International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

From awareness to action: Designing effective cybersecurity training programs

Diana Ussher-Eke *

Continental Reinsurance PLC, Human Resources, Victoria Island, Lagos, Nigeria.

International Journal of Science and Research Archive, 2025, 16(02), 494-504

Publication history: Received on 01 July 2025; revised on 08 August; accepted on 11 August 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.2.2348

Abstract

In an era where cyber threats are increasingly sophisticated and persistent, organizations must go beyond basic awareness initiatives to implement proactive and adaptive cybersecurity training programs. This study explores the design and implementation of effective cybersecurity training programs that not only raise awareness but also transform employee behavior and response capabilities. Traditional awareness campaigns often fail to instill lasting behavioral changes, largely due to their generic, compliance-driven nature. This paper adopts a multidisciplinary approach by integrating behavioral psychology, adult learning theories, and cybersecurity frameworks to develop a robust training model. The proposed model emphasizes personalized learning paths, scenario-based simulations, and continuous feedback mechanisms to enhance user engagement and retention. Additionally, the study evaluates the role of gamification, phishing simulations, and role-specific modules in reinforcing cyber hygiene across different organizational levels. Quantitative data from a controlled training experiment involving 300 employees across finance, healthcare, and education sectors indicate a 48% improvement in phishing detection rates and a 36% reduction in policy violations after three months of program deployment. The research also highlights the importance of leadership support, organizational culture, and metrics-driven evaluations in sustaining long-term effectiveness. The findings suggest that cybersecurity training must evolve from a one-size-fits-all awareness format to a dynamic, data-informed strategy that aligns with human behavior and organizational risk profiles. This paper contributes practical insights for cybersecurity professionals, HR departments, and IT trainers, providing a framework for designing and implementing effective cybersecurity training programs that shift users from passive awareness to active cyber resilience. The proposed framework can be adapted and scaled across industries to meet regulatory standards and emerging threat landscapes, positioning human factors as a critical defense line in the cybersecurity ecosystem.

Keywords: Cybersecurity training; Employee awareness; Behavioral change; Phishing simulation; Human factors; Cyber resilience

1. Introduction

In recent years, cybersecurity has emerged as one of the most critical areas of concern for organizations operating in an increasingly interconnected digital environment. As cyber threats become more sophisticated, the traditional reliance on technological solutions such as firewalls, intrusion detection systems, and encryption alone has proven insufficient. Numerous high-profile breaches—including those affecting financial institutions, healthcare systems, and government agencies—have demonstrated that human error remains one of the most exploitable vulnerabilities within any cybersecurity architecture. According to a 2024 IBM Security report, over 82% of security breaches involve a human element, either through social engineering, poor password hygiene, or unintentional policy violations. Despite substantial investments in security infrastructure, organizations continue to struggle with one fundamental issue: the lack of effective, behaviorally informed cybersecurity training programs that can instill lasting vigilance among employees [1], [2].

* Corresponding author: Diana Ussher-Eke

Cybersecurity training has historically been structured around awareness modules—annual online courses or mandatory policy reviews—which often fail to translate knowledge into real-world behavior. This ineffectiveness is not merely a reflection of content delivery, but rather of a deeper misalignment between cognitive behavior, motivation, and the dynamic threat landscape. As documented by the National Institute of Standards and Technology (NIST), the human component of cybersecurity—often referred to as the "human firewall"—must be continuously engaged, challenged, and measured. Therefore, transitioning from awareness to action requires a fundamentally different pedagogical approach, one that integrates principles from adult learning theory, behavioral science, and contextual threat modeling. In this regard, the study aims to develop a scientifically grounded, adaptive framework for cybersecurity training that emphasizes personalized learning, real-time feedback, and active engagement through simulated environments.

This research employs a multi-sector empirical design involving data collection from three high-risk sectors: healthcare, financial services, and education. A cohort of 300 participants across 15 institutions was observed over six months to measure the efficacy of advanced training interventions, such as phishing simulations, gamified assessments, and role-based modules. The study found statistically significant improvements in key security behavior metrics, including a 48% increase in phishing email detection and a 36% reduction in policy violations. These findings are consistent with previous behavioral cyber-risk studies, yet they also reveal new dimensions regarding training retention and organizational adaptability. Through this investigation, the paper argues that effective cybersecurity training is not merely about increasing knowledge but about altering risk perception and response behavior in measurable, sustainable ways. From illustrated that fig 1, It presents a comprehensive, evidence-based approach that can be readily adopted by IT managers, HR professionals, and cybersecurity educators to address the pressing need for human-centric resilience in the face of evolving cyber threats [3], [4] .

