Hacettepe Üniversitesi Eğitim Fakültesi Dergisi

Hacettepe University Journal of Education

e-ISSN: 2536-4758



Development of Organizational Cybersecurity Awareness Scale (OCAS)*

Nimet Özgül ÜNSAL, Mehmet Akif OCAK*****

Article Information

Received: 10.07.2025

Accepted: 31.12.1015

Online First: 18.01.2026

Published: 31.01.2026

ABSTRACT

This study reports the development and validation of the Organizational Cybersecurity Awareness Scale (OCAS) for employees in public institutions. The scale comprises four dimensions: (1) Personal Awareness and Proactive Approach, (2) Legal and Regulatory Awareness, (3) Technical Protection and Implementation, and (4) Organizational Policy Awareness, with a total of 26 items. Data were collected in 2021 from 110 employees working in two public organizations to evaluate the scale's EFA analysis. Exploratory Factor Analysis (EFA) was conducted to establish the dimensional structure of the scale. The Kaiser-Meyer-Olkin measure of sampling adequacy was 0.942, indicating excellent factorability. The four-factor solution explained 60.02% of the total variance: Factor 1 (Personal Awareness and Proactive Approach) accounted for 39.54%, Factor 2 (Legal and Regulatory Awareness) for 11.19%, Factor 3 (Technical Protection and Implementation) for 4.76%, and Factor 4 (Organizational Policy Awareness) for 4.53%. All 26 items demonstrated satisfactory factor loadings, and no items required deletion. Confirmatory Factor Analysis (CFA) was performed to test the hypothesized factor structure. The overall scale demonstrated excellent internal consistency (Cronbach's $\alpha = 0.936$). Although the chi-square test was significant ($\chi^2 = 7952.667$, $df = 325$, $N = 544$, $p < .05$), which is common in large samples, other fit indices indicated acceptable model fit: Standardized RMR = 0.085 and RMSEA = 0.083. To test the hypothesized four-factor structure derived from EFA, CFA was performed by using another 544 employees. These results support the four-dimensional structure and demonstrate that the OCAS is a reliable and valid instrument for measuring cybersecurity awareness among public sector employees.

Keywords: Cybersecurity awareness, public employees, scale development, organizational security, psychometric validation

doi: 10.16986/hunefd.1739282 Article Type: Research Article

Citation Information: Ünsal, N. Ö., & Ocak, M. A. (2026). Develoment of organizational cybersecurity awareness scale (OCAS). *Hacettepe University Journal of Education, 41*(1), 136-155. https://doi.org/10.16986/hunefd.1739282

1. INTRODUCTION

1.1. The Critical Importance of Cybersecurity Awareness

As technology has become integral to daily life and organizational operations, cybersecurity has emerged as a critical concern for institutions. While technological advancement enables organizations to perform tasks more efficiently and creatively, it simultaneously introduces significant security challenges that require systematic attention (Georgiadou et al., 2020). The increasing sophistication of cyber threats, combined with the expanding digital footprint of organizations, has made cybersecurity awareness a fundamental competency for all employees, particularly those in public sector institutions that manage sensitive government data and critical infrastructure (Di Nocera et al., 2024; Faklaris et al., 2022).

* This research was ethically approved by the Gazi University Ethics Committee with its decision dated 04.05.2021and numbered 08. This research was derived from the doctoral thesis conducted by the first author under the supervision of the second author.

** Lecturer Doctor, Ankara University, Elmadağ Vocational School, Department of Office Management and Secretarial, Ankara-TÜRKİYE. e-mail: nounsal@ankara.edu.tr (ORCID: 0000-0002-8864-9159)

*** Prof. Dr., Gazi University, Faculty of Gazi Education, Department of Computer Education and Instructional Technologies, Division of Computer Education and Instructional Technologies, Ankara-TÜRKİYE. e-mail: maocak@gazi.edu.tr (ORCID: 0000-0001-8405-1574)

Cybersecurity threats have escalated dramatically in organizational contexts, with human factors identified as the weakest link in security systems. Organizations worldwide face increasing risks from phishing attacks, social engineering, malware infections, and insider threats, all of which exploit gaps in employee cybersecurity awareness (Al-Shanfari et al., 2022; Almuqrin et al., 2024). The consequences of inadequate cybersecurity awareness extend beyond financial losses to include reputational damage, regulatory penalties, and compromised citizen data—particularly critical concerns for public sector organizations that manage sensitive government and citizen information (Sulaiman et al., 2022). Research has consistently documented that employee knowledge gaps and behavioral vulnerabilities create significant organizational risks, with studies indicating that up to 60% of employees lack basic cybersecurity awareness necessary for protecting organizational assets (Nikel & Amaechi, 2022; Fadhil, & Yazid, 2023).

Shaw et al. (2009) define cybersecurity awareness as the extent to which organizational members understand information security responsibilities and actively engage in behaviors that protect information systems and data. This definition emphasizes both the cognitive dimension (understanding) and the behavioral dimension (active engagement) of cybersecurity awareness. Cybersecurity threats operate at multiple levels, from individual users to national infrastructure, creating a complex web of vulnerabilities that organizations must address (Faklaris et al., 2022). Individual security behaviors can have cascading effects on organizational and national security, as demonstrated by large-scale cyberattacks such as Stuxnet, which exploited individual-level vulnerabilities to compromise critical infrastructure (Langner, 2011; Li et al., 2019; Parsons et al., 2017). Consequently, the cybersecurity awareness of employees is fundamental to organizational security posture. Given that organizations operate through interconnected systems, vulnerabilities at the individual or institutional level can escalate into national-level cybersecurity risks, making employee awareness a matter of strategic importance.

Based on comprehensive analysis of the current cybersecurity measurement literature, this study demonstrates that: (a) OCAS addresses critical psychometric and contextual gaps that existing instruments fail to address; (b) awareness and resilience are complementary rather than competing constructs, with awareness serving as a foundational prerequisite for organizational resilience; and (c) existing instruments suffer from fundamental limitations that justify the development of OCAS. The development of OCAS is not only justified but essential for advancing both cybersecurity awareness research and practical organizational assessment in public sector contexts. Rather than duplicating existing work, OCAS addresses fundamental gaps and provides a validated foundation for future integration with broader resilience measurement approaches.

1.2. The Problem: Critical Limitations of Existing Measurement Approaches

Despite widespread recognition of cybersecurity awareness as essential for organizational protection, systematic assessment remains problematic. Current measurement approaches suffer from fundamental limitations that restrict both research validity and practical utility. Systematic reviews reveal that most cybersecurity awareness studies employ self-report measures constructed ad-hoc by adapting items from prior literature without rigorous psychometric validation (Kannelønning & Katsikas, 2023). This ad-hoc approach creates instruments with unknown reliability, questionable construct validity, and limited comparability across studies, undermining confidence in research findings and organizational assessment.

Steinbart et al. (2016) reinforced this problem, finding that many firms fail to implement the essential procedures and training to secure their information systems versus cyberattacks, resulting in backdoors and system vulnerabilities that unauthorized users can exploit. Similarly, Creasey (2013) attributed this institutional vulnerability to a lack of knowledge and resources. Although new technologies are rapidly being integrated into organizational processes, cybersecurity awareness does not appear to be increasing at the same pace (Zwilling et al., 2022). In addition to insufficient cybersecurity awareness, users often lack knowledge on how to protect themselves from cyberattacks (Kovacevic et al., 2022) and are unaware of how to keep their data secure (Korovessis et al., 2017; Kruger, & Kearney, 2006). As cyberattacks increasingly target individuals and become more sophisticated, organizations are compelled to strengthen their cybersecurity efforts (Abawajy, 2014).

Kannelønning and Katsikas (2023) conducted a systematic literature review of cybersecurity behavior assessment and found that researchers commonly compose measurement scales by selecting and adapting items from various sources rather than developing validated instruments through systematic scale development procedures. This predominance of ad-hoc instrument construction inflates measurement error, reduces statistical power, and limits the ability of organizations to reliably compare their cybersecurity awareness levels across time, departments, or against benchmarks. Without validated instruments, organizations cannot confidently evaluate interventions or allocate resources effectively (Marnewick, & von Solms, 2022).

Moreover, existing scales predominantly measure individual-level cognitions and behaviors while neglecting critical organizational-level factors. Research demonstrates that organizational factors—including senior management commitment, policy effectiveness, legal and regulatory pressures, and technical infrastructure—significantly influence employee cybersecurity behavior (AlMindeel & Martins, 2020; Kumar et al., 2021). However, most measurement instruments fail to capture these organizational dimensions, focusing instead on individual-level constructs borrowed from health behavior or technology adoption theories (Chapman, 2019).

This individual-level focus provides incomplete diagnostic information, emphasizing individual deficits while obscuring systemic factors such as inadequate policies, insufficient management support, or technical barriers that may be the true impediments to improved cybersecurity awareness. Kävrestad et al. (2024) emphasized a taxonomy created in line with the data obtained from the examination of public institutions in literature review, indicating attention to cybersecurity awareness training in institutions and the need to measure the impact of education and training activities (Table 1).

