Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Development and Validation of the Organizational Cybersecurity Perception Scale: A Protection Motivation Theory Instrument Contextualized by NIST CSF 2.0

Soner Çankaya

scankaya@omu.edu.tr

University of Ondokuz Mayıs https://orcid.org/0000-0001-8056-1892

Fatih Samet Atasoy

University of Ondokuz Mayıs https://orcid.org/0000-0002-8071-6601

Muhammet Kusan

University of Ondokuz Mayıs https://orcid.org/0000-0001-6813-859X

Mustafa Tolga Bayraktar

University of Ondokuz Mayıs https://orcid.org/0000-0001-6108-3653

Hakan Can Altunay

University of Ondokuz Mayıs https://orcid.org/0000-0002-0175-239X

Erkan Faruk Şirin

Selçuk University https://orcid.org/0000-0002-6837-7758

Research Article

Keywords: Protection motivation theory, organizational cybersecurity perception, NIST CSF 2.0, scale development, psychometric validation

Posted Date: July 28th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10483187/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Abstract

Existing cybersecurity instruments largely focus on awareness, compliance, or behavioral intentions, while employees' organizational cybersecurity perceptions remain insufficiently examined from a PMT-based appraisal perspective. This study aimed to develop and psychometrically validate the Organizational Cybersecurity Perception Scale, a Protection Motivation Theory (PMT)-based instrument contextualized by the NIST Cybersecurity Framework (CSF) 2.0. The scale was designed to assess employees' cognitive appraisals of organizational cybersecurity threats, protective capacities, self-efficacy, and perceived response costs among individuals actively using institutional digital systems. NIST CSF 2.0 was used as a contextual framework during item development rather than as a latent measurement structure. Psychometric analyses were conducted using two independent samples drawn from different institutional sectors in Türkiye: an exploratory factor analysis sample (EFA; n = 519) and a confirmatory factor analysis sample (CFA; n = 400). EFA revealed a six-factor structure consisting of Perceived Severity, Perceived Vulnerability, Preventive Efficacy, Intervention Capability, Self-Efficacy, and Response Cost. This structure indicated that response efficacy differentiated into prevention-oriented and incident-management-oriented dimensions in the organizational cybersecurity context. The final scale included 27 items. Cronbach's alpha coefficients ranged from .762 to .862, and the overall scale demonstrated good internal consistency (α = .863). CFA supported the modified six-factor measurement model with acceptable overall fit indices ($\chi^2/df = 1.761$, RMSEA = .044, RMR = .040, CFI = .952, IFI = .953). Composite reliability values ranged from .727 to .866, and average variance extracted values provided acceptable evidence for convergent validity. HTMT ratios supported discriminant validity, and common method bias assessments did not indicate a substantial threat to the measurement model. Additional known-groups analyses conducted in two context-specific samples (public sports institutions, n = 188; university employees, n = 113) showed that the scale differentiated theoretically relevant groups according to cybersecurity training, incident awareness, policy/procedure awareness, and cybersecurity unit awareness. Overall, the findings indicate that the PMT-OCPS provides researchers and organizations with a theory-driven instrument for assessing organizational cybersecurity perception and evaluating human-centered cybersecurity readiness

1. Introduction

Digital transformation has fundamentally reshaped organizational structures, operational processes, and information management systems. The widespread use of cloud-based infrastructures, artificial intelligence systems, digital platforms, and interconnected information networks has increased organizations' dependence on digital ecosystems while expanding their exposure to cyber risks (Vial, 2021; Kraus et al., 2021; Thukral & Ratten, 2021). As a result, cybersecurity has become a multidimensional organizational concern that extends beyond the technical protection of information systems and is increasingly associated with governance, operational continuity, risk management, institutional reputation, and organizational resilience (Von Solms & Von Solms, 2018).

Contemporary cyber threats, including phishing, ransomware, data breaches, and denial-of-service attacks, may disrupt business processes, damage organizational reputation, generate legal and financial consequences, and weaken institutional trust (Parsons et al., 2014; Hadlington, 2021; ENISA, 2024; de Bruin & Mersinas, 2024; Bach & Pedersen, 2025). Although organizations invest substantially in technical security controls, technological safeguards alone are insufficient to ensure effective cybersecurity. Employees' perceptions of cyber threats, evaluations of institutional protective capacity, confidence in their own cybersecurity-related capabilities, and perceived costs of security practices play a critical role in shaping organizational cybersecurity outcomes (Bada et al., 2019; Nifakos et al., 2021; Inayat et al., 2024; Khadka & Ullah, 2025). Therefore, understanding cybersecurity in organizations requires not only technical assessment, but also theoretically grounded measurement of human-centered cognitive appraisals.

Protection Motivation Theory (PMT) provides a strong theoretical basis for examining such appraisals. Originally developed to explain protective responses to threatening events, PMT argues that protective motivation is shaped through two cognitive processes: threat appraisal and coping appraisal (Rogers, 1975, 1983). Threat appraisal involves perceived severity and perceived vulnerability, whereas coping appraisal involves response efficacy, self-efficacy, and response cost (Floyd et al., 2000). In cybersecurity research, PMT has been widely used to explain protective behaviors such as information security behavior, password protection, security policy compliance, and phishing avoidance (Ifinedo, 2012; Boss et al., 2015; Hanus & Wu, 2016; Haag et al., 2021; Kiran et al., 2025). However, most PMT-based cybersecurity studies have focused on individual user behavior or behavioral intention rather than employees' broader perceptions of organizational cybersecurity processes. At the organizational level, cybersecurity awareness is not limited to individual knowledge; rather, it is shaped by senior management support, user attitudes, support mechanisms, participation, governance, and training-awareness processes (Kävrestad et al., 2025). Similarly, the factors influencing cybersecurity awareness among decision-makers should be examined specifically (Vrhovec & Markelj, 2024), and organizational cybersecurity preparedness should be evaluated beyond individual awareness by considering institutional readiness, managerial perceptions, and applicable response mechanisms (Chapman, 2019). These arguments suggest that cybersecurity in organizations should be examined not only as an individual awareness or behavior issue, but also as a broader perceptual and institutional appraisal process involving threat evaluation, perceived organizational capacity, response capability, and implementation burden.

Existing cybersecurity measurement instruments have made important contributions to the assessment of cybersecurity awareness, information security behavior, policy compliance, cybercrime awareness, and individual cybersecurity resilience (Parsons et al., 2014; Crossler et al., 2013; Egelman & Peer, 2015; Hadlington, 2021; Arpaci & Sevinc, 2022; Almansoori et al., 2023; Arpaci et al., 2025; Arpaci et al., 2026; Ünsal & Ocak, 2026). Nevertheless, these instruments generally do not operationalize organizational cybersecurity perception as a PMT-based cognitive appraisal structure. In particular, there remains a need for a psychometric instrument that measures how employees evaluate the seriousness of cyber threats, the vulnerability of organizational digital systems, the effectiveness of institutional protective

measures, the organization's capacity to manage cyber incidents, their own perceived ability to respond, and the perceived burden of cybersecurity practices.

In this context, the NIST Cybersecurity Framework (CSF) 2.0 provides a useful organizational cybersecurity reference. NIST CSF 2.0 conceptualizes cybersecurity through six core functions: Govern, Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology [NIST], 2024). These functions provide a systematic vocabulary for describing organizational cybersecurity processes, including governance responsibilities, risk visibility, protective mechanisms, threat detection, incident response, and recovery capacity. However, NIST CSF 2.0 is not a psychological theory of protective motivation and does not itself define latent perceptual constructs. Therefore, in the present study, NIST CSF 2.0 was used as a contextual and operational framework for item development, rather than as an independent measurement model or latent factor structure.

Accordingly, this study aimed to develop and psychometrically validate the Organizational Cybersecurity Perception Scale, a Protection Motivation Theory-based instrument contextualized by NIST CSF 2.0. The proposed scale measures employees' cognitive appraisals of organizational cybersecurity through six dimensions: perceived severity, perceived vulnerability, preventive efficacy, intervention capability, self-efficacy, and response cost. PMT provides the theoretical basis for the latent structure of the scale, whereas NIST CSF 2.0 provides the organizational cybersecurity context within which the items were formulated. By making this distinction explicit, the study contributes to the literature by extending PMT from individual cybersecurity behavior to organizational cybersecurity perception and by offering a psychometrically validated tool for assessing human-centered cybersecurity appraisals in institutional settings.

2. Theoretical Framework

2.1. Protection Motivation Theory as the Theoretical Basis

Protection Motivation Theory (PMT) was developed by Rogers (1975, 1983) to explain how individuals cognitively appraise threatening situations and how these appraisals shape protective responses. The theory proposes that protection-related evaluations are formed through two core processes: threat appraisal and coping appraisal. Threat appraisal refers to individuals' evaluation of the seriousness of a threat and the likelihood of being exposed to it, whereas coping appraisal refers to their evaluation of the effectiveness, feasibility, and cost of protective responses.

In PMT, perceived severity and perceived vulnerability constitute the threat appraisal process. Perceived severity reflects the extent to which individuals consider the consequences of a threat to be serious, while perceived vulnerability reflects the perceived likelihood of being affected by that threat. Coping appraisal consists of response efficacy, self-efficacy, and response cost. Response efficacy refers to the belief that protective measures are effective in reducing a threat; self-efficacy refers to individuals' perceived capability to perform or support protective actions; and response cost refers to the perceived

burden, effort, time, or difficulty associated with implementing protective measures (Floyd et al., 2000; Milne et al., 2000).

Although PMT has traditionally been employed to explain individual protective behaviors in cybersecurity contexts (Ifinedo, 2012; Boss et al., 2015; Sulaiman et al., 2022; Warkentin et al., 2016; Haag et al., 2021), its threat appraisal and coping appraisal structure also provides a theoretically appropriate basis for examining employees' perceptions of organizational cybersecurity (Rogers, 1975, 1983; Floyd et al., 2000). However, organizational cybersecurity requires a broader interpretation of PMT because employees evaluate not only their own protective behavior, but also the organization's cybersecurity posture, preventive capacity, incident management capability, and the operational burden of security practices (Chapman, 2019; Vrhovec & Markelj, 2024; Kävrestad et al., 2025). For this reason, the present study uses PMT as the primary theoretical basis for defining the latent structure of organizational cybersecurity perception

2.2. NIST Cybersecurity Framework 2.0 as the Contextual Cybersecurity Reference

The NIST Cybersecurity Framework (CSF) was developed to help organizations manage cybersecurity risks through a common language and a structured set of cybersecurity outcomes. NIST CSF 2.0 extends this approach by positioning cybersecurity as an organizational governance and risk management issue rather than merely a technical control problem (NIST, 2018; NIST, 2024). The framework consists of six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Govern refers to cybersecurity strategy, policy, roles, responsibilities, and oversight; Identify concerns the recognition of assets, risks, threats, and vulnerabilities; Protect refers to safeguards that reduce cybersecurity risk; Detect concerns the identification of potential cybersecurity events; Respond refers to actions taken during or after an incident; and Recover concerns the restoration of systems, operations, and services after a cybersecurity event (Lanz, 2024).