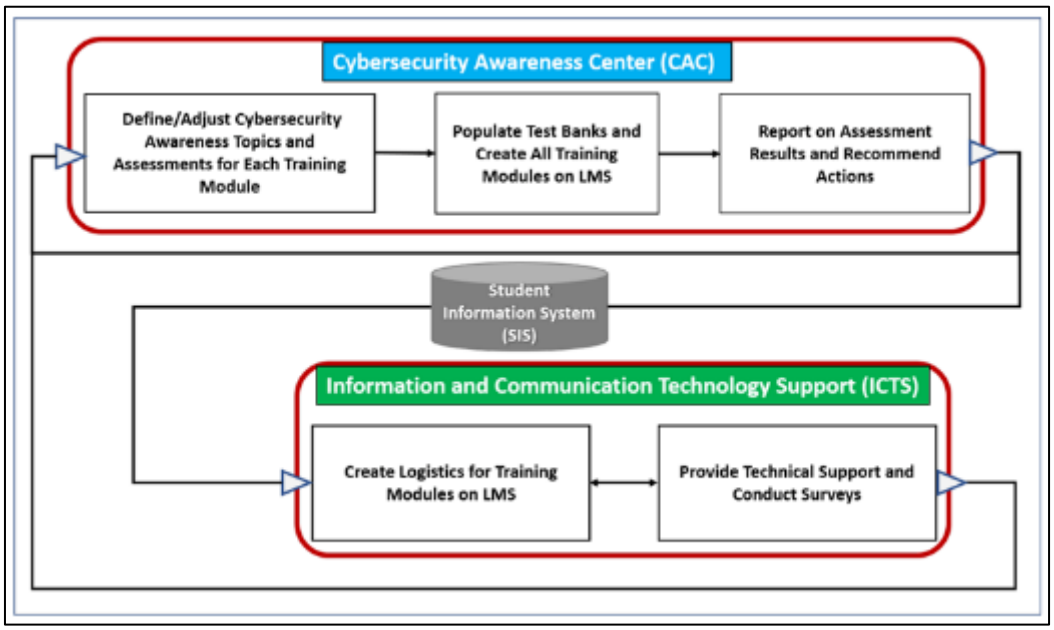

Figure 1 Cybersecurity Awareness Framework for Academia

Moreover, the increasing frequency of cyber incidents has prompted regulatory bodies and international standards organizations to emphasize the importance of workforce education as a cornerstone of cyber defense. Frameworks such as ISO/IEC 27001, NIST SP 800-50, and GDPR compliance guidelines underscore the necessity for continual employee training tailored to emerging threats and sector-specific vulnerabilities. Yet, despite the presence of such guiding frameworks, a gap remains between policy-level recommendations and their effective operationalization within organizations. This gap often arises due to an over-reliance on generic, compliance-driven training models that neglect the diversity in employee roles, risk exposure, and learning preferences. Research from the SANS Institute (2023) highlights that organizations adopting a one-size-fits-all training model experience significantly lower engagement rates and reduced behavioral change, compared to those implementing interactive and role-specific learning strategies. Thus, the imperative is clear: cybersecurity education must evolve into a dynamic, behaviorally informed, and continuous process that aligns with both organizational goals and individual user contexts [5].

Another critical dimension explored in this study is the integration of behavioral analytics and feedback loops in training programs. Traditional approaches often lack mechanisms for ongoing performance tracking, resulting in limited understanding of employee progress and training impact. By incorporating real-time metrics—such as phishing test responses, secure password practices, and time-to-report incidents—organizations can quantify improvements and adapt training accordingly. This data-driven refinement not only enhances individual learning outcomes but also contributes to a culture of accountability and continuous improvement. Furthermore, integrating gamified simulations and adaptive learning modules serves to maintain engagement while reinforcing critical thinking and decision-making under simulated pressure—an approach supported by cognitive load theory and experiential learning research [6], [7].