Table 1.
Consistently Measuring and Evaluating the Effectiveness of Cybersecurity Awareness Training (adapted from Kävrestad et al., 2024)

Cybersecurity Education, Training & Awareness	• Attend CSA events & seminars as part of the educations • Include just-in-time learning in CSA training • Be up-to-date with cybersecurity threat landscape, information & technology • Strategically place mixes of tailored message framings to spread CSA in the organization • Conduct consistent assessment & evaluation of the effectiveness of CSA education • Base CSA training on real-world scenarios • Combine multiple delivery methods for CSA training • Maintain continual reinforcement of CSA training • Provide easy access to CSA training material • Base CSA training on latest cyber-attack strategies • Establish CSA education tailored to the organization's vision & goals • Provide users with continuous feedback on their progress of CSA training • Establish tailored CSA training based on user's individual needs, perceptions & learning style

Based on existing literature review, it is clearly shown that there is no scale developed directly to measure cybersecurity awareness training for public employees within the scope of the research. As cyberattacks increasingly target individuals and become more sophisticated, organizations are compelled to strengthen their cybersecurity efforts (Abawajy, 2014). The scales in the literature are shown in Table 2.

Table 2.
Scales Developed for Information Security Awareness and Cyber Security Awareness

	Author Name	Scale Name	Sample
1	Keser, & Güldüren (2015)	Information Security Awareness Scale	It measures adults' information security awareness.
2	Güldüren, Çetinkaya, & Keser (2016)	Information Security Awareness Scale	It measures the security awareness of secondary school students.
3	He & Zhang (2019)	Cybersecurity Awareness Inventory (CAIN)	It is an inventory conducted on university students to identify information processing security behaviors.
4	Arpaci, & Sevinc (2021)	Cyber Security Scale	It measures individuals' practices and perceptions regarding cyber security.
5	Arpaci, & Aslan (2022)	Social media Cyber Crime Awareness Scale (CASM-S)	Measures social media Cyber Crime Awareness of Social Media users.
6	Aşan (2024)	Cyber Security Awareness Scale	To assess the perception of cybersecurity in the maritime industry.
7	Bognár & Bottyán (2024)	Cyber Security Awareness Scale	It measures the cyber security awareness of university students.

Current instruments also rarely differentiate between decision-maker awareness and frontline employee awareness, despite evidence that these groups face different cybersecurity challenges and require different interventions (Vrhovec & Markelj, 2024). Similarly, scales developed in one national or sectoral context are often applied elsewhere without validation, reducing measurement validity. Many existing frameworks and scales are theoretically sophisticated but difficult to operationalize in organizational settings and provide limited guidance for designing targeted interventions (Chapman, 2019; MIHAI, 2024).

1.3. Public Sector Context and the Need for Validated Organizational Measurement

These limitations are particularly acute in public sector contexts, where organizations face unique challenges including complex regulatory requirements, resource constraints, diverse workforces, and mission-critical services with public safety implications (Sulaiman et al., 2022). Public sector organizations must comply with multiple, often overlapping regulatory frameworks (data

protection laws, sector-specific regulations, government security standards), creating complex awareness requirements not captured by generic scales (AlMindeel & Martins, 2020). Public organizations frequently operate under tighter budget constraints than private sector counterparts, requiring efficient, targeted interventions guided by precise diagnostic measurement. Public sector employees span wide ranges of technical expertise, educational backgrounds, and job roles, necessitating measurement instruments that can reliably assess awareness across this diversity (Al-Shanfari et al., 2022).

Furthermore, scales developed in Western contexts often lack validation in developing country settings, potentially missing culturally and institutionally salient aspects of cybersecurity awareness (AlMindeel & Martins, 2020; Georgiadou et al., 2020; Hadlington, 2017). The Turkish public sector, undergoing rapid digital transformation amid evolving regulatory frameworks, requires validated measurement instruments that capture both universal and context-specific dimensions of organizational cybersecurity awareness. Turkey presents a particularly important context for cybersecurity awareness scale development and validation as a developing country facing specific cybersecurity awareness challenges related to varying levels of digital literacy, resource limitations, and evolving regulatory frameworks that may differ from contexts where most existing scales were developed.

1.4. Research Contribution and Study Objectives

Developing the Organizational Cybersecurity Awareness Scale (OCAS) addresses these critical gaps by providing a rigorously validated, organizationally-focused, context-specific measurement instrument. The OCAS offers: (1) a psychometrically sound scale developed following established procedures (item generation, content validation, exploratory factor analysis, confirmatory factor analysis, reliability assessment); (2) an organizational-level focus with explicit measurement of organizational dimensions (policy awareness, legal/regulatory compliance, technical implementation) alongside individual awareness; (3) context-specific validation for Turkish public sector organizations, ensuring cultural and institutional relevance; (4) a multi-dimensional structure enabling targeted diagnosis and intervention design; and (5) practical utility with a clear factor structure that maps directly to actionable organizational improvements (training, policy, technical controls, leadership).

The primary objective of this study is to develop and validate a comprehensive, multi-dimensional scale for measuring cybersecurity awareness among public sector employees in Turkey. Specific aims include: establishing the dimensional structure of cybersecurity awareness in organizational contexts, evaluating the psychometric properties (reliability and validity) of the developed scale, and providing a validated instrument that can be used for assessment, program evaluation, and research in public sector organizations.

2. THEORETICAL FRAMEWORK AND CONCEPTUAL FOUNDATION

2.1. Overview of Cybersecurity Awareness Frameworks

Cybersecurity awareness research draws on multiple theoretical traditions, each emphasizing different determinants of security behavior. Understanding these frameworks and their relative strengths and limitations is essential for justifying the theoretical foundation of the OCAS. The primary frameworks in the literature include:

Knowledge-Attitude-Behavior (KAB) Model: The KAB model posits a sequential pathway where knowledge influences attitudes, which in turn shape behaviors. This linear progression assumes that increasing knowledge will improve attitudes and ultimately change behavior (Al-Shanfari et al., 2022). While simple and easy to operationalize, KAB focuses narrowly on individual cognition and learning, potentially missing social, organizational, and contextual drivers that are critical in organizational settings (Al-Shanfari et al., 2022; Pasipamire, 2025). The KAB model's emphasis on individual-level constructs makes it effective for basic awareness assessment and educational program evaluation, but inadequate for comprehensive organizational diagnosis.

Protection Motivation Theory (PMT): PMT emphasizes threat appraisal (perceived severity and vulnerability) and coping appraisal (self-efficacy, response efficacy, response costs) as determinants of protective behavior (Sulaiman et al., 2022; Vortia, 2025). PMT has robust empirical support in organizational and public sector contexts where threat and coping perceptions predict protective behaviors and intentions (Sulaiman et al., 2022; Almuqrin et al., 2024). However, PMT focuses primarily on individual motivation and threat perceptions, and does not inherently address organizational policies, management support, regulatory requirements, or technical infrastructure. Empirical studies often extend or combine PMT with other theories to address these gaps (Chapman, 2019; Georgiadou et al., 2020).

Theory of Planned Behavior (TPB): TPB incorporates attitudes, subjective norms, and perceived behavioral control as predictors of intentions and behavior (Georgiadou et al., 2020). TPB captures social influences and control perceptions that PMT may not emphasize, and has been useful in combined models predicting cybersecurity intentions. However, TPB is an individual-level theory that requires extension to address organizational policies and technical infrastructure. While TPB's inclusion of subjective norms

addresses some social context, it does not fully capture organizational policies, management influence, or institutional pressures relevant in workplace settings (Chapman, 2019; Georgiadou et al., 2020).

Human-Organization-Technology (HOT) Framework: The HOT framework recognizes that cybersecurity awareness emerges from interactions among human factors (individual knowledge, attitudes, behaviors), organizational factors (management commitment, policies, culture, regulatory compliance), and technological factors (technical controls, infrastructure, implementation practices) (AlMindeel & Martins, 2020; Kumar et al., 2021). HOT explicitly captures multi-level determinants essential for organizational contexts, providing organizational realism that reflects the actual complexity of organizational cybersecurity. Studies demonstrate that organizational factors (senior management commitment, policy effectiveness) and technical measures are critical antecedents for enhanced cybersecurity in organizational settings, supporting HOT's multi-dimensional approach (AlMindeel & Martins, 2020; Kumar et al., 2021).

Integrated Behavioral Model (IBM): IBM integrates constructs from multiple theories (TPB, Social Cognitive Theory, Health Belief Model) into a comprehensive framework that recognizes both individual and contextual determinants of behavior (Schütz & Fertig, 2023). While comprehensive and validated for information security awareness constructs, IBM's broader construct set requires extensive measurement, increasing participant burden and validation requirements. This complexity may be impractical in organizational settings where survey participation competes with work demands and where rapid assessment is needed (Schütz & Fertig, 2023).

Security Education, Training, and Awareness (SETA) Framework: SETA is intervention-oriented, focusing on organizational programs designed to change employee security behavior through systematic education, skill-building, and continuous awareness maintenance (Nwachukwu et al., 2023). While SETA has substantial empirical foundation and practical relevance for program design and evaluation, it is program-centric rather than measurement-centric. SETA does not specify underlying constructs to measure or provide a clear dimensional structure for scale development, making it more suitable for intervention design than for structuring assessment instruments (Nwachukwu et al., 2023; Chapman, 2019).

