[1]Syahida Hassan
[2]Mohd Saffuan Che Mansor
[3]Rahayu Ahmad
[4]Suzana Zambri
[5]Rohaya Dahari
[6]Ayie Purbasari
[7]Miftahul Fadli

Critical Success Factors for Implementing Cybersecurity Awareness Programs in Organisations

Abstract: This study explores the critical success factors that influence the effectiveness of cybersecurity awareness training in four middle and large organisations. Using a qualitative case study approach, data were collected through interviews, focus groups, and document reviews. The study identified five key factors that contributed to program success: leadership support, experiential learning, clear communication, emotional engagement, and continuous evaluation. These factors varied across the organisations, leading to different levels of training effectiveness. In addition, Fogg's Behaviours Model was used to help interpret whether the training efforts led to actual behaviour change. We found that in the more effective programs, such as those that used simulations, elements like emotional content and hands-on activities supported this pattern, aligning with the components of Fogg's model (motivation, ability, and trigger). This study contributes practical insights for improving cybersecurity awareness training by showing what factors matter most in real settings. It also highlights areas that are still lacking, such as tailored content, cultural relevance, and consistent reinforcement, which should be considered in future program design.

Keywords: Cybersecurity awareness training, Behavioural Change, Phishing simulation

I. INTRODUCTION

Cyber threats continue to escalate in frequency and sophistication, posing serious risks to organisations of all sizes. Cyber breaches and ransomware incidents regularly disrupt business operations and expose sensitive data [1]. No industry is immune, as threats range from corporate data theft to sabotage of critical infrastructure. The consequences include significant financial losses and threats to public safety. Notably, the human factor remains a crucial vulnerability, with approximately 74% of data breaches involving human error, such as falling victim to phishing scams or misconfiguring systems [1]. Attackers frequently exploit social engineering and user mistakes to bypass even robust technical controls. Thus, the lack of effective cyber education addressing human behavioural factors presents a substantial challenge to maintaining cybersecurity. Strengthening the human element through education and cybersecurity awareness has become essential for building cyber resilience [2].

Past research highlights that cybersecurity training programs should be dynamically oriented toward individual behaviours rather than relying solely on local or cultural expressions [3]. Zwilling et al. [3] emphasise the significance of cybersecurity awareness and behaviours among individuals from various cultural backgrounds, suggesting the necessity of comparative analyses due to differences in cybersecurity knowledge across cultures. This shows that all employees must acquire fundamental cybersecurity knowledge, including awareness of security threats and basic security literacy, to effectively recognise and respond to threats [4].

A successful cybersecurity awareness program in an organisation depends on thorough planning and execution. Best practices identified in literature include fostering an institution-wide cybersecurity culture, integrating security practices into everyday decision-making, clearly communicating the importance of cybersecurity education to management and end-users, and measuring the success of training through reductions in employee-driven cybersecurity incidents [5]. Cybersecurity awareness training empowers employees against threats by teaching them to identify phishing emails, use strong passwords, handle data securely, and adopt security best practices, thereby minimising human-caused incidents and complementing technological safeguards [6-8].

[1] *Corresponding author: Universiti Utara Malaysia (Email: syahida@uum.edu.my)
[2] Ministry of Home Affairs, Malaysia
[3,5] Universiti Utara Malaysia
[4] Universiti Teknologi MARA
[6,7] Universitas Pasundan

However, despite its acknowledged importance, cybersecurity awareness programs often fail to produce meaningful behaviour change. Many organisations still employ outdated training methods, such as infrequent slide-deck presentations or generic annual compliance modules, which rarely improve daily security practices [6-8]. Employees frequently report fatigue or disengagement with these traditional training approaches, particularly when top management does not visibly support or prioritise cybersecurity efforts [8-12]. Consequently, gaps persist between technical security measures and human readiness to counter cyber threats.

The literature has also revealed an important point that although some people know the answer to awareness questions, they do not act accordingly in their real lives [13-15]. It is suggested that security and privacy policies should be built into a system from the beginning [16, 17]. Users will eventually make mistakes and avoid security altogether if the system is too difficult to use [18]. These problems have remained for over a decade [13, 19]. Presently, cybersecurity awareness in its current form is ineffective. When confronted with so many ambiguous warnings and complicated recommendations, a person may be tempted to disregard all protection efforts and avoid danger. Threatening or intimidating security messages don't work very well because they make people feel so stressed out that they might even be scared or deny that they need to make a security decision [13].

Therefore, this study aims to bridge this gap by identifying the critical success factors (CSFs) necessary for the effective implementation of cybersecurity awareness training programs within organisations. Specifically, it seeks to determine organisational, educational, and behavioural elements that enhance program success in positively influencing employee security behaviours. By focusing on these factors, the research contributes insights for designing impactful training initiatives that thoroughly integrate human factors into cybersecurity strategies. In addition, this study aims to examine whether different types of training lead to changes in employee behaviour, using the Fogg Behaviour Model (FBM) as the analytical framework. FBM is chosen because it provides a clear and practical explanation of how behaviour occurs when motivation, ability, and a trigger are present at the same time. This makes it especially relevant for assessing which types of cybersecurity training are most effective in motivating secure behaviour, enhancing user capability, and delivering timely prompts that drive action. This multi-case study addresses this literature gap through a detailed comparative analysis. Ultimately, effective cybersecurity awareness requires ongoing educational efforts, culture-building, and leadership engagement, which are essential for strengthening an organisation's overall cyber resilience.

II. LITERATURE REVIEW

A. Cybersecurity awareness training in an organisation

In combating cyber threats, it is crucial to have an awareness of cybersecurity. Each individual within an organisation must actively implement policies, procedures, and best practices to effectively address the challenges posed by cyber threats [20, 21]. According to NIST Special Publication 800-16 [13], "security awareness" means a program that aims to draw attention to security. Awareness presentations aim to help people understand and respond to cybersecurity issues. This makes it abundantly clear where the primary focus should be on awareness. Furthermore, it demonstrates that individuals must not only be aware of potential cyber risks but also act accordingly. Providing awareness campaigns to ensure users are up to date on the most recent cyber threat landscapes and carrying out tabletop exercises at the organisation level to test user comprehension are two of the best ways to improve an organisation's cybersecurity. For example, Cybersecurity Malaysia [22] strongly suggests that all Internet users keep up with the latest cybercrime trends and follow the most effective cyber hygiene practices. This also includes safe email handling, safe web browsing, safe online transactions, safe internet banking, safe online product purchases, and safe use of social media applications. As a result, an awareness program should be used to teach employees about good "cyber hygiene," including what to do, what not to do, and why they need to do it [23, 24]. These exercises not only simulate cyberattacks but can also help determine whether the current cybersecurity awareness and training program is working and which employees may require additional training based on the results.

In order to implement a successful awareness program in cybersecurity, there are many challenges for all organisations. Humans remain a critical vulnerability in cybersecurity defence due to their susceptibility to errors, manipulations, and psychological biases [25-27]. This is because they are usually the weakest link in an organisation's information security program [25-27], particularly when employees lack awareness of the potential risks they may introduce. Given the rapid network speeds and ready access to data, even via mobile devices or web-based cloud applications, cybersecurity threats and breaches can occur quickly [21, 28-31].

Many employees lack basic cybersecurity practices, making them vulnerable to cyber threats [32]. Employees often lack the practical knowledge required to respond effectively to cybersecurity threats, even when theoretical

understanding exists [15]. This discrepancy between knowledge and behaviour, known as the knowledge-behaviour gap, is frequently cited as a significant cybersecurity challenge [20]. Research has shown that factors such as complacency, stress, workload, and cognitive biases significantly influence employees' cybersecurity behaviours [16]. Traditional cybersecurity programs frequently overlook these human cognitive and psychological elements, leading to ineffective training outcomes [20].

