LISA: A Scale-Optimized and Psychometrically-Validated Instrument for the Lightweight Assessment of Organizational Information Security Awareness in Heterogeneous Organizations

David Langer
Justus Liebig University Giessen
Giessen, Germany
david.langer@uni-giessen.de

Jan Tolsdorf
MPI-SP
Bochum, Germany
jan.tolsdorf@mpi-sp.org

Luigi Lo Iacono
Justus Liebig University Giessen
Giessen, Germany
luigi.lo_iacono@uni-giessen.de

***Abstract*—Human factors are central to an organization's information security. Information Security Awareness (ISA) is a key construct in behavioral and organizational models explaining employees' security compliance. However, existing ISA measures often lack theoretical grounding, psychometric rigor, and organizational relevance, or are too lengthy and complex for practical application. These shortcomings hinder empirical testing of behavioral models and the integration of ISA as a variable in organizational research.**

This paper introduces the Lightweight Information Security Awareness (LISA) scale—the first theory-based, psychometrically validated, and cross-language scale for efficiently assessing ISA in heterogeneous organizational contexts, balancing measurement precision with practical feasibility. Validation involved 1,182 participants from survey panels and 579 employees of a large German university hospital, representing a heterogeneous workforce. LISA demonstrates high internal consistency, measurement invariance across English and German, and strong construct and ecological validity.

By correlating LISA with 11 enablers and barriers of organizational information security and differentiating it by a heterogeneous workforce in a hospital context, we demonstrate its ability to support both scientific investigations and practical assessments. LISA provides a quick, reliable, valid, and practical solution for measuring organizational ISA, ultimately offering researchers and practitioners without psychometric expertise a validated tool that is applicable in both behavioral models and everyday organizational environments.

1. Introduction

Information Security Awareness (ISA) is widely recognized as a fundamental element of organizational information security [1], [2], [3], [4]. ISA captures employees' security-related knowledge, attitudes, and behaviors [2], [5]. Recent regulatory developments, such as the EU NIS2 Directive [6], emphasize the need for organizations to implement measures to strengthen information security awareness. Within human-factor research on organizational security, ISA is frequently employed as a theoretical construct or empirical variable and is consistently associated with individuals' security behaviors and policy compliance across sectors [7], [8], [9]. Reliable ISA measurement is essential for informing organizational decision-making, evaluating compliance readiness, and guiding targeted awareness interventions. Surveys remain the dominant method for assessing ISA in organizations. However, researchers and practitioners encounter persistent challenges regarding the availability of reliable and valid ISA measurement instruments. Existing instruments have several limitations that hinder their applicability across industries, job roles, and organizational contexts, thereby complicating efforts to assess ISA reliably, validly, and efficiently. First, many focus narrowly on IT- or cybersecurity-specific behaviors (e.g., password practices, software updates) and thereby fail to capture broader, domain-general aspects of information protection that are relevant across diverse organizational settings. For example, many sectors of critical infrastructure, including healthcare, public administration, social services, transportation, critical infrastructures, and laboratory or diagnostic environments, are highly heterogeneous. In these contexts, information handling extends far beyond digital systems to encompass communication, documentation, coordination, and decision-making processes embedded in daily workflows. Second, most instruments are available only in English, restricting their applicability in non-English-speaking contexts where organizations require linguistically adapted measures. Third, many instruments are extremely long, creating a considerable response burden and reducing their practicality in real-world use. Finally, several lack adequate psychometric evidence, including reliability, structural validity, and criterion validity, which limits confidence in the accuracy and interpretability of the resulting scores.