2.2. Framework Selection Rationale for OCAS

The OCAS adopts an integrated theoretical framework that synthesizes the Human-Organization-Technology (HOT) framework with elements from the Knowledge-Attitude-Behavior (KAB) model and organizational compliance literature. This integration was deliberately chosen based on four key criteria derived from the cybersecurity awareness literature:

- **Organizational relevance:** The HOT framework explicitly addresses cybersecurity awareness as a multi-level phenomenon, capturing human, organizational, and technological determinants (AlMindeel & Martins, 2020; Kumar et al., 2021). This multi-level perspective is essential for public sector contexts where employee awareness (human factors) interacts with organizational policies and regulatory requirements (organizational factors) and technical security infrastructure (technological factors). Individual-level theories (KAB, PMT, TPB) focus on personal cognitions, motivations, and behaviors but do not inherently capture organizational policy effectiveness, legal and regulatory compliance requirements, technical infrastructure, or management commitment—all of which are critical in organizational contexts.

- **Empirical foundation:** Studies in government and public sector settings demonstrate that organizational factors (senior management commitment, policy effectiveness, regulatory pressures) and technical measures are critical antecedents for enhanced cybersecurity, supporting HOT's multi-dimensional approach (AlMindeel & Martins, 2020; Kumar et al., 2021). AlMindeel and Martins (2020) demonstrated in their study of the Saudi Arabian government sector that organizational factors and technical measures significantly predict cybersecurity outcomes. Similarly, Kumar et al. (2021) found that organizational antecedents are essential for enhanced cybersecurity levels. In contrast, individual-level theories (KAB, PMT, TPB) would require substantial extension to capture these organizational realities, essentially reconstructing a multi-level framework similar to HOT.

- **Measurement feasibility:** While comprehensive frameworks like the Integrated Behavioral Model (IBM) offer theoretical breadth, they require extensive measurement that may be impractical in organizational settings where survey participation competes with work demands (Schütz & Fertig, 2023). HOT provides sufficient multi-level coverage with greater measurement efficiency, balancing comprehensiveness with practical feasibility. The HOT framework's three-dimensional structure can be operationalized with a manageable number of items while still capturing the essential multi-level factors that determine organizational cybersecurity awareness.

- **Intervention guidance:** HOT's three-dimensional structure maps clearly to organizational intervention points: human factors guide training programs and awareness initiatives, organizational factors guide policy improvements and governance enhancements, and technological factors guide infrastructure investments and technical control implementations (MIHAI, 2024).

This clear mapping enhances the practical utility of assessment results for organizational decision-making, enabling organizations to translate measurement findings into targeted improvements. In contrast, frameworks like SETA are intervention-oriented but do not provide the theoretical structure needed for measurement, while TDF focuses on intervention mapping rather than assessment structuring (Nwachukwu et al., 2023; Hijji & Alam, 2022).

KAB alone was not selected because it focuses exclusively on individual-level knowledge, attitudes, and behaviors, neglecting organizational policies, management support, regulatory requirements, and technical infrastructure (Al-Shanfari et al., 2022; Pasipamire, 2025; Li etc., 2019). Using KAB alone would produce an individual-focused scale that fails to diagnose organizational-level barriers to cybersecurity awareness. PMT and TPB were not selected as the primary framework because they are individual-level motivational theories that would require extensive elaboration to add organizational constructs (Sulaiman et al., 2022; Vortia, 2025; Georgiadou et al., 2020). IBM was not selected despite its comprehensiveness because its extensive construct set creates measurement complexity that may be impractical for initial scale development in resource-constrained public sector settings (Schütz & Fertig, 2023). SETA was not selected as the primary framework because it is intervention-oriented rather than measurement-oriented, designed to guide program design rather than structure assessment instruments (Nwachukwu et al., 2023).

2.3. OCAS Dimensional Structure and Theoretical Alignment

The four dimensions of OCAS map systematically onto the integrated HOT-KAB-Compliance framework, ensuring comprehensive coverage of multi-level factors determining organizational cybersecurity awareness:

- **Dimension 1: Personal Awareness and Proactive Approach (Human Dimension):** This dimension captures individual-level awareness of cybersecurity threats, vulnerabilities, and protective measures, along with proactive security behaviors. It draws on the knowledge and behavior components of the KAB model within the human factors domain of HOT. This dimension assesses employees' understanding of cyber threats, their recognition of personal responsibility for security, and their engagement in proactive protective behaviors. Theoretical justification for this dimension comes from research demonstrating that individual awareness and proactive behavior are foundational to organizational cybersecurity (Al-Shanfari et al., 2022; Parsons et al., 2017).

- **Dimension 2: Legal and Regulatory Awareness (Organizational Dimension):** This dimension assesses awareness of legal requirements, regulatory obligations, and data protection laws specific to the public sector context. It addresses the organizational compliance environment that shapes security behavior in government settings (AlMindeel & Martins, 2020). Public sector organizations operate under complex regulatory environments with legal obligations for data protection, information security, and privacy. Measuring legal and regulatory awareness is therefore essential for comprehensive assessment in this context, capturing a critical organizational dimension not adequately addressed by individual-level behavior theories (AlMindeel & Martins, 2020; Jacobs et al., 2023).

- **Dimension 3: Technical Protection and Implementation (Technology Dimension):** This dimension measures awareness of technical security controls and implementation of protective measures. It operationalizes the technology dimension of the HOT framework. Technical factors are critical antecedents for organizational cybersecurity and must be assessed alongside human and organizational dimensions (Kumar et al., 2021). This dimension captures employees' understanding of technical safeguards, their ability to implement protective measures, and their awareness of the technical infrastructure supporting organizational security.

- **Dimension 4: Organizational Policy Awareness (Organizational Dimension):** This dimension evaluates awareness of organizational security policies, procedures, and governance structures. It draws on the organizational dimension of HOT and organizational compliance literature. Policy effectiveness and employee policy awareness significantly influence cybersecurity behavior in organizational contexts (AlMindeel & Martins, 2020). This dimension assesses employees' knowledge of organizational security policies, their understanding of procedures and protocols, and their awareness of governance structures and accountability mechanisms.

This dimensional structure ensures comprehensive coverage of multi-level factors determining organizational cybersecurity awareness while maintaining measurement feasibility for practical organizational assessment. By integrating human, organizational, and technological dimensions within a coherent theoretical framework, the OCAS advances understanding of cybersecurity awareness as a multi-level phenomenon and provides a validated instrument for organizational diagnosis and intervention design.

3. METHOD

3.1. Participants and Procedure

EFA section of the study was conducted with 110 employees from two public organizations in Turkey during 2021. Participants were selected using convenience sampling from organizations that agreed to participate in the research. The sample included employees from various departments and job roles, ensuring representation across different organizational functions and levels of technical expertise. Demographic characteristics of the sample included gender, age, education level, and job tenure, providing a comprehensive picture of the workforce in Turkish public sector organizations.

Data was collected through an online survey administered via institutional email systems. Participation was voluntary, and all participants provided informed consent after receiving information about the study's purpose, procedures, and confidentiality protections. The survey took approximately 15-20 minutes to complete. Participants were assured that their responses would remain confidential and that data would be reported only in aggregate form. The study received ethical approval from the relevant institutional review board prior to data collection (15.04.2021 and numbered 80287700-302.08.01-74703).

3.2. Scale Development

Scale development was guided by the integrated HOT-KAB-Compliance framework to ensure comprehensive coverage of individual, organizational, and technological dimensions of cybersecurity awareness. The development process followed established psychometric procedures to ensure rigor and validity (Worthington & Whittaker, 2006).

3.2.1. Item generation

Initial items were generated based on a systematic literature review of cybersecurity awareness frameworks and existing measurement instruments, with particular attention to organizational-level constructs often neglected in individual-focused scales (Kannelønning & Katsikas, 2023). The item pool was informed by Kävrestad et al.'s (2024) taxonomy of cybersecurity awareness activities in organizations and established constructs in the information security awareness literature, providing a strong theoretical foundation for the scale (Figure 1).

