International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I10P128

Volume 74 Issue 10, 390-402, October 2026
© 2026 Seventh Sense Research Group®

Original Article

Design and Evaluation of a User-Centric Gamified Cyber-Security Awareness Framework with Behavioral Change Impact Assessment

Biju Abraham Verghese[1], Lakshmi Sudha Kondaka[2]

[1,2]*Department of Information Security, SIES Graduate School of Technology, Navi Mumbai, Maharashtra, India.*

[1]*Corresponding Author : bijuavimeis23@gst.sies.edu.in*

Received: 26 June 2026 Revised: 08 September 2026 Accepted: 18 September 2026 Published: 27 October 2026

Abstract - *The rapid advancement of technology has resulted in increase in cybercrime activities on organization and individuals, which has intensified nowadays. Cybercrime incidents in India have sharply soared from 10.29 lakh in 2022 to 22.68 lakh in 2024, with financial losses touching ₹22,845 crore that is a 206% year on year increase. Regardless of the increase in investments of strengthening the security infrastructure, these numbers continue to increase due to ineffective management of human-related challenges. Traditional methods of conducting cybersecurity awareness sessions are unable to engage the participants, rendering such sessions ineffective. The existing solutions are developed to provide cybersecurity awareness through phishing simulations, content libraries and gamified engagement, but have several limitations. A training platform has been developed using Design Science Research methodology, incorporating skill-based segmentation training along with a comprehensive reporting mechanism highlighting the overall performance of the user and providing recommendations to enhance their approach towards real time incidents. As per the findings, knowledge gain of 30.0 percentage points in threat identification ability, a System Usability Scale score of 71.83, along with an engagement mean of 4.08 out of 5.00, confirming the platform's effectiveness as an interactive training tool.*

Keywords - *Behavioral change, Cybersecurity awareness, Design Science Research, Gamification, User segmentation.*

1. Introduction

The shift towards digital transformation has broadened the threat landscape for organizations and individuals alike, yet the human element remains the most exploited vulnerability in the domain of cybersecurity. Alkhazi et al. [1] identify that security breaches are caused due to employee's naive and accidental behaviors. Koza et al. [5] emphasizes that the human element is the most influential factor in information security incidents. According to the Ministry of Home Affairs [13], the incidents related to cybercrime in India has observed an upward trend between 2022 and 2024 while the reported incidents has substantially increased from 10.29 lakh to 22.68 lakh. Along with that the financial losses have climbed to ₹22,845 crore during the same period. Despite the increase in investments in the strengthening of the security infrastructure, these numbers continue to rise since the challenge related to the human element is not effectively addressed.

The challenge related to the human element in the domain of cyber security has two dimensions that is rarely acknowledged together. The first dimension is prevention, users and employees lack the understanding of effectively applying the lessons learnt in the security awareness sessions in real-world scenarios. The second dimension is reactive. Whenever a user becomes a victim of a cyber incident or encounters a suspicious event, they lack accessible, real-time guidance on what immediate measures need to be taken, how to preserve evidence and where to report. The second dimension is compounded by Indian context by social stigma around being scammed, according to the NITI Aayog observation that shame prevents reporting [14]. The I4C makes this crucial, while 28 lakh cases were reported in 2025, only 55,484 FIRs were filed, which indicates that the vast majority of victims receive no resolution.

The motivation behind this study is when organizations became aware that traditional cyber security awareness training is not effective enough. Since the trainers provide training sessions which the employees do not engage effectively in the training, thereby defeating the very purpose of the cyber security awareness trainings. The users or employees attend the training sessions since these trainings have become mandatory, or for the sake of achieving compliance, both the trainers and the users or employees were performing their respective roles. While the users or employees were pretending to listen to the training sessions,

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

the trainer was focussed on delivering the lessons learnt from various cyber-attacks, including the data breach incidents occurred in large organizations. It was observed that both parties did not engage effectively to understand the message that the cyber security awareness training sessions had intend to deliver. This realization resulted in understanding that user engagement plays a crucial role in determining quality of the training session delivered. Traditional cyber security awareness training heavily rely on the expertise of the trainer in creating a cultural change within the organization, as well as impacting the long-term behavior change for users or employees within the organization.

There are several existing platforms such as KnowBe4, Hoxhunt, Cofense and Cyber Ready to provide cybersecurity awareness through phishing simulations, content libraries and gamified engagement. However, these platforms have several limitations. First, they are exclusively preventive, providing no guidance either when a user becomes a victim of a cyber incident or when the user encounters a suspicious event, which can result in a future cyber incident. Second, these existing platforms evaluate the binary outcomes, such as click or report, providing no visibility into the user's decision-making reasoning or approach during a cyber incident or a suspicious event. Finally, these platforms are designed for Western enterprise contexts with no contextualization for region-specific threats such as Aadhar suspension scams, UPI fraud, or digital arrest scams prevalent in India. To bridge the revealed gaps this study examines the following research questions:

- RQ1: To measure the effectiveness of the proposed narrative-based interactive cybersecurity awareness training platform in improving user's threat identification ability and security knowledge compared to their pre-training baseline?
- RQ2: How does the skill-based routing mechanism (technical vs non-technical tracks) influence training effectiveness and user perception of content relevance?
- RQ3: To what extent does the gamified narrative-based approach with decision-tree scenarios influence user engagement and preference compared to traditional lecture-based cybersecurity awareness training?
- RQ4: How effective is the integrated analytics dashboard in enabling users to determine their capabilities, weaknesses, and refinement areas in cybersecurity awareness?

2. Literature Review

Alkhazi et al. [1] analysed the impact of various information security awareness training approaches on knowledge, attitude, and behavior using the HAIS-Q questionnaires grounded in the KAB model. According to the findings mentioned in this study, which indicate that employing multiple delivery methods to deliver the same message positively affects the user's attitude, while text-based and game-based methods exhibit stronger influence on behavioral change in comparison with other methods. Nevertheless, the assessment is heavily dependent on self-reported instruments and does not validate whether reported positive behavioral changes translate to actual user actions. Moreover, the study has not explored implementing an interactive training platform by integrating these effective methods.