Besides that, one of the main challenges is limited resources and time constraints faced by organisations [32]. This issue is due to the lack of data-intensive practices, which makes it difficult to identify areas where employees need more training [32]. Furthermore, it argues that cybersecurity awareness methods, such as policies, procedures, and training sessions, are often dull and ineffective in engaging users and promoting long-term behaviour change. Other than that, the lack of digital security awareness can affect their ability to recognise threats, even if there are apparent signs [33].

Furthermore, with internet technology and mobile applications increasing in volume and complexity, malicious cyberattacks are evolving, and society faces more significant security risks in cyberspace than ever [23]. Additionally, the limitations of current methodologies used in creating training and awareness programs can result in overly general models that fail to meet the specific demands of many cybersecurity jobs [34]. Another research study identifies several challenges faced in promoting cybersecurity awareness among individuals and organisations [35]. These include a lack of awareness, limited resources, expertise in cybersecurity, resistance to change, a lack of regulation and human error. Besides that, the limited resources, lack of time, and competing priorities as the challenges in implementing cyber hygiene.

A cybersecurity awareness program alone can't help with the awareness. The policy, procedure, and best practices must all be put into action by every person in an organisation [36-38], not only the IT-related department. Many people and organisations do not properly understand cyber threats and the measures they must take to protect themselves [39]. On top of that, most available courses and/or training do not explicitly address human cognition and behaviours, which is a challenge in implementing effective cybersecurity awareness programs [40]. Challenges in cybersecurity awareness programs include measuring their effectiveness because it is not enough to rely solely on audience feedback to evaluate a program's success, implementing and assessing cybersecurity awareness programs in a remote work environment and tailoring awareness programs to different employee groups with varying levels of technical expertise [41]. Besides that, many students claim to have basic cybersecurity knowledge [42]. Still, they are unaware of how to protect their data or mitigate cyberattacks.

B. Factors Affecting the Effectiveness of Cybersecurity Awareness Initiatives

Cybersecurity awareness initiatives must go beyond knowledge transmission to actively influence behaviour [43]. A major reason many awareness programs fail is that they are treated as checkbox compliance exercises rather than sustained behaviour-change interventions [44]. Traditional approaches such as annual lectures or static e-learning modules often have limited impact on day-to-day security practices [45]. Instead, research highlights the need for engaging, practical training grounded in principles of adult learning and behaviour change. One-size-fits-all programs are often unsuccessful because they fail to resonate with employees' varied roles, levels of technical knowledge, and daily risk scenarios. Research suggests that cybersecurity messages should be concise, relevant, and engaging to overcome information overload and apathy [46]. A well-designed awareness program can help employees understand the importance of information security and their role in protecting organisational assets and information [28]. It is important to build a culture of cybersecurity awareness by engaging all employees, ensuring that policies and procedures are kept up to date, conducting regular risk assessments, and providing continuous training and education. Involving staff at every level and making security a routine part of the organisation's processes helps create vigilance and proactive behaviour [2, 32]. Many employees find cybersecurity training boring, overly complex, or irrelevant, which causes them to disengage [47]. This shows the importance of using training methods that hold employees' attention and make the material meaningful [48].

A growing body of literature emphasises experiential learning as a powerful method for cybersecurity education [23, 46, 49-55]. Traditional lecture-based training often fails to change behaviour because it stays theoretical. In contrast, experiential approaches immerse employees in realistic scenarios, allowing them to learn through direct experience and reflection. Simulated phishing campaigns are a prime example: employees receive fake phishing emails and, if they click, are immediately shown a teachable moment about what clues they missed. Studies have shown that such hands-on simulations significantly improve employees' ability to recognise and resist actual attacks [56, 57]. Beyond phishing, some organisations run broader cyber drills or games (e.g. mock ransomware outbreaks or capture-the-flag events) to build practical skills. These methods are rooted in established

learning theory, Kolb's experiential learning cycle and other models which hold that adults learn best by doing and then reflecting on that experience[58-60]. Nasir [47] supports the use of "simulators, quizzes, games", and other interactive media as part of training, noting that these tools can significantly improve learning outcomes by making training more engaging. Taherdoost [61] similarly observes that several studies have explored serious games and simulations as educational tools for cybersecurity awareness. Such approaches allow employees to practice identifying and responding to threats in a safe environment, which builds practical skills and confidence. Recent systematic evidence by Amjad et al. [62] reinforces this point by identifying that serious games effectively engage learners and facilitate knowledge sharing in realistic cybersecurity environments. In summary, incorporating simulations and other interactive elements is considered a best practice for awareness programs, greatly enhancing their effectiveness [41, 57, 63].

Next, the study by Mufor et al. [39] emphasises that having a reliable instrument to measure cybersecurity assessment helps mitigate failed attempts by pinpointing areas where training is needed before campaigns can be organised. It is important to measure the effectiveness of the awareness program through metrics such as employee engagement levels, number of reported incidents, and reduction in security incidents over time [28]. Common evaluation methods include pre- and post-training assessments to gauge knowledge gain, tracked click rates from simulated phishing campaigns to monitor behaviour change, and monitoring of incident reports or security mistakes to see if human error incidents decline over time. Regularly reviewing such metrics allows organisations to identify which aspects of their program are working and which are not. Additionally, reporting these metrics to leadership can help maintain management support by demonstrating return on investment. Programs that regularly assess and refine their content tend to stay relevant in the face of evolving threats and avoid stagnation. By contrast, organisations that lack systematic evaluation may miss emerging weaknesses in human behaviour, undermining the long-term impact of their training efforts [64]. In short, strong evaluation and feedback processes support continuous improvement, which is a key feature of successful programs [57].

Empirical studies confirm that management commitment strongly correlates with effective information security programs, as leadership support helps establish clear policies, provide adequate funding, and hold staff accountable for following best practices [57]. Similarly, Dawson [65] notes that an anti-phishing training program is most effective when it includes leadership involvement and buy-in. Leaders set the tone for cybersecurity culture, whereby when executives visibly prioritise security, for example, by allocating resources, enforcing policies, and even participating in training themselves, employees are far more likely to take awareness initiatives seriously. Management support creates a positive security climate that encourages everyone's buy-in and accountability [66, 67]. This cultural alignment and leadership-driven empowerment are repeatedly cited as prerequisites for changing employee attitudes and behaviours around cybersecurity. Conversely, when leaders don't actively participate in security initiatives, employees may see those initiatives as less important or optional. This can negate the impact of training programs as employees may not take them seriously or apply the learned concepts in their daily work [68]. Moreover, active leadership involvement fosters a culture of cybersecurity where safe behaviours are ingrained in daily operations rather than seen as optional. A recent study found that top management engagement is correlated with fewer cyberattacks, highlighting leadership's role in fostering a security-conscious culture [69].

Booker and Rebman Jr [69] identify communication as one of the critical factors in building a cybersecurity culture, implying that clear and continuous messaging from the organisation helps align everyone with security goals [69]. A success factor for awareness training is a well-crafted communication strategy that pairs effective content design (relevant, role-specific, and engaging material) with strategic delivery (using the right mix of channels and repetition to reinforce learning). When done correctly, employees better understand the training content and see its value, which improves their willingness to apply security practices in their daily work.

Table 1 shows a summary of the success factors from previous studies.