We address these limitations by introducing the Lightweight Information Security Awareness (LISA) scale, a compact, psychometrically validated instrument for theory-based, multilingual ISA assessment that extends beyond purely technical cybersecurity behaviors. LISA provides a robust yet efficient measure that is brief enough

Accepted for publication in: 2026 IEEE Symposium on Security and Privacy (SP).

for integration into organizational surveys and practical for use as a control variable in empirical research. In developing LISA, we pursued the following objectives:

O1: Develop a theory-based, concise, psychometrically sound, multilingual, minimal-effort instrument to measure information security awareness in organizational contexts. To address this objective, we created and validated the Lightweight Information Security Awareness (LISA) scale. We first generated and refined items through expert interviews and focus groups (n = 18), followed by expert evaluation (n = 11). A subsequent web-based access panel survey (n = 1,182) was conducted in English and German with working adults from the UK and the DACH region. The final 21-item LISA scale includes three individually assessable seven-item subdimensions—knowledge, attitude, and behavior—and shows strong psychometric performance, including convergent, discriminant, and nomological validity, high internal consistency, and good model fit. Evidence of measurement invariance additionally supports its applicability across languages.

O2: Validate the practicality of the LISA scale under real-world operational constraints in a heterogeneous organizational context. LISA was deployed in a large German university hospital (n = 571) to evaluate its performance under time-critical operational conditions. The scale demonstrated clear ecological validity, as its factorial structure and internal consistency closely matched the initial validation results. The average completion time was 2.76 minutes, with each subdimension requiring approximately 1 minute.

LISA reliably differentiates between staff groups (n = 579) and demonstrates criterion validity through expected correlations with established constructs. Additionally, simple sum scores correlate strongly with the corresponding factor scores, which enables practical score calculation without advanced statistical methods and ensures accessible applicability for researchers and practitioners.

Our paper makes the following contributions:

C1 Domain-General ISA Instrument: We introduce LISA, the first concise and psychometrically validated instrument specifically designed to measure information security awareness reliably, validly, and efficiently. LISA captures the core dimensions of knowledge, attitude, and behavior while maintaining a strong theoretical foundation and minimal completion time.

C2 Cross-Lingual Measurement Invariance: We demonstrate configural, metric, and scalar invariance of LISA across English- and German-speaking samples. This establishes its applicability in multilingual organizational environments, including the DACH region with roughly 100 million inhabitants, and enables reliable cross-national and cross-context comparisons.

C3 Tool for Research and Organizational Diagnostics: LISA provides a validated basis for both academic research and applied organizational diagnostics. It supports theory-driven ISA studies, role-specific assessments, and the development of targeted awareness interventions across diverse job profiles and organizational settings.

2. Background

2.1. Information Security Awareness

Information Security Awareness (ISA) is widely recognized as a critical component of organizational information security [2], [5]. ISA in organizations has been defined as *"the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly"* [10]. Researchers have conceptualized ISA in three more or less interrelated ways: First, ISA as a state of security-relevant behavior [10]. Second, ISA as a cognitive mental state, encompassing general and specific knowledge as well as an understanding of security issues and their potential consequences [11]. Third, ISA as a continuous process aimed at cultivating this mental state, which seeks to influence individuals' perceptions, values, attitudes, behavior, norms, work habits, and organizational culture and structures in relation to secure information practices [3].

In this work, we adopt a working definition of ISA as a cognitive and behavioral state, distinguishing it from the continuous process, such as the implementation of policies, technologies, procedures, and training initiatives that precede and aim to develop this state. By positioning knowledge, personal accountability, and behavior at the core of the construct, our definition enables its use as a measurable construct in behavioral security research and allows for the evaluation of organizational efforts aimed at cultivating a cognitive and behavioral state.

A related but distinct construct in human-centered information security literature is information security culture. Unlike ISA, it is grounded in organizational culture theory, particularly Schein's three-layer model of underlying assumptions, values, norms, and observable artifacts [12], which has been extended to information security contexts [13], [14]. Information security culture reflects shared norms and values at the collective level, whereas ISA captures individual-level knowledge, attitudes, and behaviors. Although the two constructs influence each other, they remain conceptually distinct. Information security culture is not further considered within the scope of this paper.