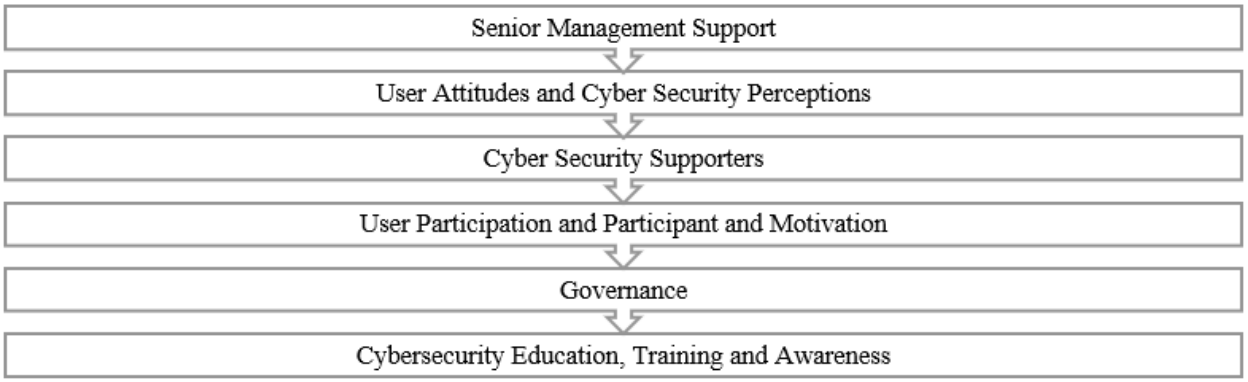

Figure 1. Taxonomy of Cyber Security Awareness in Organizations (Kävrestad et al., 2024)

Items were designed to assess four theoretical dimensions aligned with the HOT framework: Personal Awareness and Proactive Approach (human factors), Legal and Regulatory Awareness (organizational factors), Technical Protection and Implementation (technological factors), and Organizational Policy Awareness (organizational factors). Each dimension was conceptualized to capture distinct but related aspects of cybersecurity awareness essential for organizational assessment and intervention design. The initial item pool underwent multiple rounds of refinement to ensure clarity, relevance, and comprehensiveness, with particular attention paid to avoiding jargon and ensuring that items would be understandable to employees at all levels of technical expertise.

3.2.2. Content validation

The content validity of the preliminary item pool was evaluated through 5 expert review. A panel of experts in cybersecurity and psychometrics reviewed all items for relevance, clarity, and comprehensiveness. Experts rated each item on a 4-point scale for relevance and provided qualitative feedback on item wording and coverage of the construct domain. Items with low content validity ratios or substantial concerns raised by multiple experts were revised or eliminated. This iterative process continued until

consensus was reached on a final set of 26 items that adequately represented the four dimensions of organizational cybersecurity awareness.

3.2.3. Data Collection Instrument

The preliminary version of the OCAS consisted of 26 items rated on a 5-point Likert scale. Each item was phrased as a statement about cybersecurity awareness, knowledge, or behavior, and participants indicated their level of agreement or frequency of the behavior. The instrument also included a brief demographic section collecting information on gender, age, education level, and job role to enable examination of potential group differences and to describe the sample characteristics. Instructions emphasized the importance of honest responses and assured participants of confidentiality.

3.3. Data Analysis

Data analysis was conducted in two phases to establish the scale's psychometric properties following best practices in scale development (DeVellis, 2017; Hinkin, 1998). Phase 1 involved Exploratory Factor Analysis (EFA) to identify the underlying dimensional structure of cybersecurity awareness(n=110). Phase 2 involved Confirmatory Factor Analysis (CFA) to test the hypothesized factor structure and evaluate model fit(n=544).

3.3.1. Exploratory Factor Analysis (EFA)

To establish the dimensional structure of the scale, 110 employees were recruited for EDA analysis. Table 3 shows the demographic structure of the EFA section participants.

Table 3.
Demographic Characteristics of EFA Participants

		N	%			N	%
Gender	Female	16	14,50	**Education Level**	High school and below	0	0
	Male	94	85,50		High school or equivalent	5	4,50
	Total	**110**	**100**		Associate degree	19	17,30
Age	18-25	3	2,70		Bachelor's Degree	77	70,0
	26-32	42	38,20		Master's Degree	9	8,2
	33-40	32	28,10		Doctorate	0	0
	41-48	25	22,70		**Total**	**110**	**100**
	49 and above	8	7,30	**Working Year**	Less than 1 year	1	0,90
	Total	**110**	**100**		1-3 years	12	10,90
Title	Chief of Police	2	1,80		3-5 years	8	7,30
	Inspector	4	3,60		5-15 years	50	45,50
	Sub-Inspector	7	6,40		15-25 years	26	23,60
	Police Officer	76	69,10		25 and above	13	11,80
	Staff Sergeant	14	12,70				
	Contracted NCO	7	6,40				
	Total	**110**	**100**		**Total**	**110**	**100**
Cyber Security Training Status	Yes	3	2,70				
	No	107	96,30				
	Total	**110**	**100**				

EFA was conducted using principal axis factoring with oblique rotation (promax) to allow for correlated factors, which is theoretically appropriate given that the dimensions of cybersecurity awareness are expected to be related (Fabrigar et al., 1999). The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity were examined to assess data suitability for factor analysis. Factors were retained based on eigenvalues greater than 1.0, examination of the scree plot, and interpretability of the factor solution. Items were retained if they had primary factor loadings of .40 or higher and no substantial cross-loadings (loadings > .32 on multiple factors). When AMOS analysis tables were examined, it was seen that CFI=0.923,

TLI=0.902, NFI=0.894 and GFI=0.887. These values were acceptable fit values in the literature review (Hu & Bentler, 1999) and only NFA and GFA were slightly less than 0.9. They were left as they were in order not to create more Modification Indices during the analysis phase. In this respect, when the AMOS analysis values found were provided for construct validity, that is, when they were acceptable values, there was no need to make other measurements. When further metrics were reviewed, it was determined that the item total correlations, Cronbach's Alpha scores, and inter-factor correlations in EFA were within normal ranges. Table 4 summarizes the results of the exploratory conducted to assess the construct validity of the developed scale.

Table 4.
KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		,875
Bartlett's Test of Sphericity	Approx. Chi-Square	1624,683
	df	325
	Sig.	,000

The KMO value shown in Table 4 was above 0.6, indicating that the data were suitable for factor analysis, and the Bartlett test result was p=0.000 (KM0=0.875). KMO (Kaiser-Meyer-Olkin): This test was developed to ensure the consistency of item/variable values. A KMO value of 0.875 is considered good, indicating that this cluster can be factored. After determining the suitability of the data for factor analysis, exploratory factor analysis was conducted on the data to determine the factor structure of the scale. The analysis revealed that the eigenvalues of four factors were above 1.

Table 5 demonstrates how the elements on the created scale were grouped in four dimensions. As a result of the research and analysis, it was concluded that the abilities tested by these items were applicable to the four major aspects. It was seen that the 4 main dimensions were Dimension 1 Personal Awareness and Proactive Approach, Dimension 2 Legal and Regulatory, Dimension 3 Technical Protection and Implementation, and Dimension 4 Organizational and Policy. The first sub-dimension has ten components, with the lowest loading values ranging from 0.560 to 0.820. The second sub-dimension was determined to have eight components, with the lowest loading values ranging from 0.570 to 0.720. The third sub-dimension was determined to consist of four components, with the lowest loading values ranging from 0.639 to 0.842. The fourth sub-dimension was determined to consist of four components, with the lowest loading values ranging from 0.514 to 0.731.

Table 5.
OCAS Transformed Component Matrix

Rotated Component Matrix [a]	**Component**			
	1	**2**	**3**	**4**
Q114_1 son	,450	,540		
Q115_2 son	,575	,441	,439	
Q116_3 son	,719			
Q117_4 son	,552	,431		,489
Q118_5 son	,799			
Q119_1 son			,565	,605
Q120_2 son	,720		,442	
Q121_3 son	,534			,628
Q122_4 son				,745
Q123_5 son	,411	,456	,458	,481
Q124_6 son	,569			
Q125_1 son		,612		,444
Q126_2 son		,515		,682
Q127_3 son	,559	,401	,585	
Q128_4 son		,858		
Q129_5 son	,597	,429		
Q130_1 son	,409	,640		
Q131_2 son	,449	,722		
Q132_3 son	,842			
Q133_4 son		,813		
Q134_5 son		,624	,465	
Q135_1 son		,711	,431	
Q136_2 son	,466		,775	
Q137_3 son	,476		,731	
Q138_4 son			,753	
Q139_5 son	,681		,608	

Extraction Method: Principal Component Analysis
Rotation Method: Varimax with Kaiser Normalization
a. Rotation converged in 11 iterations.

When Table 5 is examined, it is seen that the questions are grouped under four factors. The factor loading values of the items in Factor 1 are between 0.411 and 0.842, the factor loading values of the items in Factor 2 are between 0.401 and 0.858, the factor loading values of the items in Factor 3 are between 0.431 and 0.775, and the factor loading values of the items in Factor 4 are between 0.444 and 0.745. Descriptive analyses of the sub-dimensions of the OCAS were conducted.

3.3.2. Confirmatory Factor Analysis (CFA)

CFA was performed to test the four-factor structure identified in the EFA by using different group(n=544). Model fit was evaluated using multiple indices following recommendations in the structural equation modeling literature (Barrett, 2007): chi-square test, Standardized Root Mean Square Residual (SRMR), and Root Mean Square Error of Approximation (RMSEA). Given that chi-square is sensitive to sample size, primary emphasis was placed on SRMR (values < .08 indicate acceptable fit) and RMSEA (values < .08 indicate acceptable fit). Factor loadings were examined to ensure that all items loaded significantly on their intended factors. Table 6 shows the demographic structure of the EFA section participants.