In the present study, NIST CSF 2.0 was not used as a psychological theory, a latent measurement model, or an alternative factor structure. Instead, it was used as a contextual cybersecurity reference to ensure that the PMT-based items reflected realistic organizational cybersecurity processes. This distinction is important because PMT and NIST CSF 2.0 operate at different conceptual levels. PMT explains cognitive appraisal processes, whereas NIST CSF 2.0 describes organizational cybersecurity functions and operational outcomes. Therefore, the role of NIST CSF 2.0 in this study was to inform the cybersecurity content of the items, not to determine the latent dimensions of the scale. NIST CSF 2.0 was selected because it is one of the most widely adopted and internationally recognized cybersecurity governance frameworks and provides comprehensive coverage of organizational cybersecurity processes

2.3. A PMT-Based Model of Organizational Cybersecurity Perception Contextualized by NIST CSF 2.0

This study conceptualizes organizational cybersecurity perception as a multidimensional cognitive appraisal structure grounded in PMT and contextualized by NIST CSF 2.0. Drawing on Protection Motivation Theory (PMT) and the organizational cybersecurity literature, the present study conceptualizes organizational cybersecurity perception as employees' cognitive appraisals of cyber threats, organizational vulnerability, institutional preventive and incident-response capacities, their own response capabilities, and the perceived costs associated with cybersecurity practices within organizational digital environments. The scale is therefore designed to measure cybersecurity-related perceptions rather than actual cybersecurity behavior, behavioral intention, technical knowledge, or organizational cybersecurity performance.

The latent structure of the proposed scale is grounded in PMT. Perceived severity and perceived vulnerability represent threat appraisal, whereas preventive efficacy, intervention capability, self-efficacy, and response cost represent coping appraisal in the organizational cybersecurity context. In this study, response efficacy was adapted to the organizational context and empirically represented by two related but distinct dimensions: preventive efficacy and intervention capability. Preventive efficacy reflects employees' beliefs regarding the effectiveness of preventive cybersecurity measures such as access control, software updates, security training, and authentication mechanisms. Intervention capability reflects employees' evaluations of the organization's capacity to detect, respond to, coordinate, and recover from cybersecurity incidents. This distinction is theoretically meaningful because organizational cybersecurity requires not only preventive safeguards but also institutional capacity to manage incidents when they occur.

NIST CSF 2.0 informed the operational cybersecurity context of the item pool. Its Govern, Identify, Protect, Detect, Respond, and Recover functions were used to ensure that the items were connected to realistic organizational cybersecurity processes such as governance responsibilities, risk visibility, protective safeguards, detection mechanisms, response coordination, recovery capacity, workload, and procedural burden. However, these NIST functions were not specified as latent factors and were not expected to correspond one-to-one with the PMT dimensions. Rather, they served as an operational vocabulary that contextualized PMT-based cognitive appraisals within institutional cybersecurity practice.

Table 1

Conceptual Relationship Between PMT Dimensions and the Contextual Role of NIST CSF 2.0

PMT Dimension	PMT Domain	Contextual Role of NIST CSF 2.0	Illustrative Organizational Cybersecurity Context
Perceived Severity	Threat Appraisal	Not directly mapped	Psychological appraisal of cyber incident consequences, business disruption, reputational damage, legal liabilities
Perceived Vulnerability	Threat Appraisal	Identify	Assets, threats, vulnerabilities, exposure to cyber risks
Preventive Efficacy	Coping Appraisal	Protect	Security awareness training, access control, software updates, multifactor authentication
Intervention Capability	Coping Appraisal	Detect, Respond, Recover	Threat detection, incident response, coordination, recovery capacity
Self-Efficacy	Coping Appraisal	Respond	Individual response capability, incident reporting, coordination with relevant units
Response Cost	Coping Appraisal	Govern	Workload, time burden, procedural complexity, organizational compliance

Note. Protection Motivation Theory (PMT) constitutes the theoretical basis of the latent structure of the scale. NIST Cybersecurity Framework (CSF) 2.0 functions were used solely as contextual references during item development and were not specified as latent factors or as an independent measurement model. Perceived Severity was not directly mapped to a specific NIST CSF 2.0 function because it represents psychological appraisals of the potential consequences of cybersecurity incidents rather than an operational cybersecurity process. Therefore, the contextual role of NIST CSF 2.0 should not be interpreted as a one-to-one correspondence with PMT dimensions.

Accordingly, the final measurement model was specified and tested according to six PMT-based dimensions: perceived severity, perceived vulnerability, preventive efficacy, intervention capability, self-efficacy, and response cost. PMT constitutes the theoretical foundation of the scale's latent structure, whereas NIST CSF 2.0 provides the organizational cybersecurity context within which the items were formulated. This model therefore preserves the conceptual boundaries between psychological appraisal and organizational cybersecurity operations while offering a governance-contextualized measurement tool for assessing employees' organizational cybersecurity perceptions.

As illustrated in Fig. 1, organizational cybersecurity perception is conceptualized through the two cognitive appraisal processes of PMT: threat appraisal and coping appraisal. Threat appraisal comprises employees' perceptions of the severity of cybersecurity threats and the vulnerability of organizational digital systems, whereas coping appraisal comprises preventive efficacy, intervention capability, self-efficacy, and response cost. These appraisal dimensions jointly constitute the latent structure of organizational cybersecurity perception. NIST CSF 2.0 does not represent an additional latent dimension or a sequential stage in this structure; rather, its Govern, Identify, Protect, Detect, Respond, and Recover

functions provide the operational cybersecurity context used to formulate and interpret the PMT-based items.

Accordingly, organizational cybersecurity perception is conceptualized as a multidimensional cognitive appraisal construct grounded in PMT and contextualized within organizational cybersecurity processes. This conceptualization extends the application of PMT beyond its predominant focus on individual protective motivation and behavior by examining how employees cognitively evaluate organizational cyber threats, institutional coping capacities, and the perceived costs associated with cybersecurity practices.

3. Method

3.1. Item Development

The item development process was grounded in Protection Motivation Theory (PMT). Accordingly, the threat appraisal and coping appraisal components of PMT were used as the primary theoretical basis for generating the item pool. Perceived severity and perceived vulnerability were conceptualized as threat appraisal dimensions, whereas response efficacy, self-efficacy, and response cost were conceptualized as coping appraisal dimensions (Rogers, 1983; Floyd et al., 2000). Given the organizational focus of the scale, these PMT components were adapted to the context of institutional cybersecurity, where employees evaluate not only personal protective behavior, but also organizational cyber risks, preventive security practices, institutional response capacity, and the perceived burden of cybersecurity procedures.

NIST CSF 2.0 was used as a contextual and operational reference during item development. It was not treated as an independent measurement model, latent factor structure, or alternative theoretical model. Rather, the Govern, Identify, Protect, Detect, Respond, and Recover functions of NIST CSF 2.0 were used to ensure that the PMT-based items reflected realistic organizational cybersecurity processes. In this respect, NIST CSF 2.0 provided the operational cybersecurity vocabulary for item content, whereas PMT determined the theoretical structure of the scale. During the construction of the item pool, the literature on information security behavior, organizational digital risks, cyberattack scenarios, security awareness practices, cybersecurity governance, and organizational response processes was reviewed in detail (Ifinedo, 2012; Parsons et al., 2014; Boss et al., 2015; Posey et al., 2015; Egelman & Peer, 2015; Arpaci & Sevinc, 2022; Almansoori et al., 2023; Kiran et al., 2025; Khadka & Ullah, 2025; Arpaci et al., 2026; Ünsal & Ocak, 2026).

The initial item pool was generated through an iterative process involving: (1) a structured review of the PMT and organizational cybersecurity literature; (2) examination of existing cybersecurity awareness, information security behavior, and related measurement instruments; (3) contextual mapping of organizational cybersecurity processes using NIST CSF 2.0; and (4) formulation of original candidate items representing each PMT construct within organizational settings. The items were formulated to be clear, comprehensible, unidimensional, and appropriate for employees who actively use institutional

digital systems. Each item was designed to represent a PMT-based cognitive appraisal while being contextually linked to organizational cybersecurity operations. The items were formulated to be clear, comprehensible, unidimensional, and appropriate for employees who actively use institutional digital systems. Each item was designed to represent a PMT-based cognitive appraisal while being contextually linked to organizational cybersecurity operations. Items under perceived severity addressed the potential seriousness of cyber incidents for organizational operations, data security, legal responsibility, financial consequences, and institutional reputation. Items under perceived vulnerability addressed the perceived exposure of organizational digital data, infrastructure, systems, and operations to cyber threats. Items under response efficacy initially addressed the perceived effectiveness of institutional cybersecurity responses, including preventive measures, detection mechanisms, response procedures, and recovery capacity. Because organizational cybersecurity involves both prevention-oriented and incident-management-oriented capacities, response efficacy items were formulated to capture both preventive cybersecurity effectiveness and institutional intervention capability. Items under self-efficacy assessed employees' perceived ability to recognize cybersecurity incidents, follow response procedures, coordinate with relevant units, and contribute to appropriate organizational responses. Items under response cost addressed the perceived time, effort, workload, operational complexity, and procedural burden associated with cybersecurity practices.

The resulting 46-item pool constituted the preliminary form of the instrument and was subsequently submitted to expert review and content validity assessment before pilot testing. All items were rated using a five-point Likert-type response format ranging from 1 ("Strongly disagree") to 5 ("Strongly agree"). This response format was selected because it enables participants to express their level of agreement clearly, is straightforward to administer, and is widely used in psychometric instrument development (Joshi et al., 2015; Boone & Boone, 2012). The inclusion of a midpoint also allowed participants to indicate a neutral or undecided position when appropriate, although frequent midpoint responding may introduce central tendency bias (Douven, 2018).

The PMT-OCPS was developed specifically for the present study and has not been published previously. The instrument was originally developed and administered in Turkish. A complete English-language version of the final 27-item PMT-OCPS, including the instructions, response options, item content, dimensional structure, and scoring procedures, is provided in Supplementary Material 1.

3.2. Expert Evaluation and Content Validity Process

The preliminary form of the scale was prepared using the initial 46-item pool developed on the basis of Protection Motivation Theory (PMT), NIST CSF 2.0, and the organizational cybersecurity literature. In this process, PMT was used to define the theoretical dimensions of the scale, whereas NIST CSF 2.0 was used as a contextual reference to ensure that the items reflected realistic organizational cybersecurity processes. Accordingly, the expert evaluation process focused not only on the clarity and representativeness of the items, but also on their theoretical alignment with PMT and their contextual appropriateness for organizational cybersecurity.

The draft form was submitted to an eight-member expert panel. The panel consisted of two experts in behavioral sciences and PMT, two experts in cybersecurity and organizational governance, two experts in measurement and evaluation and psychometrics, one expert in organizational risk management, and one expert in language and academic expression. Experts were selected on the basis of their academic work in the relevant field, experience in scale development, and demonstrated expertise in the subject area (Lynn, 1986; Polit & Beck, 2006).

The experts were asked to evaluate each item using a four-point rating form in terms of clarity, comprehensibility, representativeness, appropriateness for the assigned PMT dimension, and contextual relevance to organizational cybersecurity. The response options were structured as follows: “1 = Not appropriate,” “2 = Somewhat appropriate,” “3 = Quite appropriate,” and “4 = Highly appropriate.” In addition to quantitative ratings, the experts were asked to provide qualitative comments and revision suggestions for items that required improvement in wording, theoretical fit, dimensional clarity, or organizational cybersecurity relevance.