2.2. Knowledge-Attitude-Behavior Model

Given our conceptualization of ISA, the Knowledge–Attitude–Behavior (KAB) model offers a suitable theoretical foundation. Originally developed in domains such as health promotion [15], [16], [17] and environmental

education [18], [19], [20], [21], it has been increasingly applied to ISA [10], [22], [23]. The KAB model conceptualizes behavior as shaped by the interaction between knowledge and attitudes. Although empirical studies show that these relationships are not strictly linear or deterministic [24], the framework remains theoretically coherent and widely accepted. The KAB model is well-suited for ISA research as long as its constructs are clearly defined, properly operationalized, and meaningfully linked to relevant variables [23]. It provides a structured basis for examining ISA, designing ISA interventions, and assessing cognitive and behavioral states [23], [25].

Within ISA, the KAB model provides a simplified approach to understanding how individuals internalize and respond to security-related expectations. *Knowledge* refers to an individual's understanding of relevant information security policies and procedures [23], [25]. *Attitude* is defined as an evaluative disposition to respond favorably or unfavorably [26] to those policies and procedures. *Behavior* reflects the extent to which individuals actually comply with established security guidelines. The relationship between knowledge, attitude, and behavior is conceptualized as a sequential process, in which the influence of knowledge on behavior is partially mediated by attitude [23].

The dimensions of knowledge, attitude, and behavior related to information security are central to most psychometric operationalizations of ISA [27] and align with the broader conceptual understanding of information security awareness [10], [11]. This alignment provides a robust theoretical anchor for the development of LISA, ensuring its conceptualization is grounded in established ISA scholarship and enabling systematic evaluation of related research.

2.3. Psychometrics

Psychometrics is concerned with the development, validation, and evaluation of measurement instruments designed to assess psychological concepts, referred to as constructs [28], [29]. Constructs are abstract, theoretical ideas that cannot be directly observed but are inferred through measurable indicators. The process of operationalizing a construct involves defining its dimensions and generating items (e.g., survey questions or tasks) that reflect those dimensions. Many constructs consist of multiple subconstructs, i.e., distinct but related dimensions that together capture the complexity of the overarching concept. These sub-constructs are often informed by theoretical models or identified through empirical methods such as exploratory factor analysis (EFA) or confirmatory factor analysis (CFA), which reveal or support latent structures by clustering items into coherent factors [30], [31]. A psychometric instrument's validity, i.e., the extent to which it measures what it intends to measure, is typically established through content, criterion, and construct validation methods. Reliability, on the other hand, assesses the consistency and stability of the measurements across time or contexts [29]. A psychometric scale with robust properties must be both reliable and valid [32], [33], achieved through a rigorous development process that includes three phases: item development (e.g. item generation and content validation), scale development (e.g. pre-testing, survey administration, factor extraction and item reduction), and scale evaluation (e.g. tests of reliability and validity) [29]. In this work, we introduce LISA, a scale designed in accordance with these rigorous guidelines to produce a psychometrically sound measure of information security awareness.

3. Related Work

Research on information security awareness (ISA) measurement spans multiple domains within security and human-centered computing. Rather than providing an exhaustive survey, we focus on a representative subset of established instruments, drawing on the systematic review by Rohan et al. [27] and related human-centered security literature. We include scales that (i) were introduced as primary research contributions rather than artifacts (e.g., [44]), (ii) target generalizable contexts rather than narrowly scoped domains such as mobile-only settings [45] or specific professional groups [46], and (iii) operationalize ISA rather than adjacent constructs such as security culture [47]. The resulting set of instruments (Tab. 1) serves as the basis for the following synthesis.

Scope and Contextual Limitations. Existing ISA instruments predominantly focus on cybersecurity, devices, and online security, addressing IT-centric topics such as password practices, email, internet and social media use, mobile device security [25], [37], [41], mobile phone security [40], cybersecurity perceptions across technical domains [35], [44], end-user security attitudes and deviant behavior in IT systems [38], and secure computer use more generally [43]. While these studies provide robust approaches for measuring ISA in technology-mediated environments, broader aspects of information security, such as offline information handling, physical document practices, and organizational safeguards, remain underrepresented. Instruments such as the HAIS-Q [25] and HAIS-SDT [41] extend coverage beyond purely digital behaviors, but they were validated in administrative, university, financial, and office-based contexts [23], [25], making them less applicable to non-desk-bound and non-computer-focused organizations and jobs.