Chua et al. [2] explored the impact of data breach publicity on information security awareness and determined that exposure to data breach incidents is a significant predictor which positively influences ISA in comparison with other established factors. The study suggests that organizations leveraging such publicity within their information security awareness programs can significantly improve the employee's awareness. Nevertheless, the focus of this study is limited to the statistical relationship between data breach publicity and information security awareness levels, without evaluating the training methods that can enhance and support long term adoption of security behaviors.

In an effort to bridge the gap between human risks and widely adopted security practices. Nurse et al [3] has conducted an interview with 20 CISOs and cybersecurity professionals to explore the concept of Human Risk Management. The study reveals a broad spectrum of views regarding Human Risk Management, spanning from reinterpretation of traditional security awareness training to a novel human and data-centric cybersecurity strategy. Despite the study providing such valuable insights, the proposed vision remains conceptual in nature without implementing or validating the system to support the training delivery of HRM based training to end users.

Alyami et al. [4] investigated the impact of the SETA programmes in influencing the employee behavior and determined 11 Critical Success Factors (CSF's) that affects the effectiveness of the programme through an exploratory research study. As per the findings mentioned in this study, which highlights the importance of the diverse delivery methods and thorough understanding of the audience as key influential factors for the effectiveness of the programs. However, the study does not examine the effectiveness of the delivery methods, such as gamification and interactive storytelling in achieving enhanced engagement and knowledge retention. Moreover, the participants population is constrained to participants from the Gulf nations, Middle East, US, UK, and Ireland, overlooking regions such as South Asia, where varying threat landscapes and digital literacy levels may affect the applicability of the determined CSFs.

Koza et al. [5] draws attention towards the human element, which plays a crucial role in information security, and developed the Awareness Continuum Management Model

(ACM2), which is a role based and topic-oriented approach to information security awareness training utilizing Boyd's OODA loop framework. The model mitigates heterogeneity by categorizing employees according to their roles and tailoring awareness activities to each category. The study, however, recognizes that these approaches fail to completely capture the behavioral and cognitive factors associated with human failures in the security chain, and the proposed model remains conceptual in nature, which lacks validation based on user interaction or engagement metrics.

Chaudhary et al. [6] emphasized that cybersecurity awareness expands beyond obtaining knowledge to its effective practical implementation. In addition, the study introduces a new set of indicators to assess the effectiveness of CSA programs, comprising of four factors, namely impact, sustainability, accessibility, and monitoring. The study determines that existing assessment approaches are predominantly constrained to knowledge, attitude, and behavior factors while ignoring diverse dimensions such as accessibility and stakeholder engagement. Despite the proposed metrics, which offers a well-defined approach for assessing cybersecurity awareness programs, it remains conceptual in nature which has not been validated in a functional training environment. Furthermore, the study does not address translating the cybersecurity knowledge into practical application of security related behaviors through interactive training methods.

Cletus et al. [7] have outlined an improvement to Social Engineering Awareness, Training and Education (SEATE) programs by employing innovative content, a hybrid delivery method, and a behavioral change model known as ATAC based on Stable-Quasi-Stationary Equilibrium theory. The model was evaluated by five domain experts, which yielded an average score of 73.6% and performance metrics at 92%. Although the model yielded promising results, its evaluation solely depended on qualitative expert assessment without integrating quantitative assessment with participation from end users or empirical measurements of actual behavioral change.

Fujs et al. [8] have introduced a segmentation approach for segmenting users into smaller groups based on cybersecurity competence by employing a two-step clustering algorithm on HAIS-Q questionnaire data, with the main purpose of customizing the training content as per the requirements of each user segment. The study intends to mitigate limitations, namely, lack of engagement and declining user motivation, which is widely recognized in the predominant cybersecurity education methods. Nevertheless, the model was validated on a single homogenous user group using HAIS-Q questionnaire, which is self-administered, restricting it to seven security areas, thereby constraining its applicability across wider range of diverse user segments.

Chowdhury et al. [9] proposed a personalized learning theory-based model for implementing cybersecurity training frameworks which assimilates game-based scenarios and tabletop exercises. As per the findings mentioned in this study, which reveals that the participants illustrated higher engagement when involved in the development of training exercises. Despite the framework was assessed in a controlled environment with students it does not extend to a deployable training platform for contexts tailored for heterogeneous user groups, including corporate and individuals.

Baigi et al. [10] examined several measurement instruments for technology-enhanced instructional games and confirmed that no single tool assesses all dimensions of a game simultaneously, confirming both accuracy and consistency. The review highlights widely recognized guidelines such as MEEGA+ and observes that the System Usability Scale has been prevalent for assessing digital educational games, although it was not built for this purpose. Nevertheless, the study is restricted to reviewing the existing evaluation tools without implementing a gamified training platform for cybersecurity awareness.

Arishi et al. [11] have performed a rigorous examination on cybersecurity awareness in schools. The findings as per the review highlight that the educational gaming platforms, mobile applications and personalised programs are effective for enhancing cybersecurity awareness. However, the review is restricted to school-level education and suggests customization of diverse learning needs, which lacks the development or assessment of an interactive training platform for heterogenous user groups with users having different technical backgrounds. Syafitri et al. [12] have conducted a comprehensive review to determine the critical methods for developing social engineering policy model. The gap identified in this study is that the review focuses on policy design methodology rather than implementing user engagement approaches or developing mechanisms to deliver training that can counter social engineering.

3. Research Gap

The following research gaps have been identified, and the comparison of the existing methods and the proposed system is presented in Table 1.

- Segmentation based on user background: While the research illustrates the benefits of segmentation, no training awareness platforms have implemented skill-based content adaptation. The industry still utilizes the one size fits all approach for training despite proven ineffectiveness with segmentation limited to controlled research environments.
- Gamification approach limited to studies: Research validates the effectiveness of game-based learning, but no comprehensive platform integrates games throughout security training curriculum. Proven approaches remain

in research studies with limited implementations rather than scalable production systems.

