Computers & Security 166 (2026) 104904

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

Development and cross-cultural validation of the cybersecurity resilience scale (CSRS)

Ibrahim Arpaci [a,b,*], Naurin Farooq Khan [c], Tahira Nazir [c]

[a] Department of Computer Engineering, Faculty of Engineering, Bursa Uludag University, 16059 Bursa, Türkiye
[b] Department of Computer Science and Engineering, College of Informatics, Korea University, 02841 Seoul, Republic of Korea
[c] Faculty of Computing, Riphah International University, 44000 Islamabad, Pakistan

ARTICLE INFO

Keywords:
Cybersecurity
Resilience
Scale development
CSRS

ABSTRACT

This study aimed to develop the Cybersecurity Resilience Scale (CSRS) and to evaluate its cross-cultural validity to assess individuals' resilience to cybersecurity threats. The psychometric properties of the new scale were evaluated using data obtained from Türkiye and Pakistan. An exploratory factor analysis was conducted to identify the scale's factor structure, yielding a five-factor solution ($N = 1982$). The Cronbach's alpha coefficient for each sub-dimension ranges from 0.75 to 0.90. The total scale, comprising 54 items, demonstrated reliability with a Cronbach's alpha value of 0.93. Confirmatory factor analysis (CFA) results revealed that the five-factor measurement model provided a good fit to the data ($N = 898$). A multi-group CFA was conducted to test measurement invariance across Turkish ($n = 440$) and Pakistani ($n = 458$) samples, supporting full measurement invariance between the two groups. The results indicate that the scale possesses sufficient convergent and discriminant validity. In the final stage, concurrent validity was supported through criterion-related validity analysis. Overall, the results indicate that the CSRS provides a reliable and valid measure of cybersecurity resilience at the individual level.

1. Introduction

In the modern digital age, cybersecurity has become a significant concern as digital systems, services, and communication tools rapidly advance (Gibreel and Arpaci, 2025). Everyone, including organizations, relies on digital and information systems for most purposes, such as communication, education, transactions, storage, and decision-making (Al-Sharafi et al., 2023). Due to this dependence, cybersecurity threats are increasing, including malware, data breaches, and phishing, which may result in serious risks of financial loss and erosion of user trust (Aşan, 2024). To strengthen security mechanisms, various efforts have been undertaken; however, cybersecurity incidents continue to increase, and, as a result, recovery mechanisms following recent attacks remain inadequate. This is evident in the fact that 70% of organizations are not cyber-resilient. The research demonstrates a high need for cyber resilience by individuals as well as organizations (Woods, 2015). The idea behind cyber resilience (Moonsammy et al., 2024) is that 100% security cannot be guaranteed by keeping cybercriminals out; however, the impact of cyber breaches needs to be contained, thereby undermining the cyber resilience of individuals and organizations (Hausken, 2020).

Cyber resilience is a new concept proposed by consulting firms, companies, and research organizations; it is relatively NASA-centric (Brown et al., 2017). Most scholarly work on cyber resilience is technical in nature (Lezzi et al., 2025). This involves research and development to enhance the resilience of the technical infrastructure. Cybersecurity resilience in this study is defined as an individual's ability not only to adopt preventive measures against cyber threats but also to respond effectively and recover from security incidents. Unlike prior awareness-focused scales, the CSRS integrates professional, proactive, and adaptive behaviors, offering a more comprehensive assessment of resilience at the individual level.

According to recent studies, human behavior is the weakest link in cybersecurity, and many incidents occur due to a lack of awareness, insufficient practices, and an inability to recognize cyber threats (Rohan et al., 2023; Xie et al., 2025). Users habitually use weak passwords, click on malicious links, neglect to install system updates, and fail to follow basic data protection principles, thereby unintentionally facilitating cyberattacks. The study of cyber resilience also involves human factors and has been examined to a limited extent.

The cyber resilience of an organization also involves working

* Corresponding author.
E-mail addresses: ibrahimarpaci@uludag.edu.tr (I. Arpaci), naurin.zamir@riphah.edu.pk (N. Farooq Khan), tahira.nazir@riphah.edu.pk (T. Nazir).

https://doi.org/10.1016/j.cose.2026.104904
Received 5 February 2026; Received in revised form 6 March 2026; Accepted 17 March 2026
Available online 18 March 2026

towards building cyber resilience at an individual level (Parsons et al., 2015). Individuals are often exploited to gain backdoor access to the organization's critical infrastructure. Therefore, cyber resilience includes protection from harm that can occur due to employees (van der Kleij and Leukfeldt, 2019). This can be achieved by instilling cybersecurity awareness and practices to improve cyber hygiene among employees (Karayel et al., 2025). Cybersecurity awareness encompasses a person's understanding, insights, and actions regarding the safe and appropriate use of digital systems (Akter et al., 2025). When individuals are sufficiently informed, they are better equipped to recognize security risks, follow protective online habits, and take suitable action when cyber incidents occur (Adeshola and Oluwajana, 2025). Though recent research indicates that awareness of cybersecurity issues is still inadequate among diverse populations, like students, organizational staff, and even professionals working in highly digital settings (Kaleli, 2024). This lack of awareness increases exposure to cyber threats and undermines the effectiveness of institutional security measures and awareness initiatives (Awang et al., 2024).

Although the significance of cybersecurity resilience has recently been acknowledged, accurately estimating its value remains problematic. Many existing studies rely on unplanned or situation-specific surveys that lack detailed validation, making it hard to compare results across groups or to evaluate the real impact of awareness programs (Rohan et al., 2023). The lack of well-established, reliable measurement tools limits researchers' and practitioners' ability to pinpoint weaknesses in the human aspect of cybersecurity resilience clearly and to develop focused, effective improvement strategies.

Consequently, there is a considerable demand to design and validate a robust cybersecurity resilience scale. Although several instruments have been developed to assess cybersecurity awareness and security behaviors, such as the "Security Behavior Intentions Scale" (SeBIS), existing measures typically focus on specific aspects of cybersecurity practices rather than capturing the broader concept of resilience (Egelman and Peer, 2015). Similarly, studies examining cybersecurity practices in organizational contexts highlight the importance of awareness, behavioral compliance, and security culture, but often rely on limited behavioral indicators (Corallo et al., 2022; Tolah et al., 2021). These limitations suggest a gap in the literature regarding comprehensive measurement tools capable of assessing different levels of cybersecurity resilience at the individual level.

2. Theoretical framework

2.1. Protection motivation theory (PMT)

PMT was proposed by Rogers (1975) to understand how individuals respond to threats to protect themselves (Rogers, 1975). Initially adopted in the health and social sciences, the theory has recently been applied to cybersecurity (Khan et al., 2023). Given the most frequent adoption of PMT (Khan et al., 2022), individuals' cybersecurity behaviors can be explained by two appraisals: "threat appraisal" and "coping appraisal" (Rogers, 1983). Threat appraisal comprises threat vulnerability, the probability of a threat's enactment, and threat susceptibility, the severity of the aftermath once the threat materializes (Kiran et al., 2025). The coping appraisal consists of three components: Self-efficacy, response efficacy, and response cost.

Self-efficacy is an individual's perceived ability to carry out a protective response to a threat (Rogers et al., 1997). Response efficacy is the individual's perception of the effectiveness of the threat aversion response. Response cost is the cost of protective response, expressed as monetary or time costs. The two threat and coping appraisals of the PMT work in parallel when an individual recognizes a cybersecurity threat. Upon detecting a potential cyber threat, the individual assesses its consequences (threat, vulnerability, and severity). At the same time, the coping appraisal comes into play as individuals assess their self-efficacy in implementing a protective cybersecurity measure against the identified cyberthreat (Rogers, 1983). The individual also assesses the efficacy of the protective action in mitigating the cybersecurity threat, as well as the time and monetary costs associated with it. The two appraisals motivate the individual to implement protective measures against cyber threats (Kiran et al., 2025).

For instance, an individual learns that they are vulnerable to falling for viruses and worms, and that the consequences of such threats include the loss of personal data. The individual then appraises that, in response to the threat, installing antivirus software is effective in averting the virus's threat (response efficacy). The installation of antivirus software is easy to conduct (self-efficacy). The effort and time required to install antivirus software are manageable for the individual (response cost). By conducting threat and coping appraisals, the individual performs a cost-benefit analysis of risks posed by viruses and the costs of installing antivirus software, motivating them to engage in cybersecurity behavior.

2.2. Theory of planned behavior (TPB)

TPB is also a popular theory in cybersecurity behavior research (Almansoori et al., 2023). It focuses on individuals' intentions in driving their cybersecurity actions. The TPB has been extended from the "Theory of Reasoned Action" (TRA) and shares the same theoretical bases (Ajzen, 1991; Conner, 2020). TPB essentially explains the overall attitude of an individual in terms of feelings, which can be either positive or negative, towards a particular behavior (Sulaiman et al., 2022). Three psychological factors drive cybersecurity intention in TPB. These factors are "subjective norms" (SNs), "perceived behavioral control" (PBC), and "attitude" (Zhang et al., 2009).

Attitude is an individual's belief that security actions are beneficial or worthwhile. The second factor, subjective norm, reflects social pressure on individuals to follow specific security actions (Ajzen, 1991). This social pressure stems from people's views and norms regarding security actions. For instance, in organizational settings, subjective norms for a particular cybersecurity action arise when employees comply with security practices, thereby creating social pressure to follow suit. Conversely, organizational culture can sometimes discourage safe behaviors if security practices are perceived as unnecessary or disruptive, highlighting that social influence can operate in both supportive and inhibitory directions.