In addition, many instruments are designed for private end-user contexts or narrowly defined cybersecurity settings [35], [36], [37], [38], [40], which may limit their applicability in organizational environments. The extent to which knowledge, attitudes, and behaviors (KAB) are explicitly and systematically operationalized also varies significantly across scales, with many focusing on only a single dimension (knowledge only [39], attitudes only [38], behavior only [34], [35], [36], [37], [42]) or two dimensions [40], [44], indicating variability and limitations in theoretical grounding. Taken together, this focus constrains the ability of existing instruments to capture ISA in heterogeneous organizations and organizations where security-relevant practices extend beyond individual interaction with digital systems. LISA addresses this limitation by adopting a

TABLE 1. COMPARISON LISA WITH COMMON SCALES TO ASSESS INFORMATION SECURITY AWARENESS.

Ref.	Scale	ISA-Scope	Application Context	KAB Coverage	# Items	Language Invariance	Psychometric Quality	
							Reliability & Validity	Overall
*	LISA	Information Security	Organizational	K, A, B	21	yes	Reliability, CFA, convergent, discriminant, nomological, criterion, known-groups	●
[25]	HAIS-Q	Information Security	Organizational	K, A, B	63	no	Test–retest reliability, PCA, convergent, criterion, known-groups	●
[34]	Misuse & Carelessness Scales	Computer & Mobile Security	Organizational	B	7	no	Reliability, EFA/CFA, convergent, discriminant, nomological	●
[35]	CS-S	Cybersecurity	Personal	B	25	no	Reliability, EFA/CFA, convergent, discriminant, known-groups	●
[36]	SeBIS	Device & Online Security	Personal	B	16	no	Reliability, EFA/CFA, discriminant, nomological	●
[37]	ESBS	Device & Online Security	Personal	B	20	no	Reliability, EFA/CFA, criterion, nomological	●
[38]	SA-6	Online Security	Personal	A	6	no	Reliability, EFA/CFA, convergent, discriminant, nomological, known-groups	●
[39]	CAIN	Cybersecurity	Organizational	K	30	no	Reliability, known-groups, criterion	◐
[40]	MISAS	Mobile Device Security	Personal	K, B	17	no	Reliability, EFA/CFA	◐
[41]	HAIS-SDT	Information Security	Organizational	K, A, B	63	no	Reliability, EFA factors only (no detailed metrics)	○
[42]	CSEC	Online Security	Organizational	B	7	no	No reliability, limited construct checks	○
[43]	SISA	Computer Security	Organizational	K, A, B	3	no	No psychometric properties	○
[44]	4-Measurement Scales	Online Security & Privacy	Organizational	A, B	89	no	No psychometric properties	○

Note: The *Overall*-column is a visual summary of the "Reliability & Validity" column, indicating ○ Low quality: No psychometric assessment or only minimal evidence. ◐ Moderate quality: Some psychometric assessment (e.g., reliability, EFA) but lacking full psychometric rigor. ● High quality: Comprehensive psychometric assessment including reliability, EFA/CFA, and multiple validity types (e.g., convergent, discriminant, nomological, or known-groups differences). K, A, B = Knowledge, Attitude, Behavior; HAIS-Q = Human Aspects of Information Security Questionnaire, HAIS-SDT = Human Aspects of Information Security based on Self-Determination Theory, CSEC = Cybersecurity Questionnaire, SISA = Simplified Information Security Awareness Scale, CAIN = Cybersecurity Awareness Inventory Scale, SeBIS = Security Behavior Intentions Scale, ESBS = Extended Security Behavior Scale, MISAS = Mobile Information Security Awareness Scale, SA-6 = Security Attitudes Scale.

broader conceptualization of ISA that explicitly incorporates both digital and non-digital practices, is grounded in a consistent KAB framework, and is designed for applicability across diverse organizational contexts.

