International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 3, June 2025, pp. 2986~2997
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i3.pp2986-2997

Enhancing cybersecurity awareness strategies in organization using Delphi technique

Anawin Kaewsa-Ard, Nattavee Utakrit
Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand

Article Info

Article history:

Received Jun 28, 2024
Revised Jan 2, 2025
Accepted Jan 16, 2025

Keywords:

Awareness
Cybersecurity
Delphi technique
Strategy
Training

ABSTRACT

Cybersecurity concerns were once primarily perceived as technical issues, prompting many organizations to prioritize investments in security technologies. However, it has become increasingly evident that cybersecurity is not solely a technical matter. In fact, a significant number of cybersecurity breaches arise from users' lack of awareness about secure technological practices. This research aims to develop a cybersecurity awareness strategy using the Delphi technique over three rounds, involving 15 cybersecurity experts. The findings indicate a consensus among experts that cybersecurity awareness training is an effective strategy to enhance an organization's overall cybersecurity posture. However, the true essence of cybersecurity lies in fostering secure technology usage practices among all users within the organization. To address this, the researcher developed systematic training content for cybersecurity awareness, which was evaluated and refined by experts using the Delphi technique to ensure its effectiveness in promoting genuine cybersecurity awareness.

Corresponding Author:

Nattavee Utakrit
Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok
1518 Pracharat 1 Road, Wongsawang, Bangsue, Bangkok 10800, Thailand
Email: nattavee.u@itd.kmutnb.ac.th

1. INTRODUCTION

The organization has undergone significant technological advancements to align with the modern era, where technology has inevitably become an integral part of the organization. These technological changes are not only essential for the organization itself but also play a crucial role in enhancing the quality of life for the general public [1]. This shift emphasizes the importance of digital literacy as an indispensable competency that will become a fundamental component of lifelong learning for individuals. Despite the clear benefits that technology brings, it is also accompanied by numerous cyber threats that lurk in the digital world, poised to attack whenever we lack awareness [2]. In contemporary organizations, we observe that personnel, operational processes, and technology are integrated to drive the organization's mission. Therefore, any cyber incident affecting these elements would undoubtedly disrupt the organization's mission [3].

A critical review of Taherdoost's work on cybersecurity awareness frameworks and training models concluded that the implementation of well-defined cybersecurity awareness and training programs can substantially reduce the cost and frequency of security incidents for businesses, thereby strengthening their overall security posture and cyber resilience [4]. Additionally, Limna *et al.* research [5], which investigates the relationship between cybersecurity knowledge, awareness, and behavioral protection among mobile

banking users in Thailand, confirmed the proposed conceptual framework. The findings indicate that cybersecurity knowledge significantly influences cybersecurity awareness and behavior, with cybersecurity awareness serving as a crucial mediator between knowledge and behavior. Similarly, Popoola *et al.* [6] conducted a comparative analysis of cybersecurity awareness and training programs between Africa and the U.S., revealing that the effectiveness of theoretical constructs in achieving cybersecurity awareness varies significantly between countries, largely due to differences in infrastructure, digital literacy, and cultural factors. This highlights the importance of contextual analysis in developing strategies to enhance cybersecurity awareness. Without a deep understanding of the specific cyber challenges and contexts, efforts to raise awareness may fail. Given that the scope of our research is at the organizational level, it is essential to seek the support of cybersecurity experts who understand the broader context of organizational management and the role of information technology in organizations. This ensures that the strategies we propose are aligned with the current organizational context and effectively enhance cybersecurity awareness. Aphane's research further emphasizes the importance of cybersecurity awareness in combating cybercrime, using a qualitative approach to gain insights into the level of awareness among youth in Gauteng, South Africa [7]. The findings reveal a lack of existing initiatives in policing cybercrime and the absence of cybersecurity awareness programs in South Africa, which lags in strategy development in this area. This study also utilized in-depth interviews, demonstrating how expert interviews can reveal critical issues within specific contexts. From these findings, it is evident that technology, security, and human factors are inseparable.

The problem addressed in this paper is the challenge of insufficient cybersecurity awareness programs in organizations [8]–[11], which leaves individuals vulnerable to evolving cyber threats. To resolve this issue, this paper proposes the integration of structured cybersecurity awareness programs tailored to an organization's environment and culture [12]–[15]. The solution involves using the Delphi technique to gather expert opinions and achieve consensus on the most effective strategies for enhancing awareness. This qualitative method helps refine and validate the approaches for improving cybersecurity behavior and response to threats [16]. By understanding the role of human factors such as age, gender, education, and IT experience, the proposed solution also suggests creating more targeted and personalized training programs that address specific needs within the organization [17], [18]. To clarify these issues, the main research questions (RQs) of this study are as follows:

RQ1: Can the Delphi technique help identify the issues that affect cybersecurity awareness within an organization?

RQ2: Can the Delphi technique guide the development of cybersecurity awareness strategies?

2. PROPOSED METHOD

2.1. Cyber security awareness building

NIST special publication 800-16 distinguishes awareness from training and highlights its ability to modify behavior patterns or reinforce good security practices. The principal objective of awareness presentations is to draw attention to security-related topics, empowering people to recognize and resolve IT security vulnerabilities. On the other hand, training takes a more structured approach and seeks to develop knowledge and skills that will improve job performance [19]. The terms awareness is important for cyber security. Due to the increased usage of internet networks, the utilization of online services has rapidly expanded, resulting in an endless occurrence of cyberattacks and data breaches. Moreover, the nature of cyber-attacks and threats affecting online service users has evolved significantly, becoming increasingly sophisticated, paralleling the advancements in information and communication technology [20], [21]. As previously mentioned, promoting organizational awareness among users or all personnel within an organization regarding cyber security and learning how to appropriately handle cyber threats or attacks is crucial. Therefore, cyber security awareness is a key factor in organizational training to prepare for unforeseen incidents in the future [22]. When planning to enhance awareness within the organization, it is essential to analyze training needs and design programs suited to the organization's environment or culture, as the context of technology use varies across different business sectors [23], [24]. Regarding cyber security awareness, numerous factors influence this awareness, especially human factors. These factors include age, gender, education, and information technology experience [25], [26]. After reviewing previous research studies on the key success factors of cyber security awareness, we found many interesting studies that provide useful information and concepts applicable to this research, as shown in Table 1. This research proposes the development of tailored training programs that consider human factors in cybersecurity awareness, promote behavioral change, utilize the Delphi technique for expert insights, and create practical cybersecurity tools to enhance organizational preparedness.