TABLE 1. Summary of the success factors from previous research

Success Factor	Sector(s)	Sources
Blended delivery methods (e.g., videos, games)	Corporate, Education, General workforce	[23] [70]
Clear metrics and evaluation frameworks	Education, Corporate	[71] [28]
Continuous & updated training	Remote workforces, Government, Education, Industry	[28] [66] [72] [54] [70] [73]

Cultural alignment and employee empowerment	Critical infrastructure (energy, water)	[53]
Experiential/simulation-based learning gamification for engagement	Government agencies and enterprises, Industry, SMEs, Public & Private sector, Information technology firms, Banking, Education	[49] [50] [51] [46] [52] [23] [54] [66]
Frequent and continuous training	Private-sector	[74]
Measurement and feedback mechanisms	Corporate, Academic, Industry	[51] [50]
Management support and leadership commitment	General corporate, Public sector	[57]
Policy and structure alignment	Public Sector, Education	[71] [52] [75]
Tailored, role-specific training	Financial services, Multinational firms	[76]
Top management commitment	Government, Private sector	[77] [78] [67]

The reviewed literature highlights a wide spectrum of critical success factors that contribute to effective cybersecurity awareness programs, emphasising that success is multi-dimensional and context-dependent. While factors such as top management commitment, experiential learning, clear evaluation frameworks, and tailored, role-specific training recur across sectors, their specific application often varies based on organisational needs and industry risks. For instance, gamification and blended delivery methods have proven effective in both corporate and educational settings by increasing engagement, while frequent training and feedback loops are especially vital in high-risk or fast-paced environments like the private sector and critical infrastructure. The integration of organisational culture, policy alignment, and employee empowerment further enhances program sustainability and relevance. However, no single combination of factors guarantees success. Instead, the literature highlights the importance of adopting a contextual and adaptive approach, where organisations continuously assess and refine their training strategies based on evolving threats, workforce dynamics, and technological changes. In sum, cybersecurity awareness success is best achieved through a flexible, evidence-based framework that balances leadership, learning design, evaluation, and cultural fit.

Despite significant research in this field, gaps remain concerning the comprehensive exploration of critical success factors across diverse organisational contexts. Limited studies have investigated how these factors differ by organisational size, industry, cultural settings, and risk profiles. The current study addresses these gaps by employing a multi-case study approach to analyse the effectiveness of cybersecurity awareness training programs across various organisations. By systematically identifying and examining organisational, educational, and behavioural elements that contribute to successful cybersecurity awareness initiatives, this research provides valuable insights and actionable guidance for researchers and practitioners aiming to enhance cybersecurity resilience.

C. The Fogg Behaviour Model (FBM),

The Fogg Behaviour Model offers a practical framework for understanding how behaviour change occurs, particularly in digital and organisational contexts [79]. The model explains that behaviour happens when three elements are present, which are: motivation, ability, and a trigger. If any of these components is missing, the intended behaviour is unlikely to occur. In the context of cybersecurity awareness, this model has been increasingly applied to explain why employees may fail to adopt secure practices despite being trained or informed.

Several studies highlight the relevance of FBM to cybersecurity training design. For instance, Cone et al. [51]and Jansson & von Solms [46] emphasised that users often lack either the motivation or the ability to act securely, and effective training must therefore provide clear prompts (e.g., phishing simulations), enhance perceived ease-of-use, and evoke personal relevance to motivate compliance. In more recent work, Dash and Ansari [54] stressed that behavioural change requires training methods that incorporate emotionally engaging simulations, which function as strong triggers while reinforcing ability through practice.

In practical application, FBM has been used to design gamified cybersecurity training [55], where interactive environments increase ability, point-based rewards increase motivation, and challenge-based scenarios act as timely triggers. This triadic interaction helps convert abstract security policies into personally meaningful experiences, thereby enhancing behaviour change. Furthermore, Kioskli et al. [80] recognised that the gap between

knowledge and behaviour, which is commonly observed in cybersecurity, is often due to a missing trigger or lack of perceived ability, reinforcing FBM's diagnostic value in program design.

III. RESEARCH METHODOLOGY

This study adopted a qualitative multiple-case study design to explore cybersecurity awareness training practices in depth. We examined four different organisations (identified anonymously as Organisation A, Organisation B, Organisation C, and Organisation D for confidentiality) that had established security awareness programs. The cases were selected to provide diversity in organisational characteristics (e.g., size, industry, and culture) to capture a range of experiences. A case-study approach was appropriate given the exploratory nature of our inquiry and the desire to understand contextual factors in each organisation. By comparing multiple cases, we aimed to identify common success factors as well as unique challenges or practices in each setting. This study was guided by these research questions: What are the critical success factors for the effective implementation of cybersecurity awareness training programs in organisations, and do these programs result in behavioural changes in how employees respond to cybersecurity threats.

A. Data Collection

Data were collected through a combination of focus group discussions and semi-structured interviews with stakeholders involved in or affected by the awareness training programs at each organisation.

We used purposive sampling to recruit participants who had relevant knowledge about their organisation's cybersecurity training efforts. These included IT and security personnel, program managers, and general staff from various departments. In two organisations (Organisation A and Organisation C), we conducted focus group discussions to collect a range of perspectives at once. For example, the focus group in Organisation A included eight participants from different parts of the organisation, such as senior managers, front-line employees, and technical staff. This diverse group was chosen on purpose to encourage a well-rounded discussion that reflected both leadership and staff viewpoints. In contrast, for Organisations B and D, there was no dedicated department responsible for cybersecurity training. As a result, we were only able to interview one member from the IT department in each case. Table 2 shows the demographic information for each organisation.

TABLE 2. Organisational Demographics of Participating Cases

Organization Code	Size	Primary Function	Dedicated Cybersecurity Training Unit	Training Format Used
Organization A	Large	Healthcare	Yes (IT Department)	Posters, emails, talks/conference, tests, and limited simulations
Organization B	Medium	Legislation & Regulation	No (Initiated by champion)	Simulations (Social Engineering, Phishing, Hacking), Workshop
Organization C	Large	Science & Technology	Yes (IT Department – Network Security Unit)	Phishing simulations, videos, talks/conference and workshops
Organization D	Medium	Agriculture	No (Initiated by IT team)	Email bulletins, static training, and limited feedback

The focus groups and interview sessions were facilitated by the researchers using a semi-structured guide of open-ended questions. We prompted participants to discuss topics such as their experiences with current training methods, perceptions of what makes training effective or ineffective, challenges faced in engaging employees, and suggestions for improvement. Five core questions were posed to all focus groups, covering areas like preferred training delivery formats, the use of real-world examples or simulations, communication channels for awareness messages, the role of management in supporting training, and the importance of continuous reinforcement. Follow-up probing questions were used to investigate deeper into any interesting or unexpected points that emerged.

Interviews lasted between 45–60 minutes and were conducted in the participants' preferred language (with translation to English later as necessary). All focus groups and interviews were audio-recorded with consent and transcribed for analysis. We also collected relevant documents from each organisation (such as training materials,

policy documents, and awareness campaign artefacts) to supplement the interview/focus group data and provide contextual understanding.

B. Data Analysis

The data (transcripts and documents) were analysed using thematic analysis to identify recurring patterns and key factors related to training effectiveness. We followed an iterative coding process combining inductive and deductive approaches. First, an initial codebook was developed based on concepts from the literature review and our research questions. It includes the anticipated codes such as "leadership support," "training content/design," "employee engagement," "challenges," "evaluation methods," etc. Next, two researchers independently read through a subset of transcripts to apply the initial codes and noted any new emergent themes. We then met to compare and discuss coding, refining the code definitions and adding new codes where needed to capture unexpected insights. Once the codebook was finalised, we systematically coded all transcripts using ATLAS.Ti software. To ensure reliability, multiple researchers coded overlapping portions of the data and resolved any discrepancies through discussion.