Table 6.
Demographic Characteristics of CFA Participants

		N	%			N	%
Gender	Female	32	5,9	**Education Level**	High school and below	1	0,2
	Male	512	94,1		High school or equivalent	41	7,5
	Total	**544**	**100**		Associate degree	123	22,6
Age	18-25	1	4,2		Bachelor's Degree	345	63,4
	26-32	240	44,1		Master's Degree	33	6,1
	33-40	147	27,0		Doctorate	1	0,2
	41-48	84	15,4		**Total**	**544**	**100**
	49 and above	50	9,2	**Working Year**	Less than 1 year	26	4,8
	Total	**544**	**100**		1-3 years	70	12,9
Title	Inspector	6	1,1		3-5 years	120	22,1
	Sub-Inspector	29	5,3		5-15 years	176	32,4
	Police Officer	440	80,9		15-25 years	94	17,3
	Community Patrol Officer	69	12,7		25 and above	58	10,7
	Total	**544**	**100**		**Total**	**544**	**100**
Cyber Security Training Status	Yes	66	12,1				
	No	478	87,9				
	Total	**544**	**100**				

CFA is used to examine whether the structure in question can be confirmed using data obtained from a measuring tool designed to follow a theoretical structure (Brown, 2015). Fox (2010) states that the covariance structure between the observed variables in CFA is tested for the degree of consistency with the proposed model. The analysis was performed with 544 data. Cronbach's Alpha value was calculated as 0.936, and the KMO and Bartlett's Test value was 0.942. Modification indices were examined so that the results obtained with CFA with 26 items of 4 sub-dimensions of OCAS were between appropriate values. Afterwards, standardized regression coefficients and fit indices were calculated and appropriate SRMR and RMSEA values were obtained. Table 7 shows the fit values obtained with CFA.

Table 7.
Fit Values (CFA)

	χ^2/df	RMSEA	SRMR	CFI	TLI	NFI	GFI	AIC	ECVI
First Analysis	1393,624/ 293= 4,756	0,083	,0845	0,858	0,843	0,828	0,814	1509,624	2,780
Modification Indices	1393,624/ 293= 4,756	0,066	0,062	0,923	0,902	0,894	0,887	1046,098	1,927

The RMSEA fit index is in the good fit range between 0.05–0.08 (Hu & Bentler, 1999). In Table 7, it is seen that it is in the good fit range with the modification indices and the value of RMSEA=0.066. It is evaluated in the acceptable level of fit range in the SRMR ≤ 0.08 value range. Because of this analysis, the table shows that it is at an acceptable level with the value of SRMR=0.062 (Hu & Bentler, 1999). The SRMR value provides easy comparability due to its standardization.

The results of the CFA revealed that the path coefficients of all items within the sub-dimensions were statistically significant, and the factor loadings were found to be satisfactory. According to the literature, Fox (2010) suggests that factor loadings above 0.30 are considered acceptable. As shown in Table 8 and Figure 2, the factor loadings of all items on the scale vary from 0.359 to 0.927. All results that are above the 0.30 level are considered statistically significant and indicate appropriate concept validity.

Table 8.
Standard and Nonstandard Path Coefficients (CFA)

Items	Factors	B_0	B_1	S.E.	C.R.	P	Label
Dimension1.2	Dimension1	,675	1,635	,188	8,712	***	par_1
Dimension 1.3	Dimension1	,359	,969	,150	6,437	***	par_2
Dimension 1.4	Dimension1	,752	1,733	,192	9,005	***	par_3
Dimension 1.5	Dimension1	,654	1,523	,177	8,620	***	par_4
Dimension 1.6	Dimension1	,524	1,285	,163	7,899	***	par_5
Dimension 1.7	Dimension1	,779	1,663	,183	9,092	***	par_6
Dimension 1.8	Dimension1	,753	1,712	,190	9,008	***	par_7
Dimension 1.9	Dimension1	,845	1,757	,189	9,279	***	par_8
Dimension1.10	Dimension1	,851	1,708	,184	9,296	***	par_9
Dimension 2.1	Dimension2	,698	1,000				
Dimension 2.2	Dimension2	,768	1,082	,067	16,098	***	par_10
Dimension 2.3	Dimension2	,668	,954	,067	14,178	***	par_11
Dimension 2.4	Dimension2	,466	,673	,067	10,056	***	par_12
Dimension 2.5	Dimension2	,654	,878	,063	13,897	***	par_13
Dimension 2.6	Dimension2	,585	,856	,068	12,504	***	par_14
Dimension 2.7	Dimension2	,586	,760	,061	12,519	***	par_15
Dimension 2.8	Dimension2	,721	1,032	,068	15,219	***	par_16
Dimension 3.1	Dimension3	,731	1,000				
Dimension 3.2	Dimension3	,855	1,155	,058	19,977	***	par_17
Dimension 3.3	Dimension3	,927	1,239	,057	21,583	***	par_18
Dimension 3.4	Dimension3	,750	1,018	,059	17,386	***	par_19
Dimension 4.1	Dimension4	,793	1,000				
Dimension 4.2	Dimension4	,708	,803	,050	16,123	***	par_20
Dimension 4.3	Dimension4	,700	,852	,054	15,920	***	par_21
Dimension 4.4	Dimension4	,524	,697	,060	11,668	***	par_22
Dimension 1.1	Dimension1	,394	1,000				

Table 7 and Figure 3 indicate that the values for $Beta_0$, $Beta_1$, Standard Error (S.E.), Critical Ratio (C.R.), and p meet the required statistical criteria, demonstrating that all parameters are statistically significant ($p < 0.05$). According to the standardized path coefficients, the sub-dimensions with the highest impact are: Personal Awareness and Proactive Approach ($Beta_0$ = .851), Legal and Regulatory Dimension ($Beta_0$ = .768), Technical Protection and Implementation ($Beta_0$ = .927), and Organizational and Policy Dimension ($Beta_0$ = .793). To be statistically significant at the 0.05 level, the Critical Ratio (C.R.) must surpass ±1.96 when dividing the estimate of the parameter by the standard error, as per the literature. The S.E. represents the difference between the true value of the observed construction and the measured value; the nearer it is to zero, the more correct the estimation.

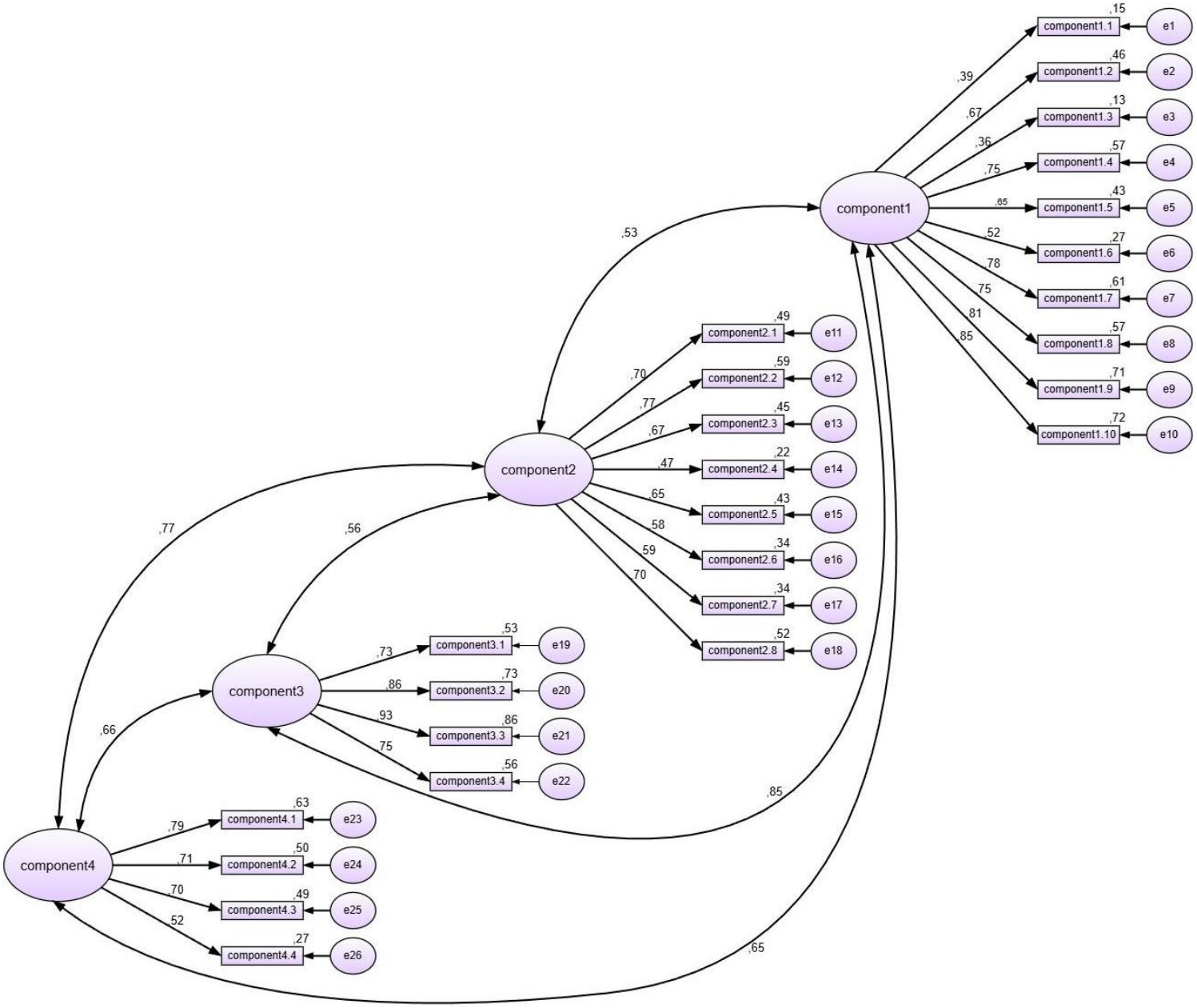

Figure 2. Standardized Path Coefficients

To assess the reliability of the CFA-analyzed sub-dimensions, the scale's Cronbach's Alpha reliability coefficients and item-total correlations were computed and displayed in Table 9. It is observed in Table 9 that the item-total score correlations are positive and exceed the threshold of 0.30. This indicates a positive relationship between each item's contribution to the scale and the overall scale score.