Table 1. Summary of previous research works

Author	Research themes	Delivery methods	Main finding
Chen *et al.* [27]	Building security culture	Structural equation modeling (SEM)	Security education, training and awareness (SETA) program and security monitoring are importance in building security culture.
Kim *et al.* [28]	Understanding of the user behavior in cyber security context	A trend analysis an interview online survey study	This study presents an analysis of user characteristics concerning, i) cyber security awareness issues, ii) digital device usage, and iii) approaches to addressing privacy concerns in product usage.
Yeom *et al.* [29]	Security education	Training through scenario-based methodologies	Engaging in situation awareness training within real organizational settings leads trainees to become more familiar with system operations and perform more effectively compared to the traditional approach of building new systems and learning to use them for each scenario.
Alzahrani [30]	Cybersecurity awareness in students	Quantitative analysis	Institutions ought to incorporate education on anti-cybercrime legislation and pertinent information security awareness (ISA) issues identified within this study into their curriculum.
Grassegger and Nedbal [31]	Factors affecting ISA of employees	SEM	It is important for organizations to understand that technical measures alone are not enough to ensure information security. The promotion of ISA should be central to the development of information security protection measures.
Daengsi *et al.* [32]	Security awareness enhancement	Phishing scenario-based learning quantitative analysis	The concept of a cyber-attack simulation and knowledge transfer is highly recommended for use in other organizations, and in other countries as well, to enhance the cyber security awareness level of employees in order to prevent damage from cyber-attacks.

2.2. Delphi technique

The use of consensus-building strategies has increased as a result of the Delphi technique's ability to draw conclusions in the face of contradicting or insufficient data. Thus, the Delphi is a multistage, iterative procedure that combines opinion with group consensus [33]. The method of data analysis and results reporting are directly related to the type of questions used in the Delphi instrument. The Delphi method can be seen at its best as an expert method. Experts are often regarded as leaders in envisioning the future due to their extensive understanding across various fields such as technology, sociology, medicine, and politics, or their ability to creatively anticipate developments in these areas [34]. In the recruitment process for Delphi studies, the assembly of an expert panel and its composition is crucial, but it also poses methodological concerns that could potentially compromise the quality of the outcomes [35], [36]. Presently there is no agreement in the literature concerning expert panel size [37]. Varndell *et al.* [38] suggests that when a Delphi panel is homogenous 10 to 15 people are adequate. Grime and Wright [39] highlight the following principles for utilizing expert opinion in applications of the Delphi method.

a. Use experts with appropriate domain knowledge between 5 and 20 experts.
b. For Delphi feedback, provide the mean or median estimate of the panel plus the rationales from all panellists for their estimates.
c. Continue Delphi polling until the responses show stability, Generally, three structured rounds are enough.
d. Obtain the final forecast by weighing all the experts' estimates equally and aggregating them.

Beiderbeck *et al.* [40] delineated the procedural steps involved in executing the Delphi technique a methodological framework employed in scholarly endeavors to orchestrate and regulate structured group communication processes. Its primary objective is to elicit insights pertaining to existing or anticipated challenges, particularly in contexts characterized by limited data availability. Delphi studies commonly utilize rank-order questions, rating scales, or open-ended questions, with a predominant focus on gauging consensus levels among experts. Analogous to conventional research methodologies, empirical evidence suggests that engaging approximately 15 initial experts typically yields optimal results. After each round, panelists have the possibility to review the aggregate results and to reconsider their assessment based on the added quantitative and qualitative information [41]–[43]. The literature review uncovers research findings pertaining to cybersecurity obtained through the application of the Delphi method, as outlined in Table 2.

A key methodological approach in this research is the Delphi technique, which gathers insights from cybersecurity experts over multiple rounds of surveys or interviews. This method helps refine the proposed strategies for improving cybersecurity awareness by achieving consensus among professionals. The result is a set of validated recommendations that are both practical and grounded in expert knowledge.

Table 2. Summary of Delphi method in cyber security research area and related

Author	Participants	Rounds	Outcome	Main finding
Chowdhury *et al.* [44]	10	2	Cyber security training framework	The Delphi methodology was employed for the refinement and validation of researcher judgments throughout the iterative development process of the specialized issues training framework model.
Parekh *et al.* [45]	20	2	Core concepts of cyber security education	Providing a foundation for developing evidence-based, cyber security educational assessment tools that will identify and measure effective methods for teaching.
Haynes and Robinson [46]	15	2	Online risk to individuals.	The following topics were identified as priorities for further investigation: i) Personalization versus privacy, ii) Responsibility for privacy on social networks, iii) Measuring privacy risk and perceptions of power-lessness and iv) The resulting apathy.
Nugraha *et al.* [47]	20	3	Requirement for state cyber of defense against foreign intelligence surveillance	The people element is a current weakness in Indonesia. Creating a security mindset and a culture of cyber security awareness within the organizations are the biggest challenges.
Worrell *et al.* [48]	IT Auditor N=17 Business Manager N =15 IT Manager N = 12	3	IT risk factors	IT risk factors identified across all three expert panels, only three issues were common across all panels: i) lack of organizational alignment between business and IT, ii) interdependencies between systems, and technical complexity, and iii) The IT auditors panel consistently ranked issues related to IT governance.