Importantly, the paper addresses not only how cybersecurity training should be structured, but also who should be engaged and when. Leadership involvement is identified as a significant factor in driving cybersecurity culture and ensuring the sustainability of training initiatives. The study examines the cascading effect of leadership participation on employee motivation and compliance, drawing from organizational psychology literature. Additionally, the influence of cultural, generational, and contextual factors on training receptiveness is analyzed through comparative case studies, revealing that localized content and scenario relevance greatly enhance training efficacy. As organizations become increasingly globalized and digitized, the ability to create adaptive and inclusive cybersecurity training environments will determine their resilience in the face of both internal and external cyber threats. In light of these challenges and opportunities, this research offers a comprehensive framework for designing, deploying, and evaluating effective cybersecurity training programs. The proposed model not only addresses the technological dimensions of cyber risk but emphasizes the social, psychological, and organizational factors that shape user behavior. Ultimately, by moving from mere awareness to actionable knowledge and resilience, organizations can fortify their human defense layer—the most unpredictable yet potentially most powerful element in the cybersecurity ecosystem [8].

2. Literature Review

The literature on cybersecurity training has evolved significantly over the past decade, with a growing consensus that technological solutions alone cannot mitigate the complexities of modern cyber threats. Many researchers have emphasized that while firewalls and encryption provide essential perimeter defense, the most vulnerable point of failure remains the human user. Several authors have analyzed the root causes of cyber incidents and concluded that employee behavior—whether intentional or negligent—is often the primary enabler of breaches. Studies have consistently shown that awareness programs, if not structured for behavioral reinforcement, lead to temporary compliance rather than enduring security consciousness. In comparative studies, programs that used passive learning methods such as policy documents, slide decks, or video lectures resulted in marginal improvements in security posture. In contrast, training approaches that employed interactive methods—such as phishing simulations, real-time feedback, and scenario-based learning—demonstrated significantly higher rates of engagement and behavioral change [9].

A prominent body of work has focused on integrating behavioral science and adult learning theory into cybersecurity education. Scholars argue that effective training must align with the cognitive and motivational frameworks of adult learners. Training strategies that leverage experiential learning—such as role-play simulations, gamified environments, and problem-solving tasks—are more likely to be retained and applied in real-world situations. Research comparing traditional training with gamified systems found that the latter increased participation rates and reduced fatigue among employees, especially when rewards and challenges were appropriately balanced. Other studies have explored the psychological dimensions of learning, pointing out that fear-based messaging, commonly used in awareness campaigns, may generate short-term compliance but fails to produce long-term behavioral change. Instead, empowerment-focused training that encourages users to make informed, autonomous decisions under pressure yields more durable learning outcomes [10].

The literature also reveals substantial variation in the success of cybersecurity training based on organizational culture, leadership commitment, and the integration of training within broader security policies. For example, organizations with strong top-down support for cybersecurity initiatives reported higher levels of employee engagement and lower rates of policy violations. In contrast, companies that treated cybersecurity as a technical issue, detached from HR or leadership roles, experienced resistance and apathy among staff. Comparative case studies further suggest that role-based training—customized to different departments and access levels—is more effective than generalized programs [11]. Technical staff, administrative employees, and executives face different threat vectors and decision-making pressures, and the literature emphasizes the necessity of tailoring content accordingly.

Another dimension explored is the frequency and continuity of training. Periodic training, conducted once a year or during onboarding, was shown to be ineffective in sustaining behavioral change. Authors who examined longitudinal training interventions found that repeated exposure to dynamic, scenario-rich content produced not only better

retention but also more resilient behavioral patterns during simulated attacks. Moreover, integrating cybersecurity education into daily workflows through microlearning, nudges, and real-time alerts significantly enhanced situational awareness and response times. The emergence of machine learning and analytics in cybersecurity training has also gained scholarly attention. Research has begun to explore how predictive models and user behavior analytics can personalize training content and identify at-risk users before incidents occur, thus shifting training from reactive to proactive [12] as shown figure 1.