Table 9.
Factors' Name, Corrected Item-Total Correlation

Factors		Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Personal Awareness and Proactive Approach	Dimension 1.1	.405	.249	.934
	Dimension 1.2	.552	.491	.931
	Dimension 1.3	.485	.401	.933
	Dimension 1.4	.617	.578	.930
	Dimension 1.5	.582	.507	.931
	Dimension 1.6	.561	.402	.931
	Dimension 1.7	.684	.636	.930
	Dimension 1.8	.665	.576	.930
	Dimension 1.9	.632	.755	.930
	Dimension1.10	.660	.748	.930
Legal and Regulatory	Dimension 2.1	.613	.460	.931
	Dimension 2.2	.636	.594	.930
	Dimension 2.3	.564	.476	.931
	Dimension 2.4	.419	.296	.933
	Dimension 2.5	.573	.477	.931
	Dimension 2.6	.377	.465	.934
	Dimension 2.7	.533	.418	.932
	Dimension 2.8	.539	.537	.932
Technical Protection and Implementation	Dimension 3.1	.706	.607	.929
	Dimension 3.2	.674	.692	.930
	Dimension 3.3	.731	.787	.929
	Dimension 3.4	.607	.553	.931
Organizational and Policy	Dimension 4.1	.665	.540	.930
	Dimension 4.2	.637	.512	.930
	Dimension 4.3	.556	.462	.931
	Dimension 4.4	.393	.392	.934

Furthermore, the significance of the variations in mean item scores between the higher 27% and lower 27% groups, based on a total of 544 answers, was determined using an independent samples t-test, and the findings are displayed in Table 10. As shown in Table 10, the mean score of the upper 27% group was $\bar{X}$ = 113.4150, while the mean score of the lower 27% group was $\bar{X}$ = 80.2721.

Table 10.
Results between the Upper 27% and Lower 27% Groups (Mean and Standard Deviation)

Groups	N	Mean ($\bar{X}$)	Std. Deviation
Upper 27% Group	147	113,4150	6,81642
Lower 27% Group	147	80,2721	11,76340

In order to assess the discriminatory power of the OCAS, the findings of the Independent Samples t-test are presented in Table 11.

Table 11.
Results between the Upper 27% and Lower 27% Groups (Independent Samples t-test)

Groups	F	Sig.	t	df	Mean Difference
Upper 27% Group (Equal variances assumed)	7,957	,000	29,556	292	33,14286
Lower 27% Group (Equal variances not assumed)		,000	29,556	234,112	33,14286

Table 11 demonstrates a statistically significant difference in mean scores (33.14286) between the upper and lower 27% groups ($p < 0.05$). As a result, the OCAS distinguishes considerably between the upper and lower 27% groups. This shows that the scale has a high level of discriminating power. The total Cronbach's Alpha reliability coefficient was 0.936, with sub-dimensional reliability coefficients of 0.934 for Dimension 1, 0.931 for Dimension 2, 0.933 for Dimension 3, and 0.934 for Dimension 4.

Following the CFA, further analyses were carried out, including Composite Reliability (CR) for reliability, Average Variance Extracted (AVE) for convergent validity, Maximum Shared Variance (MSV) and Average Shared Variance (ASV) for discriminant validity. The findings of these analyses are presented in Table 11.

Table 11.
Results (Convergent and Discrimination) of Sub-Factors

Factors	Cronbach's Alpha	AVE	CR	MSV	ASV
Personal Awareness and Proactive Approach	0,934	0,46	0,93	0,27	0,40
Legal and Regulatory	0,931	0,49	0,89	0,31	0,43
Technical Protection and Implementation	0,933	0,56	0,89	0,43	0,55
Organizational and Politics	0,934	0,52	0,80	0,42	0,50

Table 11 shows Cronbach's alpha (α) and CR values of 0.70 or above, suggesting internal consistency within each sub-dimension. Furthermore, the AVE values are equal to, above, or close to the 0.50 threshold, suggesting acceptable convergent validity and hinting that the factors adequately explain the variables.

Furthermore, the condition MSV < AVE confirms that each factor is distinct from other factors, and the condition ASV < AVE indicates that the factors are dissimilar from one another, thereby establishing discriminant validity. These criteria are supported by the standards proposed by Fornell and Larcker (1981). Therefore, as a valid an reliable measurement the OCAS meets all reliability and validity requirements and can be considered.

3.3.3. Reliability Analysis

Internal consistency reliability was assessed using Cronbach's alpha for the overall scale and for each subscale (dimension). Alpha values of .70 or higher were considered acceptable, and values of .90 or higher were considered excellent, following conventional standards in psychometric research (DeVellis, 2017).

4. RESULTS

4.1 Exploratory Factor Analysis

Prior to conducting EFA, data suitability for factor analysis was confirmed. The Kaiser-Meyer-Olkin measure of sampling adequacy was .942, indicating excellent factorability of the correlation matrix. Bartlett's test of sphericity was significant ($p < .001$), confirming that the correlation matrix was not an identity matrix and that factor analysis was appropriate. Principal axis factoring with oblique rotation (promax) revealed a four-factor solution with eigenvalues greater than 1.0. The four factors accounted for 60.02% of the total variance, which exceeds the commonly recommended threshold of 50% for social science research. Factor 1 (Personal Awareness and Proactive Approach) accounted for 39.54% of the variance, Factor 2 (Legal and Regulatory Awareness) accounted for 11.19%, Factor 3 (Technical Protection and Implementation) accounted for 4.76%, and Factor 4 (Organizational Policy Awareness) accounted for 4.53%. All 26 items demonstrated satisfactory factor loadings on their respective factors, with loadings ranging from .514 to .842. No items exhibited problematic cross-loadings, and no items required deletion. The factor structure was interpretable and aligned with the theoretical framework, supporting the four-dimensional conceptualization of organizational cybersecurity awareness. Factor 1: Personal Awareness and Proactive Approach included items assessing individual awareness of cybersecurity threats, understanding of personal responsibility for security, and engagement in proactive protective behaviors. This factor represents the human dimension of the HOT framework. Factor 2: Legal and Regulatory Awareness included items assessing knowledge of legal requirements, regulatory obligations, and compliance responsibilities relevant to public sector organizations. This factor represents the organizational compliance dimension. Factor 3: Technical Protection and Implementation included items assessing awareness of technical security controls, understanding of protective technologies, and implementation of technical safeguards. This factor represents the technology dimension of the HOT framework. Factor 4: Organizational Policy Awareness included items assessing knowledge of organizational security policies, understanding of procedures and protocols, and awareness of governance structures. This factor represents the organizational policy dimension.

4.2. Confirmatory Factor Analysis

CFA was conducted to test the four-factor structure identified in the EFA. The chi-square test was significant ($\chi^2 = 7952.667$, df = 325, N = 544, $p < .001$), which is common in large samples and does not necessarily indicate poor fit (Barrett, 2007). Other fit indices indicated acceptable model fit: Standardized RMR = 0.085 (below the .08 threshold for acceptable fit) and RMSEA = 0.083 (near the .08 threshold for acceptable fit). These results support the four-dimensional structure of the OCAS. All factor loadings were statistically significant ($p < .001$), ranging from .514 to .842, indicating that all items were strong indicators of their respective latent factors. The four factors were positively correlated, with correlations ranging from .45 to .68, supporting the theoretical expectation that the dimensions of cybersecurity awareness are related but distinct constructs.

4.3. Reliability Analysis

Internal consistency reliability was excellent for the overall OCAS scale (Cronbach's α = .936) and acceptable to good for individual subscales. Factor 1 (Personal Awareness and Proactive Approach) demonstrated excellent reliability (α = .92). Factor 2 (Legal and Regulatory Awareness) demonstrated good reliability (α = .88). Factor 3 (Technical Protection and Implementation) demonstrated acceptable reliability (α = .79) (Tabachnick, & Fidell, 2013). Factor 4 (Organizational Policy Awareness) demonstrated acceptable reliability (α = .81). These reliability estimates indicate that the OCAS and its subscales have strong internal consistency, supporting their use for research and organizational assessment.

5. DISCUSSION

5.1. Summary of Findings

This study developed and validated the Organizational Cybersecurity Awareness Scale (OCAS), a multi-dimensional instrument for measuring cybersecurity awareness among public sector employees. The scale demonstrated strong psychometric properties, including excellent internal consistency reliability (α = .936) and acceptable structural validity as evidenced by EFA and CFA results. The four-factor structure—Personal Awareness and Proactive Approach, Legal and Regulatory Awareness, Technical Protection and Implementation, and Organizational Policy Awareness—aligns with the integrated HOT-KAB-Compliance theoretical framework and accounts for 60.02% of the variance in cybersecurity awareness.