The third factor is PBC, which refers to the individual's perceived capability and control in carrying out the security action (Ajzen, 1991). This can also be considered the individual's security competence in recognizing threats and subsequently using security tools to protect against them. According to the TPB, an individual's behavioral intention to carry out security behavior is positive when they view the security action to be positive, feel confident in their capability to carry out the security action, and believe that important personnel in that environment expect them to comply with carrying out the security action (Sulaiman et al., 2022).

2.3. Technology threat avoidance theory (TTAT)

Liang and Xue developed the TTAT for understanding the individual's response to threats, specifically in cyberspace (Liang and Xue, 2009). It explains how individuals are motivated to avoid those cyber threats. TTAT proposes that an individual will avoid the cyber threat due to two elements: the threat appraisal and coping appraisal (Gillam and Foster, 2020). Despite significant overlap with the PMT, TTAT differs in that it focuses on threat avoidance. PMT focuses on protective behavior and is used broadly across disciplines, including threats in health, the environment, and psychology, whereas TTAT focuses on threats specific to IT.

The threat appraisal comprises perceived severity, which defines the seriousness of cyber-attacks in terms of consequences, such as financial or personal information loss. Perceived susceptibility is the individual's

belief that they are prone to cyberattacks. The second element of TTAT is coping appraisal, in which safeguard effectiveness is an individual's belief that a specific action will reduce the risk of cyber threats. The safeguard cost is an individual's perception of the cost of an action, such as time, money, or inconvenience. Similarly, self-efficacy is an individual's confidence in their ability to enact the safeguarding behavior successfully (Liang and Xue, 2009).

The threat and coping appraisals operate in parallel, allowing the individual to engage in avoidance behavior. For instance, a university employee will avoid clicking on unknown links, a behavior that is voluntary and based on threat and coping appraisal. If the individual believes that phishing is dangerous to their personal information, is most likely to occur, and that they could become a target of a phishing attack, the threat appraisal is activated ((Liang and Xue, 2009). At the same time, the coping appraisal is engaged, with the individual believing that clicking on unknown links is practical and easy and feeling confident in avoiding them.

2.4. CIA triad

The "Confidentiality-Integrity-Availability" (CIA) triad is a critical framework in information security (Fenrich, 2008). It is one of the top foundational models that guides organizations in designing, implementing, and evaluating cybersecurity controls. CIA ensures that organizations receive protected, accurate information that is accessible on demand (Mohanty et al., 2018). Confidentiality concerns the access of information only to authorized individuals. Organizations should protect information from unauthorized disclosure (Samonas and Coss, 2014).

Integrity is the completeness and accuracy of information, whereas availability ensures that data or information are accessible to authorized personnel whenever needed (Death, 2017). These three components are interrelated, should complement each other, and are to be adopted in organizational settings while maintaining balance. This balance strongly influences cybersecurity behaviors, as the maintenance and violation of these three elements rest on individuals and organizations. The CIA triad, viewed from the perspective of cybersecurity behaviors, highlights that security depends on human decision-making as well as technical safeguards (Samonas and Coss, 2014). Effective cybersecurity involves integrating behavioral awareness, motivation, and intention with technical controls.

2.5. Parkerian hexad

The Parkerian Hexad (pH) model expands the traditional CIA triad and was proposed by Parker (1998). While the CIA emphasizes protecting information from disruption, alteration, and unauthorized access, it does not comprehensively capture information misuse in the modern digital landscape. The pH addresses this limitation and acknowledges that information compromises can occur despite the CIA being intact (Parker, 1998). The model identifies six core attributes for information security. In addition to confidentiality, integrity, and availability, it includes three attributes: Possession or control, authenticity, and utility. Possession denotes control over information, underscoring that data can be compromised even when it is confidential (Parker, 1998). Examples include encrypted data that can be stolen. Authenticity highlights the trustworthiness and genuineness of the information, ensuring that the data remains real and not forged (Parker, 1998). The utility, on the other hand, refers to the usefulness of the information, highlighting that data availability should be marked by its formatting and context so that it remains usable (Parker, 1998).

2.6. Health belief model (HBM)

The HBM originated in the 1950s and was developed by Hochbaum, Rosenstock, and Kegels for the U.S. public health services (Rosenstock, 1974). The primary rationale for HBM was to explain why individuals fail to adopt disease prevention measures. HBM has been used in cybersecurity behavioral research (Ng et al., 2009). It is among the most developed models that conceptualize behavior in response to threats in both physical and online spaces (Dodel and Mesch, 2017). Two factors determine health-related behaviors: threat perceptions and behavioral expectations. The threat perception consists of perceived susceptibility, an individual's perception of the likelihood of experiencing a cyber-attack, and perceived severity, the seriousness of the consequences of a cyber-attack. The second factor, behavioral expectation, has two elements. The benefits of adopting a healthy behavior include reducing susceptibility and the severity of the health condition. The second element of the behavioral expectation is the perceived barrier, the inconvenience or cost associated with that healthy behavior.

2.7. International cybersecurity standards

Several International standards exist specifically for cybersecurity management. The ISO/IEC 27,000 series is a comprehensive standard jointly developed by ISO and IEC for the implementation and continual improvement of an Information system (ISO - ISO/IEC 27000 family — Information security management, 2026). This series includes ISO/-IEC27000, which defines the terminology; ISO/IEC27001, which specifies requirements (ISO/IEC 27001:2022, 2026); and ISO/IEC27002 (ISO/IEC 27002:2022, 2026), which provides guidance on implementing cybersecurity and addresses specialized domains of privacy and cybersecurity. The ISO/IEC 27,000 series enables organizations to manage security controls in alignment with their objectives, regulations, and evolving cyber threats. An extension of this series is ISO/IEC 27,701, which guides the establishment, maintenance, and continual improvement of privacy. Privacy management involves the collection, application, and protection of personally identifiable data and ensuring compliance with the GDPR.

Whereas the ISO/IEC 27,002 security control guidelines should be implemented in accordance with an organization's risk assessment. It specifically serves as a code of practice offering security best-practice recommendations. The security controls span organizational, physical, and technological aspects, and the standard enables the design of security policies in accordance with requirements. The cybersecurity guidelines established in ISO/IEC 27,002 address security challenges in cyberspace and emphasize collaboration among stakeholders (individuals, organizations, and governments) to mitigate them. ISO/IEC 27,035 provides a structured framework for information security incident management, covering the entire incident lifecycle, from reporting and detection to response, assessment, and lessons learned. The standard supports organizations in developing consistent and effective incident response capabilities.

The "National Institute of Standards and Technology" (NIST) special publication 800 series guides on managing cybersecurity risks in information systems. This series includes NIST SP 800–53 (NIST SP 800–53, 2020), NIST SP 800–207 (Zero Trust Architecture: NIST Publishes SP 800–207, 2020), and NIST SP 800–61 (NIST SP 800–61, 2020). The first NIST SP 800–53 is a comprehensive catalog of privacy and security controls developed to help organizations implement a risk-based approach to protecting assets. It enables organizations to tailor controls based on system impact levels and threat environments. NIST SP 800–207 establishes the concept of zero trust, based on the "Never trust, always verify" mantra. The standard emphasizes policy enforcement points, policy decision points, and a continual monitoring mechanism. NIST SP 800–61, by contrast, provides guidance on establishing and operating incident response capabilities, emphasizing the importance of coordination and management among teams and external stakeholders to support organizational compliance and resilience.

2.8. Existing measurement scales and need for SCRS

Several instruments have been developed to assess different aspects of cybersecurity at the individual level. For example, the "Cybercrime Awareness Scale" (CAS) developed by Arpaci and Arpaci and Ateş (2023) measures individuals' awareness of cybercrime through a three-dimensional structure. Similarly, the "Cybersecurity Scale" (CS-S) proposed by Arpaci and Sevinc (2022) evaluates individuals' perceptions and practices related to cybersecurity across six dimensions. Other widely used instruments include the SeBIS (Egelman and Peer, 2015), which focuses on behavioral intentions related to secure technology use, and the "Human Aspects of Information Security Questionnaire" (HAIS-Q) (Parsons et al., 2014), which assesses awareness, knowledge, and attitudes toward cybersecurity. In addition, several studies have developed scales focusing specifically on cybersecurity awareness or behaviors (Addae et al., 2017; Erdoğdu et al., 2021; Erol et al., 2015). While these instruments provide valuable insights into specific components of cybersecurity, such as awareness, attitudes, or behavioral intentions, they address these aspects in isolation. Consequently, there remains a need for a more comprehensive and robust instrument capable of capturing multiple levels of cybersecurity resilience, from awareness deficits to proactive, professional cybersecurity behaviors. The CSRS was developed to address this gap by integrating different levels of cybersecurity awareness and behavior into a hierarchical multidimensional structure. A summary of existing cybersecurity scales is provided in Table 1.

The CSRS is clearly distinct from existing scales in the literature in terms of conceptual scope, level, and application area. While existing scales remain at the awareness level, the CSRS provides a multidimensional tool for measuring resilience against cyber threats. The scale is designed to evaluate not only individual perceptions and behaviors but also individual-organization interactions. In this respect, the scale goes beyond awareness-based measurement tools and addresses cybersecurity within a process-based and systemic resilience framework. It is a unique and comprehensive measurement tool for both scientific research and corporate applications.