- Western centric threat examples: Most of the phishing and awareness research uses Western centric attack examples with no adaptation to regional threat landscapes. Indian specific attacks such as digital arrest, Aadhar suspension, UPI fraud and so on are absent from literature despite different threat patterns and cultural contexts.
- Analytics without Feedback, Reporting and Visualization: Current works develop evaluation metrics but lacks delivery mechanisms. There are three critical gaps that emerge. Initially, the existing systems which are utilized by the user are rewarded with a score, excluding tailored feedback based on the user's performance.

Also, these existing systems do not highlight a particular weakness which are observed based on the user's overall performance and provide recommendations to work on their weak areas. Next, these platforms, which are mentioned in the existing systems, do not provide documentation of the user's overall performance or compliance tracking of the organization's employees.

Finally, the analytics dashboard that provides visualization graphs based on the user's performance is constrained to organization rather than providing this feature to the users who are utilizing this platform for cybersecurity awareness, which enables them to reflect upon their performance and work upon their weak areas.

Table 1. Comparison of existing methods and proposed system

Gap Identified	Existing Methods	Proposed System
Segmentation based on user background	User segmentation evaluated only in a research-controlled environment without an operational implementation [8].	The segmented approach routes users to appropriate content based on the selected background, which is implemented in the functional platform.
Gamification approach	The game-based approach is validated in a controlled research environment in contrast to a functional platform [9].	Interactive decision tree games with consequence-based visualization are integrated across all modules within this functional platform.
Western Centric threat examples	The threat context associated with the western centric attack examples lacks region specific adaptation [4, 11].	The threat context for region specific scenarios like India includes UPI fraud, Aadhar suspension and digital arrest scams, which is well associated with India's cultural context.
Analytics without Feedback, Reporting and Visualization	The metrics were proposed as a theoretical framework without implementation in an operational platform [6].	A dashboard, which is user centric in nature, is provided to users which provides personalized feedback revealing the strengths and weaknesses of the user based on their performance in the training and provides remediation measures to work upon their weak areas.

4. Research Methodology

The methodology adopted for this study is Design Science Research Methodology [15, 16] since a novel artifact is created to address the challenges faced in the traditional cybersecurity awareness training. To determine whether the novel artifact created can effectively address the challenges faced in the traditional cybersecurity awareness training, this research methodology was adopted since this methodology involves evaluating the effectiveness of the novel artifact created.

Although there are other methodologies that can be used for this study, such as case study, survey or experimental research but these methodologies cannot determine the effectiveness of the novel artifact as well as address the gaps in the traditional cybersecurity awareness training accurately.

Since case study research methodology focusses on in-depth investigation of real-world context from multiple data sources, here in this study, there are multiple case studies which are in the form of narrative stories gathered from real-world context. Hence, the case study methodology may not be suitable for this study. The survey research methodology collects large-scale data through questionnaires or statistical analysis, which is mainly used for measuring the existing state this methodology does not involve building the novel artifact and evaluating the effectiveness of the novel artifact. Hence, the survey research methodology is not suitable for this study. The experimental research will be used within this approach. Therefore, this methodology will be the most effective research methodology for this study.

The problem was identified by observing the inefficiencies of the conventional cyber security awareness training in a corporate environment. The objectives were defined for implementing an interactive training platform which delivers content using narrative-based storytelling approach, integrating segmentation of users based on the technical background, which redirects them to their appropriate content tracks, providing consequence-based

visualization through interactive decision tree games, Scenarios specific to India based threat landscape and analytics dashboard for users. The details regarding the design and development of the proposed platform are described in the system architecture and design section. The assessment was conducted using a proof-of-concept approach.

The assessment was performed as a proof-of-concept evaluation by simulating 15 user profiles, which was created to demonstrate real world behavioral and demographic distributions for the technical and non-technical segments. There are five characteristics which were taken into account, such as age group, academic status, occupational background, earlier involvement in cybersecurity awareness training, and past exposure to cyber fraud. These characteristics were chosen to reveal the diversity of a common end-user population in contrast to a desirable category. The questionnaire answers for each persona were formulated based on the characteristics of that profile. The user segment attributed by an information technology background, along with earlier training were assigned a higher baseline threat identification compared to the user segment with a non-information technology background and no training experience were modelled with a lower baseline.

An individual-level uniformity parameter was incorporated to maintain a consistent response within each scale for a given persona, thereby revealing the behavioral pattern of an individual to respond to similarly associated items. The authenticity of the simulated distributions is maintained based on the constructed responses, which were aligned to user behavioral trends as mentioned in the existing literature. The evaluation was conducted using multiple instruments, such as scenario-based assessment of threat identification, which was performed at before and after interaction stages, the System Usability Scale [18] for measuring the usability of the system and customized Likert-scale questionnaires to evaluate post-training knowledge, engagement with the platform, dashboard relevance and confidence in handling incidents. The scores of pre-assessments and post-assessment scenarios were documented as correct or incorrect responses and converted into percentage scores.

The responses of the Likert-scale items were measured on a five-point scale. Cronbach's Alpha was used to verify the internal consistency of each questionnaire scale, and the collected data were described using mean and standard deviation. Inferential statistical tests were not employed since the data originated from simulated profiles rather than obtaining data from human participants. Hence, descriptive analysis was deemed suitable for the first cycle proof-of-concept evaluation in Design Science Research.

The indicators used to perform statistical analysis are defined as follows. Equation (1) was used to compute the mean of each item, and Equation (2) represents the spread of scores using the sample standard deviation. The score of the System Usability Scale was assessed using Equation (3). The Cronbach's alpha is used to measure the reliability of each questionnaire scale, which is derived using Equation (4).

$$\bar{x} = 1/n \ \sum_{i=1}^{n} x_i \tag{1}$$

$$s = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - x)^2} \tag{2}$$

$$SUS = 2.5 \times \left(\sum_{odd(x_i-1)} + \sum_{even(5-x_i)} \right) \tag{3}$$

$$\alpha = \frac{k}{k-1} \left(1 - \left(\sum_{i=1}^{k} \sigma_i^2 \right) / \sigma_t^2 \right. \tag{4}$$

5. Contributions

5.1. User Background-Oriented Segmentation

The proposed system has built a mechanism that redirects the users to the appropriate modules based on the background selected by the user, such as technical users and non-technical users, where the technical users will able to engage all modules present in the platform, whereas non-technical users will be able to engage in modules which are designed specifically for them, thereby transitioning towards practical deployment, which was constrained to research studies.