After coding, we examined the codes to identify broader themes and patterns, especially focusing on factors that participants felt influenced the success of cybersecurity awareness efforts. We grouped related codes into candidate themes and checked these against the data to confirm that they were representative and distinct. Through this iterative process, several major themes (and sub-themes) emerged. These themes were derived from the data but also resonated with constructs highlighted in prior literature. As a final step, we constructed a comparative matrix to summarise how each theme manifested in each case, facilitating a cross-case analysis.

IV. FINDINGS AND DISCUSSIONS

Through our thematic analysis and cross-case comparison, six critical success factors (CSFs) emerged as fundamental to effective cybersecurity awareness training programs. Together, these factors form a holistic picture of what drives successful security awareness and behaviour change in organisations.

A. Leadership Commitment and Support

Visible, sustained leadership advocacy was found to significantly influence the success of cybersecurity awareness initiatives. Participants across cases emphasised that without strong and consistent management backing, awareness programs struggle to gain legitimacy, resources, and employee buy-in. As one participant (Organisation C) said:

> *"Implementation needs management commitment. It's easier if (security is) directed from above."*

In Organisation A, for example, participants shared that employees took the training more seriously when top management actively supported the implementation of the awareness program by giving official instructions and attending the sessions. Similarly, Organisation B showed a clear example of how leadership attitudes changed over time.

> *"Management didn't see the importance. After showing real attack results (like) demonstrating data leaks, management started supporting."*

Initially, Organisation B's executives were not interested in addressing cybersecurity issues as there had been no threat targeting their organisation. However, once the IT team presented tangible evidence of security gaps through a live simulation that revealed nearly all staff fell for a phishing email, the executives reacted by increasing their support and allocating more budget for training. This story illustrates the value of evidence-based advocacy, that the leadership needs to witness concrete risk data before fully committing to an initiative. By contrast, Organisation D's team claim the lack of engagement from senior leaders:

> "*Another major challenge is the lack of strong support from senior management. Often, we have to wait for the management action."*

We found that policy documents existed on paper, but there was a gap whereby, without active pushing from the top, many of the awareness efforts stalled at the lower levels. Organisation D also noted a cultural mindset where cybersecurity was seen as purely an IT department's responsibility, largely due to limited leadership engagement beyond the IT function.

These observations align strongly with prior research that highlights leadership as a pivotal factor in security initiatives. When leaders champion cybersecurity, it sends a clear signal that security is a priority [63]. Our findings are supported by Safa et al. [81] that leadership must drive organisational change for cybersecurity, ensuring that security is not siloed but embraced organisation-wide. In practice, this means executives should not only approve policies but also visibly participate (e.g., in training or awareness campaigns) and communicate expectations regularly. The case of Organisation B suggests an important strategy, such as using metrics and incident simulations, to make the case to leadership that can convert passive support into active commitment. Overall, leadership commitment provides the foundation upon which all other success factors rest, where it legitimises the training program, secures necessary resources, and empowers program champions to enforce and innovate the awareness efforts.

B. Experiential and Simulation-Based Learning

All cases identified interactive, hands-on training as far more engaging and impactful than passive learning, confirming that experiential learning is a critical success factor. Participants reported that active involvement in realistic cyber scenarios greatly enhanced employees' understanding and retention of good security practices. Organisation B's organised phishing email simulations and noted,

"Last year, 99% of staff clicked. This year, only 6 out of 100 clicked."

This huge improvement, from nearly every employee being phish-prone to only 6% after training, demonstrates the value of simulation-based learning. In addition, Organisation B staff mentioned how they provided immediate feedback after simulations:

"We showed the (phishing) victims their mistakes... One click and the attacker could control the device."

This debriefing allowed employees to feel the consequences of a mistake in a safe environment, which several interviewees said left a lasting impression. Organisation C similarly recognised the need for more hands-on activities.

"*I think maybe we can do hands-on activities, a simulation that causes the user to feel the loss of data. When there is a simulation like ransomware, the user will feel the need for backup. Right now, they know the information, but they don't experience the real situation. Maybe that's what's lacking."*

This indicates an awareness that knowledge of threats alone is inadequate; people need to experience a scenario (like a mock ransomware attack causing data loss) to truly internalise the lesson. Notably, Organisation A's insight shows a broader principle articulated by Fogg [79] Behaviour Model for persuasive design, whereby behavioural change occurs when motivation, ability, and a compelling trigger converge. Without a strong trigger, such as experiencing a realistic security breach, even well-informed employees may not modify their behaviour. Our findings suggest that regular practical exercises, including phishing simulations, live drills, or interactive workshops, can serve as such triggers. These strategies help close the gap between abstract knowledge and concrete action by making cybersecurity threats feel immediate and personally relevant. Organisation C and Organisation D also acknowledged the need to have such training. For example, Organisation C staff agreed that realistic drills would likely improve engagement, but these organisations had not yet implemented such methods, citing hurdles like time, expertise, or tools.

"I think maybe we can do hands-on activities, a simulation that causes the user to feel the loss of data. When there is a simulation like ransomware, the user will feel the need for backup. Right now, they know the information, but they don't experience the real situation. Maybe that's what's lacking."

The effectiveness of experiential training observed in our cases reinforces findings from the literature. Security awareness studies have long suggested that learning by doing brings better outcomes than lectures. The improvement seen in Organisation B is in line with Chaudhary et al. [41] and Parsons et al. [57]. They argue that organisations using simulations and games in their awareness programs saw significant boosts in users' ability to detect threats and in their overall security posture. These methods work because they actively involve the learner

and often inject a dose of reality (and sometimes emotional adrenaline) that static content cannot. Organisations that incorporate realistic workplace simulations such as phishing email drills or mock cyber-attacks tend to see higher employee engagement and measurable reductions in incidents [41, 57]. Rather than blaming employees as "the weakest link," modern approaches emphasise empowering employees as the first line of defence, transforming security from a purely technical challenge into a shared behavioural responsibility [57].

Effective cybersecurity awareness training goes beyond lectures and memos; it engages participants through hands-on, experiential learning. Simulation-based learning, which includes realistic cyber-attack simulations, phishing drills, and serious games, has emerged as a game-changer in this field.

C. Communication Strategies and Content Design

The form and manner in which cybersecurity awareness content is communicated emerged as a third key success factor. Across the cases, participants highlighted that training materials and messages must be concise, clear, and engaging to hold employees' attention. Organisation C's approach is shown below:

> *"We minimise the wording… If possible, they can see it with a blink of an eye."*

This shows their focus on keeping messages short and easy to understand. Their posters and bulletins are designed to be brief and direct, giving key advice at a glance. The idea is that busy staff are more likely to notice and remember a quick 10-second message than read a long memo.

Organisation C's approach to content was to incorporate multimedia:

> *"Once in a while, a video will come out. If users just see a poster, they will close it… But when they see a video playing, they might stop for a while."*

The use of short videos and dynamic media is seen as a way to break through the monotony of text and catch the eye. This strategy is supported by learning research that shows visual and audio content can increase engagement.

Meanwhile, Organisation D mentioned a practice of sending out monthly infographics summarising key points of their cybersecurity policy.

