password security and software updates [13].

iii) **Japan's Cybersecurity Month**: Features community-driven awareness programs combining digital tools and in-person workshops to cater to diverse user groups [14].

While these programs show promise, they often fail to personalise training for varying demographics or to integrate behavioral insights comprehensively.

2.2 The Role of Human Behavior in Cybersecurity

Behavioral Theories Relevant to Cybersecurity

Behavioral science plays a crucial role in cybersecurity awareness:

i) **Protection Motivation Theory (PMT)**: Emphasizes the impact of perceived threats and coping mechanisms on user behavior. For example, Ifinedo *(2021)* highlighted the theory's relevance in explaining why some users respond more effectively to cybersecurity training [15].
ii) **Habit Formation Theory**: Demonstrates how consistent reinforcement can establish secure practices. Smith et al. (2022) found that frequent reminders and microlearning sessions improved users' adherence to cybersecurity protocols [16].

Empirical Studies on Vulnerability and Compliance

Empirical research underscores the importance of behavioral insights in addressing user vulnerabilities:
Veksler et al. (2020) [17]: Identified that Symbolic Deep Learning (SDL) reduced missed cyber threats by 25%.
Krawczyk et al. (2013): Explored how heuristics and biases influence cybersecurity expertise, highlighting the need for tailored approaches.
Wu He et al. (2019) [18]: Noted that generic training programs often fail to engage older adults and non-native digital users, reinforcing the need for segmentation.
Veksler et al. (2018) [19]: Reviewed cognitive modelling in cybersecurity, highlighting the importance of simulations in addressing human factors and improving training effectiveness
Krawczyk et al. (2013)[20]: Measured expertise and bias in cybersecurity using cognitive and neuroscience approaches, emphasizing the role of heuristics and biases in cyber security expertise

2.3 Research Gaps and Needs

The review identifies critical gaps in current cybersecurity awareness practices:

i) Lack of Personalization: Existing programs often adopt one-size-fits-all approaches. Training that ignores demographic diversity (e.g., cultural or age-related differences) limits its effectiveness. Wu He et al. (2019) [18], specifically called for targeted interventions for underrepresented groups.
ii) Insufficient Behavioral Science Integration: Few programs leverage robust behavioral theories like PMT or Habit Formation to inform their designs. Authors in [6, 7] recommended interdisciplinary collaborations to address this gap.
iii) Inadequate Evaluation Mechanisms: Programs often lack iterative feedback loops or rigorous long-term impact evaluations. Renaud et al. (2022) advocated for dynamic frameworks that adapt based on user feedback.

Overemphasis on Technology: Many initiatives prioritize technological solutions over human-centric strategies. While tools like AI-driven simulations are powerful, Smith et al. (2022) argued they are ineffective without user trust and understanding.

The following table summarises the key studies and their contributions, limitations, and gaps:
Table 1: summary of literature review

Study	Focus	Key Findings	Limitations/Gaps
Trombino (2023)	Hack The Box (HTB) for gamified learning	Enhanced engagement and knowledge retention	Limited scalability across cultural contexts
Pramod (2024)	Gamification in cybersecurity education	Gamified platforms improve engagement and efficacy	Needs more testing in diverse demographics
Chen et al. (2023)	Gamified ISES for user awareness	Enhanced awareness via emotional and cognitive paths	Retention over the long term remains unclear
Google Security Report	Real-time feedback in phishing training	40% reduction in phishing success	Requires continuous updates and customization
UK NCSC	"Cyber Aware" campaign	Focused on small businesses with password and update training	Variable impact across business sizes
Japan's Cybersecurity Month	Community-driven awareness programs	Integrates digital and in-person approaches for inclusivity	Needs localized needs assessments
Ifinedo (2021)	PMT application to user response	Validates PMT's relevance in user training	Not all aspects are applicable to diverse users
Smith et al. (2022)	Habit formation theory in cybersecurity	Reinforcement improves adherence to secure practices	Behavioral nuances may require deeper exploration

This literature review provides a comprehensive analysis of cybersecurity awareness programs, examining their evolution, integration with behavioral science, and critical gaps. While significant progress has been made, the need for personalised, behaviorally informed, and rigorously evaluated strategies remains paramount. These insights form the foundation for developing a user-centric framework for enhancing cybersecurity awareness.