5.2. Consequence-based Visualization

The proposed system fills the gap between knowledge and behavior using branching narrative simulation games, indicating the direct consequences of the choices made by the user with respect to the security context in a simulated real world like environment, translating from evaluation of knowledge acquired to measurement of behavioral change from information security standpoint.

5.3. Indian Threat Landscape Adaptation

The proposed system specifically adapted for Indian specific threat related landscape, including Aadhar suspension scams, UPI fraud scenarios, and PAN card phishing, with culturally contextualized examples.

5.4. Integrated Analytics System

The proposed system provides a comprehensive analytics framework with three components. First, the personalized performance feedback with module-level breakdown and recommendations. Second, multi-stakeholder reporting mechanisms for users and organizations. Finally, a visual analytics dashboard with five design principles for intuitive performance comprehension.

6. System Architecture and Design

6.1. System Overview

The Overview of the System Architecture is shown in Figure 1. The user is required to provide the required details

in the registration page, such as Name, Age, email ID, password for login and role. The role is a dropdown menu which has two background options, which are technical and non-technical. Once the user has registered, the user needs to sign in to the website. The user will enter the login credentials in the login page, where the website platform will redirect the user to the content based on the background option selected. The Technology stack is mentioned in Table 2. For users who have selected the non-technical background role, will be provided the content related to their non-technical role whereas user who selected the technical background role will be provided the content related to their technical role. The user can choose from various topics provided by the platform based on the role selected by the user. These topics follow a narrative-based storytelling approach, which are events that can be suspicious, resulting into a cyber incident or fraud at the end of the story, the users will be equipped with the knowledge to protect themselves by enabling the users to spot the red flags from such scams or cyber incidents and report them to the relevant authorities in future. Once the user has completed a particular topic, the user will be required to play a game to test the effectiveness of the knowledge gained from the training. The game will display the end result of the consequences based on the choices selected by the user. The end result will also include the remediation steps, which equip the user to handle cyber incidents or scams in the future.

Table 2. Technology stack

Component	Technology / Tool
Backend Development	Node.js
Frontend Development	React.js
Database	MongoDB
PDF Generation	jsPDF
Development Environment	Visual Studio Code

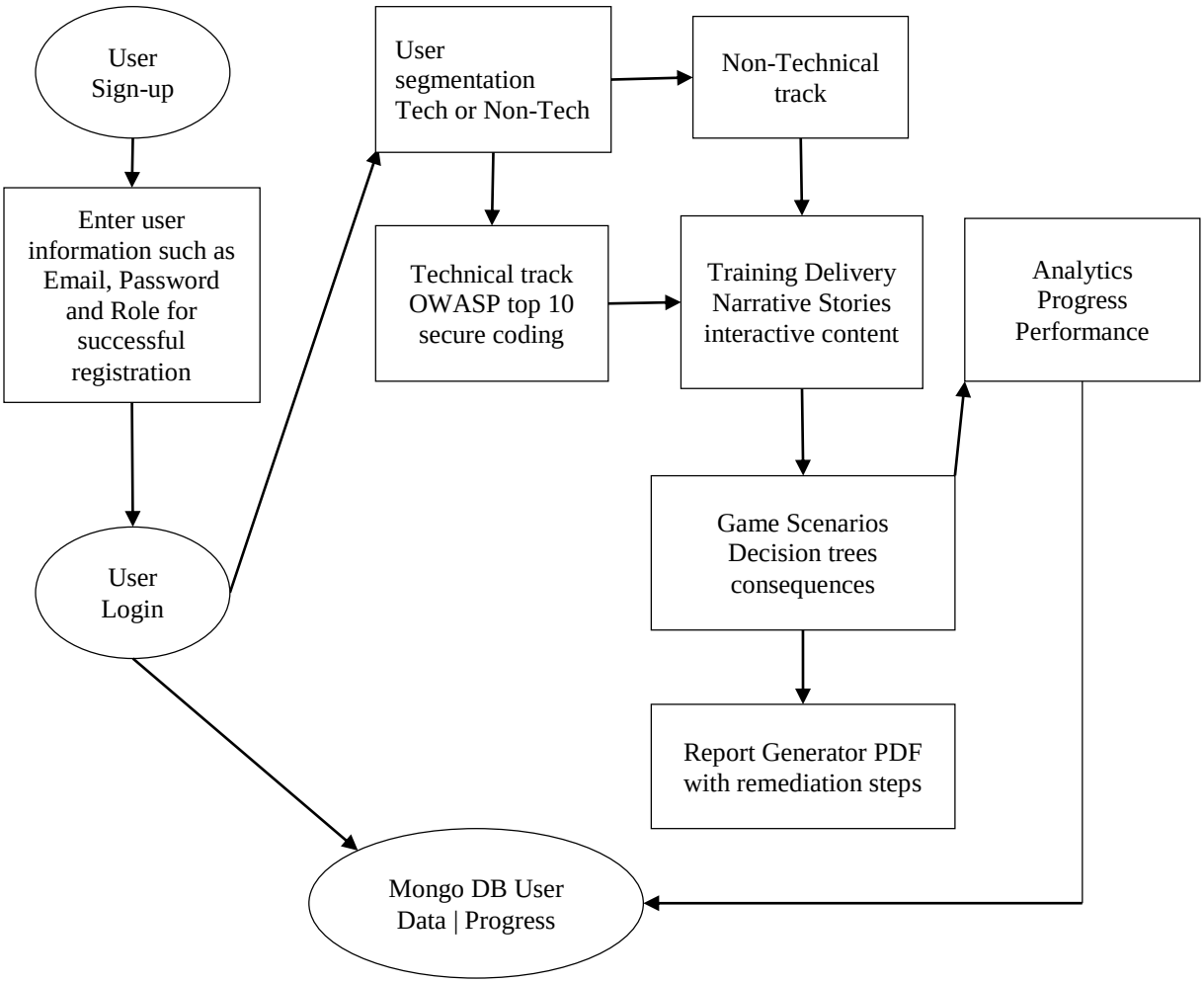

Fig. 1 The overview of the system architecture

6.2. User Segmentation

The segmentation of users is done based on their backgrounds, which are technical users and non-technical users. The users who opted for the technical segment have access to OWASP Top 10 - related sessions combined with non- technical sessions.