> *"Every month, we distribute infographics, summarising key points from our Cybersecurity Policy to all personnel"*

While this shows effort to communicate regularly, the infographics were described as somewhat repetitive (the same policy points each month) and may lack novelty to continually engage staff. Organisation D's participants admitted that cybersecurity communications were often ignored or dismissed, suggesting the content was not sufficiently engaging or user-friendly

Our case findings on communication align with established best practices. Jansson and von Solms [46] stress that security messages should be short, relevant, and easy to understand, to combat information overload and apathy. Indeed, one risk in security awareness campaigns is, when employees receive so many warnings and lengthy guidelines, they will start to ignore them. The success of Organisation A's brief messages and Organisation B's varied media suggests that content must be digestible at a glance and ideally somewhat novel or visually appealing. These findings are also supported by Bada, et al. [13], Jansson and von Solms [46], Alshaikh, et al. [76] who found that using engaging formats (like videos or interactive content) significantly improved employee response to awareness campaigns, which resonates with Organisation B's thinking that people are more likely to watch a short animation than read a static poster.

Another aspect is contextual relevance: communications should tie security advice to situations employees actually encounter (e.g., "beware of emails about X that you might receive"). Some participants across cases noted that generic slogans were less effective than messages that felt directly applicable to their work or recent threats. In sum, the effective design of awareness content is as important as the content itself. Programs that succeeded paid attention to packaging the message through clarity, brevity, visual design, and medium selection, to ensure the message was received and remembered. Those that didn't struggle with low engagement and retention of their communications.

Our data shows that how cybersecurity awareness content is designed and communicated plays a critical role in its effectiveness.

"Without real consequences, posters and slides alone are ineffective. Our hands-on methods, such as real attacks, real consequences, are far more effective"

This finding aligned with Nasir [47], who found that a good cybersecurity training program should have content that is up-to-date, relevant, and targeted to the participants' roles and threat landscape. This means avoiding generic checklists in favour of context-specific guidance. For example, training developers on secure coding practices, or finance staff on spotting phishing in payment requests.

D. Emotional Resonance and Personal Relevance

An interesting and important theme that surfaced is the role of emotional engagement in motivating behaviour change. Participants observed that employees are more likely to adopt secure behaviours when they feel that cyber threats pose a real, personal risk, as opposed to viewing security as a distant or purely theoretical issue.

Organisation B's training coordinator articulated this as follows:

"*People don't learn by seeing posters. They learn when they feel the threat, when they see their data exposed. Otherwise, it's useless."*

This statement highlights that giving factual instructions alone, such as 'Don't click on suspicious links', may not be effective unless they are supported by an emotional element that helps people clearly understand and feel the risk. In Organisation B, as noted earlier, they created an emotional impact by showing employees the consequences of a click during simulations. For example, demonstrating how an attacker could take over a device or leak data. This kind of controlled scare tended to jolt employees into realising that this threat could happen to them, thereby motivating them to be more vigilant.

Organisation D's team similarly noted that many employees tended to underestimate cybersecurity issues

"They usually underestimate the risk and threats if they haven't personally experienced an attack."

In other words, those who have never suffered a phishing scam or malware incident often remain complacent, thinking of security breaches as something that happens to others or only to big companies.

Meanwhile, Organisation C did not have many real incidents to draw lessons from, which staff felt was a double-edged sword:

"Maybe that's what's lacking... Right now, they know the information, but they don't experience the real situation"

Organisation A made small efforts to close the emotional gap by sometimes using real breach stories or case-based simulations in their training sessions to create concern and increase awareness of the risks:

"After the phishing attack, the training came in. It's human nature that once they experience the consequences, they become cautious..."

The importance of emotional connection is supported by research in behavioural psychology and risk communication. People are more likely to change their behaviour when an issue affects them emotionally, such as evoking fear, empathy, or a sense of personal risk, rather than solely through logic. As mentioned before, Fogg's Behaviour Model [79] states that motivation is one of the key elements needed for behaviour to occur, and emotional responses can significantly increase that motivation. Parsons et al. [57] also explain that emotional triggers can make security threats feel more real and increase the impact of training, provided they are used carefully. Too much fear, however, can cause people to avoid the issue instead of taking action to deal with it. In our study, the organisations that had better outcomes created a sense of urgency without causing panic. For example, Organisation B showed employees how a phishing click could lead to serious consequences, but the training was conducted in a safe learning environment where they could see how to avoid it next time. This

approach aligns with the Protection Motivation Theory [82, 83], which posits that people take action when they perceive both risk and the capability to respond effectively. Overall, our findings show that one key success factor is designing cybersecurity training that not only teaches information but also builds an emotional connection to the topic. Methods like storytelling, realistic simulations, or hearing real experiences from colleagues can help employees see cybersecurity as a personal responsibility and not just an IT issue.

Furthermore, interactive and immersive training tools can heighten engagement. Contrary to the literature, none of the organisations in our study employed this method.

Organisation C claims that:

"We do not have a dedicated team to explore gamification. At most, we can do is use Kahoot"

While Amjad et al. [62] highlight the potential of serious games to create immersive environments with realistic scenarios and role-play, which can lead to greater emotional engagement and a sense of personal involvement in learning. When learners virtually experience a cyber incident and must make decisions, it elicits emotions like urgency or cautiousness in a safe setting. Our results suggest a gap in the application of emotionally engaging tools such as gamification, which may present opportunities for future improvement in cybersecurity awareness training, as none of the organisations engaged with such methods.

E. Continuous Assessment and Improvement

The importance of continuous evaluation of the awareness program itself was identified in our study as a driver of long-term success. Organisations that treat the cybersecurity awareness initiative as a living program, which includes ongoing monitoring, feedback, and updating, can benefit in terms of keeping training effective and relevant. Organisation C exemplified this with its practice of regular Security Posture Assessments (SPAs) and other audits.

One Organisation C manager described,

"We conduct a security posture assessment to assess the level of security, including the users. For example, we have included a social engineering test in the SPA. Through that, we know the level of our users' awareness."

By formally testing and measuring user awareness, Organisation C can quantify progress and identify remaining weak spots. They used results to report to leadership and to adjust their training focus (for example, if the assessment showed low awareness about a certain policy, that policy would be re-emphasised in the next training cycle). Organisation A and Organisation D did some periodic evaluations as well, although less rigorously. They mentioned using short post-training quizzes or tracking the number of security incidents, but these were not part of a structured framework. Organisation B did not conduct systematic evaluations of the training methods themselves. Instead, they relied on comparing results from earlier and later phishing simulations and social engineering tests. For example, after the first session, feedback was given to staff, and improvements were observed in the second session (e.g., a reduced click rate). However, there was no structured assessment of training effectiveness beyond these before-and-after comparisons, meaning the organisation had limited insight into which specific elements of the program contributed to the behavioural change.

Our findings reinforce what cybersecurity frameworks and experts often recommend: that security awareness should be managed with the same Plan-Do-Check-Act cycle as any other business process [41]. First, it provides evidence of whether the training is effective. By tracking metrics such as phishing test results, the number of incidents caused by human error, or employee attitudes toward security over time, organisations can determine whether their training efforts are working. Second, regular evaluation helps identify specific areas that need improvement. For example, if a particular department repeatedly falls for phishing emails, targeted training can be introduced for that group. This approach is supported by existing research and reflected in the strategy used by Organisation C. Third, visible improvements, such as the significant drop in click rates achieved by Organisation B, can help maintain both executive and employee support for the program. In this way, cybersecurity awareness becomes more than a compliance requirement. It becomes a performance measure that can be tracked, celebrated, and continuously improved.

In contrast, organisations without clear feedback loops often struggle to progress. For instance, Organisation D's training program remained largely unchanged, possibly because its impact was never measured and there was

no strong reason presented to revise it. Overall, this highlights that treating awareness training as a one-off event is ineffective. Instead, it should be viewed as an ongoing cycle of evaluation and improvement.