Content validity was assessed using the Item-Level Content Validity Index (I-CVI) and the Scale-Level Content Validity Index/Average method (S-CVI/Ave) (Lynn, 1986; Polit & Beck, 2006). For the I-CVI calculation, expert ratings of “3 = Quite appropriate” or “4 = Highly appropriate” were considered positive evaluations for each item. In the eight-member expert panel, an I-CVI value of .78 or higher was adopted as the acceptability criterion; accordingly, items positively rated by at least seven experts were considered sufficient in terms of content validity (Polit & Beck, 2006; Polit et al., 2007).

Based on the expert evaluations, some items were revised to improve clarity of expression, theoretical representativeness, dimensional fit, and appropriateness for the organizational cybersecurity context. Items with I-CVI values below the acceptable threshold, or those judged insufficient based on qualitative expert feedback, were removed from the scale. The S-CVI/Ave value, calculated as the arithmetic mean of the I-CVI values for the 32 items retained in the pilot form, was .883. This value indicates that the pilot form demonstrated an acceptable level of content validity. Accordingly, the resulting 32-item version was retained for pilot testing.

As a result of the expert evaluation and content validity process, the initial 46-item form was reduced to a 32-item pilot form. The pilot form was structured under five PMT-based theoretical dimensions: Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, and Response Cost. NIST CSF 2.0 was retained as a contextual item-development reference rather than as a separate dimension or latent measurement structure.

3.3. Sample and Data Collection Process

The data were collected from individuals working in various institutional fields in Türkiye, including education, higher education, sport management, public administration, security, health, banking, telecommunications, and information technologies. The inclusion criterion was active use of organizational digital systems in the workplace. This criterion was adopted because the scale was

designed to assess organizational cybersecurity perceptions among individuals who interact with institutional digital infrastructures, systems, or platforms as part of their work.

Participants were recruited using convenience sampling. Although this sampling strategy limits the generalizability of the findings, it is commonly used in scale development studies when the target population consists of individuals who meet specific practical criteria, such as active use of institutional digital systems (Etikan et al., 2016). Participation was voluntary. All responses were collected anonymously, and confidentiality was ensured throughout the research process. Informed consent was obtained from all participants, who were informed about the purpose of the study, the voluntary nature of participation, and their right to withdraw. The study was reviewed and approved by the Human Sciences Research and Publication Ethics Committee of Ondokuz Mayıs University (Decision Date: 28.11.2025; Meeting No: 10; Decision No: 2025 – 1457) and was conducted in accordance with the principles of the Declaration of Helsinki.

Data collection was conducted in three stages. In the first stage, the expert-reviewed scale form was piloted with 47 participants who had characteristics similar to those of the target population. This sample size is consistent with the recommended range of 30–50 participants for pilot testing (Şeker & Gençdoğan, 2014). During the pilot implementation, the clarity, comprehensibility, and linguistic appropriateness of the items were evaluated, and necessary revisions were made based on participant feedback. In addition, a test–retest procedure was conducted within the pilot study to examine the temporal stability of the scale (DeVellis & Thorpe, 2021).

The second and third stages involved the main psychometric analyses. Exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were conducted using two independent samples. This approach was preferred to identify the factor structure in one dataset and validate the resulting structure in a separate dataset, thereby reducing the risk of sample-specific factor solutions and strengthening evidence for construct validity (Kline, 2016; Worthington & Whittaker, 2006). The EFA sample consisted of 519 participants, and the CFA sample consisted of 400 participants. Both sample sizes exceeded the commonly recommended criterion of at least 5–10 participants per item for factor analytic studies (Kline, 2016; Pett et al., 2003; Tavşancıl, 2010). Demographic characteristics of the pilot, EFA, and CFA samples are presented in Table 2.

Table 2
Demographic Characteristics of the Pilot, EFA and CFA Samples

Variable	Category	Pilot Sample (n = 47)	EFA Sample (n = 519)	CFA Sample (n = 400)
Age	18–34 years	42.6%	34.9%	32.3%
	35–44 years	51%	32.0%	30.5%
	45–54 years	4.3%	20.4%	23.2%
	55 years and older	2.1%	12.7%	14.0%
Gender	Male	80.9%	71.7%	69.0%
	Female	19.1%	28.3%	31.0%
Educational level	Associate degree	4.3%	6.9%	6.5%
	Bachelor's degree	40.4%	48.7%	48.3%
	Master's degree	29.8%	23.8%	22.7%
	Doctoral degree	25.5%	20.6%	22.5%
Previous cybersecurity training	Yes	19.1%	21.0%	22.5%
	No	80.9%	79.0%	77.5%
Cybersecurity unit in the institution	Yes	14.9%	22.2%	24.8%
	No	46.8%	37.5%	37.5%
	Do not know	38.3%	40.3%	37.7%
Previous cyberattack experience	Yes	21.3%	25.4%	25.2%
	No	78.7%	74.6%	74.8%
Institution Type	Public Sector	61.7%	75.7%	79.7%
	Private Sector	38.3%	24.3%	20.3%

3.4. Pilot Study

The 32-item scale form was piloted with 47 participants who had characteristics similar to those of the target population. The purpose of the pilot study was to evaluate the clarity, comprehensibility, linguistic appropriateness, and preliminary usability of the items before the main psychometric analyses. During the pilot implementation, participants were asked to complete the scale and provide feedback on items that they found unclear, repetitive, ambiguous, or difficult to answer. Based on this feedback, the items

were reviewed and revised where necessary. Following the pilot implementation, the revised items were re-examined in terms of theoretical alignment with PMT, contextual appropriateness for organizational cybersecurity, and clarity of expression. Three items that were found to be insufficient in terms of wording clarity, theoretical fit, or preliminary psychometric performance were removed. As a result, the 32-item pilot form was reduced to a 29-item version of the scale (DeVellis & Thorpe, 2021). To assess the temporal stability of the 29-item version, a test–retest procedure was conducted with the same 47 participants at a three-week interval. The relationship between the two administrations was examined using Pearson correlation analysis. Mean score differences between the two administrations were tested using a paired-samples t-test, and temporal stability was evaluated using the intraclass correlation coefficient (ICC) calculated with a two-way mixed-effects model based on absolute agreement (Koo & Li, 2016; Streiner et al., 2024). The findings are presented in Table 3.

Table 3 presents the test–retest reliability findings for the PMT-OCPS. A positive and statistically significant correlation was found between the first and second administration scores ($r = .758$, $p < .001$). No significant mean score difference was observed between the two administrations ($t = 0.510$, $p = .613$), indicating that the scale scores remained stable over time. In addition, the ICC value of .882 demonstrated high temporal consistency. Taken together, these findings support the test–retest reliability of the 29-item version of the scale.

Following the pilot study and temporal stability analysis, the 29-item form was used for preliminary item analyses and exploratory factor analysis. Corrected item–total correlations, internal consistency coefficients, item discrimination indices, and normality indicators were examined before proceeding to factor analysis.

Table 3
Test–Retest Reliability Findings for the PMT-OCPS Scale

Scale	Pearson r	p	t	p	ICC
PMT-OCPS	.758	< .001	.510	.613	.882

Note. PMT-OCPS = Protection Motivation Theory-Based Organizational Cybersecurity Perception Scale; Pearson r = Pearson correlation coefficient; ICC = Intraclass Correlation Coefficient. ICC values were calculated using a two-way mixed-effects model with absolute agreement. $p < .05$ indicates statistical significance.

3.5. Preliminary Item Analysis

Before exploratory factor analysis, preliminary item analyses were conducted on the 29-item form. The items were examined in terms of corrected item–total correlations, Cronbach's alpha if item deleted, and item discrimination. Corrected item–total correlations were used to evaluate the consistency of each item with the overall scale structure. Cronbach's alpha if item deleted was examined to determine whether the removal of any item would improve internal consistency. Item discrimination was assessed by comparing the upper and lower groups, thereby evaluating whether each item could significantly differentiate between participants with high and low levels of organizational cybersecurity perception. In

addition to these psychometric indicators, each item was mapped to the relevant NIST CSF 2.0 function based on its cybersecurity content. This mapping was used only to document the operational cybersecurity context of the items and was not treated as evidence of a separate NIST-based factor structure. The results are presented in Table 4.

Table 4
Preliminary Item Analysis and NIST CSF 2.0 Contextual Mapping

Items	Corrected Item–Total Correlation	Cronbach's *α* if Deleted	Item Discrimination		NIST CSF 2.0 Contextual Reference
			t	p	
Item 1	.647	.847	-9.003	< .001	Not directly mapped
Item 2	.605	.857	-9.677	< .001	Not directly mapped
Item 3	.729	.833	-9.598	< .001	Not directly mapped
Item 4	.753	.829	-8.637	< .001	Not directly mapped
Item 5	.634	.850	-7.329	< .001	Not directly mapped
Item 6	.637	.849	-9.884	< .001	Not directly mapped
Item 7	.498	.690	-13.230	< .001	Identify
Item 8	.638	.606	-8.413	< .001	Identify
Item 9	.653	.602	-12.176	< .001	Identify
Item 10	.339	.776	-3.904	< .001	Identify
Item 11	.365	.734	-1.560	0.120	Identify
Item 12	.506	.785	-8.280	< .001	Protect
Item 13	.613	.729	-9.714	< .001	Protect
Item 14	.649	.713	-9.176	< .001	Protect
Item 15	.635	.720	-9.839	< .001	Protect
Item 16	.701	.827	-12.188	< .001	Detect
Item 17	.768	.798	-11.555	< .001	Detect
Item 18	.702	.827	-11.564	< .001	Recover
Item 19	.666	.841	-11.908	< .001	Recover
Item 20	.594	.843	-10.809	< .001	Respond
Item 21	.707	.814	-12.296	< .001	Respond
Item 22	.700	.816	-10.543	< .001	Respond
Item 23	.698	.816	-11.482	< .001	Respond

Note. NIST CSF 2.0 functions were used only as contextual references to indicate the organizational cybersecurity content of each item. They were not treated as latent dimensions, independent factors, or a separate measurement structure. Perceived Severity was not directly associated with any specific NIST CSF 2.0 function because it represents a psychological appraisal of the potential consequences of cybersecurity incidents rather than an operational cybersecurity process.

Items	Corrected Item–Total Correlation	Cronbach's *α* if Deleted	Item Discrimination		NIST CSF 2.0 Contextual Reference
			t	p	
Item 24	.641	.831	-10.731	< .001	Respond
Item 25	.603	.821	-6.305	< .001	Govern
Item 26	.634	.812	-5.288	< .001	Govern
Item 27	.578	.827	-6.822	< .001	Govern
Item 28	.691	.796	-7.314	< .001	Govern
Item 29	.725	.787	-5.673	< .001	Govern

Note. NIST CSF 2.0 functions were used only as contextual references to indicate the organizational cybersecurity content of each item. They were not treated as latent dimensions, independent factors, or a separate measurement structure. Perceived Severity was not directly associated with any specific NIST CSF 2.0 function because it represents a psychological appraisal of the potential consequences of cybersecurity incidents rather than an operational cybersecurity process.