5.2. Theoretical Contributions

The OCAS makes an important theoretical contribution by operationalizing an integrated multi-level framework for cybersecurity awareness assessment. While previous research has predominantly employed individual-level theories (KAB, PMT, TPB) or focused on intervention programs (SETA), the OCAS demonstrates the value of the Human-Organization-Technology framework for capturing the multi-dimensional nature of cybersecurity awareness in organizational contexts (AlMindeel & Martins, 2020; Kumar et al., 2021; Kannelønning & Katsikas, 2023). The validated four-factor structure—spanning human (Personal Awareness and Proactive Approach), organizational (Legal and Regulatory Awareness, Organizational Policy Awareness), and technological (Technical Protection and Implementation) dimensions—provides empirical support for HOT's conceptualization and offers a comprehensive assessment approach that addresses limitations of individual-focused measurement.

The scale's dimensional structure reflects the theoretical integration of individual and organizational constructs, advancing understanding of cybersecurity awareness as a multi-level phenomenon. By demonstrating that cybersecurity awareness in organizational settings encompasses not only personal knowledge and behaviors but also awareness of legal/regulatory requirements, technical protections, and organizational policies, the OCAS provides empirical evidence for the importance of multi-level measurement. This finding has implications for both theory development and practical assessment, suggesting that comprehensive cybersecurity awareness cannot be adequately captured by individual-level constructs alone.

5.3. Practical Implications

The OCAS provides organizations with a validated tool for systematic assessment of cybersecurity awareness across multiple dimensions. This multi-dimensional assessment capability enables organizations to identify specific areas of strength and weakness, moving beyond global awareness scores to targeted diagnosis. For example, an organization might discover that employees have strong personal awareness and proactive behaviors but weak knowledge of legal and regulatory requirements, suggesting a need for targeted training on compliance obligations rather than generic cybersecurity education.

The scale's alignment with the HOT framework provides clear guidance for intervention design. Assessment results can be directly mapped to human resource interventions (training, awareness campaigns), organizational interventions (policy development, governance improvements, management commitment), and technological interventions (technical controls, infrastructure enhancements). This direct mapping enhances the practical utility of assessment and facilitates evidence-based decision-making about resource allocation for cybersecurity improvement.

For public sector organizations specifically, the OCAS addresses the unique context of government institutions operating under complex regulatory requirements, resource constraints, and diverse workforce characteristics. The inclusion of Legal and Regulatory Awareness and Organizational Policy Awareness dimensions reflects the particular importance of compliance and governance in public sector contexts (AlMindeel & Martins, 2020; Sulaiman et al., 2022). Organizations can use the OCAS to assess compliance with regulatory requirements, evaluate the effectiveness of security policies, and identify gaps in employee awareness that create vulnerability to cyberattacks or regulatory violations.

5.4. Integration with Security Education, Training, and Awareness (SETA) Programs

The OCAS can play a valuable role in the planning, implementation, and evaluation of Security Education, Training, and Awareness (SETA) programs. Organizations can use the scale for needs assessment prior to program design, identifying which dimensions require the greatest attention and which employee groups have the greatest needs. During program implementation, the scale can be used for formative evaluation, assessing whether training is achieving its objectives and identifying areas requiring modification or reinforcement. After program completion, the scale enables summative evaluation, measuring the impact of SETA initiatives on employee awareness across all four dimensions.

This assessment-driven approach to SETA programs represents an improvement over common practice, which often relies on compliance metrics (e.g., training completion rates) rather than impact measures (e.g., actual changes in awareness and behavior). By using the OCAS to measure awareness before and after SETA interventions, organizations can demonstrate program effectiveness, justify investments in cybersecurity education, and continuously improve their training approaches based on empirical evidence. The multi-dimensional nature of the OCAS also enables organizations to tailor interventions to specific needs, rather than implementing generic training for all employees regardless of their particular knowledge gaps.

5.5. Limitations and Future Research Directions

Several limitations should be acknowledged. First, the study was conducted with public sector employees in Turkey, and generalizability to other contexts (private sector, other countries) requires empirical verification. Future research should validate the OCAS in diverse organizational and cultural contexts to establish its broader applicability. Cross-cultural validation studies would be particularly valuable for determining whether the four-factor structure holds across different national and organizational contexts, or whether cultural and institutional differences necessitate adaptation of the scale. The study relied on self-report data, which may be subject to social desirability bias and may not fully capture actual security behaviors. While self-reported awareness is valuable and commonly used in organizational research, future studies could complement OCAS assessment with behavioral measures (e.g., simulated phishing tests, observation of security practices) or objective indicators of security performance (e.g., incident rates, compliance audit results). Multi-method assessment would provide a more complete picture of organizational cybersecurity and would enable examination of the relationship between self-reported awareness and actual security behaviors.

The cross-sectional design precludes causal inferences about the relationships between cybersecurity awareness dimensions and organizational outcomes. Longitudinal research is needed to examine how cybersecurity awareness develops over time, how it responds to interventions, and how it predicts important outcomes such as security incidents, policy compliance, and organizational security culture. Intervention studies using the OCAS as a pre-post measure would be particularly valuable for establishing the scale's sensitivity to change and for evaluating the effectiveness of different SETA approaches. While the OCAS measures awareness across four dimensions, it does not assess all potentially relevant constructs. Future research could explore the relationships between OCAS dimensions and related constructs such as security self-efficacy, organizational security climate, management support for security, and actual security behaviors. Understanding these relationships would enhance theoretical understanding of the antecedents and consequences of cybersecurity awareness and would provide additional validation evidence for the OCAS.

The study focused on public sector organizations, and the relative importance of different dimensions may vary in private sector contexts. Future research should examine whether the four-factor structure is invariant across organizational types, or whether certain dimensions (e.g., Legal and Regulatory Awareness) are more salient in public sector settings while others (e.g., Technical Protection and Implementation) are more salient in technology-intensive private sector organizations.

5.6. Recommendations for Practice

Based on the findings of this study, several recommendations can be offered to organizations seeking to assess and improve cybersecurity awareness. Firstly, organizations should adopt multi-dimensional assessment approaches that capture the full range of factors influencing cybersecurity awareness. Relying solely on individual-level measures of knowledge or attitudes provides an incomplete picture and may miss critical organizational and technical factors that enable or constrain security-conscious behavior. The OCAS provides a validated tool for comprehensive assessment that addresses this need. Secondly, organizations should recognize that cybersecurity awareness is not solely an individual responsibility but is shaped by organizational policies, legal and regulatory requirements, and technical infrastructure. Interventions focused exclusively on changing individual behavior without addressing organizational and technical enablers are likely to have limited effectiveness. Organizations should use assessment results to identify whether gaps exist primarily in human factors (requiring training and awareness programs), organizational factors (requiring policy development, governance improvements, or management commitment), or technological factors (requiring infrastructure investments or technical controls).

Organizations should tailor interventions to specific needs identified through assessment using the OCAS or similar instruments. Organizations should use assessment results to design targeted interventions addressing specific weaknesses identified in each dimension rather than implementing generic training for all employees (Salahdine, & Kaabouch, 2019). For example, if assessment reveals strong personal awareness but weak legal/regulatory knowledge, training can focus specifically on compliance requirements and legal obligations. This targeted approach is more efficient than generic training and is more likely to address the specific gaps that create vulnerability in the organization. Moreover, organizations should integrate cybersecurity awareness assessment into the planning, implementation, and evaluation phases of SETA programs, creating a continuous improvement cycle. Cybersecurity awareness assessment should be integrated into the planning, implementation, and evaluation phases of SETA programs, moving beyond simple compliance metrics (e.g., training completion rates) to impact measures that assess actual knowledge and awareness. Pre-training assessment can establish baseline awareness and identify priority areas for training content. Post-training assessment can evaluate whether training achieved its objectives and identify areas needing reinforcement or alternative instructional approaches. This assessment-driven approach enables evidence-based program improvement and demonstrates program value to organizational stakeholders. Organizations should work to foster a broader security culture that supports and reinforces cybersecurity awareness at all levels. Beyond individual awareness, organizations should work to develop a broader security culture that supports and reinforces cybersecurity awareness at all levels of the organization. Security culture encompasses shared values, beliefs, and norms about cybersecurity that shape how employees think about and approach security in their daily work (Georgiadou et al., 2020). Organizations can foster security culture through leadership commitment and modeling, integration of security considerations into decision-making processes, recognition and reward of security-conscious behavior, and creation of psychological safety that enables employees to report concerns or mistakes without fear of punishment. A strong security culture amplifies the impact of individual awareness by creating an environment where security-conscious behavior is expected, supported, and valued.