3. RESEARCH METHOD

The Delphi technique is a structured approach used to guide expert discussions, aiming to generate insights on complex topics with limited available information. This method has gained prominence and is increasingly published across various academic fields. In this research, the Delphi technique was implemented in the context of cyber security to explore and formulate strategies for improving cyber awareness [40]. The research methodology is divided into 3 phases to facilitate the presentation of the overall research process. Specifically, Phase 3 will be explained in the results and discussion section. The details for Phases 1 and 2 are provided in Figure 1.

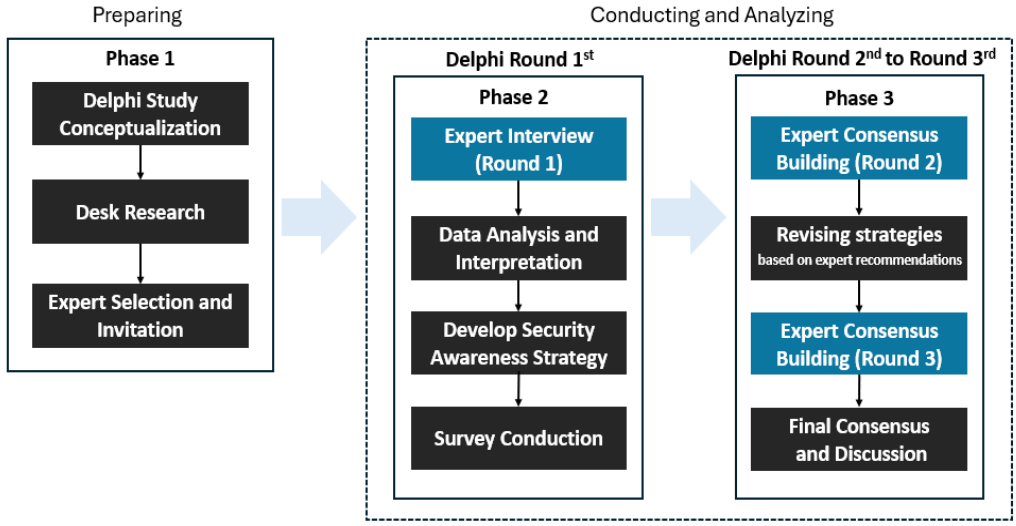

Figure 1. The research method

3.1. Delphi study conceptualization

Systematic preparation and planning are crucial tasks in the Delphi process, as they significantly impact its accuracy and validity [49], [50]. Therefore, it is essential to clearly define the scope of the Delphi process. This clarity helps researchers determine the desired outcomes of the Delphi process. The scope, as defined by the researcher, is detailed in Table 3.

Table 3. Delphi study overview

Delphi study goals	Delphi format	Delphi statement
a. Identify issues affecting cyber security awareness in organizations. b. Assist in developing guidelines for cyber security awareness.	a. Scope: cyber security awareness and human behavior in organizations. b. Theory/framework: NIST framework or related cyber security principles. c. Delphi structure: systematic multiple sequential rounds d. Data collection: using open-ended questions and questionnaires for collecting opinions and feedback.	The statement in this study is based on following: a. Human factors that affect security behavior. b. Challenges in implementing effective security awareness strategy.

3.2. Desk research

In addition to conducting a systematic literature review, the researcher has studied current trends in cyber security issues at both organizational and individual user levels. This includes examining emerging technologies to ensure that the scope leading to the design of the questionnaire is up to date. This approach aims to secure responses that are genuinely beneficial to the research.

3.3. Expert participation and invitation

The experts invited to participate in this Delphi process are 15 professionals working in the field of cybersecurity, both at the operational and executive levels. The selection criteria include educational background, roles and responsibilities, possession of cybersecurity certifications, and work experience [51]. The specific selection criteria are outlined in Table 4.

Table 4. Participant's information criteria

Education background	Professional experiences	Certification
Master's degree in computer engineering, computer science, information technology, or related fields.	Management level: 15 years Operations level: 5 years	Possessing an ANSI accredited cyber security certification, which guarantees adherence to ISO 17024.

3.4. Expert interview

During the first round of the Delphi, we scheduled all interviews for 60 minutes. The initial 15 minutes were dedicated to providing participants with an overview of the research background and explaining the key characteristics of a Delphi survey to ensure they understood the methodology. Following this, we allocated 30 minutes to an in-depth discussion on the primary challenges of developing a security awareness strategy, allowing participants to share their insights and experiences. Finally, we reserved the last 15 minutes of the interview to summarize the key points discussed, ensuring clarity and alignment on the main takeaways from the session.

3.5. Data analysis and interpretation

After interviewing all 15 experts through the first round of the Delphi process, the next step involves analyzing and interpreting the collected data to identify relationships and consistencies among the experts. This analysis will be conducted using qualitative data analysis tools. QDA Miner is a qualitative data analysis software that integrates advanced statistical and visualization tools, enabling rapid identification and exploration of patterns and trends in the scenarios.

3.6. Develop strategy and survey conduction

The development of strategies to enhance cybersecurity awareness within organizations will be undertaken after the analysis and interpretation of the data are completed. The researcher will develop these strategies based on the input from cybersecurity experts. Upon completion of strategy development, in the survey conduct process, the researcher will distribute questionnaires using a 5-point Likert scale to the 15 experts to achieve consensus [52]. Descriptive statistics, including arithmetic mean, interquartile ranges (IQR) and mode frequency (MOD), will be used to determine consensus. This will be carried out through the second and third rounds of the Delphi process. Von der Gracht's review of Delphi methodologies highlights that consensus measures such as mean and standard deviation, typically used for continuous scales or ratios, are not suitable for Likert-type scale surveys. Instead, mode and interquartile ranges (IQRs) are more relevant, with an IQR of 1 or less indicating consensus [53], [54]. An advantage of this approach is that outliers do not unduly affect the average score or the dispersion of scores.