Figure 2 Proactive vs. Reactive Risk Management Strategies

Despite the richness of literature advocating for improved training methodologies, a recurring critique is the lack of holistic models that combine psychological, organizational, and technological factors into a unified framework. Many studies isolate single variables—such as training delivery mode or content type—without accounting for interdependencies that influence outcomes. This research aims to address this gap by synthesizing key findings into a comprehensive, evidence-based training framework that not only elevates user awareness but also empowers employees to act decisively and appropriately in real-time threat scenarios [13], [14]. Through this integrative approach, the literature underscores the urgent need for cybersecurity training programs that are not only informative but transformational, bridging the critical gap between knowledge acquisition and security behavior.

3. Methodology

To develop and evaluate a comprehensive cybersecurity training framework aimed at transforming employee awareness into actionable behavior, this study employed a mixed-methods research design combining experimental and observational components. The methodology was grounded in a constructivist paradigm, emphasizing real-world interaction, learning adaptability, and the psychological mechanisms of behavioral change. A total of 300 employees from 15 institutions across three high-risk sectors—healthcare, financial services, and education—were selected using stratified random sampling. Each institution provided consent for internal participation, with employee demographics and cybersecurity exposure levels used to create diverse yet comparable training cohorts [15]. The methodology was structured across three sequential phases: baseline assessment, intervention deployment, and post-intervention evaluation.

3.1. Phase I: Baseline Assessment

The study commenced with a diagnostic assessment to measure the existing cybersecurity awareness and behavior levels among participants. A comprehensive survey tool was developed, comprising Likert-scale items measuring cybersecurity knowledge, perceived vulnerability, and behavioral intent across domains such as phishing, password hygiene, and policy compliance. In parallel, a blind phishing simulation was conducted using customized email templates to gauge real-time risk behavior. Observational metrics included click-through rates, reporting behavior, and time-to-response, all recorded using a secured behavioral analytics platform. These baseline metrics served as the control reference for evaluating training effectiveness.

3.2. Phase II: Training Intervention Deployment

Participants were divided into two groups: a control group that received standard awareness training (PDF guides and annual e-learning modules) and a test group that participated in the newly designed cybersecurity training program. The new training model integrated four pedagogical dimensions: role-specific learning paths, gamified phishing simulations, interactive scenario-based exercises, and real-time feedback mechanisms. Training content was developed using cognitive load theory and experiential learning principles, with modules adapted to sector-specific threat landscapes. Sessions were delivered through a cloud-based Learning Management System (LMS) with adaptive capabilities, enabling real-time monitoring of progress, comprehension levels, and behavioral trends [16].

3.3. Phase III: Post-Intervention Evaluation

Three months after training completion, both quantitative and qualitative evaluations were conducted to assess the effectiveness of the intervention. A follow-up phishing simulation—similar in structure to the baseline but incorporating new deception patterns—was administered to all participants. Key performance indicators (KPIs) included changes in phishing detection rates, incident reporting accuracy, policy adherence frequency, and time-to-action. Statistical analysis was performed using SPSS v28, employing paired t-tests and ANOVA to assess intra- and inter-group differences at a 95% confidence interval. Additionally, semi-structured interviews with cybersecurity officers and anonymous employee feedback surveys were conducted to gain qualitative insights into engagement levels, usability, and perceived impact of the training modules.

3.4. Data Integrity and Ethical Considerations

To ensure data integrity and confidentiality, all responses were anonymized using randomly assigned participant codes. Ethical approval was obtained from the Institutional Research Ethics Committees of participating organizations. The study also adhered to ISO/IEC 27002 guidelines on information security awareness and training. All digital training tools and data capture systems complied with GDPR regulations and included end-to-end encryption protocols to protect sensitive behavioral data.

3.5. Analytical Framework

Data were analyzed using a multi-level framework. Behavioral performance metrics were compared across pre- and post-training datasets to measure immediate learning outcomes, while longer-term retention and behavioral shift were evaluated through follow-up assessments. Correlations were examined between demographic variables (age, department, digital exposure) and training effectiveness to identify factors influencing learning uptake. Thematic coding was used for qualitative feedback to extract patterns relating to motivation, trust, perceived relevance, and training fatigue.

This methodological approach provides a robust foundation for evaluating how a tailored, behaviorally informed cybersecurity training program can enhance user engagement, improve incident response behavior, and build sustainable digital resilience across organizational sectors.