Table 4 presents the preliminary item analysis results for the 29-item form. The corrected item–total correlation values were generally within acceptable ranges, indicating that most items were sufficiently consistent with the overall scale structure. Item discrimination analyses showed that almost all items significantly differentiated between the lower and upper groups ($p < .001$). However, Item 11 did not demonstrate significant item discrimination ($t = -1.560$, $p = .120$). In addition, its corrected item–total correlation was relatively low compared with the other items. Therefore, Item 11 was removed from the scale based on psychometric evidence, theoretical evaluation, and expert judgment. Accordingly, exploratory factor analysis was conducted using the remaining 28-item form.

3.6. Exploratory Factor Analysis (EFA)

Exploratory factor analysis (EFA) was conducted to determine the factor structure of the scale. Prior to the analysis, the suitability of the data for factor analysis was assessed using the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity. The normality assumption was evaluated through skewness and kurtosis coefficients. According to George and Mallery (2003), skewness and kurtosis values between − 2 and + 2 indicate an acceptable approximation to normal distribution. However, as some values in the present study fell outside this range, Principal Axis Factoring (PAF), which is less sensitive to violations of normality, was used as the factor extraction method (Fabrigar et al., 1999; Costello & Osborne, 2005; Hair et al., 2019). Given the theoretical expectation that the factors would be meaningfully correlated, Direct Oblimin, an oblique rotation method that allows inter-factor correlations, was preferred. The number of factors was determined by jointly considering eigenvalues greater than 1, the scree plot, and theoretical interpretability. Factor loadings, communalities, and cross-loading patterns were also examined to evaluate item suitability within the factor structure. Based on these criteria, no additional items were removed, and the confirmatory factor analysis (CFA) stage proceeded with the 28-item form.

Table 5
Normality Indicators for the PMT-OCPS and Its Subscales

Dimensions	Items	Mean	Standard Deviation	Normality Indicators	
				Skewness	Kurtosis
Perceived Severity	Item 1	25.59	3.93	-1.498	3.871
	Item 2				
	Item 3				
	Item 4				
	Item 5				
	Item 6				
Perceived Vulnerability	Item 7	10.62	2.52	-0.203	-0.126
	Item 8				
	Item 9				
Preventive Efficacy	Item 12	14.11	4.22	0.381	0.150
	Item 13				
	Item 14				
	Item 15				
Intervention Capability	Item 16	12.90	3.24	-0.062	0.156
	Item 17				
	Item 18				
	Item 19				
Self-Efficacy	Item 20	16.08	2.57	-0.976	3.028
	Item 21				
	Item 22				
	Item 23				
	Item 24				

Dimensions	Items	Mean	Standard Deviation	Normality Indicators	
				Skewness	Kurtosis
Response Cost	Item 25	13.95	3.02	-0.103	0.030
	Item 26				
	Item 27				
	Item 28				
	Item 29				
PMT-OCPS	Total	93.25	12.10	-0.335	3.962

Whether the data met the normality assumption was evaluated using skewness and kurtosis coefficients; however, not all values were found to fall within the acceptable range (George & Mallery, 2003).

Table 6
KMO and Bartlett’s Test of Sphericity Results

Statistical Measure	Value
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	0.872
Bartlett's Test of Sphericity - Approx. Chi-Square	6739.367
Degrees of Freedom (df)	378
Significance Level (p)	< .001

The KMO and Bartlett’s test of sphericity results indicate that the dataset was suitable for factor analysis. The KMO value of .872 demonstrates high sampling adequacy, while the significant Bartlett’s test result indicates that there were sufficient inter-item correlations to support factorization (Bartlett, 1954; Kaiser, 1974).

Table 7
Exploratory Factor Analysis (EFA) Results for the PMT-OCPS

Factors	Items	Communalities	λ	RE	TVE %
Perceived Severity	Item 1	.487	.689	4.627	54.924
	Item 2	.432	.573		
	Item 3	.643	.775		
	Item 4	.701	.869		
	Item 5	.477	.679		
	Item 6	.509	.635		
Perceived Vulnerability	Item 7	.487	.480	2.557	
	Item 8	.614	.796		
	Item 9	.650	.703		
	Item 10	.340	.448		
Preventive Efficacy	Item 12	.348	.449	3.710	
	Item 13	.493	.663		
	Item 14	.620	.762		
	Item 15	.576	.702		
Intervention Capability	Item 16	.643	.775	3.554	
	Item 17	.742	.827		
	Item 18	.564	.671		
	Item 19	.600	.556		
Self-Efficacy	Item 20	.463	.578	3.960	
	Item 21	.599	.758		
	Item 22	.632	.833		
	Item 23	.607	.754		
	Item 24	.488	.686		
Response Cost	Item 25	.432	.647	2.880	
	Item 26	.518	.697		
	Item 27	.416	.650		
	Item 28	.611	.767		

Factors	Items	Communalities	λ	RE	TVE %
	Item 29	.674	.816		

Table 7 shows that the PMT-OCPS yielded a six-factor structure. The factor loadings and communality values were within acceptable ranges (Hair et al., 2019). Overall, these findings indicate that the scale has a psychometrically adequate factor structure consistent with the theoretical framework.

3.7. Confirmatory Factor Analysis

Confirmatory factor analysis (CFA) was conducted to validate the six-factor structure obtained from the exploratory factor analysis. Within the CFA, factor loadings, composite reliability (CR), average variance extracted (AVE), discriminant validity based on the heterotrait–monotrait ratio (HTMT), and model fit indices were evaluated. Based on the modification indices, Item 10, which had a low factor loading, was removed from the model. In addition, a limited number of theoretically meaningful error covariances were specified between error terms within the same latent construct. Following these modifications, the scale reached its final form with six factors and 27 items. The findings indicated that the modified measurement model demonstrated good fit and supported the factorial validity of the scale.

Table 8
Cronbach's Alpha Coefficients for the Scale and Its Subdimensions

Scale / Subdimensions of the Scale	Cronbach's Alpha (α)	Evaluation
PMT-OCPS Total Scale	.863	Good Reliability
Perceived Severity	.862	Good Reliability
Perceived Vulnerability	.762	Acceptable Reliability
Preventive Efficacy	.778	Acceptable Reliability
Intervention Capability	.843	Good Reliability
Self-Efficacy	.853	Good Reliability
Response Cost	.842	Good Reliability

Cronbach's alpha coefficients indicate that the scale and its subdimensions demonstrated adequate internal consistency. Alpha values for the subdimensions ranged from .762 to .862, while the overall alpha coefficient for the scale was .863. These coefficients suggest that the items produced consistent measurements within their respective dimensions and that the scale reliably assesses PMT-based organizational cybersecurity perceptions (Nunnally & Bernstein, 1994; DeVellis & Thorpe, 2021).

Table 9
Confirmatory factor analysis results for the six-factor measurement model

Factors / Items	Standardized Loadings (λ)	t-value	CR	AVE	R^2
Perceived Severity					
Item 1	.644	—	.866	.521	.415
Item 2	.648	11.716			.420
Item 3	.823	12.959			.677
Item 4	.773	12.936			.597
Item 5	.653	10.999			.426
Item 6	.767	12.013			.589
Perceived Vulnerability					
Item 7	.794	—	.727	.480	.630
Item 8	.481	7.679			.231
Item 9	.761	11.349			.580
Preventive Efficacy					
Item 12	.549	—	.788	.486	.301
Item 13	.690	9.517			.476
Item 14	.774	10.048			.599
Item 15	.752	9.931			.565
Intervention Capability					
Item 16	.629	—	.819	.532	.395
Item 17	.722	15.758			.521
Item 18	.750	11.395			.562
Item 19	.806	11.792			.650
Self-Efficacy		—			
Item 20	.789	—	.839	.513	.622
Item 21	.770	13.685			.593
Item 22	.713	12.764			.508

Note. λ = standardized factor loading; CR = composite reliability; AVE = average variance extracted; R^2 = squared multiple correlation.

Factors / Items	Standardized Loadings (λ)	t-value	CR	AVE	R^2
Item 23	.722	12.244			.521
Item 24	.565	10.385			.319
Response Cost					
Item 25	.652	—	.847	.529	.425
Item 26	.756	11.798			.571
Item 27	.571	9.604			.327
Item 28	.828	12.416			.686
Item 29	.799	13.309			.639

Note. λ = standardized factor loading; CR = composite reliability; AVE = average variance extracted; R^2 = squared multiple correlation.

The standardized factor loadings obtained from the CFA ranged from .481 to .828. Overall, the item loadings were within acceptable levels, with many items exceeding the recommended .60 threshold. Composite reliability (CR) values for the six-factor measurement model ranged from .727 to .866 across the Perceived Severity, Perceived Vulnerability, Preventive Efficacy, Intervention Capability, Self-Efficacy, and Response Cost dimensions, exceeding the recommended threshold in all dimensions. This finding indicates that the subdimensions of the scale demonstrated adequate internal consistency and construct reliability (Hair et al., 2019; Kline, 2016). The average variance extracted (AVE) values ranged from .480 to .532. The AVE values for Perceived Severity, Intervention Capability, Self-Efficacy, and Response Cost met the recommended .50 criterion, whereas the values for Perceived Vulnerability and Preventive Efficacy were slightly below this threshold. However, because the CR values for these dimensions exceeded .70, the findings suggest that these constructs demonstrated adequate reliability and that convergent validity was generally supported at an acceptable level (Fornell & Larcker, 1981; Hair et al., 2019). Taken together, the standardized factor loadings, CR values, and AVE values provide sufficient psychometric evidence for the reliability and convergent validity of the six-factor measurement model.

Table 10
Goodness-of-fit indices for the initial and modified CFA models

Fit Index	First Analysis Value	Modified Indices Value	Recommended Threshold	Interpretation
χ^2/df	2.552	1.761	< 3.00	Good fit
RMSEA	.062	.044	< .08 acceptable; < .05 excellent	Good fit
RMR	.047	.040	< .05	Good fit
NFI	.849	.897	≥ .90	Slightly below recommended threshold
TLI / NNFI	.889	.945	≥ .95	Slightly below recommended threshold
CFI	.902	.952	≥ .95	Good fit
IFI	.903	.953	≥ .95	Good fit
GFI	.871	.911	≥ .90	Good fit
AGFI	.842	.888	≥ .85	Good fit
AIC	917.303	683.946	-	Improved relative fit
Hoelter (.05)	180	258	> 200	Good fit

Note. χ^2/df = chi-square divided by degrees of freedom; RMSEA = root mean square error of approximation; RMR = root mean square residual; NFI = normed fit index; TLI/NNFI = Tucker–Lewis index/non-normed fit index; CFI = comparative fit index; IFI = incremental fit index; GFI = goodness-of-fit index; AGFI = adjusted goodness-of-fit index; AIC = Akaike information criterion. Interpretations are based on the modified CFA model.