The literature consistently affirms that effective, metrics-based management of security awareness programs is a defining characteristic of mature organisational security cultures [56]. In summary, building continuous assessment and iterative improvement into the program is itself a success factor that ensures all the other factors (leadership support, content, methods, etc.) remain aligned with the organisation's evolving threat landscape and learning needs.

F. Bridging the Policy–Practice Gap

A strong theme from the data is the gap between formal cybersecurity policies and actual daily practices. All organisations in this study had official policy documents and procedures. However, participants shared that these documents often failed to influence employee behaviour on the ground.

For example, a participant from Organisation D explained:

> *"We have published version 1.0 of the Cybersecurity Policy and distributed a copy to every department."*

> *"Some employees are responsive and take the information seriously, but many still tend to treat cybersecurity issues lightly."*

This shows that while the policy was formally distributed, it did not always lead to meaningful engagement or behaviour change.

Another issue raised by Organisation D was the perception that security is not everyone's responsibility:

> *"There's a perception that cybersecurity is purely an IT department's responsibility, not a shared one."*

This highlights a cultural barrier where non-IT staff do not feel accountable for cybersecurity, even when policies assign shared responsibilities.

In comparison, Organisation A and Organisation B demonstrated some practices that helped reduce the gap between policy and behaviour. In Organisation A, training was aligned with specific policy items. For example, rules like "do not share passwords" were directly reflected in training materials and use cases. Meanwhile, Organisation B, after facing leadership pressure and showing real simulation results, began making policies more visible in meetings and reinforcing them through active communication. These steps helped make the policy more than just a formal document.

Despite these efforts, participants across organisations admitted that keeping staff behaviour aligned with policy remains a challenge over time. Some employees tend to forget or ignore guidelines unless there is continuous reinforcement and reminders.

G. Summary of Key Findings

This section presents a summary of key findings for each organisation based on the thematic factors identified in this study. It compares the four cases, highlighting similarities and differences in their approaches to cybersecurity awareness training. The case studies provided rich insights into how organisations design and implement cybersecurity awareness initiatives, as well as the factors that shape their effectiveness. While several critical success factors were consistently identified across all four cases, the extent to which these were present or actively applied varied. For example, some organisations benefited from strong top management support and allocated dedicated resources to awareness efforts, while others faced challenges in securing leadership buy-in. Similarly, while some had adopted innovative practices such as phishing simulations and scenario-based learning, others relied more heavily on passive, text-based modules.

Table 3 illustrates how each critical factor manifested in Organisations A, B, C, and D, providing a comparative view of their strengths and areas for improvement.

TABLE 3. Cross-case comparison of cybersecurity awareness training factors across four organisations

Organization/ Characteristics	**Organisation A**	**Organisation B**	**Organisation C**	**Organisation D**
Size	Large	Medium	Large	Medium
Leadership Support	Leadership support increased with visible directives and participation.	Initial scepticism turned to support after evidence of attack simulations.	Leadership support varied; often awaited higher-level direction.	Minimal leadership advocacy; cybersecurity is seen as the IT department's responsibility.
Experiential Learning	Recognises the value of simulations but has limited hands-on implementation.	Conducted phishing simulations; saw significant improvement in click rates.	Acknowledges importance but lacks simulations due to resource constraints.	Very limited hands-on methods; primarily theoretical training.
Communication & Content	Focus on concise, easily digestible messages; use posters and briefings.	Uses varied multimedia like videos to increase engagement.	Uses short messages and occasional videos for communication.	Long, generic emails; infographics not consistently engaging.
Emotional Engagement	Employees only become cautious after experiencing real consequences.	Shows real consequences to drive emotional engagement.	No real events to trigger urgency; staff recognise lack of impactful scenarios.	Low urgency; staff underestimate risks unless directly affected.
Assessment & Feedback	Informal checks like quizzes; no formal metrics or dashboards.	Relied on before-and-after comparisons; no structured evaluation.	Regular security assessment and social engineering tests.	Occasional IT reviews; no systematic feedback or improvement loop.
Policy–Practice Gap	Policies exist but require active top-down enforcement to be effective.	Reinforced policies through meetings and awareness content after simulations.	Policies are distributed, but real practice lags.	Policy exists, but many treat cybersecurity casually.

These cross-case differences reveal patterns that help explain why certain programs were more impactful than others. As presented in Table 3, the four organisations exhibited varying degrees of effectiveness across the six critical success factors (CSFs). Leadership support emerged as a clear differentiator. Organisations A and B showed a strengthening commitment from top management once the benefits of training were made evident. In particular, Organisation B experienced a significant increase in leadership engagement following simulations that revealed concrete vulnerabilities. In contrast, Organisations C and D lacked visible senior leadership involvement. In Organisation D, cybersecurity was still perceived as the sole responsibility of the IT department, reflecting a siloed security culture.

On experiential Learning, Organisation B led by example through the implementation of phishing simulations, which resulted in a notable reduction in click rates from 99% to 6%. This hands-on approach fostered meaningful behavioural change. Organisations A and C acknowledged the value of experiential learning but faced implementation hurdles, including a lack of resources and limited institutional support. Organisation D continued to rely on passive training formats, which likely hindered employees' ability to internalise security practices.

Communication strategies and Content Design also varied across cases. Organisation A emphasised brevity, using short messages and posters for quick, at-a-glance consumption. Organisation B adopted multimedia strategies such as video content to maintain interest and engagement. In contrast, Organisation C's reliance on static infographics and Organisation D's use of lengthy and often overlooked emails reduced the impact of their

communication. The absence of user-centred design approaches in these cases indicates a need for more dynamic and tailored communication strategies.

In terms of emotional engagement, Organisation B actively incorporated real-life scenarios and consequences into its simulations, helping employees emotionally connect with cybersecurity risks. Organisations A and C recognised the emotional gap but had not yet operationalised strategies to bridge it. Organisation D acknowledged the problem but made only minimal efforts to address it, which may have affected the perceived urgency among staff.

Assessment and feedback mechanisms were most developed in Organisation C, which conducted structured Security Posture Assessments (SPA) and social engineering tests to evaluate user awareness and inform training adjustments. Organisation A conducted periodic quizzes, although in an informal manner. Organisation B relied on outcome comparisons between training sessions but lacked a systematic evaluation framework. Organisation D had no consistent monitoring or feedback system in place, limiting its ability to track progress or improve training quality.

A shared limitation across all organisations was the lack of customisation and needs-based training. None of the organisations conducted prior assessments to tailor cybersecurity content based on user roles, prior knowledge, or departmental risk exposure. Training remained generic, which reduced its effectiveness in delivering context-specific skills and knowledge. This finding diverges from current best practices in cybersecurity awareness literature, which recommend tailoring content and delivery methods to meet the needs of diverse employee groups.

In summary, the cross-case analysis shows that while all four organisations acknowledged similar CSFs conceptually, their implementation practices varied significantly. Organisations A and B demonstrated stronger leadership engagement, interactive training strategies, and moderate assessment processes, positioning them as relatively more effective. In contrast, Organisations C and D showed limited leadership involvement, static communication formats, low emotional engagement, and insufficient evaluation, which created key barriers to success. These comparative insights provide a critical foundation for the discussion section, where the alignment between these findings and established literature is further explored.