Whereas the non-technical segment includes various types of phishing attacks, various types of methods where the cyber criminals can exploit the physical security of the organization, data security awareness from a non-technical perspective, promoting awareness regarding secure online behavior, handling incident response on a personal level as well as organization level, deepfakes and various types of impersonation techniques used by cyber criminals to deceive victims.

6.3. Narrative Approach

The main intention of selecting this approach is to enhance the user engagement, which is lacking in traditional cyber security awareness training. The narrative approach ensures that the users are engaged as the events described in the story are inspired by real life events related to cyber incidents in the digital era. A website platform with the right visuals and animations can convey the cybersecurity awareness topics in an interesting manner, thereby effectively engaging the users.

6.4. Game Mechanics

In the game-based scenario, the user is required to distinguish between two scenarios presented before them. The user is required to identify which scenario is a legitimate event and which scenario is a cyber incident or scam. The game mechanics used in this website platform is a decision tree model based on the choices selected by the user. The story changes with two outcomes either the user becomes the victim of the cyber incident or effectively tackles the cyber incident or scam.

In the legitimate scenarios, the platform provides a gentle nudge to the user to report the incident gradually and take extra precautions, promoting a security-conscious culture.

7. Results

The results section demonstrates the assessment of the results based on the proof-of-concept performed using 15 simulated profiles of the user. The proposed system was tested functionally to verify whether all the components had performed properly as anticipated. The user profiles that were simulated depict the practical demographic and behavioral distributions throughout the technical and non-technical user segments.

These user segments were then utilized to predict the expected responses from the users. Based on the characteristics of the user profiles, the questionnaire responses were generated for each user profile, which are then calibrated against the findings from the existing literature.

7.1. Internal Consistency

Cronbach's Alpha was used to examine the internal consistencies of the questionnaire scales. The reliability coefficients are presented in Table 3 below.The reliability of the questionnaire instruments has concluded with an excellent internal consistency across all scales where the reliability coefficients are greater than 0.93 ($\alpha > 0.93$).

Table 3. Cronbach's alpha reliability coefficients

Scale	Items (k)	n	α	Interpretation
Pre-Assessment IR (IR1-IR5)	5	15	0.935	Excellent
Post-Knowledge (K1-K7)	7	15	0.946	Excellent
SUS (U1-U10)	10	15	0.942	Excellent
Engagement (G1-G7)	7	15	0.937	Excellent
Dashboard (AD1-AD7)	7	15	0.950	Excellent
Incident Confidence (IC1-IC8)	8	15	0.947	Excellent

7.2. Pre-Assessment Baseline

Before using this platform, the participant's abilities, such as identifying cyber threats and awareness regarding responding to cyber incidents, were examined.

The score of the pre-assessment scenario was 47.78% (SD = 19.79), and the mean of the incident response awareness was 2.28 on a 5-point scale with a standard deviation of 0.67, showing that the baseline level was moderate with further opportunities for enhancement. In the pre-assessment scenario, the technical users scored higher than the non-technical users, having scores of 57.14% and 39.58% respectively, thereby highlighting the foreseen gap of knowledge which is based on the professional background.

7.3. Post-Training Knowledge Gain (RQ1)

The scores of the pre-post scenario and the knowledge gain by the user segment is presented in Table 4 below. In general, the knowledge gain was 30.0 in percentage points. The non-technical users have outperformed with a higher gain of 35.4 pp in comparison with the technical users, which is 23.8 pp, which is in line with a lower baseline, providing a broader scope for progress among non-technical participants. The below mentioned Table 5 represents the scores of the

post-training knowledge assessment (K1 - K7). On the whole, the mean of the post-training knowledge was 3.85 on a 5-point scale. Amongst all the items from K1 to K7, the highest rated items are K1 (phishing identification) and K4 (India-specific scam awareness), where both the rated items are having a mean of 3.93(M = 3.93). Also, amongst all these items, the lowest-rated item was K6 (preparedness), which has mean of 3.60. Based on the observation of Table 5, the technical users (M = 4.06) have scored regularly higher than the non-technical users (M = 3.66).

Table 4. Pre-Post scenario scores by user segment

Segment	Pre (M ± SD)	Post (M ± SD)	Gain (pp)
Overall (n=15)	47.78% ± 19.79	77.78% ± 13.61	**+30.0**
Technical (n=7)	57.14% ± 16.27	80.95% ± 17.81	**+23.8**
Non-Technical (n=8)	39.58% ± 19.79	75.00% ± 8.87	**+35.4**

Table 5. Post-Training knowledge assessment (K1 - K7)

Item	Tech (M±SD)	Non-Tech (M±SD)	Overall (M±SD)
K1 - Phishing identification	4.14 ± 0.38	3.75 ± 0.71	3.93 ± 0.59
K2 - Social engineering	4.00 ± 0.58	3.75 ± 0.71	3.87 ± 0.64
K3 - Deepfake awareness	4.00 ± 0.58	3.38 ± 0.52	3.67 ± 0.62
K4 - India-specific scams	4.14 ± 0.38	3.75 ± 0.71	3.93 ± 0.59
K5 - Consequence awareness	4.14 ± 0.69	3.62 ± 0.52	3.87 ± 0.64
K6 - Preparedness	3.71 ± 0.76	3.50 ± 0.53	3.60 ± 0.63
K7 - Track appropriateness	4.29 ± 0.49	3.88 ± 0.64	4.07 ± 0.59
Overall	4.06 ± 0.47	3.66 ± 0.55	3.85 ± 0.54

7.4. Skill Track Appropriateness (RQ2)

The reported relevance of the skill-based routing was measured by means of the item K7. The appropriateness rating of the technical users track has a mean score of 4.29, along with a standard deviation of 0.49, whereas the non-technical users track has an appropriateness rating with a mean score of 3.88, along with a standard deviation of 0.64, on a 5-point scale, respectively. The routing rates reported for both the user segments has exceeded the scale midpoint of 3.00, which reveals that the users in both tracks have observed that the content within their segment is appropriate based on their background.