Weighted Kappa was used to measure the stability of responses between the 2nd and 3rd round of Delphi. Weighted Kappa can be used to test the stability of ordinal responses in Delphi surveys by measuring within-participant agreement between rounds. This measure is more suitable than the unweighted Kappa test, which does not consider the size of disagreements between two scores. Kappa values between 0.81-0.99 indicate almost perfect agreement, 0.61-0.80 indicate substantial agreement, 0.41-0.60 indicate moderate agreement, and 0.21-0.40 indicate fair agreement [55].

4. RESULTS AND DISCUSSION

4.1. 1st round of Delphi method

The researcher analyzed interview data from 15 cybersecurity experts using the QDA Miner 3.0 software in the first round of the Delphi process. This approach ensured a systematic examination of qualitative data, enabling the identification of key themes. The analysis revealed four key issues that influence the promotion of cybersecurity awareness in organizations, as detailed in sub-sections 4.1.1 to 4.1.4.

4.1.1. The evolving landscape of cyber-attacks targeting individual

The analysis revealed that the most significant cyberattacks affecting end-users, as agreed upon by 14 out of 15 experts, are related to social media attacks and information gathering. This category includes phishing, romance scams, SMS phishing, vishing, and whaling. Additionally, 13 out of 15 experts expressed concern over malware, specifically ransomware and mobile malware targeting personal data and devices. Furthermore, 7 out of 15 experts noted the ongoing issue of pirated software use, which leads to other problems such as ransomware infections or unauthorized remote access to computers.

4.1.2. An analysis of security risks faced by modern organizations

14 out of the 15 experts concurred that a significant risk arises from not promoting cybersecurity awareness or training. They believe this neglect stems from a perception that such initiatives are time consuming and costly. This risk is often overlooked by executives, who view cybersecurity incidents as rare and place undue reliance on the organization's security technology. Additionally, 8 experts pointed out that most executives prefer to invest in IT services to enhance customer service rather than in security measures, as they do not see a tangible return on investment from the latter.

4.1.3. Beyond traditional threat: Emerging challenges to organizational cyber security

This issue is particularly noteworthy because 10 out of 15 experts agreed that the most frightening cybersecurity threat is actually the insider threat. In this context, insider threat refers to users who lack cybersecurity awareness and use technology carelessly, believing they are not likely targets for hackers. Additionally, 8 out of 15 experts highlighted the concern of supply chain attacks. These attacks target a company's procurement processes or internal operations. Attackers exploit weaknesses in these systems to undermine internal security, potentially inserting malicious software during the procurement process or altering confidential information. Such attacks can result in financial losses, impact brand networks or partners, and erode trust.

4.1.4. Optimizing security awareness initiatives: A guide to implementing problem-solving techniques in organizations

The experts proposed solutions to enhance cybersecurity awareness, emphasizing several key actions to prioritize for improving organizational cybersecurity awareness:

a. Cultivating cybersecurity awareness behaviour: establishing a culture where cybersecurity awareness becomes a habitual practice for all employees.
b. Mandatory training sessions: conducting cybersecurity awareness training at least once a year or whenever a cyber incident with potential organizational impact occurs.
c. Awareness testing: implementing awareness tests or evaluations after each training session to ensure that the training effectively increases awareness among employees.
d. Adopting cybersecurity frameworks: integrating a cybersecurity framework tailored to the organization's specific context.

All experts unanimously agreed that these measures should be immediately implemented by senior management to effectively enhance cybersecurity awareness within the organization.

4.2. Cyber security awareness strategy

All 15 experts unanimously agreed that enhancing cybersecurity awareness is crucial for fostering a secure culture within organizations. This secure culture leads to security-conscious behavior among all employees, not just end-users. Furthermore, the experts suggested that cybersecurity awareness training is

essential for bolstering the overall cybersecurity posture of an organization. They emphasized that cyber security should not focus solely on technology; the key lies in ensuring that everyone in the organization who uses technology adopts secure behavior. This holistic approach to cybersecurity integrates technological measures with the human element, ensuring that all employees understand and practice secure technology use. Building cybersecurity awareness might seem straightforward, but it is important to remember that each organization faces unique cyber threats due to differences in their information technology contexts. Therefore, fostering cybersecurity awareness behavior should focus on the risk scenarios that the organization has previously encountered. This approach leads to genuine solutions for the organization's cybersecurity challenges. The development strategy for raising cyber awareness is detailed in Figure 2.