Similarly, cultural and linguistic adaptation of training materials was not mentioned in any case. All organisations appeared to use generic content formats, often policy-based or technically worded, without adapting to the organisational culture, language preferences, or communication styles of diverse employee groups. Furthermore, although gamification and interactive learning are emphasised in current research, none of the organisations used cybersecurity games or immersive training tools. Only Organisation B used simulations consistently (for example, phishing tests), but even that was not framed as part of a gamified strategy. There was also no structured use of multi-channel reinforcement. Awareness efforts were often periodic or one-off rather than continuous campaigns. Finally, incentives or positive reinforcement mechanisms were absent across all four cases. Training participation was driven more by compliance than motivation or recognition. These gaps suggest significant opportunities for improvement if organisations wish to adopt more engaging, personalised, and sustained awareness strategies.

V. CONCLUSION

This study explored what makes cybersecurity awareness training successful by comparing practices across four organisations in four different sectors. The findings identified six main factors that contributed to effective awareness programs: leadership support, hands-on or experiential learning, clear and simple communication, emotional engagement, and continuous evaluation and feedback. These factors appeared in different ways and at different levels in each organisation, which influenced the overall outcomes.

While the overall study focused on identifying critical success factors for cybersecurity awareness training, Fogg's Behaviour Model was used to assess whether these programs led to actual behavioural change among employees. The model suggests that behaviour occurs when motivation, ability, and a trigger are present at the same time. In this study, only some organisations demonstrated clear signs of behavioural change. For example, in the organisation that used phishing simulations, employees showed increased awareness and caution after experiencing simulated attacks. The emotional impact of realising their vulnerability (motivation), combined with practical guidance (ability) and real-time feedback (trigger), appeared to influence safer behaviour. In contrast, organisations that lacked emotional engagement or hands-on activities saw less noticeable changes, with employees often reverting to old habits over time. These findings suggest that when the three elements of Fogg's model are present (motivation, ability, and trigger), cybersecurity awareness training is more likely to produce lasting behavioural change. This research contributes to both theory and practice by showing how Fogg's model can

explain success in real-world training programs. It also offers practical insights for organisations that want to improve their awareness strategies.

However, the study has some limitations. It was based on qualitative data from only four organisations from a specific sector and does not reflect other types of organisations. The data collection took place within a limited time frame, which may not capture long-term changes in awareness or behaviours. A longitudinal approach could offer a better view of how cybersecurity practices evolve. Future studies can expand by testing these findings in larger and more diverse samples. There is also room to explore how specific training designs can be better matched to employee motivation and learning styles using models like Fogg's.

ACKNOWLEDGMENT

This research was funded by a matching grant from Universiti Utara Malaysia (UUM) and Universitas Pasundan (UNPAS), Indonesia (Kod S/O: 21559).

REFERENCES

[1] Verizon, "2023 Data Breach Investigations Report: Public Sector Snapshot. Verizon Business." [Online]. Available: https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf

[2] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model," Information Technology & People, vol. 36, no. 8, pp. 94-125, 2023.

[3] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 62, no. 1, pp. 82-97, 2022.

[4] Z. Tu and Y. Yuan, "Critical success factors analysis on effective information security management: A literature review," 2014.

[5] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," Information, vol. 12, no. 10, p. 417, 2021.

[6] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," Journal of Organizational Computing and Electronic Commerce, vol. 29, no. 4, pp. 249-257, 2019.

[7] M. L. Bacud and S. Mäses, "Game-based learning for cybersecurity awareness training programmes in the public sector," in ECEL 2021 20th European Conference on e-Learning, 2021: Academic Conferences International limited, p. 50.

[8] A. Reeves, D. Calic, and P. Delfabbro, "'Get a red-hot poker and open up my eyes, it's so boring' 1: Employee perceptions of cybersecurity training," Computers & security, vol. 106, p. 102281, 2021.

[9] A. Reeves, D. Calic, and P. Delfabbro, "'Generic and unusable' 1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue," Computers & Security, vol. 128, p. 103137, 2023.

[10] A. Reeves, P. Delfabbro, and D. Calic, "Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue," SAGE open, vol. 11, no. 1, p. 21582440211000049, 2021.

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

[12] O. Fagbule, "Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs," Bournemouth University, 2023.

[13] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," in International Conference on Cyber Security for Sustainable Society, Coventry, 2019.

[14] D. T. Smith and A. I. Ali, "YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS," Issues in Information Systems, vol. 20, no. 1, 2019.

[15] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," arXiv preprint arXiv:1901.02672, 2019.

[16] E. C. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," Information, vol. 13, no. 4, p. 192, 2022.

[17] A. Georgiadou et al., "Hospitals' cybersecurity culture during the COVID-19 crisis," in Healthcare, 2021, vol. 9, no. 10: MDPI, p. 1335.

[18] D. L. Coventry, P. Briggs, J. Blythe, and M. Tran. "sing behavioural insights to improve the public's use of cyber security best practices." Government Office for Science. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (accessed 2022).

[19] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in 2011 third international workshop on cyberspace safety and security (CSS), 2011: IEEE, pp. 21-26.

[20] K. Kioskli, T. Fotis, S. Nifakos, and H. Mouratidis, "The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0," Applied Sciences, vol. 13, no. 6, p. 3410, 2023.

[21] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," Journal of Reliable Intelligent Environments, vol. 7, no. 2, pp. 69-84, 2021.

[22] CyberSecurityMalaysia, "Be wary of cybercrime trends. ," Cyber999 Advisories. [Online]. Available: https://www.cybersecurity.my/portal-main/advisories-details/e14a3424-f7d4-11ef-9a4c-005056812d51
[23] J. Abawajy, "User preference of cyber security awareness delivery methods," Behaviour & Information Technology, vol. 33, no. 3, pp. 237-248, 2014, doi: 10.1080/0144929X.2012.708787.
[24] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), 2018: IEEE, pp. 62-68.
[25] S. T. Argaw et al., "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," BMC medical informatics and decision making, vol. 20, no. 1, p. 146, 2020.
[26] S. S. Bhuyan et al., "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations," Journal of medical systems, vol. 44, no. 5, p. 98, 2020.
[27] L. Kim, "Cybersecurity awareness: Protecting data and patients," Nursing management, vol. 48, no. 4, pp. 16-19, 2017.
[28] A. Alghamdi, "A Systematic Review on Human Factors in Cybersecurity," International Journal of Computer Science & Network Security, vol. 22, no. 10, pp. 282-290, 2022.
[29] N. Ahmad, P. A. Laplante, J. F. DeFranco, and M. Kassab, "A cybersecurity educated community," IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 3, pp. 1456-1463, 2021.
[30] J. Haney, J. Jacobs, S. Furman, and F. Barrientos, "Approaches and Challenges of Federal Cybersecurity Awareness Programs," 2022.
[31] A. Alruwaili, "A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS," International Journal of Advanced Research in Computer Science, vol. 10, no. 5, 2019.
[32] K. Johansson, T. Paulsson, E. Bergström, and U. Seigerroth, "Improving cybersecurity awareness among SMEs in the manufacturing industry," in SPS2022: IOS Press, 2022, pp. 209-220.
[33] A. AlQadheeb, S. Bhattacharyya, and S. Perl, "Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior," Array, vol. 14, p. 100146, 2022.
[34] A. Kovačević and S. D. Radenković, "SAWIT—security awareness improvement tool in the workplace," Applied Sciences, vol. 10, no. 9, p. 3065, 2020.
[35] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," Sensors, vol. 23, no. 15, p. 6666, 2023.
[36] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," Information & management, vol. 51, no. 5, pp. 551-567, 2014.
[37] T. Daengsi, P. Wuttidittachotti, P. Pornpongtechavanich, and N. Utakrit, "A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization," in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021: IEEE, pp. 102-106.
[38] I. Al-Shanfari, W. Mohamed, N. Tabook, R. Ismail, and A. Ismail, "Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees," International Journal of Advanced Computer Science and Applications., 2022, doi: 13. 479-490. 10.14569/IJACSA.2022.0130855. .
[39] B. S. Mufor, A. Marnewick, and S. von Solms, "The development of cybersecurity awareness measurement model in the water sector," in International conference on cyber warfare and security, 2022, vol. 17, no. 1: Academic Conferences International Limited, pp. 211-218.
[40] K. Kioskli, L. M. Bishop, N. Polemi, and A. Ramfos, "Towards a Human-Centric AI Trustworthiness Risk Management Framework. ," Human Factors in Cybersecurity, vol. 127, p. 63, 2024.
[41] S. Chaudhary, "Driving behaviour change with cybersecurity awareness," Computers & Security, p. 103858, 2024.
[42] A. Garba, M. B. Sirat, S. Hajar, and I. B. Dauda, "Cyber security awareness among university students: A case study," Science Proceedings Series, vol. 2, no. 1, pp. 82-86, 2020.
[43] J. Haney and W. Lutters, "From compliance to impact: Tracing the transformation of an organisational security awareness programme," Cyber Security: A Peer-Reviewed Journal, vol. 8, no. 2, pp. 110-130, 2025.
[44] F. Ugbebor, O. Aina, M. Abass, and D. Kushanu, "Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents," Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), vol. 3, no. 3, pp. 382-409, 2024.
[45] J. Mungo, "Examining the Aspects of Self Paced Cybersecurity Awareness Training: A Generic Qualitative Inquiry," Capella University, 2022.
[46] K. Jansson and R. von Solms, "Phishing for phishing awareness," Behaviour & information technology, vol. 32, no. 6, pp. 584-593, 2013.
[47] S. Nasir, "Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions," in Proceedings of the Cyber Secure Nigeria Conference, 2023, pp. 151-160.
[48] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, "A novel SETA-based gamification framework to raise cybersecurity awareness," International Journal of Information Technology, vol. 13, no. 6, pp. 2371-2380, 2021.
[49] R. H. B. H. Rife, "Improving Information Security Awareness Training Through Real-Time Simulation Augmentation," Northcentral University, 2019.