The development of the CSRS was guided by multiple theoretical frameworks and standards that informed both its conceptualization and operationalization. Each scale dimension is explicitly linked to relevant standards and policies, including ISO/IEC 27,001, NIST CSF, ISO/IEC 27,035, ISO/IEC 27,002, and COBIT 2019. Additionally, theoretical frameworks such as PMT, TTAT, and the TPB guided item development. Finally, the scale incorporates core technical principles from the CIA triad to ensure that individual-level cybersecurity behaviors align with essential security objectives. Table 2 presents a concise mapping of these theories and standards to the five CSRS dimensions, demonstrating how each influenced item development and the overall structure of the scale.

Table 1
Summary of existing cybersecurity scales.

Reference	Scale	Method	Results
(Arpaci and Ateş, 2023)	CAS	EFA, CFA	A three-dimensional and reliable scale for assessing cybercrime awareness.
(Arpaci and Sevinc, 2022)	CS-S	EFA, CFA	A six-dimensional and reliable scale measuring perceptions and practices.
(Egelman and Peer, 2015)	SEBIS	EFA, CFA	A four-dimensional scale measuring cybersecurity intentions.
(Parsons et al., 2014)	HAIS-Q	EFA, CFA	A seven-dimensional scale measuring awareness, knowledge, and attitude in cybersecurity.
(Erdoğdu et al., 2021)	Cybersecurity Awareness	EFA, CFA	A six-factor scale measuring cybersecurity awareness.
(Erol et al., 2015)	Personal cybersecurity behaviors	EFA, CFA	A five-factor instrument measuring personal cybersecurity behaviors.
(Addae et al., 2017)	Cybersecurity Awareness	EFA, CFA	A six-factor scale for measuring cybersecurity awareness.

3. Method

The research method used in this study is based on a multi-stage research design for scale development (DeVellis, Robert F., 2021). This sequential approach to developing and evaluating the developed scale consists of six basic phases: (1) developing the initial item pool, (2) examining content validity through expert panel evaluations, revising the item pool based on the feedback obtained, and reviewing the items again by performing a pilot study, (3) collecting data for "Exploratory Factor Analysis" (EFA), and conducting EFA, (4) collecting data for "Confirmatory Factor Analysis" (CFA) and conducting CFA, (5) assessing convergent and discriminant validity, and (6) testing concurrent validity. Fig. 1 shows an overview of the multi-phase scale development and validation framework.

3.1. Item development

Researchers developed the item pool in accordance with universal standards. In this context, the principles of "confidentiality, integrity, and availability" within the CIA triad framework have been adopted. Additionally, international cybersecurity standards, including the ISO/IEC 27,000 series, ISO/IEC 27,701, ISO/IEC 27,032, and the NIST, were referenced during the scale development process. Theoretical frameworks and models were also considered in developing the scale items, including the PMT, the TTAT, and the TPB. The total of 88 items developed in this direction have been categorized into five levels. The distribution of items is as follows: 15 in the first category, 20 in the second, 15 in the third, 20 in the fourth, and 18 in the fifth.

The new scale uses a "five-point Likert-type" scale ranging from 1 ("strongly disagree") to 5 ("strongly agree"), including a neutral midpoint. This option allows respondents to express ambivalence or uncertainty, thereby improving validity by capturing genuine indecision rather than forcing a choice. The five-point format also provides sufficient sensitivity to capture meaningful differences in responses. However, the design may introduce central tendency bias if the midpoint is overused (Winke and Brunfaut, 2020).

Table 2
Mapping CSRS dimensions to standards, policies, and theoretical frameworks.

CSRS Dimension	Key Standards / Policies	Theoretical Frameworks	CIA Triad Focus
Level 1 – Lack of Awareness	NIST Cybersecurity Framework: Identify; ISO/IEC 27,001: Awareness & Training	PMT	Confidentiality (awareness)
Level 2 – Basic Cybersecurity Awareness	NIST CSF: Protect; ISO/IEC 27,001: Access Control & Awareness	PMT, TPB	Confidentiality (awareness)
Level 3 – Standardized Cybersecurity Behaviors	ISO/IEC 27,001: Access Control, Asset Management; NIST CSF: Protect	PMT, TTAT	Confidentiality, Integrity
Level 4 – Measurable Cybersecurity Behaviors	NIST CSF: Detect & Respond; ISO/IEC 27,002: Security Operations	PMT, TTAT	Confidentiality, Integrity, Availability
Level 5 – Professional & Proactive Cybersecurity Behaviors	NIST CSF: Respond & Recover; ISO/IEC 27,035: Incident Management; COBIT 2019: Risk Management	PMT, TTAT, TPB	Confidentiality, Integrity, Availability

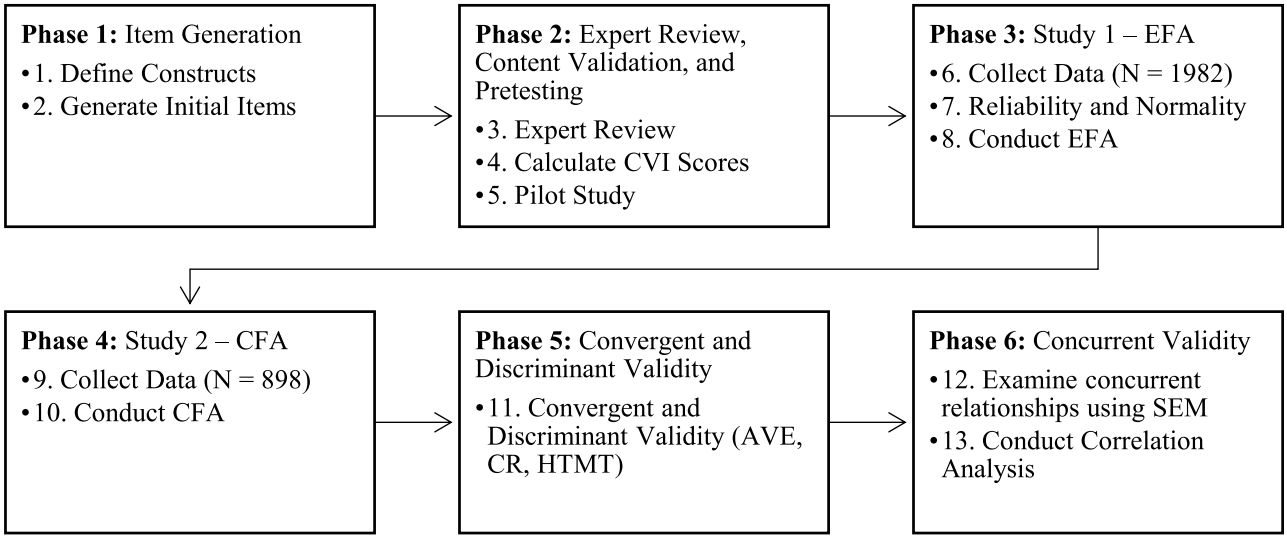

Fig. 1. Scale development and validation process.

3.2. Content validity

As part of the expert opinion process, two language experts were consulted to evaluate the linguistic accuracy, grammatical correctness, and clarity of the scale items. In addition, two experts with PhDs in Information Systems and one expert with a PhD in Law reviewed the scale; the Delphi method was used to compile the experts' opinions systematically. The experts were requested to assess the items on appropriateness, relevance, difficulty, and ambiguity.

The content validity of the scale was assessed by using the "content validity ratio" (CVR) and "content validity index" (CVI). The CVR was used to determine the necessity of each item. In this context, the scale was presented to ten subject matter experts, and they were requested to rate each item on a three-point scale: "1. Not necessary," "2. Useful but not necessary," and "3. Necessary." Based on the experts' evaluations and the Lawshe table, it was determined that items with a CVR of 0.62 or higher would remain on the scale (Lawshe, 1975).

In the CVI analysis, each item was evaluated by using a 5-point Likert-type scale, based on the criteria of simplicity, fluency, appropriateness, and clarity. Items with a CVI value above 0.79 were retained in the scale, while items in the 0.70–0.79 range were considered to require revision, and items below 0.70 were considered to be statements that should be removed (Lawshe, 1975). Based on expert feedback, 26 items were removed from the scale.

Subsequently, a pilot study was performed with 20 participants to assess the comprehensibility of the final version of the scale. Participants were asked whether the items were clear and understandable. Statements that were considered problematic in terms of language and meaning were revised accordingly. After revision, the items were reviewed again to ensure consistency with the study's objectives.

3.3. Sample and procedure

Data for this research study were collected from Türkiye and Pakistan. To ensure participant confidentiality, all responses were kept confidential and anonymous. Informed consent was obtained from participants who voluntarily participated, and they were fully informed of their rights and the purpose of the research. Furthermore, the research was conducted in accordance with the university's ethical standards (Decision No. 2025–9, 09/25/2025), and the research protocol was evaluated and approved by the relevant committee.

Separate datasets were collected for the EFA and CFA to mitigate concerns about "Common Method Variance" (Campbell, 1976). The sample size of the first study (EFA) is 1982. Participants' ages range from 18 to 55 years, with a mean of 21.60 (SD = 3.96). The gender distribution is balanced, with 52.1% of participants being women and 47.9% being men. In terms of educational level, the majority of participants are college graduates (81.0%), followed by high school graduates (11.7%) and associate degree graduates (5.8%). Master's and doctoral students and graduates account for 1.8% of the total.