The goodness-of-fit indices indicated that the initial CFA model showed an acceptable fit; however, several indices remained below the recommended thresholds. After theoretically justified modifications were applied, a clear improvement in model fit was observed. In particular, the decrease in the χ^2/df ratio to 1.761 and the low RMSEA (.044) and RMR (.040) values indicated a good fit between the model and the data. Similarly, the CFI (.952) and IFI (.953) values exceeded the recommended threshold of .95, supporting the adequacy of the measurement model. Although the TLI/NNFI (.945) and NFI (.897) values remained slightly below the recommended cut-off values, they were close to the acceptable range and did not indicate serious model misspecification. Furthermore, the GFI (.911) and AGFI (.888) values supported an acceptable model fit. The decrease in the AIC value from 917.303 to 683.946 suggested that the modified model provided an improved relative fit compared with the initial CFA model. In addition, the Hoelter value (.05 = 258) indicated that the model was adequately supported in terms of sample size. Overall, these findings suggest that the modified CFA model demonstrated an acceptable

overall fit and provided empirical support for the factorial validity of the proposed measurement structure (Hu & Bentler, 1999; Schermelleh-Engel et al., 2003; Byrne, 2012).

To ensure methodological transparency, modification indices were examined to identify local fit issues in the CFA model. The initial CFA results showed that Item 10 had insufficient psychometric performance within the measurement model and was therefore removed before the modified CFA model was estimated. After the model was respecified, the modification indices suggested that residual covariances could be specified between certain item error terms within the same latent construct. As illustrated in Fig. 2, theoretically justified residual covariances were specified between e1 ↔ e2, e5 ↔ e6, e7 ↔ e10, e10 ↔ e11, e13 ↔ e15, e17 ↔ e18, and e26 ↔ e27.

These covariance paths were not treated as automatic statistical adjustments. Each modification was evaluated in relation to the theoretical structure of the scale and the semantic proximity between the relevant items. This approach is important because allowing correlated errors without theoretical justification may artificially improve model fit and weaken the interpretability of the measurement model (Hermida, 2015). Accordingly, only a limited number of theoretically defensible residual covariances were specified between item error terms within the same latent construct. These residual associations were interpreted not as indicators of cross-loading or factorial instability, but as limited item-level shared measurement variance arising from semantic or contextual similarity. No factor–item cross-loadings or error–factor paths were added to the model (MacCallum et al., 1992; Brown, 2015; Kline, 2016). This approach improved model fit while preserving conceptual coherence and factorial integrity. As shown in Table 10 and Fig. 2, the modified CFA model demonstrated acceptable overall goodness-of-fit values, thereby supporting the factorial validity of the measurement model.

3.8. Discriminant validity

Table 11
HTMT Ratios for Discriminant Validity

Constructs	**1**	**2**	**3**	**4**	**5**	**6**
1. Perceived Severity	—					
2. Perceived Vulnerability	.618	—				
3. Preventive Efficacy	.598	.437	—			
4. Intervention Capability	.264	.264	.354	—		
5. Self-Efficacy	.157	.185	.308	.647	—	
6. Response Cost	.075	.117	.066	.183	.192	—

Note. HTMT = Heterotrait–Monotrait ratio. All HTMT values were below the conservative threshold of .85 recommended by Henseler et al. (2015), supporting discriminant validity.

The HTMT results indicated that all inter-construct ratios were below the conservative threshold of .85 proposed by Henseler et al. (2015), ranging from .066 to .647. These findings suggest that the latent

constructs were empirically distinct and that no problematic overlap existed among the dimensions of the measurement model. Therefore, the results provide strong evidence for the discriminant validity of the PMT-OCPS.

3.9. Common Method Bias Assessment

To assess the risk of common method bias, Harman's single-factor test and the full collinearity VIF approach were used (Podsakoff et al., 2003; Kock, 2015). In Harman's single-factor test, the final 27 items were entered into an unrotated principal axis factoring analysis, and the first factor accounted for 23.926% of the total variance. Since this value was substantially below the recommended 50% threshold, common method bias was not considered a serious concern. In the full collinearity assessment, the resulting VIF values ranged from 1.039 to 1.606, all of which were well below the conservative threshold of 3.3 suggested by Kock (2015). Accordingly, the findings indicated that neither multicollinearity nor common method bias posed a substantial threat to the validity of the measurement model.

3.10. Additional Evidence of Known-Groups Validity

Known-groups validity was used as an additional source of construct validity evidence by examining whether PMT-OCPS scores differed across groups expected to differ theoretically in PMT-based appraisal dimensions (Mokkink et al., 2010; Boateng et al., 2018). Additional evidence of known-groups validity was examined across two context-specific samples: employees of public sports institutions (n = 188) and university employees who actively used institutional digital systems in their work processes (n = 113). The grouping variables were selected on theoretical grounds because cybersecurity training, awareness of previous cybersecurity incidents, awareness of institutional cybersecurity policies or procedures, and the presence of a cybersecurity unit were expected to be associated with specific PMT-based appraisal dimensions. In addition, gender, educational level, and daily digital system use were examined as contextual group-comparison variables in the university sample.

Independent samples t-tests were conducted for two-group comparisons, whereas one-way ANOVA was used for comparisons involving three groups. Levene's test was examined to assess the homogeneity of variance assumption. When significant ANOVA results were obtained, Tukey post-hoc comparisons were conducted to determine which groups differed from each other. Effect sizes were reported using Cohen's d for independent samples t-tests and eta squared (η^2) for one-way ANOVA to complement statistical significance with estimates of practical magnitude (Cohen, 1988; Lakens, 2013). Only statistically significant findings are presented in Table 12.

Table 12
Significant Known-Groups Validity and Contextual Group-Difference Findings Across Samples

Sample	Grouping variable	Dimension	Test statistic	p	Effect size
Public sports institutions	Cybersecurity training	Self-Efficacy	t = 2.441	.016	d = 0.43
Public sports institutions	Cybersecurity training	Total score	t = 2.627	.009	d = 0.46
Public sports institutions	Previous incident awareness	Perceived Severity	F = 3.613	.029	η^2 = .038
Public sports institutions	Previous incident awareness	Perceived Vulnerability	F = 3.852	.023	η^2 = .040
Public sports institutions	Previous incident awareness	Total score	F = 4.684	.010	η^2 = .048
Public sports institutions	Policy/procedure awareness	Intervention Capability	F = 8.089	< .001	η^2 = .080
Public sports institutions	Policy/procedure awareness	Self-Efficacy	F = 4.646	.011	η^2 = .048
Public sports institutions	Policy/procedure awareness	Total score	F = 5.865	.003	η^2 = .060
University sample	Gender	Perceived Severity	t = 2.856	.005	d = 0.60
University sample	Gender	Perceived Vulnerability	t = 3.587	< .001	d = 0.75
University sample	Gender	Total score	t = 2.089	.039	d = 0.44
University sample	Cybersecurity training	Perceived Severity	t = 2.007	.047	d = 0.50
University sample	Cybersecurity training	Preventive Efficacy	t = 2.140	.035	d = 0.54
University sample	Cybersecurity training	Response Cost	t = -2.551	.012	d = -0.64
University sample	Cybersecurity training	Total score	t = 3.358	.001	d = 0.84
University sample	Educational level	Perceived Severity	F = 6.498	.002	η^2 = .106

Note. Only statistically significant group differences are presented. Cohen's d was reported for independent samples t-tests, and eta squared (η^2) was reported for one-way ANOVA.

Sample	Grouping variable	Dimension	Test statistic	p	Effect size
University sample	Educational level	Response Cost	F = 3.823	.025	η^2 = .065
University sample	Educational level	Total score	F = 4.288	.016	η^2 = .072
University sample	Cybersecurity unit	Intervention Capability	F = 5.020	.008	η^2 = .084
University sample	Cybersecurity unit	Self-Efficacy	F = 5.564	.005	η^2 = .092
University sample	Cybersecurity unit	Total score	F = 6.712	.002	η^2 = .109
University sample	Daily digital system use	Perceived Severity	F = 5.504	.005	η^2 = .091
University sample	Previous incident awareness	Perceived Vulnerability	F = 5.593	.005	η^2 = .092
University sample	Policy/procedure awareness	Perceived Severity	F = 3.612	.030	η^2 = .062
University sample	Policy/procedure awareness	Perceived Vulnerability	F = 4.464	.014	η^2 = .075
University sample	Policy/procedure awareness	Intervention Capability	F = 3.097	.049	η^2 = .053
University sample	Policy/procedure awareness	Self-Efficacy	F = 4.838	.010	η^2 = .081
University sample	Policy/procedure awareness	Response Cost	F = 4.218	.017	η^2 = .071
University sample	Policy/procedure awareness	Total score	F = 10.559	< .001	η^2 = .161

Note. Only statistically significant group differences are presented. Cohen's d was reported for independent samples t-tests, and eta squared (η^2) was reported for one-way ANOVA.

The known-groups validity analyses yielded theoretically interpretable patterns across the two context-specific samples. In the public sports institution sample, cybersecurity training was associated with higher self-efficacy and total PMT-OCPS scores, previous incident awareness was associated with higher perceived severity, perceived vulnerability, and total scores, and policy/procedure awareness was associated with higher intervention capability, self-efficacy, and total scores. In the university sample, cybersecurity training was associated with higher perceived severity, preventive efficacy, and total scores, as well as lower response cost. Cybersecurity unit awareness was associated with higher intervention capability, self-efficacy, and total scores, whereas previous incident awareness was associated with higher perceived vulnerability. Policy/procedure awareness showed the broadest

differentiation in the university sample. Overall, these findings suggest that the PMT-OCPS differentiated groups in theoretically expected and contextually meaningful directions.

4. Discussion

This study extends the application of PMT by conceptualizing organizational cybersecurity perception as a multidimensional cognitive appraisal construct encompassing employees' evaluations of organizational cyber threats, coping capacities, and response costs. The findings supported a theoretically coherent six-factor structure consisting of Perceived Severity, Perceived Vulnerability, Preventive Efficacy, Intervention Capability, Self-Efficacy, and Response Cost. Evidence from exploratory and confirmatory factor analyses indicated that the scale demonstrated acceptable psychometric performance. Internal consistency coefficients were within acceptable to good ranges (α = .762–.863), composite reliability values exceeded recommended thresholds (CR = .727–.866), and the modified CFA model showed acceptable overall fit ($\chi^2/df = 1.761$, RMSEA = .044, RMR = .040, CFI = .952, IFI = .953). Although some fit indices and convergent validity indicators were close to conventional thresholds, the overall pattern of evidence supported the reliability, factorial validity, convergent validity, and discriminant validity of the scale.

A central finding of the study was that response efficacy, which is generally conceptualized as a single coping appraisal component in PMT, differentiated into two related but distinct dimensions in the organizational cybersecurity context: Preventive Efficacy and Intervention Capability. This suggests that employees do not evaluate organizational cybersecurity effectiveness only in terms of preventive measures, such as awareness training, access control, software updates, and authentication mechanisms. They also appear to evaluate whether the organization has sufficient capability to detect cyber incidents, coordinate responses, and restore operations after cybersecurity events. Therefore, the six-factor structure does not indicate a departure from PMT; rather, it suggests that response efficacy may become functionally differentiated when PMT is applied to complex organizational cybersecurity environments.