[50] M. Adams and M. Makramalla, "Cybersecurity skills training: An attacker-centric gamified approach," Technology Innovation Management Review, vol. 5, no. 1, 2015.
[51] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," computers & security, vol. 26, no. 1, pp. 63-72, 2007.
[52] G. Angafor, I. Yevseyeva, and L. Maglaras, "MalAware: A tabletop exercise for malware security awareness education and incident response training," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 280-292, 2024.
[53] H. Hanna, "Re-Envisioning Education for Increased Complexity: Embedding a Security Mindset Into Complex Adaptive Learning Systems," Wilkes University, 2025.
[54] B. Dash and M. F. Ansari, "An effective cybersecurity awareness training model: First defense of an organizational security strategy," ed, 2022.
[55] T. van Steen and J. R. Deeleman, "Successful gamification of cybersecurity training," Cyberpsychology, Behavior, and Social Networking, vol. 24, no. 9, pp. 593-598, 2021.
[56] S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," Journal of Cybersecurity, vol. 8, no. 1, p. tyac006, 2022.
[57] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): two further validation studies," Computers & Security, vol. 66, pp. 40-51, 2017.
[58] M. Wijnen-Meijer, T. Brandhuber, A. Schneider, and P. O. Berberat, "Implementing Kolb s experiential learning cycle by linking real experience, case-based discussion and simulation," Journal of medical education and curricular development, vol. 9, p. 23821205221091511, 2022.
[59] A. Kolb and D. Kolb, "Eight important things to know about the experiential learning cycle," Australian educational leader, vol. 40, no. 3, pp. 8-14, 2018.
[60] A. Y. Kolb and D. A. Kolb, "Experiential learning theory," in Encyclopedia of the Sciences of Learning: Springer, 2012, pp. 1215-1219.
[61] H. Taherdoost, "A critical review on cybersecurity awareness frameworks and training models," Procedia computer science, vol. 235, pp. 1649-1663, 2024.
[62] K. Amjad, K. Ishaq, N. A. Nawaz, F. Rosdi, A. B. Dogar, and F. A. Khan, "Unlocking cybersecurity: A game‐changing framework for training and awareness—A systematic review," Human Behavior and Emerging Technologies, vol. 2025, no. 1, p. 9982666, 2025.
[63] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," Computers & security, vol. 42, pp. 165-176, 2014.
[64] P. K. Makanto and J. S. Eze, "Mitigating Human Vulnerabilities in Cybersecurity: Understanding Human Flaws and Implementing Effective Countermeasures."
[65] A. Dawson, "Exploring strategies for implementing information security training and employee compliance practices," Walden University, 2019.
[66] R. Sabillon, "The cybersecurity awareness training model (CATRAM)," in Research Anthology on Advancements in Cybersecurity Education: IGI Global, 2022, pp. 501-520.
[67] M. R. Yerabolu, "Cyber Security Awareness Training: Strategies for educating employees on cyber threats and safe practices," 2024.
[68] F. Ismail, N. A. Arumugan, A. A. Kadir, and A. A. Hassan Alhosani, "Impact of leadership styles toward employee engagement among Malaysian Civil Defence Force," International Journal of Business & Society, vol. 22, no. 3, 2021.
[69] Q. E. Booker and C. M. Rebman Jr, "Factors influencing the development of a successful cybersecurity culture," Issues in Information Systems, vol. 24, no. 4, p. 51, 2023.
[70] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior," IEEE access, vol. 10, pp. 132132-132143, 2022.
[71] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "Cyber-Security Culture Assessment in Academia: A COVID-19 Study: Applying a Cyber-Security Culture Framework to assess the Academia's resilience and readiness," in Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1-8.
[72] R. Sabillon, J. Serra-Ruiz, and V. Cavaller, "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: IGI Global, 2021, pp. 174-188.
[73] D. A. Schroeder, "Cybersecurity Approaches for The Internet of Things," 2017.
[74] M. Bada and J. R. Nurse, "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)," Information & Computer Security, vol. 27, no. 3, pp. 393-410, 2019.
[75] M. O. Arowosegbe, "Exploring Cybersecurity Policy Compliance Strategies to Secure E-Government Systems," Walden University, 2025.
[76] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An exploratory study of current information security training and awareness practices in organizations," 2018.
[77] M. M. Hanna, "Exploring cybersecurity awareness and training strategies to protect information systems and data," Walden University, 2020.

[78] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "Evaluating The Cyber-Security Culture of the EPES Sector: Applying a Cyber-Security Culture Framework to assess the EPES Sector's resilience and readiness," in Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1-10.
[79] B. J. Fogg, "A behavior model for persuasive design," in Proceedings of the 4th international Conference on Persuasive Technology, 2009, pp. 1-7.
[80] K. Kioskli, L. M. Bishop, N. Polemi, and A. Ramfos, "Human Factors in Cybersecurity, Vol. 127, 2024, 62-78 AHFE," Human Factors in Cybersecurity, p. 63, 2024.
[81] N. S. Safa et al., "Deterrence and prevention-based model to mitigate information security insider threats in organisations," Future Generation Computer Systems, vol. 97, pp. 587-597, 2019.
[82] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change1," The journal of psychology, vol. 91, no. 1, pp. 93-114, 1975.
[83] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," Social psychology: A source book, pp. 153-176, 1983.