Trade-offs Between Scope, Length, and Psychometric Quality. Prior ISA instruments exhibit inherent trade-offs between construct coverage, administration length, and psychometric rigor. Comprehensive instruments such as the HAIS-Q [25] and HAIS-SDT [41] cover a broad range of ISA aspects with full KAB coverage, but their extensive length (63+ items) limits suitability for large-scale or time-constrained studies, and only the HAIS-Q demonstrates consistently high psychometric quality. Medium-length instruments (e.g., SeBIS [36], CS-S [35], ESBS [37]) achieve strong reliability and validity but are primarily focused on digital behaviors in personal-use contexts. Short instruments offer more efficient measurement, with some (e.g., Misuse and Carelessness Scales [34], SA-6 [38]) providing acceptable psychometric properties, albeit capturing narrower facets of ISA, while others (e.g., CSEC [42], SISA [43]) provide limited validation evidence. Collectively, these patterns highlight the difficulty of simultaneously achieving broad construct coverage, organizational applicability, conciseness, and robust psychometric support. LISA addresses these limitations by providing a concise, 21-item instrument with full KAB coverage, validated psychometric properties, and applicability across organizational contexts, including both digital and non-digital information security practices.

Limited Cross-Language Validity. ISA measurement is increasingly applied in international and multilingual contexts, including cross-country comparisons [48] and deployments in non-English-speaking organizations [39]. However, most existing ISA instruments are developed and validated in a single language (predominantly English), and cross-language applications often rely on ad hoc translation procedures [39], [48] without explicit assessment of measurement invariance [49]. Establishing measurement invariance is necessary to ensure that a scale captures the same latent construct across language groups. Without such evidence, it remains unclear whether translated instruments preserve construct equivalence, as observed differences may reflect linguistic variation rather than ISA differences. This limitation is particularly restrictive in multinational organizational contexts. LISA addresses this gap by combining

a state-of-the-art translation process with formal tests of language invariance across English and German. In doing so, LISA provides the first validated bilingual instrument and a methodological blueprint for future research on cross-language ISA measurements.

4. Methodology

To develop and validate the LISA scale, we followed a two-stage research design. In Study I, we addressed objective **O1** by developing and validating the LISA scale in both English and German. Construct validation was conducted via an online survey with 1,182 employed participants recruited through the research panels Prolific (English-speaking) and Bilendi (German-speaking).

In Study II, we addressed objective **O2** by deploying the LISA scale at a large German university hospital. Based on n = 579 valid responses, we evaluated its ecological validity and applicability in a real-world, time-critical, and heterogeneous organizational context. Details of Study I and Study II are presented in Sec. 5 and Sec. 6, respectively. All study materials are available in the supplementary materials repository [50].

5. Study I: Development and Psychometric Validation of LISA

Study I followed established guidelines for scale development (see e.g. [29], [31], [51], [52], [53]) and structured it into three phases: (1) scale construction, involving theory-driven item generation, expert feedback, item translation and multilingual survey design; (2) scale refinement, based on exploratory and confirmatory factor-analytic item reduction and model fit estimation; and (3) scale evaluation, assessing reliability and multiple forms of validity. This process resulted in the final 21-item multilingual version of LISA.

5.1. Phase I: Scale Construction

5.1.1. Pre-Item Generation Workshops and Interviews. To ground scale development in organizational contexts, we conducted six expert interviews with information security professionals and four focus groups with 13 employees from a large German university hospital. The hospital setting was deliberately selected because existing organizational ISA instruments were developed primarily in office-based and computer-focused environments (cf. Sec. 3). University hospitals employ a highly diverse workforce, providing a cross-section of job profiles commonly found outside the medical sector.