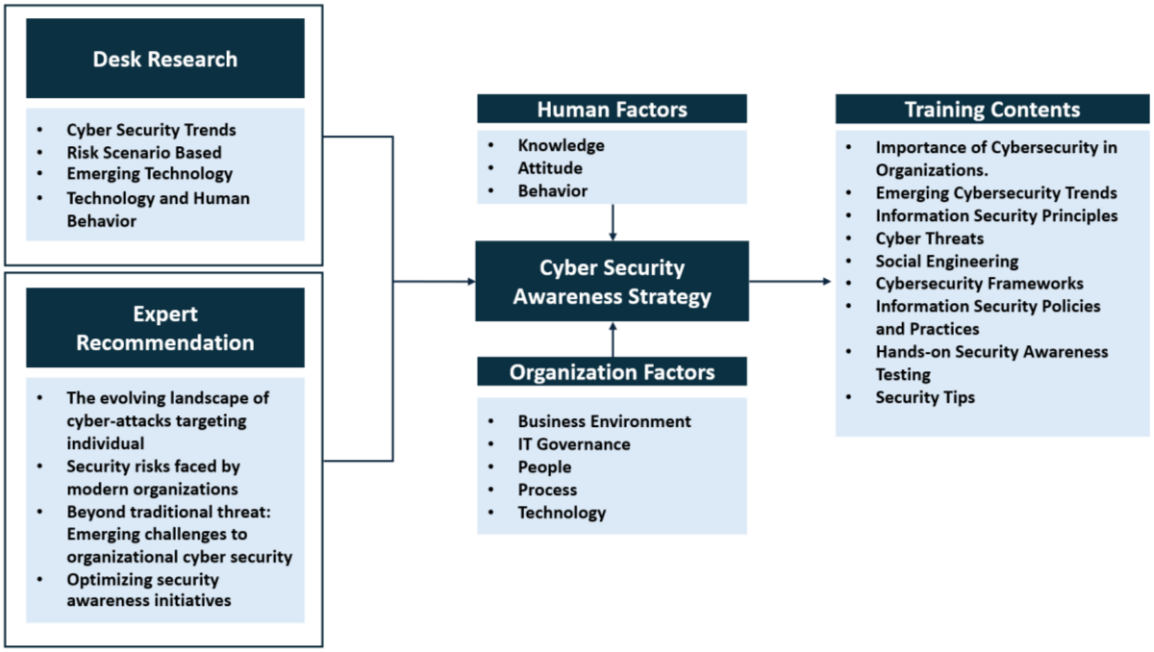

Figure 2. Cybersecurity awareness strategies development

Based on a review of related literature and desk research, which included studying cybersecurity risk management and industry trends, the training content scope was developed as follows:

a. Importance of cybersecurity in organizations: understanding the significance of cybersecurity based on the context of the organization's information technology and business operations.
b. Cyber threats: identifying and understanding various cyber threats.
c. Emerging cybersecurity trends: keeping up-to-date with the latest trends in cybersecurity.
d. Social engineering: recognizing and mitigating social engineering attacks.
e. Cybersecurity frameworks: implementing cybersecurity frameworks relevant to the organization.
f. Information security principles: fundamental principles of information security.
g. Information security policies and practices: establishing and adhering to robust information security policies and practices.
h. Hands-on security awareness testing: practical exercises such as phishing simulations to test and reinforce awareness.
i. Security tips: practical advice, such as using VirusTotal for checking files and links, and employing password managers for secure password practices.

4.3. Expert consensus building in the 2nd and 3rd rounds of Delphi

In the second round of the Delphi process, consensus among the 15 experts remained largely inconsistent. The experts recommended updating the training content to ensure it is current, easily understandable for non-technical users, and avoids delving too deeply into technical details. After revising the training content to be more comprehensive and user-friendly, all experts reached a consensus. The details are outlined in Table 5.

While previous studies have focused on the development of cyber security awareness programs, none have utilized the Delphi method to systematically gather expert opinions in the development process. This study is innovative as it applies Delphi methodology to create a tailored awareness program that not only considers a wide range of expert insights but also ensures the program's relevance and effectiveness through multiple rounds of expert feedback. Unlike prior works, which primarily rely on generalized surveys or existing frameworks, this approach allows for more precise and context-specific outcomes, addressing critical gaps in the current literature.

Table 5. Results of consensus analysis of Delphi statement

No.	Delphi statement	Delphi round 2			Delphi round 3			Weighted Kappa
		MEAN (R2)	MOD (R2)	IQR (R2)	MEAN (R3)	MOD (R3)	IQR (R3)	
1.	Instructional materials that are applicable to both everyday life and organizational functions.	3.3	3.0	1.0	4.4	4.0	1.0	0.85
2.	The training materials for instructional use are current and easily comprehensible.	3.5	4.0	1.0	4.7	5.0	1.0	0.68
3.	The IT Security department can utilize this set of training materials to conduct training sessions aimed at enhancing organizational awareness.	3.7	4.0	1.0	4.8	5.0	1.0	0.67
4.	Training materials that promote the development of learners' skills in secure and safe digital usage.	3.3	3.0	1.0	4.5	5.0	1.0	0.90
5.	Training materials aligns with international standards such as the NIST framework and ISO 27001:2022.	3.6	4.0	1.0	4.5	5.0	1.0	0.82
6.	Training materials enhance learners' awareness.	3.8	5.0	1.0	4.7	5.0	1.0	0.64
7.	This training manual assists personnel in understanding cyber security threats in various forms, as well as strategies for managing the diverse range of cyber threats prevalent today.	3.3	4.0	2.0	4.5	4.0	1.0	0.87
8.	The presentation of various scenario based cyber situations in the manual contributes to personnel developing security awareness behaviors.	3.6	3.0	1.0	4.5	4.0	1.0	0.78
9.	The training content helps staff understand how to configure privacy settings to prevent accidental exposure of personal information or data leaks to outsiders.	3.6	4.0	1.0	4.7	5.0	1.0	0.68
10.	Training aids personnel in fostering awareness to create complex passwords, thereby enhancing the security of their accounts	3.6	3.0	1.0	4.7	5.0	1.0	0.52
11.	The malware detection tools and URLs included in the training manual are presented clearly and simply, making them easy for end-users to understand.	3.8	4.0	0	4.6	5.0	1.0	0.80
12.	Learners can readily adhere to the cyber threat mitigation guidelines outlined in this manual.	3.7	4.0	1.0	4.7	5.0	1.0	0.70

4.4. Discussion

In the first round of the Delphi method, interviews with 15 experts revealed a consensus that sustainable cybersecurity within an organization must begin with users being aware of their role in maintaining the organization's security. This finding aligns with the broader research of Chen *et al.* [27], Kim *et al.* [28], Grassegger and Nedbal [31], and Daengsri *et al.* [32]. However, during the second and third rounds of the Delphi process, Kappa statistics analysis, as detailed in Table 5, highlighted some observations. Specifically, Delphi statements No. 4 and No. 7, which addressed the enhancement of skills and knowledge, exhibited high weighted Kappa values of 0.90 and 0.87, respectively, indicating almost perfect agreement among the experts. Conversely, Delphi statement No. 10, concerning individual-level security awareness, had a lower weighted Kappa value of 0.52, indicating moderate agreement. This discrepancy suggests that while experts agree that training content effectively enhances users' knowledge, it may not directly influence their cybersecurity behavior.