7.5. Platform Usability and Engagement (RQ3)

The proposed system was evaluated using a System Usability Scale (SUS), where this system has obtained an SUS score of 71.83 with a standard deviation of 13.45 that is in line within the good usability range determined by Bangor et al. [18], thereby surpassing the industry benchmark of 68. The aggregate engagement mean score obtained was 4.08 on a 5-point scale with a standard deviation of 0.51. Amongst other items, G4 has been rated the highest with a mean of 4.33. Both items, G2 (decision tree visualization) and G7 (active participant), have obtained identical scores of 4.27. The item G5 was rated the lowest with a mean score of 3.60.

Table 6. System usability scale item scores (U1 - U10)

Item	Type	Mean	SD
U1- I would like to use this platform frequently	Positive	3.53	0.52
U2- I found the platform unnecessarily complex.	Negative	1.87	0.64
U3- I thought the platform was easy to use	Positive	3.73	0.46
U4- I would need technical support to use this platform	Negative	2.07	0.70
U5- The various functions were well integrated	Positive	3.80	0.68
U6- There was too much inconsistency	Negative	1.87	0.74
U7- Most people would learn to use it very quickly	Positive	3.80	0.77
U8- I found the platform very cumbersome to use	Negative	2.13	0.64
U9- I felt very confident using the platform	Positive	3.73	0.70
U10- I needed to learn a lot before I could get going	Negative	1.93	0.70
Overall, SUS Score		71.83	13.45

Table 6, mentioned above, represents the System Usability Scale results.

Table 7, mentioned below, summarizes the engagement scores.

Table 7. Gamification and engagement scores (G1 - G7)

Item	Mean	SD
G1 - Storytelling made topics interesting	4.00	0.65
G2 - Decision tree helped visualize consequences	4.27	0.46
G3 - Challenges motivated completion	3.87	0.74
G4 - Seeing both outcomes were valuable	4.33	0.62
G5 - Visuals helped understanding	3.60	0.51
G6 - Prefer gamified over lecture-based	4.20	0.68
G7 - Felt like active participant	4.27	0.46
Overall Engagement	4.08	0.51

7.6. Analytics Dashboard Evaluation (RQ4)

Table 8 provides an overview of the evaluation scores of the analytics dashboard, which is mentioned below. The analytics dashboard element has obtained a mean score of 3.85 on 5-point scale with a standard deviation of 0.64.

The items with strongest ratings are AD2 (graphs easy to understand) and AD3 (Progress bar tracking), where each item has obtained an identical mean score of 4.00. The lowest mean score of 3.60 was obtained by AD7 (motivation to revisit weak modules).

Table 8. Analytics dashboard evaluation (AD1 - AD7)

Item	Mean	SD
AD1 - Performance display clarity	3.93	0.70
AD2 - Graphs easy to understand	4.00	0.76
AD3 - Progress bar tracking	4.00	0.76
AD4 - Strengths and weaknesses identified	3.87	0.74
AD5 - Actionable recommendations	3.67	0.72
AD6 - Scoring fairness	3.87	0.74
AD7 - Motivated to revisit weak modules	3.60	0.63
Overall Dashboard	3.85	0.64

7.7. Incident Handling Confidence Improvement

The summary of the post-training incident handling confidence scores for each item is provided below in Table 9.

Table 9. Incident handling confidence scores (IC1 - IC8)

Item	Mean	SD
IC1 - Know exact steps after fraud	3.07	0.59
IC2 - Know relevant reporting authorities	3.13	0.64
IC3 - Preserve evidence	2.93	0.70
IC4 - Comfortable reporting without stigma	3.40	0.63
IC5 - Identify further exploitation paths	2.93	0.70
IC6 - Guide a friend or family member	3.00	0.65
IC7 - Assess whether event is suspicious	3.33	0.72
IC8 - Timeline sensitivity for reporting	2.80	0.56
Overall IC Mean	3.08	0.56

The items IC4 (Comfortable reporting without stigma) and IC7 (Assess whether event is suspicious) have scored the highest with a mean score of 3.40 and 3.33 for each, respectively. Meanwhile, the item IC8 (Timeline sensitivity for reporting) received the lowest mean score of 2.80, while the items IC3 (Preserve evidence) and IC5 (Identify further exploitation paths) both have equal mean scores of 2.93. Table 10 provides an incident handling confidence comparison of pre-assessment and post-assessment.

The results of the simulated evaluation are based on the below Table 10, which demonstrates a gain of positive 0.80 on a 5-point scale with the pre-assessment mean increasing from 2.28 (SD = 0.67) to post-assessment mean of 3.08 (SD = 0.56). The findings indicate meaningful progress, but the moderate post-training score of 3.08 reveals that training enhances the foundational confidence, which may not be fully sufficient to prepare the users for handling real-world incident handling tasks without additional support structures.

Table 10. Pre assessment and post assessment for incident handling confidence

Metric	Mean	SD
Pre-Assessment IR Mean (IR1-IR5)	2.28	0.67
Post-Assessment IC Mean (IC1-IC8)	3.08	0.56
Improvement	0.80	-

8. Discussions

The evaluation findings in this section are analysed in relation to the four research questions, which is followed by the discussion of practical implications and limitations. The study utilizes the simulated user profiles, which is calibrated against the existing literature that is aligned with the first cycle of Design Science Research evaluation practices [15, 16].