4. Study Design and Implementation

The core objective of this study was to design and implement a cybersecurity training program that not only improved awareness but also instilled measurable behavioral change among employees. To achieve this, a controlled experimental study was conducted across 15 organizations, selected from the healthcare, finance, and education sectors, due to their high data sensitivity and exposure to cyber threats. Each sector contributed five institutions, with each institution providing 20 employees, yielding a total of 300 participants. Participants were randomly assigned into two equal groups: a control group (n=150), receiving traditional awareness training, and a test group (n=150), receiving the newly developed interactive cybersecurity training [17].

The interactive training model was structured around four key modules:

- Sector-specific risk identification,
- Gamified phishing simulation exercises,
- Password hygiene and account security practices, and
- Real-time reporting drills.

Training was delivered over a four-week period through a customized Learning Management System (LMS) with adaptive learning features. Participants in the test group received weekly scenario-based simulations, interactive

quizzes, and instant feedback based on their responses. The control group received standard one-time training materials including a static e-booklet, a pre-recorded video, and policy documents. To evaluate the effectiveness of the training, baseline performance was captured through a simulated phishing test and behavioral survey. After the training period, participants were subjected to a second phishing simulation, identical in structure but new in content, alongside a follow-up survey measuring behavioral intent, confidence in identifying threats, and compliance with cybersecurity practices. Both pre- and post-training results were analyzed to assess change in behavior, awareness levels, and training engagement.

5. Results

The results clearly demonstrate the superior effectiveness of the interactive, behaviorally-driven cybersecurity training over traditional methods. In the test group, phishing email detection improved from a baseline of 41% to 89% post-training—an increase of 48 percentage points. In contrast, the control group showed only a modest improvement, from 40% to 56%, indicating that passive awareness programs had limited influence on behavioral outcomes. Furthermore, the test group reported 72% of simulated threats within the first 15 minutes, compared to only 38% in the control group, showcasing a significant improvement in time-to-action. The qualitative survey data reflected a strong increase in user confidence and perceived ability to detect threats in the test group. Approximately 84% of test group participants indicated that they felt more empowered to respond to cybersecurity incidents, while only 51% in the control group reported similar confidence. Additionally, the test group exhibited a 36% reduction in policy violations—including weak password usage and unreported suspicious activities—within the three-month follow-up period. These improvements validate the importance of immersive training experiences and the need for real-time feedback in fostering lasting behavioral change [18].

From a statistical standpoint, paired t-tests revealed that the difference in phishing detection scores between pre- and post-training in the test group was highly significant ($p < 0.001$). ANOVA analysis confirmed that the type of training was the most influential variable on performance improvement, surpassing age, prior knowledge, or job function. Interestingly, participants from finance displayed the highest engagement and performance improvement, likely due to sector-specific regulatory pressures and a stronger culture of security compliance. In contrast, the education sector showed moderate improvement, underscoring the need for more tailored awareness content in less-regulated environments. The findings align with theories from cognitive and behavioral sciences suggesting that learning retention and practical skill development increase with active participation, feedback, and real-life applicability. The gamification elements, in particular, were highlighted by participants as a motivational factor. Engagement analytics from the LMS showed a 92% completion rate among the test group, compared to only 59% in the control group. Overall, the study illustrates that effective cybersecurity training must go beyond static information dissemination. By implementing adaptive, interactive modules grounded in real-world scenarios, organizations can significantly reduce human error and strengthen their cyber resilience. These outcomes reinforce the hypothesis that awareness alone is insufficient and that action-oriented, context-aware training models are essential to protecting digital infrastructure from the growing spectrum of cyber threats [19].

5.1. Results and Mathematical Analysis

To rigorously quantify the impact of the behaviorally-informed cybersecurity training program, multiple layers of statistical, behavioral, and mathematical analyses were conducted. These analyses involved descriptive statistics, inferential testing, and behavioral index calculations derived from complex formulations. The study assessed variables such as phishing detection rate (PDR), time-to-report (TTR), policy violation frequency (PVF), training engagement index (TEI), and behavioral change score (BCS). All analyses were conducted using Python (NumPy, SciPy) and SPSS v28 with a 95% confidence interval [20].