4.1. Theoretical implications

One of the central theoretical findings of this study is that response efficacy, which is traditionally treated in PMT as a single component of coping appraisal, differentiated into two related but distinct dimensions in the organizational cybersecurity context: Preventive Efficacy and Intervention Capability. In classical PMT, response efficacy refers to the belief that a recommended protective action will be effective in reducing a threat (Rogers, 1975, 1983; Floyd et al., 2000). Cybersecurity studies grounded in PMT have often examined this construct through user-level behaviors such as password protection, security policy compliance, phishing avoidance, or continued protective behavior (Warkentin et al., 2016; Haag et al., 2021; Kiran et al., 2025). However, organizational cybersecurity involves a broader evaluative context in which employees assess not only whether preventive controls are effective, but also whether the

organization has sufficient capacity to detect incidents, coordinate responses, and restore operations after cyber events.

This differentiation can be explained by the layered nature of organizational cybersecurity. Preventive Efficacy reflects the perceived effectiveness of access controls, software updates, awareness training, authentication mechanisms, and other safeguards intended to reduce the likelihood of cyber incidents. Intervention Capability, in contrast, reflects the perceived organizational capacity for threat detection, incident response, coordination, and recovery when incidents occur and organizational continuity is at risk. Thus, the six-factor structure does not represent a departure from PMT; rather, it extends PMT by showing that coping appraisal in organizational cybersecurity may involve both prevention-oriented and intervention-oriented evaluations.

A second theoretical implication concerns the role of NIST CSF 2.0 in the proposed measurement model. PMT and NIST CSF 2.0 operate at different conceptual levels. PMT explains psychological appraisal processes, whereas NIST CSF 2.0 describes organizational cybersecurity functions and operational outcomes (NIST, 2024). For this reason, NIST CSF 2.0 was not specified as a latent measurement structure in this study. Instead, it was used as a contextual and operational reference to ensure that the PMT-based items reflected realistic organizational cybersecurity processes. This distinction is important because treating NIST functions as psychological constructs could blur the boundary between individual cognitive appraisals and organizational cybersecurity operations. Accordingly, the latent dimensions of the PMT-OCPS were derived from PMT, while NIST CSF 2.0 informed the organizational cybersecurity context in which the items were formulated.

This theoretical positioning also differentiates the PMT-OCPS from existing cybersecurity scales in terms of both the construct it measures and its theoretical foundation. Many available instruments focus primarily on cybersecurity awareness, technical knowledge, security practices, policy compliance, behavioral intentions, or individual security behavior. For example, the Security Behavior Intentions Scale (SeBIS) measures individual security-related behavioral intentions (Egelman & Peer, 2015), while the Human Aspects of Information Security Questionnaire (HAIS-Q) assesses awareness, knowledge, and attitude structures related to information security (Parsons et al., 2014). Similarly, the Cyber Security Scale evaluates individuals' cybersecurity perceptions and practices (Arpaci & Sevinc, 2022), the Cybercrime Awareness Scale (CAS) measures cybercrime awareness (Arpaci & Ateş, 2023), and the scale developed by Bognár and Bottyán (2024) assesses university students' personal cybersecurity awareness. Moving from this individual and user-centered measurement tradition toward a more organizational context, the Organizational Cybersecurity Awareness Scale (OCAS) developed by Ünsal and Ocak (2026) evaluates organizational cybersecurity awareness among public employees through the dimensions of personal awareness and proactive approach, legal-regulatory awareness, technical protection and implementation, and organizational policy awareness. Although these instruments provide valuable contributions to the cybersecurity measurement literature, they do not operationalize organizational cybersecurity perception as a PMT-based cognitive appraisal structure. The PMT-OCPS does not measure cybersecurity awareness, technical knowledge, actual security behavior, policy

compliance, or protection motivation as an outcome. Instead, it conceptualizes organizational cybersecurity perception as employees' cognitive appraisal of cyber threat severity, organizational vulnerability, institutional preventive capacity, intervention capability, personal response capability, and the perceived burden of cybersecurity practices. In this respect, the PMT-OCPS differs from existing instruments by extending PMT from individual-level cybersecurity behavior and awareness toward a broader organizational perception framework contextualized by institutional cybersecurity processes.

The key theoretical contribution of the study is therefore the development of a governance-contextualized PMT measurement model for organizational cybersecurity perception. By preserving PMT as the theoretical basis of the latent structure and using NIST CSF 2.0 only as an operational cybersecurity context, the PMT-OCPS maintains conceptual clarity while extending PMT beyond individual user-level cybersecurity behaviors. In this respect, the scale provides a theoretically grounded instrument for examining employees' perceptions of organizational cybersecurity threats and institutional security capacity across preventive, response-oriented, and governance-related domains. Importantly, the PMT-OCPS should not be interpreted as a measure of cybersecurity awareness, technical cybersecurity knowledge, organizational cybersecurity maturity, or actual cybersecurity behavior. Instead, it assesses how employees cognitively evaluate cyber threats and the organization's capacity to prevent, detect, respond to, and recover from cybersecurity incidents. This distinction is theoretically important because perceptions, motivations, and behaviors represent conceptually different constructs. By focusing specifically on organizational cybersecurity perception, the PMT-OCPS occupies a distinct position within the broader cybersecurity measurement literature. Beyond its measurement contribution, the PMT-OCPS extends the application of PMT to employees' multidimensional cognitive appraisals of organizational cybersecurity threats and institutional coping capacities, providing a theoretically grounded basis for future research at the intersection of cybersecurity psychology and organizational behavior. By focusing specifically on organizational cybersecurity perception, the PMT-OCPS occupies a distinct position within the broader cybersecurity measurement literature.

4.2. Methodological and practical contributions

Methodologically, this study contributes to the organizational cybersecurity measurement literature by following a multi-stage scale development and validation process. The use of two independent samples, including 519 participants for EFA and 400 participants for CFA, enabled the factor structure identified in the exploratory phase to be tested in a separate confirmatory sample. This design reduces the risk of sample-specific factor solutions and strengthens the construct validity evidence for the PMT-OCPS. In addition, the inclusion of participants from diverse institutional fields, including education, health, banking, telecommunications, security, public administration, sport management, and information technologies, provided an initial basis for examining the scale across different organizational contexts. However, the PMT-OCPS should not be interpreted as a sector-specific technical cybersecurity assessment tool. Rather, it is designed to measure employees' perceptions of organizational cybersecurity threats, preventive capacity, intervention capability, self-efficacy, and response costs across digital institutional environments.

The study also contributes methodologically by combining multiple sources of validity and reliability evidence. Expert evaluation and content validity analysis supported the theoretical and contextual adequacy of the item pool. The pilot study and test–retest analysis provided preliminary evidence of item clarity and temporal stability. The subsequent EFA and CFA supported the six-factor structure, while internal consistency coefficients, composite reliability values, AVE estimates, HTMT ratios, and common method bias assessments provided additional evidence for the reliability and validity of the measurement model. Moreover, the CFA modifications were limited to theoretically defensible residual covariances within the same latent construct. These modifications were not used as purely data-driven adjustments; rather, they were based on semantic proximity and content similarity between items.

This approach supports the methodological transparency and factorial integrity of the measurement model (MacCallum et al., 1992; Brown, 2015; Kline, 2016). Although the AVE values for Perceived Vulnerability and Preventive Efficacy remained slightly below the conventional threshold of .50, their composite reliability values exceeded the recommended criterion of .70. Previous methodological studies suggest that convergent validity may still be considered acceptable when AVE is below .50 but composite reliability is adequate and the factor structure is theoretically coherent (Fornell & Larcker, 1981; Hair et al., 2022). Therefore, the slightly lower AVE values observed in this study do not appear to substantially compromise the convergent validity of the PMT-OCPS.

The known-groups validity findings provide additional methodological support for the construct validity of the PMT-OCPS. Beyond the evidence obtained from EFA, CFA, reliability coefficients, convergent validity, discriminant validity, and common method bias analyses, the scale differentiated theoretically relevant groups across two institutional contexts. Cybersecurity training was associated with higher self-efficacy, preventive efficacy, perceived severity, and total PMT-OCPS scores, while trained participants in the university sample reported lower response cost. Awareness of previous cybersecurity incidents was mainly reflected in threat appraisal dimensions, particularly perceived severity and perceived vulnerability. Similarly, awareness of cybersecurity policies or procedures and awareness of cybersecurity units were primarily associated with coping appraisal dimensions, including intervention capability and self-efficacy. These patterns are consistent with the PMT distinction between threat appraisal and coping appraisal (Rogers, 1975, 1983; Floyd et al., 2000) and suggest that the PMT-OCPS is sensitive to organizational cybersecurity experiences and institutional awareness conditions.

From a practical perspective, the PMT-OCPS provides organizations with a structured tool for diagnosing employees' perceptions of cybersecurity risks and institutional security capacity. The scale can help identify perceived weaknesses in preventive security measures, intervention capability, employee self-efficacy, and perceived response costs. These results may inform targeted cybersecurity awareness training, human-centered risk management strategies, and organizational security culture assessments. By contextualizing PMT-based appraisal dimensions within the operational logic of NIST CSF 2.0, the PMT-OCPS may complement existing cybersecurity assessment practices by adding a perceptual layer that captures how employees evaluate cyber threats, controls, response capacity, and implementation burdens (NIST, 2024; Khadka & Ullah, 2025). Future studies should further examine the measurement

invariance of the model across sectors, institutional types, and cultural contexts. From a practical perspective, the known-groups findings indicate that the PMT-OCPS may help organizations evaluate how cybersecurity training, policy visibility, incident awareness, and institutional cybersecurity structures are reflected in employees' perceptions. The higher scores observed among participants who were aware of cybersecurity policies, procedures, or cybersecurity units suggest that visible institutional arrangements may strengthen perceived response capacity and self-efficacy. Conversely, the lower response cost reported by trained participants in the university sample suggests that cybersecurity training may reduce the perceived burden of cybersecurity practices. Therefore, the PMT-OCPS can be used not only as a diagnostic measurement tool but also as an evaluative instrument for monitoring the perceptual outcomes of cybersecurity training, policy communication, and organizational security capacity-building efforts.

5. Conclusions

This study developed and psychometrically evaluated the Organizational Cybersecurity Perception Scale, a Protection Motivation Theory (PMT)-based instrument contextualized by NIST CSF 2.0. The findings provided evidence that the six-factor structure consisting of Perceived Severity, Perceived Vulnerability, Preventive Efficacy, Intervention Capability, Self-Efficacy, and Response Cost offers a theoretically coherent and psychometrically acceptable framework for assessing employees' organizational cybersecurity perceptions in digital institutional environments.

The study contributes to the literature by extending PMT-based cognitive appraisal processes from user-level cybersecurity behaviors to organizational cybersecurity perception. By preserving PMT as the theoretical basis of the latent structure and using NIST CSF 2.0 as a contextual cybersecurity reference, the PMT-OCPS offers a measurement tool for examining how employees evaluate cyber threats, institutional preventive capacity, intervention capability, personal response capability, and perceived response costs.

A particularly important finding is the differentiation between Preventive Efficacy and Intervention Capability. This indicates that employees distinguish between the perceived effectiveness of preventive cybersecurity measures and the organization's perceived capability to detect, respond to, coordinate, and recover from cyber incidents. Overall, the PMT-OCPS may support future cybersecurity research, organizational risk assessment, security culture evaluation, and human-centered cybersecurity strategies by providing a structured perceptual measurement model for organizational cybersecurity.