The research questions were thus addressed, confirming that the Delphi method can effectively identify key factors influencing the success of cybersecurity awareness initiatives within organizations and aid in formulating appropriate strategies. This finding is consistent with the research of Haynes and Robinson [51] who also employed the Delphi method, although their focus was on issues related to personal information disclosure rather than cybersecurity awareness. Nonetheless, the issue of user cybersecurity awareness remains within the scope of their research. It can therefore be concluded that the Delphi technique is effective in enhancing cybersecurity awareness and in identifying the organizational level challenges and solutions. The findings from the first round of the Delphi process provide crucial insights, and the subsequent rounds, supported by Kappa statistics, validate the proposed strategies through expert consensus. However, the strategies emerging from this study predominantly focus on education and awareness through training, which may be influenced by the fact that the participating experts were solely from the cybersecurity domain. Future research should include experts from other organizational fields, as this may reveal more effective strategies for enhancing cybersecurity awareness beyond those identified in the current study.

5. CONCLUSION

The Delphi method has demonstrated that a lack of cyber awareness among organizational personnel critically undermines overall cybersecurity efforts. This method effectively identifies and highlights specific issues that hinder awareness, enabling the development of targeted, systematic strategies for improvement. Consequently, it is crucial for organizations to shift their approach to cybersecurity from being solely the responsibility of the technical department to being a shared concern across all levels of the organization. Promoting cybersecurity as a collective responsibility is essential for fostering a culture of security and achieving long-term, sustainable protection against cyber threats.

However, this study is limited because it only includes perspectives from cybersecurity professionals. To better understand how cyber awareness affects organizational security, future research should actively involve experts from other departments. Gaining these diverse insights will offer a more complete view of the organizational dynamics and help develop more effective strategies to enhance cybersecurity awareness throughout the organization.

ACKNOWLEDGMENTS

The author would like to thank the experts who participated in the Delphi process, as well as those involved in providing valuable information for this research.

FUNDING INFORMATION

There is no financial support for this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Anawin Kaewsa-ard	✓	✓	✓			✓	✓	✓	✓					
Nattavee Utakrit	✓			✓	✓			✓		✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors would like to inform that there is no conflict of interest.

INFORMED CONSENT

The authors obtained comprehensive informed consent documentation, including written permission from all participants, prior to their inclusion in the study. In terms of the tools used for data collection, they have been reviewed and approved for human research ethics by the Human Research Ethics Committee under the collaboration Naresuan University Network Research Ethics (NU-NREC), Thailand.

ETHICAL APPROVAL

This research did not involve any practices related to animals and vulnerable groups. However, the authors have considered and complied with all relevant national regulations and institutional policies regarding the care and use of human rights.

DATA AVAILABILITY

The data that supports the findings of this study are available from the corresponding author, NU, upon reasonable request.

REFERENCES

[1] M. Fanea-Ivanovici and M.-C. Pana, "From culture to smart culture. how digital transformations enhance citizens' well-being through better cultural accessibility and inclusion," *IEEE Access*, vol. 8, pp. 37988–38000, 2020, doi: 10.1109/ACCESS.2020.2975542.

[2] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, p. 23, May 2021, doi: 10.3390/bdcc5020023.

[3] R. Willison, M. Warkentin, and A. C. Johnston, "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives," *Information Systems Journal*, vol. 28, no. 2, pp. 266–293, Mar. 2018, doi: 10.1111/isj.12129.

[4] H. Taherdoost, "A critical review on cybersecurity awareness frameworks and training models," *Procedia Computer Science*, vol. 235, pp. 1649–1663, 2024, doi: 10.1016/j.procs.2024.04.156.

[5] P. Limna, T. Kraiwanit, and S. Siripipattanakul, "The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand," *International Journal of Computing Sciences Research*, vol. 7, pp. 1133–1151, Jan. 2023, doi: 10.25147/ijcsr.2017.001.1.123.

[6] O. A. Popoola, M. O. Akinsanya, G. Nzeako, E. G. Chukwurah, and C. D. Okeke, "Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and U.S. Initiatives," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 5, pp. 819–827, May 2024, doi: 10.51594/ijarss.v6i5.1104.

[7] M. P. Aphane, "Cybersecurity awareness on cybercrime among the Youth in Gauteng Province," *International Journal of Social Science Research and Review*, vol. 6, no. 8, pp. 23–32, Aug. 2023, doi: 10.47814/ijssrr.v6i8.1414.

[8] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, "An analysis on the dimensions of information security culture concept: a review," *Journal of Information Security and Applications*, vol. 44, pp. 12–22, Feb. 2019, doi: 10.1016/j.jisa.2018.11.003.

[9] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: current practices and future needs," *Computers & Security*, vol. 109, p. 102387, Oct. 2021, doi: 10.1016/j.cose.2021.102387.

[10] U. D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2–35, Mar. 2019, doi: 10.1108/JSIT-02-2018-0028.

[11] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: a practice perspective," *Computers & Security*, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.

[12] F. A. Aloul, "The need for effective information security awareness," *Journal of Advances in Information Technology*, vol. 3, no. 3, Aug. 2012, doi: 10.4304/jait.3.3.176-183.

[13] M. A. Sasse, J. Hielscher, J. Friedauer, and A. Buckmann, "Rebooting IT security awareness – how organisations can encourage and sustain secure behaviours," in *European Symposium on Research in Computer Security*, 2023, pp. 248–265.