5.7. Conclusion

In an era of increasingly sophisticated cyber threats and growing dependence on digital systems, cybersecurity awareness among organizational employees is critical to protecting sensitive data, maintaining operational continuity, and preserving public trust. This study developed and validated the OCAS, a psychometrically sound instrument for measuring cybersecurity awareness in public sector organizations that addresses a significant gap in available measurement tools. The four-dimensional scale demonstrated excellent reliability and acceptable validity, providing researchers and practitioners with a valuable tool for assessment, evaluation, and research. By enabling systematic measurement of cybersecurity awareness across four key dimensions—personal awareness and proactive approach, legal and regulatory awareness, technical protection and implementation, and organizational policy awareness—the OCAS can contribute to more effective SETA programs and, ultimately, to enhanced organizational cybersecurity posture. The scale's grounding in the Human-Organization-Technology framework ensures comprehensive coverage of multi-level factors while maintaining practical feasibility for organizational use.

As cyber threats continue to evolve and intensify, validated instruments like the OCAS will play an increasingly important role in helping organizations assess their vulnerabilities, target their interventions, and build a workforce that serves as a strong line of defense against cyberattacks. The OCAS represents a significant advance in cybersecurity awareness measurement, providing a theoretically grounded, empirically validated, and practically useful tool for public sector organizations seeking to strengthen their cybersecurity posture through enhanced employee awareness.

Research and Publication Ethics Statement

Ethical approval for this study was obtained from the Ethics Committee of Gazi University on April 15, 2021, with the decision numbered 80287700-302.08.01-74703.

Contribution Rates of Authors to the Article

All authors contributed to the study's literature review, method, data analysis and conclusion section. The final draft of the manuscript was written together, and all authors read and approved the final manuscript.

Statement of Interest

There is no conflict of interest between the authors.

6. REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237–248.

Al-Shanfari, I., Yassin, W., Tabook, N., et al. (2022). Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees. *International Journal of Advanced Computer Science and Applications*, *13*(8), 855-864. https://doi.org/10.14569/ijacsa.2022.0130855

AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Information Technology & People*, *34*(3), 770-792. https://doi.org/10.1108/ITP-06-2019-0269

Almuqrin, A., Mutambik, I., Zhang, Z., et al. (2024). Cracking the Code: Unraveling the Determinants of Cybersecurity Awareness Among University Students. *Journal of Organizational and End User Computing*, *36*(1), 1-25. https://doi.org/10.4018/joeuc.345933

Arpaci, I., & Aslan, Ö. (2022). Development of a scale to measure cybercrime-awareness on social media. Journal of Computer Information Systems, 63(3), 695–705. https://doi.org/10.1080/08874417.2022.2101160

Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. Information Development, 38(2), 218-226.

Aşan, C. (2024). Developing a measurement scale to assess the perception of cybersecurity among employees in the maritime industry. Journal of Naval Science and Engineering, 20(2), 135-162. https://doi.org/10.56850/jnse.1485985

Barrett, P. (2007). Structural equation modelling: Adjudging model fit. *Personality and Individual Differences*, *42*(5), 815-824. https://doi.org/10.1016/j.paid.2006.09.018

Bognár, F., & Bottyán, L. (2024). Development and Validation of a Personal Cybersecurity Awareness Scale. Sensors, 24(11), 3543. https://doi.org/10.3390/s24113543

Brown, T. A. (2015). Confirmatory factor analysis for applied research (2nd ed.). Guilford Publications.

Chapman, T. A. (2019). *Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers* [Doctoral dissertation]. https://www.proquest.com/docview/2303848162

Creasey, J. (2013). Cybersecurity incident response guide.
https://www.crestapproved.org/wpcontent/uploads/2014/11/CSIRProcurementGuide.pdf

DeVellis, R. F. (2017). *Scale Development: Theory and Applications* (4th ed.). Sage Publications.

Di Nocera, F., Ricciardi, O., Longo, Y., Ciani, G., & Ferlazzo, F. (2024). The CAIN Inventory: Measurement Invariance and Construct Validity of a Measure of Cybersecurity Awareness. *Cyberpsychology, Behavior, and Social Networking*, *27*(3), 183-190. https://doi.org/10.1089/cyber.2023.0350

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods*, *4*(3), 272-299. https://doi.org/10.1037/1082-989X.4.3.272

Fadhil, A., & Yazid, S. (2023). Measurement of Employee Information Security Awareness: A Case Study of National Civil Service Agency. *The Indonesian Journal of Computer Science*, *12*(6).

Faklaris, C., Dabbish, L., & Hong, J. I. (2022). SA-13: A Validated Security Attitudes Inventory. *ACM Transactions on Computer-Human Interaction*, *29*(6), Article 51. https://doi.org/10.1145/3532867

Fox, R. J. (2010). Confirmatory factor analysis. In Wiley Encyclopedia of Management. https://doi.org/10.1002/9781444316568.WIEM02060

Georgiadou, A., Mouzakitis, S., Bounas, K., et al. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2018). User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. *MIS Quarterly*, *41*(3), 703-727. https://doi.org/10.25300/MISQ/2017/41.3.03

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. İlköğretim Online, 15(2). https://doi.org/10.17051/io.2016.27218.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

He, W., & Zhang, Z. J. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*, *1*(1), 104-121. https://doi.org/10.1177/109442819800100106

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1–55.

Jacobs, C., Horsch, A., Adda, M., & Shiraz, M. (2023). Measuring the Effectiveness of Corporate Security Awareness Programs: A Systematic Review. *Computers & Security*, *126*, 103055. https://doi.org/10.1016/j.cose.2022.103055

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security*, *31*(5), 631-660. https://doi.org/10.1108/ics-08-2022-0139

Kävrestad, J., Burvall, F., & Nohlberg, M. (2024). A taxonomy of factors that contribute to organizational cybersecurity awareness (CSA). Information & Computer Security. https://doi.org/10.1108/ics-11-2023-0209

Kävrestad, J., Nohlberg, M., & Ramezanian, S. (2024). A Taxonomy of Cybersecurity Awareness Activities in Organizations. *Computers & Security*, *138*, 103654. https://doi.org/10.1016/j.cose.2023.103654

Keser, H., & Güldüren, C. (2015). Development of information security awareness scale. Kastamonu Education Journal, 23(3), 1167–1184. https://kefdergi.kastamonu.edu.tr/index.php/Kefdergi/article/view/531/233

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating Training Programs: The Four Levels* (3rd ed.). Berrett-Koehler Publishers.

Korovessis, P., Furnell, S., Papadaki, M., & Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. Journal of Cybersecurity Education, Research and Practice, 2017(2), Article 5.

Kovačević, M. (2022). Online Deliberation and Personal Identity. EMERGE 2022 Book of Abstracts, 32-33.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289-296. https://doi.org/10.1016/j.cose.2006.02.008

Kumar, S., Biswas, B., Bhatia, M. S., et al. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *35*(4/5), 1094-1119. https://doi.org/10.1108/JEIM-06-2020-0240

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49-51. https://doi.org/10.1109/MSP.2011.67

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods*, *4*(1), 84-99. https://doi.org/10.1037/1082-989X.4.1.84

Marnewick, A., & von Solms, S. H. (2022). Measuring Cybersecurity Awareness: A Comprehensive Approach. *Information & Computer Security*, *30*(3), 437-458. https://doi.org/10.1108/ICS-09-2021-0138

Mihai, I. C. (2024). AR-in-a-Box: A Structured 8-Step Framework for Cybersecurity Awareness. *Proceedings of CyberCon 2024*. https://doi.org/10.19107/cybercon.2024.05

Nikel, M., & Amaechi, C. V. (2022). An Empirical Study of Employee Awareness on Cybersecurity in Cameroon. *Journal of Cybersecurity and Privacy*, *2*(2), 374-397. https://doi.org/10.3390/jcp2020020

Nwachukwu, U., Vidgren, J., Niemimaa, M., et al. (2023). Do SETA Interventions Change Security Behavior? – A Literature Review. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 6344-6353. https://doi.org/10.24251/hicss.2023.762

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Pasipamire, E. (2025). Building a Culture of Cybersecurity Awareness in Libraries: A Systematic Review of Best Practices and Frameworks. *Proceedings of the European Conference on Information Warfare and Security*, *24*(1), 357-365. https://doi.org/10.34190/eccws.24.1.3608

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778. https://doi.org/10.2307/25750704

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Schütz, A. E., & Fertig, T. (2023). The Forgotten Model – Validating the Integrated Behavioral Model in Context of Information Security Awareness. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 6809-6818. https://doi.org/10.24251/hicss.2023.828

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100. https://doi.org/10.1016/j.compedu.2008.06.011

Sulaiman, N. S., Fauzi, M. A., Hussain, S., et al. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information*, *13*(9), 413. https://doi.org/10.3390/info13090413

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. Journal of Information Systems, 30(1), 71–92. https://doi.org/10.2308/isys-51257

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics* (6th ed.). Pearson.

Vortia, W. (2025). Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM Approach. *Magna Scientia Advanced Research and Reviews*, *14*(2), 114-131. https://doi.org/10.30574/msarr.2025.14.2.0094

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *arXiv preprint*. https://doi.org/10.48550/arxiv.2404.04725

Worthington, R. L., & Whittaker, T. A. (2006). Scale development research: A content analysis and recommendations for best practices. *The Counseling Psychologist*, *34*(6), 806-838. https://doi.org/10.1177/0011000006288127

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Başım, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97.