The sample for the second study (CFA) consisted of 898 participants. Participants' ages ranged between 18 and 55, with a mean of 22.26 (SD = 5.11). The gender distribution was balanced, with 50.4% female and 49.6% male participants. In terms of educational levels, the majority of participants were undergraduate students (78.1%), followed by high school graduates (10.5%), associate degree holders (8.8%), and students pursuing a master's or doctoral degree (2.6%).

4. Results

4.1. Reliability and normality

The reliability analysis and EFA of the scale were conducted using SPSS. Items 1 and 5 were eliminated because of low reliability ($\alpha < 0.70$). Items 3, 18, 23, and 56 were eliminated either because their factor loadings were below 0.40 or their communalities were below 0.30. "Corrected Item-Total Correlation" (CITC) values were all above 0.30, indicating that each item was consistent with the overall scale (Hair, J. F., Black, W.C., Babin, B.J., Anderson, 2019).

Furthermore, since the skewness (SE = 0.342) and kurtosis (SE = 0.172) values fall within the range between −3 and +3, the data are normally distributed (Hair et al., 2019). Table 3 presents item discrimination indices, as well as results on reliability and normality. The findings indicate that the developed subscales are statistically robust and reliable. First, with respect to the normality assumption, the skewness values for all items are between −1 and +1, and the kurtosis values are between −1 and +1.5; this indicates that the item distributions are acceptable for normality. Although negative kurtosis was observed in some items (e.g., Item 6, Item 9), these values do not violate the normal distribution assumption when considering the sample size ($N = 1982$). In addition, the mean age of participants was 21.60 years, with a 95% confidence interval of [21.43, 21.77]. While the age distribution is slightly skewed, this does not impact the analyses. It is important to note that formal tests such as Shapiro–Wilk or Kolmogorov–Smirnov are highly sensitive to minor deviations in large samples and may suggest significant departures even when distributions are practically normal

Table 3
Reliability and normality.

Dimension	Item	Normality		Reliability		Item discrimination	
		Skewness (SE=0.055)	Kurtosis SE=0.110)	CITC	Alpha if Item Deleted	*t*	Sig. (2-tailed)
Lack of Awareness – 9 items (α=0.754)	Item-2	−0.684	−0.742	0.438	0.731	−0.362	0.718
	Item-4	−0.316	−0.893	0.339	0.746	−3.811	0.000
	Item-6	0.032	−10.291	0.286	0.757	2.570	0.010
	Item-7	−0.300	−0.997	0.559	0.711	−2.025	0.043
	Item-8	−0.679	−0.611	0.619	0.701	−4.995	0.000
	Item-9	−0.242	−10.004	0.397	0.737	−5.806	0.000
	Item-10	−0.573	−0.740	0.526	0.716	−1.966	0.050
	Item-11	−0.110	−0.890	0.387	0.739	1.276	0.202
	Item-12	−0.004	−0.750	0.365	0.742	2.887	0.004
Basic Cybersecurity Awareness – 11 items (α=0.854)	Item-13	−0.184	−0.891	0.460	0.848	−16.202	0.000
	Item-14	−0.680	−0.651	0.582	0.839	−18.281	0.000
	Item-15	−0.129	−0.901	0.437	0.850	−16.123	0.000
	Item-16	−0.342	−0.900	0.503	0.845	−19.458	0.000
	Item-17	−0.378	−0.532	0.504	0.845	−17.337	0.000
	Item-19	−0.618	−0.572	0.602	0.838	−20.364	0.000
	Item-20	−0.360	−0.737	0.542	0.842	−23.925	0.000
	Item-21	−0.462	−0.568	0.611	0.838	−22.691	0.000
	Item-22	−0.587	−0.554	0.642	0.836	−24.028	0.000
	Item-24	−0.310	−0.541	0.527	0.843	−22.004	0.000
	Item-25	−0.248	−0.608	0.580	0.840	−28.697	0.000
Standardized Cybersecurity Behaviors – 10 items (α=0.863)	Item-26	−0.272	−0.829	0.444	0.861	−22.621	0.000
	Item-29	−0.336	−0.820	0.566	0.851	−25.124	0.000
	Item-30	0.011	−0.795	0.531	0.854	−23.294	0.000
	Item-31	−0.054	−0.897	0.603	0.848	−26.004	0.000
	Item-32	−0.112	−0.824	0.600	0.848	−22.770	0.000
	Item-33	−0.202	−0.710	0.587	0.850	−23.189	0.000
	Item-34	−0.158	−0.720	0.634	0.846	−25.403	0.000
	Item-35	−0.124	−0.765	0.626	0.846	−24.483	0.000
	Item-37	−0.325	−0.873	0.585	0.850	−27.859	0.000
	Item-38	−0.104	−0.825	0.568	0.851	−29.282	0.000
Measurable Cybersecurity Behaviors – 12 items (α=0.873)	Item-27	−0.094	−0.642	0.599	0.860	−26.313	0.000
	Item-28	0.095	−0.653	0.599	0.860	−24.372	0.000
	Item-36	0.037	−0.787	0.585	0.861	−25.151	0.000
	Item-39	−0.195	−0.645	0.628	0.858	−29.534	0.000
	Item-40	−0.444	−0.675	0.575	0.854	−25.856	0.000
	Item-41	0.003	−0.705	0.642	0.857	−27.321	0.000
	Item-42	0.110	−0.880	0.622	0.859	−22.593	0.000
	Item-43	−0.122	−0.546	0.615	0.859	−26.879	0.000
	Item-44	−0.143	−0.630	0.606	0.860	−30.166	0.000

(*continued on next page*)

Table 3 (*continued*)

Dimension	Item	Normality		Reliability		Item discrimination	
		Skewness (SE=0.055)	Kurtosis SE=0.110)	CITC	Alpha if Item Deleted	*t*	Sig. (2-tailed)
	Item-45	−0.270	−0.582	0.514	0.866	−26.028	0.000
	Item-46	−0.254	−0.779	0.523	0.858	−24.032	0.000
	Item-51	0.054	−0.751	0.523	0.866	−20.325	0.000
Professional and Proactive Cybersecurity Behaviors – 12 items (α=0.898)	Item-47	0.062	−0.779	0.637	0.888	−22.025	0.000
	Item-48	0.127	−0.797	0.684	0.886	−24.030	0.000
	Item-49	−0.034	−0.592	0.540	0.893	−23.714	0.000
	Item-50	−0.040	−0.575	0.619	0.889	−20.647	0.000
	Item-52	−0.026	−0.526	0.618	0.889	−23.941	0.000
	Item-53	−0.079	−0.593	0.595	0.891	−25.454	0.000
	Item-54	0.033	−0.702	0.633	0.889	−21.612	0.000
	Item-55	−0.153	−0.557	0.563	0.892	−23.873	0.000
	Item-57	0.273	−0.999	0.576	0.892	−14.854	0.000
	Item-58	0.023	−0.809	0.643	0.888	−20.417	0.000
	Item-59	−0.128	−0.550	0.614	0.890	−24.175	0.000
	Item-60	0.094	−0.810	0.646	0.888	−19.903	0.000

(Hair, J.F., Black, W.C., Babin, B.J., Anderson, 2019). Therefore, for this study ($N = 1982$), skewness and kurtosis were used as the primary indicators of normality, consistent with best practices for large-scale survey research.

Cronbach's alpha coefficient for each sub-dimension ranges between 0.75 and 0.90. The total scale, comprising 54 items, demonstrated reliability with a Cronbach's α value of 0.93. The reliability coefficient is well above the 0.70 threshold (Cronbach, 1951). These values indicate that the scale has high internal consistency both overall and within each dimension. In particular, the $\alpha = 0.898$ value for the fifth dimension reveals that the scale is reliable in this dimension. However, the item-total correlations for some items (e.g., Items 6 and 11) were low (CITC < 0.40).

According to item-discrimination analysis, t-values were significant ($p < .001$), indicating that the items effectively distinguished between high- and low-scoring groups. Only a few items (e.g., Item 2 and Item 11) did not show significant differences ($p > .05$), indicating that these items contribute weakly to the overall structure of the scale. Overall, the scale items are normally distributed, reliable, statistically discriminative, and successfully represent the five-factor structure.

4.2. Exploratory factor analysis

EFA was conducted by using "maximum likelihood" (ML) extraction, which is appropriate for Likert-type items and for estimating factor loadings. While Varimax (orthogonal) rotation assumes independent factors, our theoretical framework and preliminary analyses indicated that the factors are interrelated and complementary. Therefore, Promax (oblique) rotation was applied to allow for correlated factors, ensuring a more accurate representation of the scale's dimensionality and improving interpretability.

According to the total variance explanation table, five components (factors) with eigenvalues higher than one were obtained from the principal component analysis. These five factors collectively account for 45.97% of the total variance. The initial factor accounts for the largest proportion of variance (27.70%), while the second, third, fourth, and fifth factors each account for 8.49%, 4.44%, 2.70%, and 2.63%, respectively. The scree plot of the eigenvalues obtained from the analysis (See Fig. 2) supports the idea that the scale has a multidimensional, five-factor structure, as there are noticeable drops in eigenvalues after each factor.