III. METHODOLOGY

This section outlines the step-by-step process adopted to achieve the study's objectives. The methodology incorporates qualitative and participatory techniques, supported by charts and tables, to ensure actionable outcomes while extracting meaningful insights and validating the proposed framework.

3.1. Semi-Structured Interviews

Rationale:

Semi-structured interviews with domain experts provide context-specific, real-world insights into cybersecurity awareness practices, complementing theoretical approaches with practical knowledge.

Process:

1. Participant Selection:

Experts were identified from diverse fields, including cybersecurity professionals, educators, behavioral scientists, and policymakers. Selection criteria included:

i) Minimum 5 years of experience in their domain.
ii) Proven expertise in designing or implementing cybersecurity awareness initiatives.
iii) Representation from corporate, government, and academic sectors.

Table 2: Participant Demographics

Sector	Number of Participants	Average Experience (Years)	Gender Ratio (M)
Corporate	10	7	7:3
Government	8	9	6:2
Academia	7	10	4:3

2. Interview Design:

Questions were designed to address the following themes:

i) Challenges in current cybersecurity awareness programs.
ii) Behavioral factors influencing cybersecurity practices.
iii) Strategies for engaging diverse user groups effectively.
iv) Recommendations for framework development and implementation.

4. Data Collection:

Interviews were conducted virtually to ensure broader participation. Each session lasted 30–45 minutes and was recorded with participant consent.

5. Data Analysis:

Thematic coding was applied to interview transcripts to identify recurring themes and unique insights.

Figure 1: Below depict the key themes extracted from interviews.

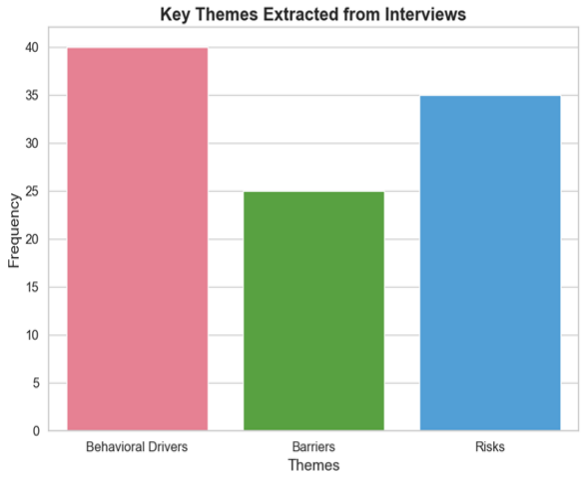

Figure 1: A bar chart depicting the frequency of recurring themes like Behavioral Drivers, Barriers, and Risks

3.2. Behavioural Insight Framework

Objective:

To understand the human factors influencing cybersecurity practices and categorise them into actionable insights.

Process:

1. Data Sources:
   i) Behavioral insights were derived from:
   ii) Thematic analysis of interview data.
   iii) Review of case studies and empirical studies identified in the literature.

2. Categorisation:

Behaviors were classified into three categories:
   i) Risks: Behaviors increasing vulnerability, such as weak password usage and susceptibility to phishing.
   ii) Drivers: Motivations promoting safe practices, such as incentives and fear of repercussions.
   iii) Barriers: Obstacles hindering secure practices, including technical complexity or lack of awareness.

Table 3: Categorization of Behavioral Insights

Category	Example Behavior	Implications for Awareness Programs
Risks	Weak password usage	Educate on password management tools.
Drivers	Incentive for safe behavior	Use rewards for phishing training tests.
Barriers	Lack of technical knowledge	Simplify cybersecurity communication.

3. Output:

Insights were synthesised to design targeted strategies for the framework.

3.3. Framework Development

Methodology:

The Design Science Research (DSR) approach was adopted to conceptualise and refine the framework.