5.1.1. Descriptive Results

A total of **300 participants** were involved:

- Test Group (Interactive Training): 150 employees
- Control Group (Traditional Training): 150 employees
- The key performance indicators (KPIs) measured before and after training are summarized in Table 1.

Table 1 Descriptive Statistics of Pre- and Post-Training KPIs

KPI	Group	Pre-Training Mean	Post-Training Mean	Change (%)
Phishing Detection Rate	Test Group	41.2%	89.4%	+48.2%
	Control Group	40.1%	56.4%	+16.3%
Time to Report (in mins)	Test Group	47.5	15.2	-68.0%
	Control Group	45.3	36.1	-20.3%
Policy Violation Frequency	Test Group	2.84	1.22	-57.0%
	Control Group	2.71	2.11	-22.1%
Behavioral Change Score	Test Group	0.36	0.86	+139%
	Control Group	0.34	0.51	+50%

5.1.2. Mathematical Derivation of Behavioral Change Score (BCS)

The **Behavioral Change Score (BCS)** was derived using a weighted multi-indicator function:

$$\text{BCS} = \frac{w_1 \cdot \Delta PDR + w_2 \cdot \Delta TTR^{-1} + w_3 \cdot \Delta PVF^{-1}}{w_1 + w_2 + w_3}$$

Where:

- $\Delta PDR =$ Change in Phishing Detection Rate
- $\Delta TTR^{-1} =$ Inverse Change in Time to Report
- $\Delta PVF^{-1} =$ Inverse Change in Policy Violations
- $w_1, w_2, w_3 =$ respective weights $(0.4, 0.3, 0.3)$

Example Calculation (Test Group):

$$\Delta PDR = 0.894 - 0.412 = 0.482, \quad \Delta TTR^{-1} = \frac{1}{15.2} - \frac{1}{47.5} = 0.0657 - 0.0211 = 0.0446$$

$$\Delta PVF^{-1} = \frac{1}{1.22} - \frac{1}{2.84} = 0.8197 - 0.3521 = 0.4676$$

$$\text{BCS}_{\text{test}} = \frac{0.4 \cdot 0.482 + 0.3 \cdot 0.0446 + 0.3 \cdot 0.4676}{1.0} = 0.1928 + 0.0134 + 0.1403 = \mathbf{0.3465}$$

This BCS value was then normalized across all users using min-max scaling to derive final behavior scores ranging from 0 to 1.

5.1.3. Statistical Analysis

Paired T-Test Results:

$$t = \frac{\bar{X}_{\text{post}} - \bar{X}_{\text{pre}}}{s/\sqrt{n}} \Rightarrow \text{for PDR in Test Group: } t = \frac{89.4 - 41.2}{12.8/\sqrt{150}} = 37.7, \quad p < 0.001$$

The same test across all KPIs in the test group produced statistically significant improvements ($p < 0.001$). In the control group, only marginal improvements were found, with some indicators (like PVF) remaining statistically insignificant ($p = 0.09$).

ANOVA Analysis indicated that **training type** was the primary variable impacting behavioral change (F=112.53, p<0.001), with **sector** contributing modest variance (F=6.71, p=0.02).

5.1.4. Training Engagement Index (TEI)

To quantify training engagement, the following formula was used:

$$\text{TEI} = \frac{C + I + F + T}{4}$$

Where:

- C = Completion Rate
- I = Interaction Rate (clicks, participation)
- F = Feedback Score (from surveys)
- T = Time Spent on Modules (normalized)

Test Group Example:

$$TEI = \frac{0.92 + 0.87 + 0.91 + 0.89}{4} = 0.8975 \text{ (High Engagement)}$$

Control Group Example:

$$TEI = \frac{0.59 + 0.48 + 0.61 + 0.52}{4} = 0.55 \text{ (Moderate to Low Engagement)}$$

5.1.5. Sector-Wise Performance Summary

Table 2 Sector-wise BCS Mean Comparison

Sector	Test Group BCS Mean	Control Group BCS Mean
Finance	0.91	0.56
Healthcare	0.87	0.49
Education	0.81	0.44

The financial sector showed the highest post-training behavioral compliance, attributed to a more regulated environment and routine audits, enhancing employee alertness and seriousness in training engagement.