[14] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "Critical success factors for security education, training and awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives," *Information & Computer Security*, vol. 32, no. 1, pp. 53–73, Jan. 2024, doi: 10.1108/ICS-08-2022-0133.

[15] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: a systematic literature review," *Computers & Security*, vol. 106, p. 102267, Jul. 2021, doi: 10.1016/j.cose.2021.102267.

[16] M. A. Alnsour, "Using modified grounded theory for conducting systematic research study on sustainable project management field," *MethodsX*, vol. 9, p. 101897, 2022, doi: 10.1016/j.mex.2022.101897.

[17] R. A. Green, "The Delphi technique in educational research," *Sage Open*, vol. 4, no. 2, Jan. 2014, doi: 10.1177/2158244014529773.

[18] J. Nworie, "Using the Delphi technique in educational technology research," *TechTrends*, vol. 55, no. 5, pp. 24–30, Sep. 2011, doi: 10.1007/s11528-011-0524-6.

[19] M. Wilson, D. E. de Zafra, S. I. Pitcher, J. D. Tressler, and J. B. Ippolito, "Information technology security training requirements : a role-and performance-based model," *NIST Special Publication 800-16*, Gaithersburg, MD, 1998. doi: 10.6028/NIST.SP.800-16.

[20] B. Madnick, K. Huang, and S. Madnick, "The evolution of global cybersecurity norms in the digital age: a longitudinal study of the cybersecurity norm development process," *Information Security Journal: A Global Perspective*, vol. 33, no. 3, pp. 204–225, May 2024, doi: 10.1080/19393555.2023.2201482.

[21] B.-H. Kim, K.-C. Kim, S.-E. Hong, and S.-Y. Oh, "Development of cyber information security education and training system," *Multimedia Tools and Applications*, vol. 76, no. 4, pp. 6051–6064, Feb. 2017, doi: 10.1007/s11042-016-3495-y.

[22] S. Alahmari, K. Renaud, and I. Omoronyia, "Moving beyond cyber security awareness and training to engendering security knowledge sharing," *Information Systems and e-Business Management*, vol. 21, no. 1, pp. 123–158, Mar. 2023, doi: 10.1007/s10257-022-00575-2.