Process:

1. Conceptualisation:

Insights from interviews and behavioral analysis were integrated into a preliminary framework. Key components included:

i. Awareness modules.

ii. Behavioral interventions.

iii. Feedback mechanisms.

2. Iterative Refinement:

The draft framework was presented to a panel of 15 experts (different from interview participants) for two rounds of feedback.

Table 4: Expert Feedback Summary

Round	Aspect Evaluated	Key Suggestions	Action Taken
1	Relevance	Include case examples.	Added real-world examples.
2	Practical Feasibility	Simplify implementation steps.	Streamlined framework.

3. Finalisation:

The framework was finalised by integrating expert feedback, ensuring it was applicable across diverse user groups.

3.4. Validation

Objective:

To assess the utility, applicability, and comprehensiveness of the proposed framework.

Process:

1. Benchmarking:

The framework was compared with existing models like the NIST Cybersecurity Framework and ENISA Awareness Programs for coverage and applicability.

Table 5: Benchmarking of Framework Features

Feature	Proposed Framework	NIST Framework	ENISA Programs
Behavioral Insights	Yes	No	Limited
Adaptability to User Groups	High	Medium	Low
Feedback Mechanisms	Included	Minimal	Minimal

2. Hypothetical Use Cases:
Scenarios were designed to test the framework's application. Examples included:

i) Corporate Environment: Development of a cybersecurity training program for employees.
ii) Healthcare: Creating tailored awareness sessions for medical staff handling sensitive data.
iii) Education Sector: Implementing gamified awareness strategies for university students.

3. Evaluation Metrics:
The framework was assessed for:

i) Relevance: Addresses key challenges identified in interviews.
ii) Flexibility: Adapts to various user groups and scenarios.
iii) Effectiveness: Incorporates behavioral insights for better outcomes.

Figure 2: Depict the evaluation metrics for framework validation

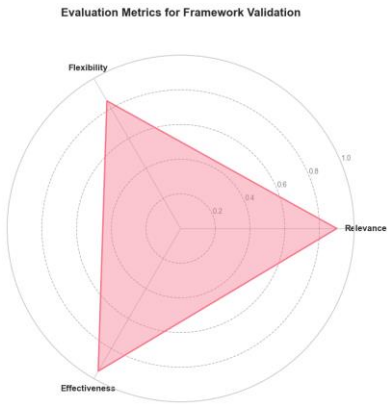

Figure 2: A radar chart showing high scores for Relevance, Flexibility, and Effectiveness

IV. CONCLUSION

This paper highlights the importance of addressing cybersecurity awareness through strategies that incorporate behavioral insights, interactive education, and structured implementation plans. By analysing the psychological, social, and cultural factors influencing user behavior, the study identifies the key drivers of cybersecurity risks and proposes targeted interventions. The approach emphasises tailored solutions for different user groups, including youth, corporate employees, and elderly users, ensuring relevance and accessibility. Practical methods such as gamified learning, scenario-based training, and dynamic assessments were proposed to enhance user engagement and retention. These strategies, combined with a phased implementation roadmap, provide a scalable model for integrating cybersecurity awareness into organisations and broader societal contexts. The framework offers actionable guidance for improving user preparedness, reducing risky behaviors, and fostering a culture of security consciousness. The results underline the need for collaborative efforts between organisations, governments, and educators to translate these strategies into effective programs. By adopting these recommendations, stakeholders can empower individuals with the knowledge and tools necessary to navigate the growing complexities of the digital world while reducing vulnerabilities and promoting safe online practices.

REFERENCES

1. K. B. Ooi et al., "The Metaverse in Engineering Management: Overview, Opportunities, Challenges, and Future Research Agenda," IEEE Transactions on Engineering Management, vol. 71, pp. 13882-13889, 2024, doi: 10.1109/TEM.2023.3307562.
2. CISOMAG. "Psychology of Human Error" Could Help Businesses Prevent Security Breaches." https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/ (accessed 18/11, 2024).
3. J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," in 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), 1-4 May 2023 2023, pp. 8-15, doi: 10.1109/CCGridW59191.2023.00017.
4. R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar Winds Hack: In-Depth Analysis and Countermeasures," in 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 6-8 July 2021 2021, pp. 1-7, doi: 10.1109/ICCCNT51525.2021.9579611.