Bartlett's "test of sphericity" ($\chi^2(1540)$ 45,634.436, $p < .001$) and the KMO measure (0.966) confirmed the suitability of the scale items for factor analysis. Table 4 shows factor loadings, which range from 0.370 to 0.806. In general, the values exceed the commonly accepted threshold of 0.40 (Hair, J.F., Black, W.C., Babin, B.J., Anderson, 2019). Similarly, the communality values range from 0.277 to 0.608, with most items exceeding the suggested threshold value of 0.30, revealing that the extracted factors adequately represent the items (Williams and Child, 1974).

4.3. Confirmatory factor analysis

CFA was performed on a separate sample ($N = 898$) to assess the construct validity of the CSRS using SPSS AMOS (ver. 29). The measurement model was tested by using standard fit indices. The model showed acceptable fit: $\chi^2(1339) = 2004.22$, $p < .001$, CMIN/DF = 2.24; SRMR = 0.0654; RMSEA = 0.026, 90% CI [0.026, 0.027], PCLOSE = 1.000. "Comparative fit indices" (CFI) were slightly below conventional thresholds: CFI = 0.884, TLI = 0.873; however, "parsimony-adjusted indices" (PNFI = 0.738, PCFI = 0.806) support the adequacy of the five-factor model. GFI = 0.837 and AGFI = 0.815 suggest an acceptable absolute fit. Overall, these results suggest that the data support the hypothesized five-factor structure.

The scale indicated strong reliability and convergent validity in the total sample ($N = 898$). Cronbach's α values ranged from 0.806 to 0.892, suggesting good internal consistency across all five factors. Composite reliability (CR = 0.860–0.912) exceeded the threshold of 0.70 for all constructs. At the same time, AVE values ranged from 0.507 to 0.519, confirming that >50% of the variance in items was explained by their

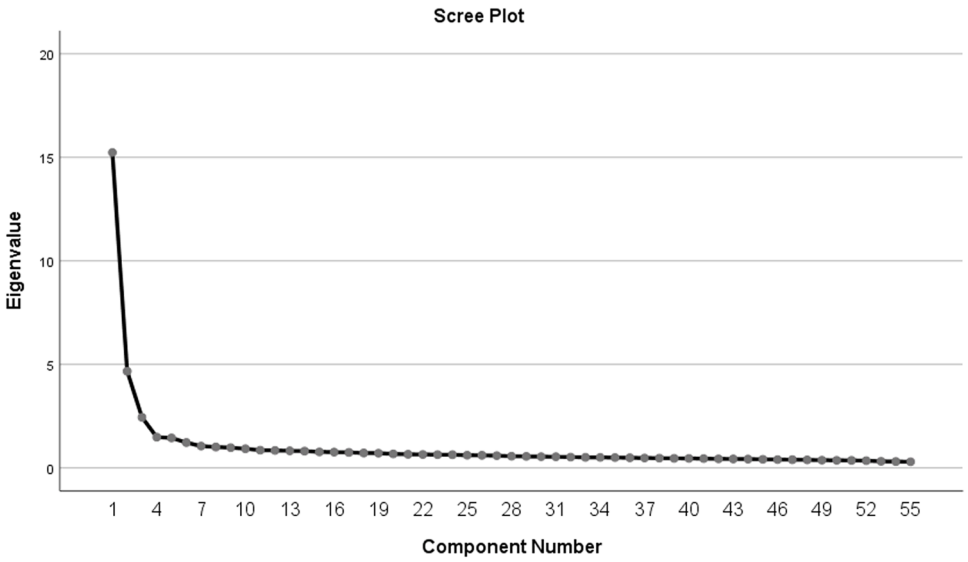

Fig. 2. The scree plot.

respective latent factor (Henseler et al., 2015)

Discriminant validity, assessed by using the "heterotrait-monotrait ratio" (HTMT), was supported for most constructs. As presented in Table 5, HTMT values between most variables were below the conservative threshold of 0.85. However, the HTMT between F3–F4 (0.835) was close to the conservative threshold, and F4–F5 (0.903) slightly exceeded the lenient threshold of 0.90 (Henseler et al., 2015), suggesting some conceptual overlap between these factors. To address concerns regarding the high conceptual overlap among Factors 3, 4, and 5 (HTMT = 0.918 and 0.904), an alternative three-factor model was evaluated, in which these three dimensions were combined into a single factor. The three-factor model indicated acceptable fit (χ^2/df = 3.74, RMSEA = 0.055, CFI = 0.822, TLI = 0.809), but the fit was noticeably worse than the original five-factor model (χ^2/df = 2.19, RMSEA = 0.026, CFI = 0.886, TLI = 0.878). Information criteria also favored the five-factor solution (AIC_5F = 9660.61 vs. AIC_3F = 5303.26, noting model complexity differences). These results support retaining all five factors in the CSRS, despite the high statistical overlap between some dimensions, as the original structure provides a more nuanced assessment of individual cybersecurity resilience across different behavioral domains.

4.5. Criterion related validity

A criterion-related validity analysis was conducted by testing a "structural equation model" (SEM) in AMOS to assess the association between the newly developed CSRS and the established "Cybersecurity Behavior Scale" (CBS) (Arpaci, 2024; Arpaci and Bahari, 2023). The CBS demonstrated good reliability and construct validity in the current sample (N = 898; Cronbach's α = 0.777; CR = 0.777; AVE = 0.469). The analysis shows a significant positive correlation between the CSRS total score and the CBS factor score, r = 0.681 (p < .001), indicating a strong concurrent relationship. The CFA results demonstrated good model fit (GFI = 0.991, AGFI = 0.973, CFI = 0.992, TLI = 0.982, RMSEA = 0.050, 90% CI [0.039, 0.062], PCLOSE = 0.469). The findings provide strong evidence for the criterion-related (concurrent) validity of the CSRS, confirming its meaningful association with an established measure of cybersecurity behaviors.

4.6. Measurement invariance

A multi-group CFA was employed to test measurement invariance across Turkish (n = 440) and Pakistani (n = 458) samples (N = 898). As presented in Table 6, the configural model, which imposed no equality constraints, indicated acceptable fit (χ^2(3912)=8741.47, CMIN/DF = 2.24, CFI = 0.884, TLI = 0.873, RMSEA=0.026, 90% CI [.026, 0.027]). Constraining all factor loadings to be equal across groups (metric invariance) produced minimal change in fit (ΔCFI = 0.002, ΔRMSEA = 0), supporting the equivalence of factor loadings across Turkish and Pakistani samples. According to established guidelines (Chen, 2007) a ΔRMSEA ≤ 0.015 and ΔCFI ≤ 0.01 indicate that the constraints do not worsen model fit, supporting full measurement invariance across Turkish and Pakistani samples.

5. Discussion

This study developed the Cybersecurity Resilience Scale (CSRS) to assess its cross-cultural validity and to evaluate individuals' resilience to cybersecurity threats. The psychometric properties of the new scale were assessed by conducting EFA and CFA. The EFA results yielded a five-factor solution (N = 1982). The Cronbach's alpha coefficient for each sub-dimension ranges from 0.75 to 0.90. The total scale, comprising 54 items, demonstrated reliability with a Cronbach's alpha value of 0.93. The CFA results revealed that the five-factor measurement model provided a good fit to the data (N = 898). Furthermore, the scale's validity was supported through concurrent validity testing. The results indicate that the scale possesses sufficient construct validity and discriminant validity. Additionally, multi-group CFA results indicate that the measurement model demonstrates good construct validity and full measurement invariance, allowing meaningful latent mean comparisons between Turkish and Pakistani participants.

Few studies have been done to develop and evaluate scales related to cybersecurity awareness (Corallo et al., 2022; Tolah et al., 2021). One of the early studies developed a scale to assess perceptions of cybersecurity. The scale consisted of six factors: Accuracy, utility, accessibility, confidentiality, ownership/control, and integrity. In another study, (Arpaci and Ateş, 2023) took a sample of 500 respondents to develop and psychometrically evaluate a cybercrime awareness scale. The study indicated a three-factor structure consisting of personal data crimes, information system crimes, and security and privacy.

One of the most commonly used scales for cybersecurity behaviors is SeBIS (Egelman and Peer, 2015). The SeBIS scale comprises four dimensions: Password creation, proactive awareness, device security, and updating. The SeBIS is relatively small, comprising 16 items, and has been psychometrically validated (Egelman et al., 2016). Another commonly used instrument for assessing cybersecurity behavior is the

Table 4
Pattern matrix.