6. Limitations and Future Directions

Several limitations should be considered when interpreting the findings of this study. First, although the test–retest analysis provided evidence for the temporal stability of the scale, the main validation data were based on cross-sectional self-report measures. This design does not allow causal interpretations

and may be subject to perceptual bias and social desirability effects. However, the common method bias analyses did not indicate a substantial method bias threat to the measurement model.

The known-groups validity analyses should also be interpreted with caution. Although these analyses provided supplementary validity evidence across two context-specific samples, some group sizes were unequal, and the findings were based on cross-sectional self-report data. Therefore, these results should not be interpreted as causal evidence that cybersecurity training, policy awareness, previous incident awareness, or cybersecurity unit awareness directly improves organizational cybersecurity perception. Future studies should test these associations using longitudinal, experimental, or intervention-based designs and should examine whether the known-groups patterns are replicated across different sectors, institutional types, and cultural contexts.

Second, the sample was recruited using convenience sampling, and most participants were employed in public institutions in Türkiye. Because organizational cybersecurity governance, security culture, regulatory requirements, and risk management practices may differ across countries, sectors, and institutional structures, the generalizability of the findings should be interpreted with caution. Future studies should examine the factor structure of the PMT-OCPS in different cultural, sectoral, and regulatory contexts.

Third, measurement invariance across sectors, institutional types, and demographic groups was not tested in the present study. Future research should examine whether the proposed six-factor structure operates consistently across different organizational groups using multi-group confirmatory factor analysis and measurement invariance testing.

Fourth, the PMT-OCPS assesses employees' organizational cybersecurity perceptions rather than directly observable cybersecurity behaviors or operational cybersecurity performance. Therefore, the findings should be interpreted as indicators of how employees perceive cyber threats, institutional preventive capacity, intervention capability, self-efficacy, and response costs, rather than as direct evidence of actual cybersecurity behavior or organizational performance.

Future studies should examine the predictive validity of the scale in relation to real-world outcomes such as cybersecurity policy compliance, incident response behaviors, security incident reporting practices, and organizational resilience indicators. In addition, future research could extend the model by incorporating organizational variables such as cybersecurity culture, leadership climate, digital resilience, and organizational trust. Such extensions may provide a more comprehensive understanding of how organizational conditions shape employees' cybersecurity perceptions.

Declarations

Ethics approval statement

Ethical approval for the study was obtained from the Ondokuz Mayıs University Social and Human Sciences Research and Publication Ethics Committee (Decision Date: 28.11.2025; Meeting No: 10; Decision No: 2025 – 1457).

Consent for publication

Not applicable.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

AI Declaration

The authors used DeepL Translate Pro and Grammarly Pro to improve grammatical accuracy, language clarity, and overall readability of the manuscript.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

Acknowledgments

We would like to express our sincere gratitude to all participants who contributed to this study. The support of individuals actively using institutional digital systems and voluntarily participating in the research by thoughtfully completing the PMT-Based Organizational Cybersecurity Perception Scale played a pivotal role in the successful execution of this study.,

Data availability statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request. Due to the institutional cybersecurity context of the study, the data are not publicly available for ethical and confidentiality reasons.

Authorship Contributions

S.Ç., **F.S.A. and E.F.Ş** jointly led the overall research process, including conceptualization, theoretical framework development, item generation, scale development, data management, statistical analyses, interpretation of findings, and manuscript preparation. **S.Ç. and E.F.Ş** additionally provided academic

supervision, methodological guidance, critical revision, and final approval of the manuscript. **M.K** provided substantial support across the main stages of the study, including conceptual design, literature review, scale development, data collection, analysis, interpretation, and manuscript revision. **M.T.B.** supported selected stages of the research, including literature review, data collection, methodological feedback, and manuscript review. **H.C.A** contributed to the theoretical framework and content evaluation by providing field-specific expertise in cybersecurity. All authors reviewed and approved the final version of the article.

References

1. Almansoori A, Al-Emran M, Shaalan K (2023) Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Appl Sci 13(9):5700. https://doi.org/10.3390/app13095700
2. Arpaci I, Ateş E (2023) Development of the cybercrime awareness scale (CAS): a validity and reliability study in a Turkish sample. Online Inf Rev 47(4):633–643. https://doi.org/10.1108/OIR-01-2022-0023
3. Arpaci I, Sevinc K (2022) Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. Inform Dev 38(2):218–226. https://doi.org/10.1177/0266666921997512
4. Arpaci I, Aslan O, Oner IE (2025) Cybersecurity awareness scale (CSAS) for social media users: Development, validity and reliability study. Inform Dev 02666669251336562. https://doi.org/10.1177/02666669251336562
5. Arpaci I, Khan NF, Nazir T (2026) Development and cross-cultural validation of the cybersecurity resilience scale (CSRS). Computers Secur 104904. https://doi.org/10.1016/j.cose.2026.104904
6. Bach TA, Pedersen L (2025) When technology is not enough: Insights from a pilot cybersecurity culture assessment in a safety-critical industrial organisation. arXiv preprint. https://doi.org/10.48550/arXiv.2508.20811. arXiv:2508.20811
7. Bada M, Sasse AM, Nurse JR (2019) Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. https://doi.org/10.48550/arXiv.1901.02672
8. Bartlett MS (1954) A Note on the Multiplying Factors for Various χ^2 Approximations. J Royal Stat Soc Ser B (Methodological) 16(2):296–298. http://www.jstor.org/stable/2984057
9. Boateng GO, Neilands TB, Frongillo EA, Melgar-Quiñonez HR, Young SL (2018) Best practices for developing and validating scales for health, social, and behavioral research: a primer. Front public health 6:149. https://doi.org/10.3389/fpubh.2018.00149
10. Bognár L, Bottyán L (2024) Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. Educ Sci 14(6):588. https://doi.org/10.3390/educsci14060588
11. Boone HN Jr, Boone DA (2012) Analyzing likert data. J Ext 50(2):48

12. Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P (2015) What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Q 39(4):837–864. https://www.jstor.org/stable/26628654
13. Brown TA (2015) Confirmatory factor analysis for applied research. Guilford
14. Byrne BM (2012) Structural equation modelling with Mplus: Basic concepts, applications, and programming. Routledge
15. Chapman TA (2019) *Factors affecting perceptions of cybersecurity readiness among workgroup IT managers* (Doctoral dissertation, University of Mississippi). https://www.proquest.com/dissertations-theses/factors-affecting-perceptions-cybersecurity/docview/2198125147/se-2?accountid = 44888
16. Cohen JE (1988) Statistical Power Analysis for the Behavioral Sciences. Lawrence ErlbaumAssociates, Hillsdale, NJ
17. Costello AB, Osborne J (2005) Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical assessment, research, and evaluation*, *10*(1). https://doi.org/10.7275/jyj1-4868
18. Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. Computers Secur 32:90–101. https://doi.org/10.1016/j.cose.2012.09.010
19. de Bruin M, Mersinas K (2024) Individual and Contextual Variables of Cyber Security Behaviour–An empirical analysis of national culture, industry, organisation, and individual variables of (in) secure human behaviour. *arXiv preprint arXiv:2405.16215*. https://doi.org/10.48550/arXiv.2405.16215
20. DeVellis RF, Thorpe CT (2021) Scale development: Theory and applications. Sage
21. Douven I (2018) A Bayesian perspective on Likert scales and central tendency. Psychon Bull Rev 25(3):1203–1211. https://doi.org/10.3758/s13423-017-1344-2
22. Egelman S, Peer E (2015) Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 2873–2882). https://doi.org/10.1145/2702123.2702249
23. ENISA (2024) European Union Agency for Cybersecurity, T*hreat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
24. Etikan I, Musa SA, Alkassim RS (2016) Comparison of convenience sampling and purposive sampling. Am J theoretical Appl Stat 5(1):1–4. https://doi.org/10.11648/j.ajtas.20160501.11
25. Fabrigar LR, Wegener DT, MacCallum RC, Strahan EJ (1999) Evaluating the use of exploratory factor analysis in psychological research. Psychol Methods 4(3):272–299. https://doi.org/10.1037/1082-989X.4.3.272
26. Floyd DL, Prentice-Dunn S, Rogers RW (2000) A meta-analysis of research on protection motivation theory. J Appl Soc Psychol 30(2):407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

27. Fornell C, Larcker DF (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J Mark Res 18(1):39–50. https://doi.org/10.1177/002224378101800104
28. George D, Mallery P (2003) SPSS for Windows step by step: A simple guide and reference, 4th edn. Allyn & Bacon
29. Haag S, Siponen M, Liu F (2021) Protection motivation theory in information systems security research: A review of the past and a road map for the future. ACM SIGMIS Database: DATABASE Adv Inform Syst 52(2):25–67. https://doi.org/10.1145/3462766.3462770
30. Hadlington L (2021) The human factor in cybersecurity: Exploring the accidental insider. In *Research anthology on artificial intelligence applications in security* (pp. 1960–1977). IGI Global. https://doi.org/10.4018/978-1-7998-7705-9.ch087
31. Hair JF, Black WC, Babin BJ, Anderson RE (2019) Multivariate Data Analysis, 8th edn. Cengage, Boston
32. Hanus B, Wu YA (2016) Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. Inform Syst Manage 33(1):2–16. https://doi.org/10.1080/10580530.2015.1117842
33. Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. J Acad Mark Sci 43(1):115–135. https://doi.org/10.1007/s11747-014-0403-8
34. Hermida R (2015) The problem of allowing correlated errors in structural equation modeling: concerns and considerations. Comput Methods Social Sci 3(1):5–17
35. Hu L, Bentler PM (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Struct Equation Modeling: Multidisciplinary J 6(1):1–55. https://doi.org/10.1080/10705519909540118
36. Ifinedo P (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers Secur 31(1):83–95. https://doi.org/10.1016/j.cose.2011.10.007
37. Inayat U, Farzan M, Mahmood S, Zia MF, Hussain S, Pallonetto F (2024) Insider threat mitigation: Systematic literature review. Ain Shams Eng J 15(12):103068. https://doi.org/10.1016/j.asej.2024.103068
38. Joshi A, Kale S, Chandel S, Pal DK (2015) Likert scale: Explored and explained. Br J Appl Sci Technol 7(4):396–403. https://doi.org/10.9734/BJAST/2015/14975
39. Kaiser HF (1974) An index of factorial simplicity. Psychometrika 39:31–36. https://doi.org/10.1007/BF02291575
40. Kävrestad J, Burvall F, Nohlberg M (2025) A taxonomy of factors that contribute to organizational Cybersecurity Awareness (CSA). Inform Comput Secur 33(2):141–160. https://doi.org/10.1108/ICS-11-2023-0209
41. Khadka K, Ullah AB (2025) Human factors in cybersecurity: an interdisciplinary review and framework proposal: K. Khadka, AB Ullah. Int J Inf Secur 24(3):119. https://doi.org/10.1007/s10207-