8.1. Training Effectiveness and Skill Routing (RQ1, RQ2)

The results of the simulated assessment demonstrate the performance of the proposed system's approach, indicating a 30.0 percentage points in the knowledge gain of participants from 47.78% to 77.78%. In comparison with the existing cybersecurity awareness training approaches, the recorded enhancement is substantially large. For instance, the Microsoft 2023 Digital Defense Report documented that the video-based training was associated with the result of 3% reduction in phishing click rates [19]. Additionally, the non-technical users had achieved a greater learning gain in comparison with the technical users, where the percentage points achieved by both are 35.4 and 23.8 percentage points, respectively. This observation aligns with Alkhazi et al. [1], who point out that the security breaches originate from the user's naive behavior due to insufficient recognition of threats, and inexperienced decision making is the result of these underlying security breaches. Therefore, the proposed system's approach is very effective for strengthening the security awareness of the users who are vulnerable to social engineering attacks.

The proposed system has demonstrated the improvement, which can be characterized based on the three decisions regarding the design compared to the existing state-of-the-art approaches. First, the traditional platforms, including KnowBe4, Hoxhunt and Cofense, mainly depend upon passive content delivery and phishing simulation campaigns. These methods examine the accuracy of users to respond to simulated phishing attacks without providing any insight into the rationale behind the user's decision.

Rather, the proposed system adopts the branching narrative scenarios method, which enables the users to observe the direct consequences of their choices and encourage active decision making. This practice-oriented approach supports the observation of Alkhazi et al. [1] that game-based methods result in achieving greater behavioral impact compared to the text-based delivery. This mechanism also explains the knowledge gain of 30.0 percentage points in comparison with the marginal enhancements observed for passive video-based training [19]. Next, the user-based segmentation mechanism routes the technical and non-technical users to the appropriate content based on the background selected by the user. The segmentation method proposed by Fujs et al. [8] groups the users based on the security performance, which was achieved by using a two-step clustering algorithm on HAIS-Q questionnaire data. This method was represented as a segmentation approach for classifying the users, while the proposed system builds upon this concept to deliver the appropriate content based on the background of the user. The non-technical users demonstrated a higher gain (35.4 percentage points) compared to the technical users (23.8 percentage points), which reveals that the appropriate content can improve the knowledge baseline of the group which are more vulnerable to social engineering, a result which cannot be achieved by the generic one-size fits all training approach.

Finally, the traditional platforms are developed specifically for the Western enterprise contexts and does not effectively address the context related to the region-specific threats. This limitation identified in the traditional platforms, which is addressed by the proposed system by integrating threats related to the Indian region-specific scenarios into the training content of the proposed system, which is a demonstrable merit for the target population. The item K4 (M = 3.93) has obtained the highest post-training score, which emphasizes that contexts with culturally grounded scenarios translate to effective engagement with the participants. This observation reinforces the contribution of the Indian specific design training, including scenarios which involves Aadhar and PAN card-related scams, phishing which utilizes typo squatting approach and digital arrest scams, promoting situational relevance, which is typically not captured by the Western-centric training content. The K6 item has received the lowest score, which aligns with the contribution of Chaudhary et al. [6] that converting knowledge into behavioral confidence requires continued reinforcement, which extends beyond initial training exposure.

The routing mechanism reveals a high degree of alignment with the skill levels of participants, as mentioned in K7 scores of 4.29 for technical users and 3.88 for non-technical users. The findings reveal that the proposed system effectively identifies the content that needs to be delivered based on the user expertise. This observation aligns with the contribution of personalized learning framework by Chowdhury et al. [9], by exhibiting practical system-level implementation. The lower rating from the non-technical users may be explained due to the heterogenous nature of their education and technical background.

8.2. Platform Experience: Engagement and Dashboard (RQ3, RQ4)

The platform demonstrates usability at acceptable levels and productive user engagement, which is confirmed by the engagement mean of 4.08 on a 5-point scale, along with a System Usability Score of 71.83. The G4 item is rated the strongest amongst other items ranging from G1 to G7, with a mean score of 4.33, which reinforces the effectiveness of the dual path decision tree-based design and highlights the effectiveness of the consequence-based visualization approach has a significant potential to experiential learning in digital cybersecurity education.

The findings, as mentioned in this study, indicate a significant contribution to the literature by applying the principles of experiential learning, which was demonstrated in the escape room environments by Papaioannou et al. [17], into adaptable digital platform. Moreover, the items G7 and G6 has exhibited a strong performance with a mean score of 4.27 and 4.20 each respectively, which reveals that the platform facilitates an interactive engagement and active participation, thereby addressing concerns related to traditional cybersecurity awareness programs highlighted by Alyami et al. [4]. The dashboard has achieved an overall mean of 3.85. Progress bar tracking (AD3, M = 4.00) feature has scored the highest, while the AD7 (Motivated to revisit weak modules) item has scored the lowest with a mean of 3.60. The findings reveal that the gap users recognize the value of the feedback, which does not result into the user taking the corrective action.

This insight is consistent with Koza et al. [5] argument regarding the human element being the most influential factor in the domain of cybersecurity. A major contribution of the proposed system is the analytics dashboard feature, which is accessible to the individual users enrolled in this platform, which differs from the existing platforms, including KnowBe4 and Hoxhunt, where the analytics feature is reserved for the leadership, in contrast to individual users.

8.3. Incident Handling Confidence

The findings indicate a notable improvement in the confidence of participants for handling incidents, which is based on the pre-assessment and post-assessment mean scores increasing from 2.28 to 3.08. However, the mean scores of pre- and post-assessments demonstrate a fair improvement, which signifies that there is more scope for further improvement.

The findings also imply that additional interventions such as reinforced learning and exposure to real-world scenarios is required to achieve higher level of confidence in handling incidents. The item IC8 is the lowest rated item in the incident handling confidence category, which reveals a weakness in the understanding of the participants regarding the reporting timelines, which requires more attention in future training platforms or programs.

8.4. Practical Implications

From individual users and organizations' perspective, the proposed system provides a feature that automates the allocation of users to the relevant content from an information security awareness perspective, which is based on the type of skillset selected by the users, thereby eliminating the burden of manually assigning the users based on their skillset.