Expert participants were recruited from five different facilities and service providers in the German medical domain. Two participants worked as Chief Information Security Officers (CISO), two as external consultants, trainers, and auditors, and two as managers in IT and ISO teams. Four experts identified as male and two as female, with job experience ranging from 1 to 20 years. Focus group participants were recruited via the hospital's internal newsletter, with open participation for all employees. The sample included medical staff (n = 6) and non-medical personnel (n = 7), such as patient management, engineering, and administration. Eight participants identified as male and five as female, with job experience ranging from 1 to 30 years.

The expert interviews explored human aspects of information security and awareness programs, including their implementation, goals, and challenges. Interviews were audio-recorded and lasted between 34 and 56 minutes. All recordings were transcribed and analyzed using thematic analysis. Further details are reported in our prior work [54].

Focus groups addressed information security policies, compliance challenges, and contextual enablers and barriers. Workshops were conducted on-site, lasted approximately two hours, and used moderation cards and affinity diagramming to structure discussions. Interviews and focus groups led to the identification of eleven thematic areas related to ISA (see Table 2), which subsequently informed item generation. The interview guidelines and focus group materials are available in the supplementary materials [50].

TABLE 2. THEMATIC AREAS OF ISA IN ORGANIZATIONS IDENTIFIED BY THE HAIS-Q AND OUR WORKSHOPS AND INTERVIEWS.

Topic		Source
Password Management Covers knowledge, attitudes, and behaviors around creating, sharing, and managing passwords securely.	*	[23]
Email Use Focuses on safely handling emails, including recognizing phishing, opening attachments, and link-clicking practices.	*	[23]
Internet Use Involves safe browsing, downloading files, accessing websites, and entering information online.	*	[23]
Social Media Use Addresses privacy settings, posting about work, and understanding consequences of online behavior.		[23]
Mobile Devices Concerns physical security of devices, secure communication over networks, and protecting sensitive information from shoulder surfing.		[23]
Information Handling Deals with secure disposal, handling of sensitive documents, use of removable media, and preventing information leakage.	*	[23]
Incident Reporting Focuses on recognizing, reporting, and responding to suspicious behaviors or security incidents.	*	[23]
Physical Security Encompasses locking rooms, cabinets, and workstations, and securing IT equipment.	*	
Device and System Security Covers securing computers, mobile devices, performing updates, and following security policies.	*	
Appropriate Use of IT Infrastructure Deals with acceptable use of company devices, networks, and personal devices at work (BYOD).	*	
Policy Awareness and Compliance Emphasizes awareness of organizational IT/security policies and participation in relevant training.	*	
Self-Induced Incident Reporting Focuses on recognizing and reporting accidental or self-caused security issues.	*	
Information Disclosure and Confidentiality Covers the protection of sensitive data, confidentiality obligations, and minimizing information leakage.	*	

Note: * indicates topics identified through our workshops and interviews; Reference indicates topics from HAIS-Q [23].

5.1.2. Item Generation and Content Validation. We generated items in two stages. First, we reviewed existing ISA measurement instruments (cf. Sec. 3) and identified the HAIS-Q [23] as the most comprehensive representation of organizational ISA within the KAB framework. The HAIS-Q has been developed and validated across multiple non-healthcare contexts (cf. Sec. 3). It covers seven core focus areas, five of which we also identified in our workshops and interviews (cf. Tab. 2). For the six additional themes identified in our workshops and interviews not covered by the HAIS-Q, we screened other ISA instruments to identify suitable candidate items. If no fitting item existed, we developed items directly from the qualitative data. This produced one to three items per theme and KAB dimension, yielding 39 new items (13 per dimension). We adapted all new items to match the HAIS-Q style and updated selected HAIS-Q items to reflect current best practices, particularly in password management, resulting in a pool of 102 items.

Candidate items were assessed for content validity by 11 experts in information security and privacy, comprising research associates and professors at our institution. For each item, we collected Likert-scale ratings on relevance and clarity, along with qualitative feedback, which informed subsequent item revision.