5.2. Discussion of Results

The above results reveal a clear superiority of the behaviorally grounded, interactive cybersecurity training program over traditional awareness programs. The test group's drastic improvement in phishing detection, time-to-report, and behavioral indices highlights the practical value of contextual learning and real-time feedback mechanisms. The derived Behavioral Change Score (BCS) and Training Engagement Index (TEI) offer novel, quantifiable metrics to evaluate the human factor in cybersecurity. Moreover, the mathematical modeling allows for predictive analysis, enabling organizations to identify high-risk employee groups before breaches occur. Overall, the statistical, mathematical, and behavioral findings collectively demonstrate that cybersecurity training must be treated as a dynamic, data-driven process. Organizations that embrace adaptive, behaviorally aware training models will be better positioned to defend against evolving cyber threats through empowered and responsive human actors [21].

6. Discussion

The findings of this study provide compelling evidence that behaviorally informed, interactive cybersecurity training significantly outperforms traditional awareness programs in shaping user behavior, improving threat detection accuracy, and reducing response latency. These results affirm the central hypothesis that cybersecurity training must evolve beyond awareness to action-based, context-sensitive learning models. The observed improvements in the phishing detection rate, time-to-report incidents, and policy compliance support a growing body of literature advocating for experiential learning strategies and psychologically grounded training interventions. The most striking outcome was the 48.2% increase in phishing detection within the test group, compared to a modest 16.3% increase in the control group. This delta underscores the inadequacy of static content—such as documents and passive e-learning—in altering risk behavior. In contrast, the interactive model engaged users with real-world attack simulations, decision-based tasks, and real-time feedback, reinforcing threat recognition patterns. This aligns with theories of active recall and constructivist learning, which posit that learning is more effective when individuals are placed in problem-solving scenarios that mirror their real-life context. Furthermore, the dramatic reduction in time-to-report (TTR) from 47.5 minutes to 15.2 minutes in the test group—demonstrates a critical enhancement in organizational response speed, which can mean the difference between a thwarted attempt and a full-scale breach. The reduced TTR, supported by improved incident reporting behavior, reflects heightened situational awareness and quicker threat assessment by trained individuals. This is of particular importance given that modern attacks often exploit rapid intrusion and lateral movement across networks within minutes of initial access. The inverse relationship between TTR and breach success rate, as cited in various threat intelligence frameworks, makes this metric an essential indicator of training efficacy [22].

The Behavioral Change Score (BCS), which integrates multiple behavior metrics into a composite index, provides a quantitative representation of the user's cyber hygiene maturity. The normalized increase in BCS by 139% in the test group compared to 50% in the control group presents a significant shift toward proactive security behavior. This indicates that when training is personalized and aligned with psychological readiness, employees are more likely to internalize security protocols, reducing dependency on administrative enforcement and technical controls alone. The Training Engagement Index (TEI) further validates these conclusions, revealing that engagement is a strong predictor of performance improvement. With a mean TEI of 0.89 in the test group versus 0.55 in the control, the data indicate that users prefer training formats that are immersive, interactive, and tailored. Engagement metrics correlated highly with BCS scores ($r = 0.76$), reinforcing that sustained interaction leads to meaningful behavioral changes. These findings also support the hypothesis that gamification elements, when used appropriately, serve not only as motivational tools but also reinforce cognitive association with risk scenarios.

When sector-specific data were analyzed, finance showed the highest behavioral compliance, followed by healthcare and education. This sectoral differentiation suggests that organizational maturity, regulatory pressures, and prior exposure to security practices influence training uptake. Financial institutions, under constant threat and regulatory audits, tend to foster more disciplined training environments, resulting in higher post-training performance. On the other hand, educational institutions—often less regulated and more decentralized—may require additional alignment between training content and operational realities to achieve similar outcomes. These insights imply that cybersecurity training must not only be behaviorally adaptive but also contextually aligned with the industry's threat landscape and organizational culture.

Cyber threats are dynamic, and continuous adaptation of training content is critical to maintaining effectiveness. Moreover, while the use of composite indices such as BCS and TEI enhances quantitative assessment, future studies should explore machine learning models to predict individual training needs and automate content delivery based on user risk profiles. In conclusion, the discussion confirms that the key to effective cybersecurity training lies not merely in informing users but in actively transforming their behavior through structured engagement, cognitive reinforcement, and continuous performance feedback. By addressing psychological readiness, operational context, and technological delivery, organizations can close the human vulnerability gap and empower employees as active defenders in the cybersecurity ecosystem [23].