The analytics dashboard, which is incorporated into the proposed system, to provide insight to the users regarding their security maturity and highlights their strengths and weaknesses with recommendations for further improvement. From the Indian context standpoint, the proposed solution addresses the gap which no existing literature and commercial solutions have addressed.

The study has identified this gap and addresses this gap by. Taking into account that the cybercrime incidents in India has soared from 4.52 lakh in 2021 to 28.15 lakh in 2025 [13]. Therefore, the solutions that offer relevant content for prevention training highlights the criticality for this requirement.

8.5. Limitations and Future Work

The study acknowledges the limitations present in the proposed system. Initially, the assessment had utilized simulated user profiles, which were calibrated against the existing literature that is in line with the first cycle of DSR evaluation practices [15, 16]. The evaluation of users in the real world is planned for future iterations. Furthermore, the assessment records, the immediate post-training results, and the follow-up studies are required to measure retention over weeks and months, which would provide stronger evidence of ongoing impact.

Additionally, the average post-training incident handling confidence rating (M = 3.08) recommends that training may not fully equip the users to face the real-world incident handling tasks, which need to be extended in future work. Finally, the participant samples must be large and heterogeneous, representing multiple organization and geographic regions within India. In spite of all these mentioned limitations the proposed system provides a foundation for cybersecurity awareness platforms featuring an interactive narrative-based storytelling along with Indian specific context, skill-based segmentation of user’s and a user centric analytics framework.

9. Conclusion

In this study, a training platform has been designed and implemented which not only enhances the user engagement but also routes them to the context based on the user's expertise. From the review of the existing literature and tools, it was found that the user segmentation was limited to studies which has been implemented in the proposed system including

a comprehensive reporting mechanism. The comprehensive reporting mechanism not only provides real time feedback to the user after completing game-based scenario challenge but also provides a report of the overall assessment of their strengths and weaknesses based on their performances in this challenge. The proposed system also provides recommendations to improve upon their weaknesses thereby creating a security conscious culture along with positively influencing the user's long term behavior regarding handling digital assets from information security perspective. The training platform has achieved both functional usability and meaningful engagement. The Future work must explore ways to design implement technology that can be engaging towards a large audience. The Future work may also explore ways to integrate regional based context within the platform including information security related concerns faced by various industry sectors. The Future work can find ways to integrate AI into the training platform to assist users to handle cyber incidents or suspicious events effectively. The Future work must evaluate the proposed system that must deployed in the real-world environment.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

This research received no external funding; However, the researchers utilized the laboratories of the organization for their research.

Acknowledgements

The authors would like to acknowledge SIES Graduate School of Technology for providing the academic support for this research.

References

[1] Bader Alkhazi et al., "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132-132143, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Hui Na Chua, Jia Sheng Teh, and Anthony Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness using Hierarchical Regression," *IEEE Access*, vol. 9, pp. 121759-121770, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jason R.C. Nurse, Joanna Milward, and Oz Alashe, "From Security Awareness and Training to Human Risk Management in Cybersecurity," *HCI for Cybersecurity, Privacy and Trust: 7th International Conference, HCI-CPT 2025, Held as Part of the 27th HCI International Conference, HCII 2025*, Gothenburg, Sweden, vol. 15814, pp. 86-104, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Areej Alyami et al., "Critical Success Factors for Security Education, Training and Awareness (SETA) Programme Effectiveness: An Empirical Comparison of Practitioner Perspectives," *Information and Computer Security*, vol. 32, no. 1, pp. 53-73, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Erfan Koza, *Information Security Awareness and Training as a Holistic Key Factor-How Can a Human Firewall Take on a Complementary Role in Information Security?*, Human Factors in Cybersecurity, vol. 53, pp. 49-57, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas, "Developing Metrics to Assess the Effectiveness of Cybersecurity Awareness Program," *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1-19, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Azaabi Cletus, Benjamin Weyory, and Alex Opoku, "Improving Social Engineering Awareness, Training and Education (SEATE) using a Behavioral Change Model," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 5, pp. 606-613, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Damjan Fujs, Simon Vrhovec, and Damjan Vavpotič, "Know Your Enemy: User Segmentation based on Human Aspects of Information Security," *IEEE Access*, vol. 9, pp. 157306-157315, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Nabin Chowdhury, and Vasileios Gkioulos, "A Personalized Learning Theory-based Cyber-Security Training Exercise," *International Journal of Information Security*, vol. 22, no. 6, pp. 1531-1546, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Seyyedeh Fatemeh Mousavi Baigi et al., "Evaluation Tools for Digital Educational Games: A Systematic Review," *Acta Medica Iranica*, vol. 60, no. 8, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Abdulrahman Abdullah Arishi et al., "Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 12, pp. 467-478, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Wenni Syafitri et al., "Methodological Review of Social Engineering Policy Model for Digital Marketing," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1, pp. 874-885, 2025. [CrossRef] [Publisher Link]

[13] Scroll Staff, Indians Lost Rs 22,845 Crore to Cyber Fraud in 2024, a 206% Rise from Previous Year: Centre, Gift Membership, 2025. [Online]. Available: https://scroll.in/latest/1084796/

[14] Sadhna Singh, Digital Arrest: The Modern-Day Cyber Scam, NITI Aayog, Government of India, 2024. [Online]. Available: https://www.niti.gov.in/node/1642

[15] Alan R. Hevner, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75-105, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ken Peffers et al., "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45-77, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[17] Thanos Papaioannou, Spyridon Eftychios Kokotos, and Aggeliki Tsohou, "Educational Escape Rooms for Raising Information Privacy Competences: An Empirical Validation," *International Journal of Information Security*, vol. 24, no. 3, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Aaron Bangor, Philip Kortum, and James Miller, "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale," *Journal of Usability Studies*, vol. 4, no. 3, pp. 114-123, 2009. [Google Scholar] [Publisher Link]

[19] Microsoft, Microsoft Digital Defense Report 2023, Microsoft Corporation, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2023