5. V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset," International Journal of Human-Computer Studies, vol. 131, pp. 169-187, 2019/11/01/ 2019, doi: https://doi.org/10.1016/j.ijhcs.2019.05.005.
6. M. Eling and K. Jung, "Optimism bias and its impact on cyber risk management decisions," Risk Sciences, vol. 1, p. 100001, 2025/01/01/ 2025, doi: https://doi.org/10.1016/j.risk.2024.100001.
7. M. Simon, S. M. Houghton, and K. Aquino, "Cognitive biases, risk perception, and venture formation: How individuals decide to start companies," Journal of Business Venturing, vol. 15, no. 2, pp. 113-134, 2000/03/01/ 2000, doi: https://doi.org/10.1016/S0883-9026(98)00003-2.
8. D. Liveri, A. Sarri, and E. Darra, "ENISA's Contribution to National Cyber Security Strategies," in Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, M. Bartsch and S. Frey Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2018, pp. 43-64.
9. G. Trombino, "Gamifying cybersecurity: a study of the effectiveness of a specific gamified tool," in International Conference on Education and New Developments, 2023: inScience Press, pp. 210-214.
10. D. Pramod, "Gamification in cybersecurity education; a state of the art review and research agenda," Journal of Applied Research in Higher Education, vol. ahead-of-print, no. ahead-of-print, 2024, doi: 10.1108/JARHE-02-2024-0072.
11. H. Chen, Y. Zhang, S. Zhang, and T. Lyu, "Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention," Education and Information Technologies, vol. 28, no. 12, pp. 15915-15948, 2023/12/01 2023, doi: 10.1007/s10639-023-11771-z.
12. A. Planqué-van Hardeveld, "Securing the platform: how Google appropriates security," Critical Studies on Security, vol. 11, no. 3, pp. 161-175, 2023.
13. A. Cartwright, E. Cartwright, and E. S. Edun, "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," Computers & Security, vol. 131, p. 103288, 2023.
14. B. Bartlett, "Why do states engage in cybersecurity capacity-building assistance? Evidence from Japan," The Pacific Review, vol. 37, no. 3, pp. 475-503, 2024.
15. P. Ifinedo, "Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors," Journal of Computer Information Systems, vol. 63, no. 2, pp. 380-396, 2023.
16. B. Smith, P. S. Gallagher, S. Schatz, and J. Vogel-Walcutt, "Total learning architecture: moving into the future," in Proceedings of the interservice/industry training, simulation, and education conference (I/ITSEC), 2018, pp. 1-11.
17. V. D. Veksler, N. Buchler, C. G. LaFleur, M. S. Yu, C. Lebiere, and C. González, "Cognitive Models in Cybersecurity: Learning from Expert Analysts and Predicting Attacker Behavior," Frontiers in Psychology, vol. 11, 2020.
18. W. He and J. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," Journal of Organizational Computing and Electronic Commerce, vol. 29, pp. 1-9, 07/29 2019, doi: 10.1080/10919392.2019.1611528.
19. V. D. Veksler, N. Buchler, B. E. Hoffman, D. N. Cassenti, C. Sample, and S. Sugrim, "Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users," (in eng), Front Psychol, vol. 9, p. 691, 2018, doi: 10.3389/fpsyg.2018.00691.
20. D. Krawczyk, J. Bartlett, M. Kantarcioglu, K. Hamlen, and B. Thuraisingham, "Measuring expertise and bias in cyber security using cognitive and neuroscience approaches," in 2013 IEEE International Conference on Intelligence and Security Informatics, 4-7 June 2013 2013, pp. 364-367, doi: 10.1109/ISI.2013.6578859.

CITATION

Livingston S. A., Sarafadeen L. L., & Muhammad A. B. (2024). Human-Centric Cybersecurity: Behavioral Insights and Strategic Approaches for Enhanced Awareness. In Global Journal of Research in Engineering & Computer Sciences (Vol. 4, Number 6, pp. 107–113). https://doi.org/10.5281/zenodo.14497164