[23] 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), Jun. 2021, pp. 102–106, doi: 10.1109/ICSCEE50312.2021.9498208.
[24] J. Khan, M. Jaafar, N. Mubarak, and A. K. Khan, "Employee mindfulness, innovative work behaviour, and IT project success: the role of inclusive leadership," *Information Technology and Management*, vol. 25, no. 2, pp. 145–159, Jun. 2024, doi: 10.1007/s10799-022-00369-5.
[25] M. V. Bordonaba-Juste, L. Lucia-Palacios, and R. Pérez-López, "Generational differences in valuing usefulness, privacy and security negative experiences for paying for cloud services," *Information Systems and e-Business Management*, vol. 18, no. 1, pp. 35–60, 2020, doi: 10.1007/s10257-020-00462-8.
[26] R. Ismailova, G. Muhametjanova, T. D. Medeni, I. T. Medeni, D. Soylu, and O. A. Dossymbekuly, "Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan," *Information Security Journal: A Global Perspective*, vol. 28, no. 4–5, pp. 127–135, Sep. 2019, doi: 10.1080/19393555.2019.1685142.
[27] Y. Chen, K. (Ram) Ramamurthy, and K.-W. Wen, "Impacts of comprehensive information security programs on information security culture," *Journal of Computer Information Systems*, vol. 55, no. 3, pp. 11–19, Mar. 2015, doi: 10.1080/08874417.2015.11645767.
[28] E. Kim, J. K. Yoon, J. Kwon, T. Liaw, and A. M. Agogino, "From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity," *Proceedings of the International Conference on Engineering Design, ICED*, pp. 1773–1782, 2019, doi: 10.1017/dsi.2019.183.
[29] S. Yeom, D. Shin, and D. Shin, "Scenario-based cyber attack·defense education system on virtual machines integrated by web technologies for protection of multimedia contents in a network," *Multimedia Tools and Applications*, vol. 80, no. 26–27, pp. 34085–34101, Nov. 2021, doi: 10.1007/s11042-019-08583-0.
[30] L. Alzahrani, "Statistical analysis of cybersecurity awareness issues in higher education institutes," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 11, pp. 630–637, 2021, doi: 10.14569/IJACSA.2021.0121172.
[31] T. Grassegger and D. Nedbal, "The role of employees' information security awareness on the intention to resist social engineering," *Procedia Computer Science*, vol. 181, pp. 59–66, 2021, doi: 10.1016/j.procs.2021.01.103.
[32] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks," *Education and Information Technologies*, vol. 27, no. 4, pp. 4729–4752, May 2022, doi: 10.1007/s10639-021-10806-7.
[33] F. Hasson, "Research guidelines for the Delphi survey technique," *Journal of Advanced Nursing*, vol. 32, no. 4, p. 1008, Oct. 2000, doi: 10.1046/j.1365-2648.2000.01567.x.
[34] K. K. Lilja, K. Laakso, and J. Palomki, "Using the Delphi method," *PICMET: Portland International Center for Management of Engineering and Technology, Proceedings*, 2011.
[35] E. Hohmann, M. P. Cote, and J. C. Brand, "Research pearls: expert consensus based evidence using the Delphi method," *Arthroscopy: The Journal of Arthroscopic & Related Surgery*, vol. 34, no. 12, pp. 3278–3282, Dec. 2018, doi: 10.1016/j.arthro.2018.10.004.
[36] S. Keeney, F. Hasson, and H. P. McKenna, "A critical review of the Delphi technique as a research methodology for nursing," *International Journal of Nursing Studies*, vol. 38, no. 2, pp. 195–200, Apr. 2001, doi: 10.1016/S0020-7489(00)00044-4.
[37] S. McPherson, C. Reese, and M. C. Wendler, "Methodology update," *Nursing Research*, vol. 67, no. 5, pp. 404–410, Sep. 2018, doi: 10.1097/NNR.0000000000000297.
[38] W. Varndell, M. Fry, and D. Elliott, "Applying real-time Delphi methods: development of a pain management survey in emergency nursing," *BMC Nursing*, vol. 20, no. 1, p. 149, Dec. 2021, doi: 10.1186/s12912-021-00661-9.
[39] M. M. Grime and G. Wright, "Delphi method," in *Wiley StatsRef: Statistics Reference Online*, Wiley, 2016, pp. 1–6.
[40] D. Beiderbeck, N. Frevel, H. A. von der Gracht, S. L. Schmidt, and V. M. Schweitzer, "Preparing, conducting, and analyzing Delphi surveys: cross-disciplinary practices, new directions, and advancements," *MethodsX*, vol. 8, p. 101401, 2021, doi: 10.1016/j.mex.2021.101401.
[41] F. Bolger and G. Wright, "Improving the Delphi process: lessons from social psychological research," *Technological Forecasting and Social Change*, vol. 78, no. 9, pp. 1500–1513, 2011, doi: 10.1016/j.techfore.2011.07.007.
[42] G. Rowe and G. Wright, "The Delphi technique: past, present, and future prospects-introduction to the special issue," *Technological Forecasting and Social Change*, vol. 78, no. 9, pp. 1487–1490, Nov. 2011, doi: 10.1016/j.techfore.2011.09.002.
[43] A. J. Fletcher and G. P. Marchildon, "Using the Delphi method for qualitative, participatory action research in health leadership," *International Journal of Qualitative Methods*, vol. 13, no. 1, pp. 1–18, Feb. 2014, doi: 10.1177/160940691401300101.
[44] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: a delphi method-based study," *Computers & Security*, vol. 113, p. 102551, Feb. 2022, doi: 10.1016/j.cose.2021.102551.
[45] G. Parekh *et al.*, "Identifying core concepts of cybersecurity: results of two Delphi processes," *IEEE Transactions on Education*, vol. 61, no. 1, pp. 11–20, Feb. 2018, doi: 10.1109/TE.2017.2715174.
[46] D. Haynes and L. Robinson, "Delphi study of risk to individuals who disclose personal information online," *Journal of Information Science*, vol. 49, no. 1, pp. 93–106, Feb. 2023, doi: 10.1177/0165551521992756.
[47] Y. Nugraha, I. Brown, and A. S. Sastrosubroto, "An adaptive wideband Delphi method to study state cyber-defence requirements," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 47–59, Jan. 2016, doi: 10.1109/TETC.2015.2389661.
[48] J. L. Worrell, P. M. Di Gangi, and A. A. Bush, "Exploring the use of the Delphi method in accounting information systems research," *International Journal of Accounting Information Systems*, vol. 14, no. 3, pp. 193–208, Sep. 2013, doi: 10.1016/j.accinf.2012.03.003.
[49] B. Förster and H. von der Gracht, "Assessing Delphi panel composition for strategic foresight-a comparison of panels based on company-internal and external participants," *Technological Forecasting and Social Change*, vol. 84, pp. 215–229, May 2014, doi: 10.1016/j.techfore.2013.07.012.
[50] L. Devaney and M. Henchion, "Who is a Delphi 'expert'? reflections on a bioeconomy expert selection procedure from Ireland," *Futures*, vol. 99, pp. 45–55, May 2018, doi: 10.1016/j.futures.2018.03.017.
[51] A. Kaewsa-ard and N. Utakrit, "Identifying key issues to enhance the cybersecurity awareness strategy within organizations," in *Lecture Notes in Networks and Systems*, 2024, pp. 1–11.
[52] L. Giannarou and E. Zervas, "Using Delphi technique to build consensus in practice," *International Journal of Business Science and Applied Management*, vol. 9, no. 2, pp. 65–82, 2014.
[53] M. Barrios, G. Guilera, L. Nuño, and J. Gómez-Benito, "Consensus in the delphi method: What makes a decision change?," *Technological Forecasting and Social Change*, vol. 163, p. 120484, Feb. 2021, doi: 10.1016/j.techfore.2020.120484.
[54] H. A. von der Gracht, "Consensus measurement in Delphi studies," *Technological Forecasting and Social Change*, vol. 79, no. 8, pp. 1525–1536, Oct. 2012, doi: 10.1016/j.techfore.2012.04.013.
[55] S. Abdi, L. de Witte, and M. Hawley, "Exploring the potential of emerging technologies to meet the care and support needs of older people: a Delphi survey," *Geriatrics*, vol. 6, no. 1, p. 19, Feb. 2021, doi: 10.3390/geriatrics6010019.

BIOGRAPHIES OF AUTHORS

Anawin Kaewsa-Ard received the B.Eng. degree in computer engineering from Thai-Nichi Institute of Technology, in 2013 and the M.S. degrees in management information systems from King Mongkut's University of Technology North Bangkok, in 2015. Currently, he is a Ph.D. Candidate of the Department of Information Technology Management from King Mongkut's University of Technology North Bangkok. His current research interests are cybersecurity management, cybersecurity awareness, information assurance, IT governance risk and compliance, cyber security strategies development, and management information systems. He can be contacted at an email: s6307021910041@email.kmutnb.ac.th.

Nattavee Utakrit received a doctoral degree from Edith Cowan University (ECU), Australia, in 2006 in information technology. He works as a lecturer and a researcher at the Department of Information Technology Management, Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand. He is also a member of the applied information systems research division (AIS) at KMUTNB. He can be contacted at an email: nattavee.u@itd.kmutnb.ac.th.