Item	Communality	Factor-1	Factor-2	Factor-3	Factor-4	Factor-5
Item-2	0.350	0.546				
Item-4	0.375	0.570				
Item-6	0.277	0.370				
Item-7	0.504	0.668				
Item-8	0.602	0.736				
Item-9	0.473	0.643				
Item-10	0.467	0.640				
Item-11	0.367	0.513				
Item-12	0.306	0.491				
Item-13	0.420		0.531			
Item-14	0.547		0.559			
Item-15	0.392		0.512			
Item-16	0.514		0.620			
Item-17	0.402		0.642			
Item-19	0.516		0.719			
Item-20	0.428		0.599			
Item-21	0.523		0.736			
Item-22	0.588		0.770			
Item-24	0.402		0.500			
Item-25	0.478		0.482			
Item-26	0.374			0.349		
Item-29	0.468			0.543		
Item-30	0.474			0.496		
Item-31	0.544			0.726		
Item-32	0.486			0.644		
Item-33	0.487			0.620		
Item-34	0.533			0.580		
Item-35	0.518			0.554		
Item-37	0.475			0.646		
Item-38	0.421			0.495		
Item-27	0.407				0.405	
Item-28	0.432				0.446	
Item-36	0.455				0.395	
Item-39	0.470				0.378	
Item-40	0.477				0.549	
Item-41	0.484				0.544	
Item-42	0.545				0.725	
Item-43	0.436				0.453	
Item-44	0.486				0.385	
Item-45	0.426				0.498	
Item-46	0.398				0.482	
Item-51	0.458				0.619	
Item-47	0.557					0.701
Item-48	0.608					0.806
Item-49	0.393					0.467
Item-50	0.462					0.641
Item-52	0.464					0.682
Item-53	0.442					0.579
Item-54	0.457					0.681
Item-55	0.397					0.557
Item-57	0.478					0.762
Item-58	0.527					0.799
Item-59	0.472					0.682
Item-60	0.524					0.799

HAIS-Q (Parsons et al., 2014), which measures individuals' understanding and compliance with cybersecurity policies in environments. The HAIS-Q contains three dimensions of knowledge, practices, and attitudes with a seven-factor structure. These seven factors align well with incident reporting, Internet use, password management, information handling, e-mail use, mobile device use, and social networking. HAIS-Q provides a comprehensive assessment of cybersecurity awareness and behaviors (McCormac et al., 2017). Another study conducted in organizational settings found a relationship between employees' cybersecurity awareness and other factors (Butavicius et al., 2020).

Another scale for information security awareness was developed by Erdoğdu et al. (2021). The authors identified a six-factor structure, including basic security practices such as password management, backups, and access permissions. The scale developed by Li (2015) assessed users' cybersecurity levels and online security performance. The study accounted for risks across environmental, technological, and organizational perspectives in the development of the scale. The study by Erol et al. (2015) developed a personal cybersecurity behaviors scale using a sample of 810 participants. The instrument addressed issues such as personal privacy, payment security, and the minimization of digital traces within a five-factor structure. On the other hand, individuals' attitudes towards their personal data security were captured using a scale developed by Addae et al. (2019). The main dimensions covered were individuals' security and privacy, with 247 participants in the sample. High internal consistency and reliability were reported for the scale measuring data security and privacy. Another study measuring cybercrime awareness levels was conducted among high school students in the Philippines by Abuda et al. (2020). The instruments contained 18 items, organized into a four-factor structure: phishing, spam awareness, cyberbullying, and antivirus software efficacy. However, despite the availability of these tools, a notable gap remains in cybersecurity scales

Table 5
Reliability, convergent and discriminant validity.

Factor	α	CR	AVE	F1	F2	F3	F4	F5
F1	0.810	0.863	0.514					
F2	0.806	0.860	0.507	0.141				
F3	0.815	0.866	0.519	0.178	0.709			
F4	0.867	0.896	0.518	0.359	0.651	0.835		
F5	0.892	0.912	0.508	0.452	0.449	0.727	0.903	

Table 6
Measurement invariance.

Model	χ^2	df	χ^2/df	CFI	TLI	RMSEA	ΔCFI	ΔRMSEA
Configural (Unconstrained)	8741.47	3912	2.235	.884	.873	.026	–	–
Metric (Measurement Weights)	8770.61	4010	2.187	.886	.878	.026	+0.002	0
Structural Covariances	8795.06	4040	2.177	.886	.879	.026	0	0
Scalar (Measurement Residuals)	8934.85	4274	2.091	.888	.888	.025	+0.002	−0.001

that assess cyber resilience at the individual level.

5.1. Theoretical implications

The developed scale is significant because it reshapes the conceptualization of resilience and the explicit study of cybersecurity behavior in organizational settings (Singh and Cheema, 2024). It extends beyond theory-based measurement of cybersecurity behaviors and adopts a resilience-oriented paradigm (Moonsammy et al., 2024). While traditional cybersecurity theories focus on threat avoidance, this scale emphasizes due diligence in recovery, adaptation, and incident anticipation. Therefore, it clearly shifts the "how users avoid attacks" to "how users cope, continue, and recover after a cybersecurity incident." Therefore, it supports dynamic cybersecurity postures rather than static cybersecurity behavior across organizations.

The cyber resilience scale consists of five levels that distinguish between a lack of basic cybersecurity awareness and proactive cybersecurity behaviors among individuals. This helps resolve conceptual ambiguity in understanding cybersecurity behavior and clearly ascertains the level of cybersecurity achieved by a particular organization. Moreover, it helps distinguish cybersecurity awareness, behavioral compliance, and professional cybersecurity behavior in individuals and organizations. This enables understanding of cybersecurity research beyond static measures toward explaining maturity-based cybersecurity resilience. This thereby aligns secure behaviors with behavioral theories (Khan et al., 2022) that focus on stage-based cybersecurity, suggesting that resilience evolves rather than appearing immediately.

The current scale conceptualizes cybersecurity behavior as a hierarchical progression from basic awareness to professional capabilities. This addresses the gap between high awareness and actual secure behavior (Gundu, 2019) since awareness alone does not always translate into action. Hence, it reinforces the need to understand the progression of behavior from simple awareness to professional cybersecurity awareness. This allows for the assessment of an individual's and, consequently, an organization's cognitive maturity, cybersecurity behavior consistency, and adaptability in responding to cyber threats and attacks.

5.2. Methodological and practical contributions

From a methodological perspective, the cross-cultural development and validation of the new cybersecurity resilience scale enable a distinction among cybersecurity awareness, compliance, and practices. This enables researchers to assess organizations' cybersecurity posture more accurately (van Steen, 2023) and to capture and understand gradual behavioral change. The scale can be applied across contexts, including educational institutions, healthcare, finance, and other industries. From a practical perspective, the scale has significant value for organizations, educators, and policymakers. It enables a structured assessment (Kannelønning and Katsikas, 2023) of cybersecurity behavior across progressive stages, ranging from basic awareness to proactive professional practices. Measuring these levels allows organizations to design targeted training programs that address specific resilience levels rather than assumed competence.

Moreover, resources can be allocated much more efficiently, and interventions can be prioritized according to the organization's needs. This is akin to risk-based decision-making (Duzenci et al., 2023; Qin et al., 2018), in which cybersecurity behavioral gaps can be identified and closed, using this cybersecurity resilience scale as a benchmark to monitor improvements over time. For professionals and academic institutions, this scale provides a framework to align cybersecurity curricula and certifications with real-world security demands, thereby fostering a transition from reactive to resilient security (Maennel and Maennel, 2025). Briefly, the scale offers observable, measurable, and actionable cybersecurity practices that enhance cybersecurity readiness at both individual and organizational levels.

6. Conclusions

In this study, we developed a new scale to measure cybersecurity resilience. The scale items were developed based on the leading theories of cybersecurity behavior. In item development, industry-standard cybersecurity frameworks were also consulted, including NIST SP 800, ISO/IEC 27,000 series, CIA Triad, and the Parkerian hexad. The scale was then content-validated through expert feedback. The statistical analysis was conducted to assess the scale's reliability, convergent and discriminant validity, and the results indicated good psychometric properties. Concurrent validity was established by correlating the cybersecurity resilience scale with the previously validated Cybersecurity Behavior Scale (CBS).

6.1. Limitations and assumptions

Several limitations exist in the current study. First, the use of convenience sampling, which allows for a larger sample size, also introduces challenges in generalizing the results to broader populations. It is worth noting that the sample includes two countries spanning two continents, Asia and Europe. Although the current studies included balanced gender distributions, the majority of participants were undergraduate students, and the age range was relatively narrow (18–55 years). These characteristics may limit the generalizability of the study findings to broader populations, including older adults and non-student groups. Future studies should evaluate the CSRS across diverse demographic groups, including individuals from different backgrounds,

age groups, and cultures, to ensure its effectiveness and usability across cultural contexts. While the 54-item structure provides comprehensive coverage of cybersecurity resilience, its length may limit practical applicability in time-constrained settings. Future research could develop and validate a short-form version of the scale while preserving its factorial integrity and psychometric strength.

Although the CSRS effectively captures preventive and professional cybersecurity behaviors, it currently provides limited coverage of post-incident recovery actions. Future research could extend the scale to include items that explicitly assess adaptive and recovery-oriented responses, further aligning with a comprehensive definition of resilience. Additionally, future research may benefit from examining attributional beliefs that influence cybersecurity behavior. For example, locus of control and attributional tendencies, such as beliefs that outcomes are determined by luck or external factors, may shape individuals' motivation to engage in secure digital practices. Integrating these considerations with existing frameworks like TPB, TTAT, and HBM, which involve implicit causal appraisals of risk (probability multiplied by consequence), could provide a richer understanding of the motivational mechanisms underlying cybersecurity resilience. Instruments such as the MMCS (Lefcourt et al., 1979) could be used in future studies to systematically measure these attributional tendencies. Finally, although Rasch modeling was not applied in the current study, it represents a robust approach for examining item-level performance, measurement invariance, and scale functioning. Future studies could incorporate Rasch analyses to complement factor-analytic results, providing additional evidence for the CSRS's precision, validity, and applicability across diverse populations.

AI declaration

"The authors used Grammarly Pro to improve readability and grammatical clarity with caution."