5.1.3. Item Translation. We translated the entire initial pool of 102 items into German using the TRAPD method [55]. TRAPD—"Translation," "Review," "Adjudication," "Pretesting," and "Documentation"—is a state-of-the-art approach for cross-cultural survey translation. It emphasizes collaborative translation by multiple professionals combined with systematic quality control to ensure conceptual and linguistic equivalence across languages. We hired two professional translators who independently produced parallel translations in accordance with the guidelines of the European Social Survey [56]. In the second step, a structured review and adjudication process was conducted by two subject matter experts with extensive experience in survey methodology and information security research to ensure cross-language equivalence and support measurement invariance analysis. This process included verifying content validity, discussing discrepancies with the translators, and resolving open questions to finalize the wording.

5.1.4. Survey Design and Participants. To develop the final set of items for the LISA scale and validate it, we administered an online survey to English- and German-speaking participants. The questionnaire was divided into three thematic sections and included 102 candidate items, along with 37 items from established scales commonly used in human-centered security research, the social sciences, and psychology, to support comprehensive validation analyses. All items are available in the supplementary materials [50].

The first section asked for participants' demographics to screen eligibility and assessed information security awareness in the workplace using the identified candidate items. The second section included established scales measuring constructs conceptually related to our own, following standard practice for assessing convergent validity. Specifically, we employed the 3-item Simple Information Security Awareness (SISA) scale [43] and the 16-item Security Behavior Intentions Scale (SeBIS) [57]. SISA has been applied in prior research on organizational information security awareness [43], whereas SeBIS is widely used in human-centered security research addressing individuals' security behavior in private contexts. The third section included additional constructs to assess nomological validity and potential response bias. Nomological validity refers to the extent to which a measure relates to other variables in a way that is consistent with theoretically predicted relationships. Specifically, general self-efficacy was measured using the ASKU (for German) and GSE-3 (for English) scales [58], [59], and personality traits were assessed with the BFI-10 [60], [61]. To control for socially desirable responding, the Social Desirability Scale (SDS-CM) was administered [62], [63].

All items were presented in randomized order within each block to minimize order effects. We employed attention checks throughout the survey to verify the response quality [64]. The survey concluded with a debriefing, during which participants confirmed the use of their data for the purpose of developing the survey instrument.

Participants for the validation study were recruited from the online panels Prolific (UK) and Bilendi (DACH region). Eligibility criteria required participants to be at least 18 years old, reside in either the UK or the DACH region (Germany, Austria, Switzerland), and have English as their primary language or German as their primary language. Participants were also required to work either full-time or part-time. A total of 1,202 participants completed the survey (UK: 581; DACH: 601 [Germany: 560, Austria: 29, German-speaking Switzerland: 12]). We excluded 20 participants who failed attention checks or displayed straightlining response patterns, as identified using the Intra-Individual Response Variability (IRV) index [65], [66]. The final sample comprised 1,182 participants (54.1% male, 46.9% female), with a mean age of 38.4 years (SD = 12.6; median = 36; range = 18–77). Employment status included 55.3% full-time workers.

5.1.5. Summary. A comprehensive, theory-driven item pool was developed by combining an established baseline instrument – HAIS-Q – with qualitative insights from expert interviews and focus groups in a heterogeneous organizational setting. This process expanded the thematic coverage of ISA beyond the HAIS-Q and resulted in 102 candidate items aligned with the KAB framework. Rigorous translation procedures and a carefully designed multilingual survey ensured conceptual equivalence and adequate data quality, providing a foundation for subsequent scale refinement and validation evaluation.

5.2. Phase II: Scale Refinement

5.2.1. Item Reduction and Model Fit. To reduce the number of items, we first conducted exploratory factor analysis

TABLE 3. ENGLISH ITEMS OF THE LISA SCALE WITH CORRESPONDING STANDARDIZED FACTOR LOADINGS. ITEMS ARE GROUPED INTO KNOWLEDGE (K), ATTITUDE (A), AND BEHAVIOR (B) SUBSCALES.