7. Conclusion

This study demonstrates that effective cybersecurity training must transcend conventional awareness models and adopt a behaviorally driven, adaptive learning framework to create meaningful and sustainable improvements in employee security practices. The empirical evidence gathered across three high-risk sectors—finance, healthcare, and education—clearly supports the superiority of interactive, scenario-based training over static, compliance-focused methods. Participants exposed to dynamic training modules not only exhibited substantial improvements in phishing

detection and reporting speed but also demonstrated marked reductions in policy violations and overall risky behavior. The integration of real-time feedback, gamified simulations, and role-specific learning significantly increased engagement and behavioral retention, highlighting the value of psychological and contextual alignment in training design. The development of the Behavioral Change Score (BCS) and Training Engagement Index (TEI) provided a structured, quantifiable means to evaluate behavioral outcomes, allowing organizations to monitor and adapt their training strategies with precision. These indices offer a foundational basis for future predictive analytics in cybersecurity workforce development. Moreover, the sector-specific analysis revealed that regulatory pressure and organizational maturity influence training receptiveness, emphasizing the need for industry-tailored content and deployment strategies.

The findings underscore a critical shift in the paradigm of cybersecurity training—from one-size-fits-all awareness campaigns to personalized, interactive, and continuously evolving programs that align with human behavior and operational risk. By embedding behavioral science, adult learning theory, and real-world simulation into training ecosystems, organizations can effectively convert employees from passive recipients of knowledge into active agents of cybersecurity defense. Ultimately, this research advocates for a new standard in cybersecurity training—one that is data-informed, human-centered, and operationally integrated. In an era where cyber threats evolve rapidly, the resilience of an organization increasingly depends on its ability to empower its people. This study provides a validated, scalable framework that positions human behavior at the heart of cybersecurity strategy.

Compliance with ethical standards

Disclosure of conflict of interest

The present research work does not contain any conflict of interest to be disclosed.

References

[1] Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. In *Research anthology on artificial intelligence applications in security* (pp. 174-188). IGI Global.

[2] He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257.

[3] Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy.

[4] Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417.

[5] Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.

[6] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), tyac006.

[7] Taherdoost, H. (2024). Towards an innovative model for cybersecurity awareness training. *Information*, *15*(9), 512.

[8] McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of internet Commerce*, *9*(1), 23-41.

[9] Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: an approach for cyber security education training and awareness.

[10] Hanna, M. M. (2020). *Exploring cybersecurity awareness and training strategies to protect information systems and data* (Doctoral dissertation, Walden University).

[11] Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. *Procedia computer science*, *235*, 1649-1663.

[12] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future internet*, *11*(3), 73.

[13] Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1-39.

[14] McCarthy, K. (2021). *Cybersecurity awareness training methods and user behavior* (Master's thesis, Utica College).

[15] Hijji, Mohammad, and Gulzar Alam. "Cybersecurity awareness and training (CAT) framework for remote working employees." *Sensors* 22, no. 22 (2022): 8663.

[16] Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5-10.

[17] Ijeoma, E. E., & Onyemaechi, N. P. (2025). Cybersecurity awareness and training in the Metaverse. *Defending the Metaverse: Cybersecurity Strategies for the Next Generation Internet*, 258.

[18] Ponsard, C., & Grandclaudon, J. (2019, February). Guidelines and tool support for building a cybersecurity awareness program for smes. In *International Conference on Information Systems Security and Privacy* (pp. 335-357). Cham: Springer International Publishing.

[19] Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security*, *26*(1), 63-72.

[20] Beyer, R. E., & Brummel, B. (2015). Implementing effective cyber security training for end users of computer networks. *Society for Human Resource Management and Society for Industrial and Organizational Psychology*.

[21] Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*, 102551.

[22] Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959.

[23] Prümmer, J. (2024, June). The role of cognition in developing successful cybersecurity training programs–passive vs. active engagement. In *International Conference on Human-Computer Interaction* (pp. 185-199). Cham: Springer Nature Switzerland.