CRediT authorship contribution statement

Ibrahim Arpaci: Writing – review & editing, Writing – original draft, Project administration, Conceptualization. **Naurin Farooq Khan:** Writing – review & editing, Writing – original draft. **Tahira Nazir:** Writing – review & editing, Writing – original draft.

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.

Acknowledgment

"This work was supported by the Scientific and Technological Research Council of Türkiye (TÜBİTAK) 1071 Program under Grant No. 124N731 (124N732) and by Pakistan Science Foundation (PSF) under the grant PSF-CRP/TUBITAK-IV/AI/C-RIU (31)."

Appendix A. Cybersecurity resilience scale (CSRS)

LEVEL 1 (Lack of Awareness)

1. I am not responsible for the materials I share on social media (R).
2. I have shared personal information on social media (R).
3. I write down my passwords and physically store them for easy recall (R).
4. I open every attachment to my email accounts (R).
5. I click on every link to my e-mail accounts (R).
6. I use unlicensed software downloaded from the Internet (R).
7. I am not responsible for my actions on the Internet (R).
8. Cyber-attacks do not target me (R).
9. Sensitive data can be stored in cloud environments (R).

LEVEL 2 (Basic Cybersecurity Awareness)

1. I do not insert other people's USB sticks into my device.
2. I do not share my data with third parties I do not know.
3. I do not turn off antivirus software, even temporarily.
4. I do not share any personal data via social media.
5. The online payment mechanisms I use are reliable.
6. The Wi-Fi Internet access I use is password-protected.
7. I am aware of phishing e-mails.
8. I am aware of which data can be shared online.
9. I am responsible for training myself on safe Internet use.
10. My computer has a firewall integrated into the current operating system.
11. I take the necessary security measures when making remote connections.

LEVEL 3 (Standardized Cybersecurity Behaviors)

1. I do not use unsecured public hotspots.
2. I use different passwords for different accounts.
3. I also use a firewall other than the firewall embedded in the operating systems.
4. I update passwords for my accounts frequently.
5. I apply filters against unwanted emails.
6. I back up my data regularly.
7. I update the Internet browsers I use periodically.
8. I periodically update the antivirus software I use.
9. I use different passwords for my email accounts.
10. I store confidential data in encrypted folders.

LEVEL 4 (Measurable Cybersecurity Behaviors)

1. I have a cybersecurity policy.
2. I have a cyber incident response plan.
3. I regularly follow news about cyber-attacks.
4. My devices have systems that protect against cyber-attacks.
5. I use two-factor authentication on my accounts.
6. I use intrusion detection systems.
7. I receive regular training on cybersecurity.
8. The Internet network I use is secure against cyber-attacks.
9. I take precautions against third-party monitoring of computer screens where my sensitive data is kept.
10. All devices I use are secure and do not contain malware.
11. I close unused applications immediately.
12. Devices where my critical data is stored are not connected to the Internet.

LEVEL 5 (Professional and Proactive Cybersecurity Behaviors)

1. I allocate financial resources for cybersecurity.
2. I have a cybersecurity disaster recovery plan.
3. I do not keep devices with data transfer capability in environments with critical data and documents.
4. My security system can detect potential cyber-attacks in advance.
5. My critical systems open to the Internet are protected by end-to-end tunneling.
6. I periodically check whether information is shared about me in digital environments.
7. I first run suspicious software in secure environments (virtual machine or sandbox).
8. I classify my data according to its degree of confidentiality.

9. I have at least one international (Cisco, CompTIA, EC—Council, Offensive Security, etc.) valid certificate showing that I am a cybersecurity expert.
10. I am familiar with cybersecurity legislation.
11. My data is protected against copying and sharing.
12. I use an authentication device (USB security token) to protect my access to computers, networks, and online services.

Scoring. The Cybersecurity Resilience Scale (CSRS) is rated on a five-point Likert-type scale ranging from strongly disagree (1) to strongly agree (5). The scale consists of 54 items across five dimensions: Lack of Awareness (F1; 9 items), Basic Cybersecurity Awareness (F2; 11 items), Standardized Cybersecurity Behaviors (F3; 10 items), Measurable Cybersecurity Behaviors (F4; 12 items), and Professional and Proactive Cybersecurity Behaviors (F5; 12 items). Items marked with (R) are reverse-coded to ensure that higher scores consistently indicate higher cybersecurity resilience. Subscale scores are calculated by averaging the items within each factor. Each factor reflects a distinct aspect of cybersecurity resilience, so interpretation should be done at the factor level rather than as a total score. Higher mean scores indicate stronger resilience in that dimension, whereas lower scores highlight areas for potential improvement. For descriptive purposes, mean scores may be divided into five equal intervals corresponding to the Likert scale (1 - 5): 1.00–1.80 = Very Low, 1.81–2.60 = Low, 2.61–3.40 = Moderate, 3.41–4.20 = High, 4.21–5.00 = Very High. These intervals provide a practical guideline for interpreting scores but are not diagnostic thresholds.

Data availability

Data will be made available on request.

References

Abuda B.F., Rivera K.D., Noroña R.V. Predictive validity of a cybercrime awareness tool: the case of senior high school students in a Philippine secondary school. Abuda, BF, Rivera, K, Noroña 2020:18–26.

Addae, J.H., Brown, M., Sun, X., Towey, D., Radenkovic, M., 2017. Measuring attitude towards personal data for adaptive cybersecurity. Inf. Comput. Secur. 25, 560–579. https://doi.org/10.1108/ICS-11-2016-0085.

Addae, J.H., Sun, X., Towey, D., Radenkovic, M., 2019. Exploring user behavioral data for adaptive cybersecurity. User Model User Adapt. Interact. 29, 701–750. https://doi.org/10.1007/s11257-019-09236-5.

Adeshola, I., Oluwajana, D.I., 2025. Assessing cybersecurity awareness among university students: implications for educational interventions. J. Comput. Educ. 12, 1283–1305. https://doi.org/10.1007/s40692-024-00346-7.

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Akter, S., Uddin, M.R., Sajib, S., Lee, W.J.T., Michael, K., Hossain, M.A., 2025. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Ann. Oper. Res. 350, 673–698. https://doi.org/10.1007/s10479-022-04844-8.

Al-Sharafi, M.S., Al-Emran, M., Arpaci, I., Marques, G., Namoun, A., Iahad, N.A., 2023. Examining the impact of psychological, social, and quality factors on the continuous intention to use virtual meeting platforms during and beyond COVID-19 Pandemic: a hybrid SEM-ANN approach. Int. J. Hum. Comput. Interact. 39, 2673–2685. https://doi.org/10.1080/10447318.2022.2084036.

Almansoori, A., Al-Emran, M., Shaalan, K., 2023. Exploring the frontiers of cybersecurity behavior: a systematic review of studies and theories. Appl. Sci. 13, 5700.

Arpaci, I., 2024. A multianalytical SEM-ANN approach to investigate the social sustainability of AI chatbots based on cybersecurity and protection motivation theory. IEEE Trans. Eng. Manag. 71, 1714–1725. https://doi.org/10.1109/TEM.2023.3339578.

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, 633–643. https://doi.org/10.1108/OIR-01-2022-0023.

Arpaci, I., Bahari, M., 2023. A complementary SEM and deep ANN approach to predict the adoption of cryptocurrencies from the perspective of cybersecurity. Comput. Human. Behav. 143, 107678. https://doi.org/10.1016/j.chb.2023.107678.

Arpaci, I., Sevinc, K., 2022. Development of the cybersecurity scale (CS-S): evidence of validity and reliability. Inf. Dev. 38, 218–226. https://doi.org/10.1177/02666669211997512.

Aşan, C., 2024. Developing a measurement scale to assess the perception of cybersecurity among employees in the maritime industry. J. Nav. Sci. Eng. 20, 135–162.

Awang, H., Mansor, N.S., Zolkipli, M.F., Malami, S.T.S., Zaini, K.M., Yau, T.D., 2024. Cybersecurity awareness among special needs students: the role of parental control. Mesopotamian. J. Cybersecur. 4, 63–73.

Brown, C., Seville, E., Vargo, J., 2017. Measuring the organizational resilience of critical infrastructure providers: a New Zealand case study. Int. J. Crit. Infrastruct. Prot. 18, 37–49.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., Calic, D., 2020. When believing in technology leads to poor cyber security: development of a trust in technical controls scale. Comput. Secur. 98. https://doi.org/10.1016/J.COSE.2020.102020.

Campbell, A., 1976. Subjective measures of well-being. Am. Psychol. 31, 117–124. https://doi.org/10.1037/0003-066X.31.2.117.

Chen, F.F., 2007. Sensitivity of goodness of fit indexes to lack of measurement invariance. Struct. Equ. Mode.l A. Multidiscip. J. 14, 464–504. https://doi.org/10.1080/10705510701301834.

Conner, M., 2020. Theory of planned behavior. Handb. Sport Psychol. 1–18.

Corallo, A., Lazoi, M., Lezzi, M., Luperto, A., 2022. Cybersecurity awareness in the context of the Industrial Internet of Things: a systematic literature review. Comput. Ind. 137. https://doi.org/10.1016/J.COMPIND.2022.103614.

Cronbach, L.J., 1951. Coefficient alpha and the internal structure of tests. Psychometrika 16, 297–334. https://doi.org/10.1007/BF02310555.

Death, D., 2017. Information Security Handbook. O'Reilly.

DeVellis, R.F., CTT, 2021. Scale development: Theory and Applications. Sage Publications.