025-01032-0

42. Kiran U, Khan NF, Murtaza H, Farooq A, Pirkkalainen H (2025) Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. Computers Secur 149:104204. https://doi.org/10.1016/j.cose.2024.104204
43. Kline R (2016) Principles and practice of structural equation modeling, 4th edn. The Guilford Press
44. Kock N (2015) Common method bias in PLS-SEM: A full collinearity assessment approach. Int J e-Collaboration (ijec) 11(4):1–10. https://doi.org/10.4018/ijec.2015100101
45. Koo TK, Li MY (2016) A guideline of selecting and reporting intraclass correlation coefficients for reliability research. J Chiropr Med 15(2):155–163. https://doi.org/10.1016/j.jcm.2016.02.012
46. Kraus S, Jones P, Kailer N, Weinmann A, Chaparro-Banegas N, Roig-Tierno N (2021) Digital transformation: An overview of the current state of the art of research. Sage Open 11(3):21582440211047576. https://doi.org/10.1177/21582440211047576
47. Lakens D (2013) Calculating and reporting effect sizes to facilitate cumulative science: a practical primer for t-tests and ANOVAs. Front Psychol 4:62627. https://doi.org/10.3389/fpsyg.2013.00863
48. Lanz J (2024) The Updated NIST Cybersecurity Framework. CPA J 94(5/6):70–72
49. Lynn MR (1986) Determination and quantification of content validity. Nurs Res 35(6):382–386
50. MacCallum RC, Roznowski M, Necowitz LB (1992) Model modifications in covariance structure analysis: The problem of capitalization on chance. Psychol Bull 111(3):490–504. https://doi.org/10.1037/0033-2909.111.3.490
51. Milne S, Sheeran P, Orbell S (2000) Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. J Appl Soc Psychol 30(1):106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x
52. Mokkink LB, Terwee CB, Patrick DL et al (2010) The COSMIN checklist for assessing the methodological quality of studies on measurement properties of health status measurement instruments: an international Delphi study. Qual Life Res 19:539–549. https://doi.org/10.1007/s11136-010-9606-8
53. National Institute of Standards and Technology (2018) *Framework for improving critical infrastructure cybersecurity*(Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
54. National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
55. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S (2021) Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors 21(15):5119. https://doi.org/10.3390/s21155119
56. Nunnally J, Bernstein I (1994) Psychometric Theory, 3rd edn. MacGraw-Hill, New York
57. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C (2014) Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers

Secur 42:165–176. https://doi.org/10.1016/j.cose.2013.12.003

58. Pett MA, Lackey NR, Sullivan JJ (2003) Making sense of factor analysis: The use of factor analysis for instrument development in health care research. Sage
59. Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 88(5):879. https://doi.org/10.1037/0021-9010.88.5.879
60. Polit DF, Beck CT (2006) The content validity index: are you sure you know what's being reported? Critique and recommendations. Res Nurs Health 29(5):489–497. https://doi.org/10.1002/nur.20147
61. Polit DF, Beck CT, Owen SV (2007) Is the CVI an acceptable indicator of content validity? Appraisal and recommendations. Res Nurs Health 30(4):459–467
62. Posey C, Roberts TL, Lowry PB (2015) The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. J Manage Inform Syst 32(4):179–214. https://doi.org/10.1080/07421222.2015.1138374
63. Rogers RW (1975) A protection motivation theory of fear appeals and attitude change1. J Psychol 91(1):93–114. https://doi.org/10.1080/00223980.1975.9915803
64. Rogers RW (1983) Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT, Petty RE (eds) Social Psychophysiology: A Source Book. Guilford Press, New York, NY, pp 153–176
65. Schermelleh-Engel K, Moosbrugger H, Müller H (2003) Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. Methods Psychol Res online 8(2):23–74. https://doi.org/10.23668/psycharchives.12784
66. Şeker H, Gençdoğan B (2014) Psikolojide ve eğitimde ölçme aracı geliştirme (2. Basım). Ankara: Nobel Yayıncılık
67. Streiner DL, Norman GR, Cairney J (2024) Health measurement scales: a practical guide to their development and use. Oxford University Press. https://doi.org/10.1016/j.jclinepi.2003.08.011
68. Sulaiman NS, Fauzi MA, Hussain S, Wider W (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
69. Tavşancıl E (2010) Tutumların ölçülmesi ve SPSS ile veri analizi.(3. Baskı). *Ankara: Nobel Yayınları*
70. Thukral E, Ratten V (2021) Sport innovation, entrepreneurship and digital ecosystems. In *Innovation and entrepreneurship in sport management* (pp. 122–136). Edward Elgar Publishing. https://doi.org/10.4337/9781783473960.00014
71. Ünsal NÖ, Ocak MA (2026) Development of organizational cybersecurity awareness scale (OCAS). Hacettepe Univ J Educ 41(1):136–155. https://doi.org/10.16986/hunefd.1739282
72. Vial G (2021) Understanding digital transformation: A review and a research agenda. Managing Digit transformation 13–66. https://doi.org/10.4324/97810 03008

73. Von Solms B, Von Solms R (2018) Cybersecurity and information security–what goes where? Inform Comput Secur 26(1):2–9. https://doi.org/10.1108/ICS-04-2017-0025
74. Vrhovec S, Markelj B (2024) We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. PLoS ONE 19(10):e0312266. https://doi.org/10.1371/journal.pone.0312266
75. Warkentin M, Johnston AC, Shropshire J, Barnett WD (2016) Continuance of protective security behavior: A longitudinal study. Decis Support Syst 92:25–35. https://doi.org/10.1016/j.dss.2016.09.013
76. Worthington RL, Whittaker TA (2006) Scale development research: A content analysis and recommendations for best practices. Couns Psychol 34(6):806–838. https://doi.org/10.1177/0011000006288127

Figures

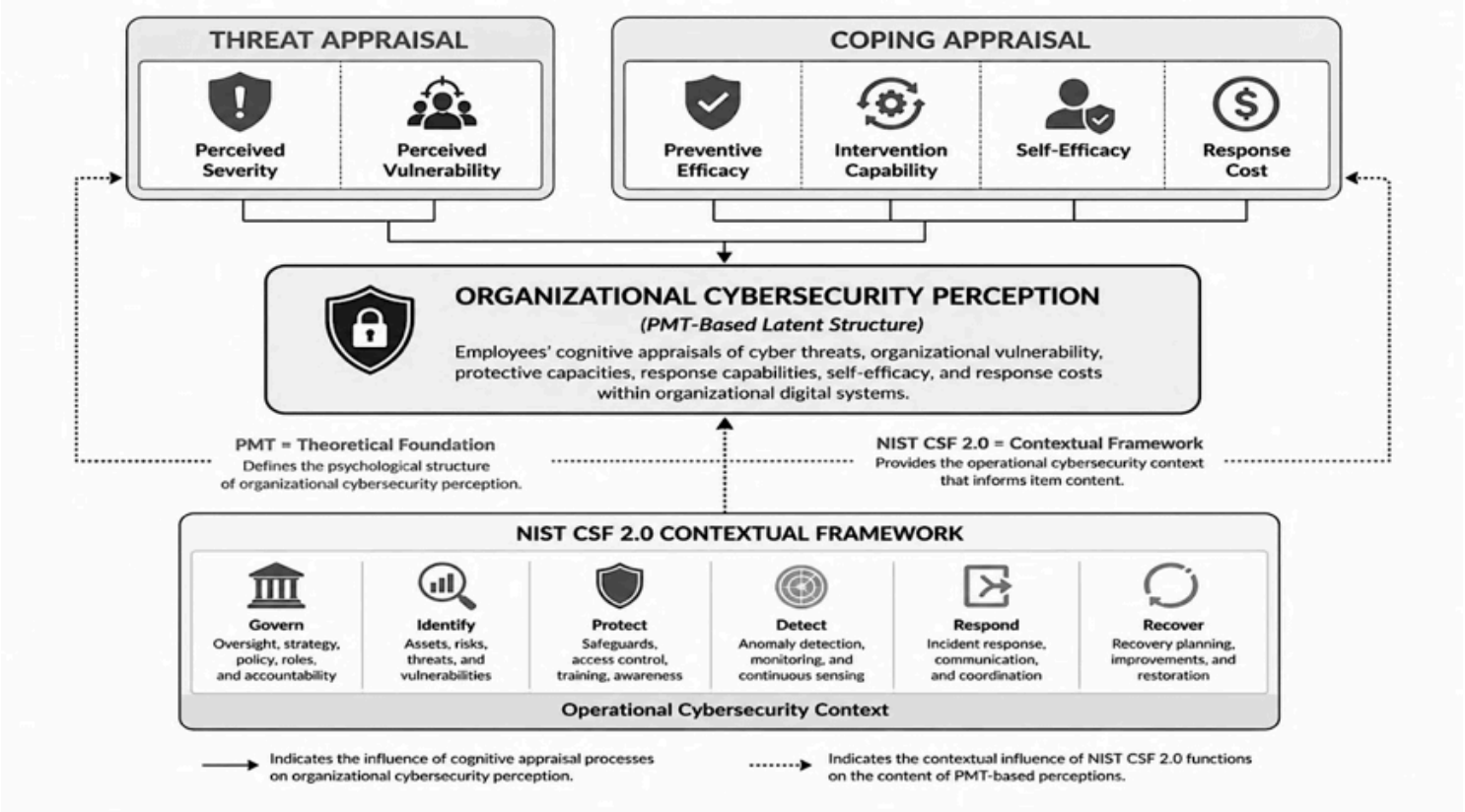


Figure 1

Conceptual Framework of Organizational Cybersecurity Perception Based on Protection Motivation Theory and Contextualized by NIST CSF 2.0

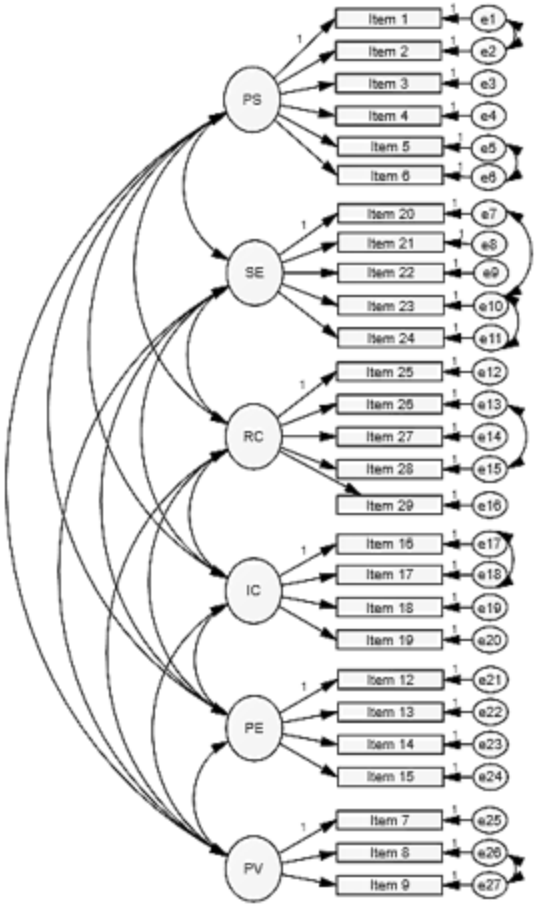


Figure 2

Final CFA Model of the Modified Six-Factor Measurement Structure

Note. PS = Perceived Severity; PV = Perceived Vulnerability; PE = Preventive Efficacy; IC = Intervention Capability; SE = Self-Efficacy; RC = Response Cost. e1–e27 represent error terms associated with the observed variables. The final CFA model is presented in Figure 2. For visual clarity, standardized factor loadings are reported in Table 9 rather than displayed in the figure.