Dodel, M., Mesch, G., 2017. Cyber-victimization preventive behavior: a health belief model approach. Comput. Human. Behav. 68, 359–367.

Duzenci, A., Kitapci, H., Gok, M.S., 2023. The role of decision-making styles in shaping cybersecurity compliance behavior. Appl. Sci. 13, 8731.

Egelman, S., Harbach, M., Peer, E., 2016. Behavior ever follows intention? A validation of the Security Behavior intentions scale (SeBIS). In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 5257–5261.

Egelman, S., Peer, E., 2015. Scaling the Security wall. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, pp. 2873–2882. https://doi.org/10.1145/2702123.2702249.

Erdoğdu, F., Gökoğlu, S., Kara, M., 2021. What about users?": development and validation of the mobile information security awareness scale (MISAS). Online Inf. Rev. 45, 406–421. https://doi.org/10.1108/OIR-04-2020-0129/FULL/HTML.

Erol, O., Şahin, Y.L., Yılmaz, E., Haseski, H.İ., 2015. Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. Int. J. Hum. Sci. 12, 75–91.

Fenrich, K., 2008. Securing your control system: the "CIA triad" is a widely used benchmark for evaluating information system security effectiveness. Power Eng. 112, 44–49.

Gibreel, O., Arpaci, I., 2025. Development and validation of the prompt engineering competence scale (PECS). Inf. Dev. https://doi.org/10.1177/02666669251336455.

Gillam, A.R., Foster, W.T., 2020. Factors affecting risky cybersecurity behaviors by US workers: an exploratory study. Comput. Human. Behav. 108, 106319.

Gundu T. Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince, 2019, p. 94–102.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., 2019. Multivariate data analysis. Hempshire: Cengage Learning, 8th ed. EMEA.

Hausken, K., 2020. Cyber resilience in firms, organizations and societies. Internet Things 11, 100204. https://doi.org/10.1016/j.iot.2020.100204.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43, 115–135. https://doi.org/10.1007/s11747-014-0403-8.

ISO/IEC 27001:2022. ISO 2026.

ISO/IEC 27002:2022. ISO 2026.

ISO, 2026. ISO/IEC 27000 Family — Information Security Management. ISO.

Kaleli, S.S., 2024. Measuring digital data security awareness: the case of higher education institution. J. Stud. Adv. Technol. 2, 108–119.

Kannelønning, K., Katsikas, S.K., 2023. A systematic literature review of how cybersecurity-related behavior has been assessed. Inf. Comput. Secur. 31, 463–477.

Karayel, T., Aktaş, B., Akbıyık, A., 2025. Human factors in remote work: examining cyber hygiene practices. Inf. Comput. Secur. 33, 96–116. https://doi.org/10.1108/ICS-11-2023-0215.

Khan, N.F., Ikram, N., Murtaza, H., Javed, M., 2023. Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model. Comput. Secur. 125, 103049. https://doi.org/10.1016/j.cose.2022.103049.

Khan, N.F., Yaqoob, A., Khan, M.S., Ikram, N., 2022. The cybersecurity behavioral research: a tertiary study. Comput. Secur. 120, 102826. https://doi.org/10.1016/j.cose.2022.102826.

Kiran, U., Khan, N.F., Murtaza, H., Farooq, A., Pirkkalainen, H., 2025. Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. Comput. Secur. 149, 104204. https://doi.org/10.1016/j.cose.2024.104204.

van der Kleij, R., Leukfeldt, R., 2019. Cyber Resilient behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities Into Cyber Security. Springer, pp. 16–27.

Lawshe, C.H., 1975. A quantitative approach to content validity. Pers. Psychol. 28.

Lefcourt, H.M., von Baeyer, C.L., Ware, E.E., Cox, D.J, 1979. The multidimensional-multiattributional causality scale: the development of a goal specific locus of control scale. Can. J. Behav. Sci. Rev. Can. Des. Sci. Du Comport. 11, 286–304. https://doi.org/10.1037/h0081598.

Lezzi, M., Corallo, A., Lazoi, M., Nimis, A., 2025. Measuring cyber resilience in industrial IoT: a systematic literature review. Manag. Rev. Q. https://doi.org/10.1007/s11301-025-00495-8.

Li, D.C., 2015. Online security performances and information security disclosures. J. Comput. Inf. Syst. 55, 20–28. https://doi.org/10.1080/08874417.2015.11645753.
Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS. Q. 71–90.
Maennel, K., Maennel, O., 2025. Human aspects of cyber security for computing higher education: current status and future directions. ACM Trans. Comput. Educ. 25, 1–30.
McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., Pattinson, M., 2017. A reliable measure of information security awareness and the identification of bias in responses. Australas. J. Inf. Syst. 21.
Mohanty, S., Ganguly, M., Pattnaik, P.K., 2018. CIA triad for achieving accountability in cloud computing environment. Int. J. Comput. Sci. Mob. Appl. 6, 38–43.
Moonsammy, A., Ahmed, M., Guidetti, O., Rashid, B., 2024. Integrating human factors and systemic resilience: an interdisciplinary approach to cybersecurity in critical infrastructures and utilities. Psybersecurity 1–34.
Ng, B.Y., Kankanhalli, A., Xu, Y.C., 2009. Studying users' computer security behavior: a health belief perspective. Decis. Support. Syst. 46, 815–825.
NIST SP 800-53. NIST 2020.
NIST SP 800-61. NIST 2020.
Parker, D.B., 1998. Fighting Computer crime: a New Framework For Protecting Information, 605. John Wiley & Sons, Inc, New York.
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput. Secur. 42, 165–176.
Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R., Jerram, C., 2015. The influence of organizational information security culture on information security decision making. J. Cogn. Eng. Decis. Mak. 9, 117–129.
Qin, Y., Zhang, Q., Zhou, C., Xiong, N., 2018. A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems. IEEE Trans. Syst. Man. Cybern. Syst. 50, 3863–3870. https://doi.org/10.1109/TSMC.2018.2861715.
Rogers, R.W., 1983. Cognitive and psychological processes in fear appeals and attitude change: a revised theory of protection motivation. Social Psychophysiology: A Sourcebook. Guilford Press, pp. 153–176.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91, 93–114. https://doi.org/10.1080/00223980.1975.9915803.
Rogers, R.W., Prentice-Dunn, S., Gochman, D.S., 1997. Handbook of Health Behavior Research 1: Personal and Social Determinants, 28. US Plenum Press, New York, NY, pp. 113–132.
Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., Thapliyal, H., 2023. A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon 9.
Rosenstock, I.M., 1974. The health belief model and preventive health behavior. Health Educ. Monogr. 2, 354–386.
Samonas, S., Coss, D., 2014. The CIA strikes back: redefining confidentiality, integrity and availability in security. J. Inf. Syst. Secur. 10.
Singh, B., Cheema, S.S., 2024. Psychology in cybersecurity: unveiling the human dimensions of digital resilience. Int. J. Adv. Netw. Appl. 16, 6281–6290.
van Steen, T., 2023. Measuring Behavioural cybersecurity: an Overview of Options. Springer, pp. 460–471.
Sulaiman, N.S., Fauzi, M.A., Wider, W., Rajadurai, J., Hussain, S., Harun, S.A., 2022. Cyber–Information Security compliance and violation behaviour in organisations: a systematic review. Soc. Sci. 11, 386. https://doi.org/10.3390/socsci11090386.
Tolah, A., Furnell, S.M., Papadaki, M., 2021. An empirical analysis of the information security culture key factors framework. Comput. Secur. 108. https://doi.org/10.1016/J.COSE.2021.102354.
Williams, J.S., Child, D., 1974. The essentials of factor analysis. In: Continuum, 3. A&C Black, London. https://doi.org/10.2307/2061984.
Winke, P., Brunfaut, T., 2020. The Routledge Handbook of Second Language Acquisition and Language Testing, 1st ed. Routledge, New York, NY. https://doi.org/10.4324/9781351034784.
Woods, D.D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9.
Xie, Y., Lei, T., Li, Z., Yang, Y., Chen, C., Long, Y., 2025. How do mental models affect cybersecurity awareness? The roles of questioning styles, need for cognition, and graphical representations. Comput. Secur. 150, 104292.
Zero Trust Architecture: NIST Publishes SP 800-207. NIST 2020.
Zhang, J., Reithel, B.J., Li, H., 2009. Impact of perceived technical protection on security behaviors. Inf. Manag. Comput. Secur. 17, 330–340.

Journal information

COMPUTERS & SECURITY

Publisher name: ELSEVIER ADVANCED TECHNOLOGY

Journal Impact Factor ™

5.4	5.9
2024	Five Year

JCR Category	Category Rank	Category Quartile
COMPUTER SCIENCE, INFORMATION SYSTEMS *in SCIE edition*	42/258	Q1

Source: Journal Citation Reports 2024. Go to Journal Citation Reports

Journal Citation Indicator ™

1.34	1.3
2024	2023

JCI Category	Category Rank	Category Quartile
COMPUTER SCIENCE, INFORMATION SYSTEMS *in SCIE edition*	44/258	Q1

The Journal Citation Indicator is a measure of the average Category Normalized Citation Impact (CNCI) of citable items (articles and reviews) published by a journal over a recent three year period. It is used to help you evaluate journals based on other metrics besides the Journal Impact Factor (JIF).

Go to Journal Citation Indicator

Publicati