#	Item	λ
K1	When working on a sensitive document, I must ensure that strangers can't see the screen of my laptop or tablet. [25]	.773
K2	I am allowed to leave print-outs containing sensitive information on my desk when I step away from it. [25]	.709
K3	It's optional to report security incidents. [25]	.617
K4	Staff must partake in training and educational courses on information security on a regular basis. [new]	.777
K5	Staff must regularly keep themselves up to date on the organisation's information security regulations and policies. [new]	.834
K6	When discussing confidential information, it is necessary to ensure that unauthorised persons cannot overhear. [new]	.774
K7	The accidental disclosure of sensitive information to unauthorised persons must be reported. [new]	.765
A1	It's risky to access sensitive work files on portable devices such as laptop or tablet if strangers can see my screen. [25]	.784
A2	It's risky to leave print-outs that contain sensitive information on my desk unattended. [25]	.796
A3	It's risky to ignore security incidents, even if I think they´re not significant. [25]	.646
A4	It is useful for staff to take part in training and educational courses on information security on a regular basis. [new]	.841
A5	It is appropriate to keep myself up to date with the organisation's regulations and guidelines on information security on a regular basis. [new]	.795
A6	It is risky to discuss confidential information if unauthorised persons are able to overhear. [new]	.809
A7	It is important to report when sensitive information is accidentally disclosed to unauthorised persons. [new]	.839
B1	I check that strangers can't see the screen of my portable device, such as laptop or tablet, if I'm working on a sensitive document. [25]	.716
B2	I leave print-outs that contain sensitive information on my desk when I'm not there. [25]	.698
B3	If I notice a security incident, I would report it. [25]	.687
B4	I regularly attend courses or training on information security. [new]	.730
B5	I regularly keep myself informed about the regulations and guidelines on information security within my organisation. [new]	.809
B6	I sometimes discuss confidential information even though others may be listening. [new]	.647
B7	I will report if I accidentally disclose sensitive information to an unauthorised person. [new]	.752

Note. English entails $n = 581$. LISA was estimated using a three-factor Confirmatory Factor Analysis with the DWLS estimator. Loadings are standardized. Global fit measures: $\chi^2(186) = 801.79,\ p < .001$, CFI = .986, RMSEA (90% CI) = .076 [.070–.081], SRMR = .067. K = Knowledge, A = Attitude, B = Behavior. K1, A1, and B1 adjusted by adding "tablet" as an additional device. German items and loadings are available in the Appendix A.

on the 39 newly generated items. Using this analysis in combination with feedback from the 11 experts, we ultimately retained 18 of the 39 items. These were then combined with the 63 HAIS-Q items to form an initial pool of 81 items, which served as the basis for the development of LISA.

Next, we examined item-level skewness and kurtosis of the initial item pool to determine the appropriate estimator for the confirmatory factor analysis (CFA). Most items showed moderate non-normality, with skewness (Mean = –1.80; 1st–3rd Qu. = –2.21 to –1.40; Min/Max = –3.92 to –0.34) and kurtosis (Mean = 3.33; 1st–3rd Qu. = 1.39 to 4.64; Min/Max = –1.17 to 16.04). Only two items from the original HAIS-Q exceeded the liberal kurtosis threshold of 10, and three items exceeded the skewness threshold of 3. Comparing these values with recommended cutoffs (skewness ≤ 2, kurtosis ≤ 7; [67]) indicated that a DWLS estimator was appropriate for handling the ordinal nature of the data. Moreover, DWLS was preferred over WLSMV because it avoids overcorrection of the robust χ^2 statistic in moderately sized samples and complex models [68], [69].

Third, a CFA of the three-factor KAB structure (27 items per dimension) guided item selection based on the highest average standardized factor loadings across the knowledge, attitude, and behavior dimensions. The final LISA scale comprises 21 items (seven per dimension), representing those with the strongest loadings, resulting in a two-thirds reduction in length compared with the original HAIS-Q.

The item initially included in the first version of LISA, depicting the disposal of sensitive printouts (based on averaged factor loadings), was replaced to broaden content validity. It was substituted with item triplet 3, "Reporting of security incidents," which captures a more general and conceptually central aspect of security-related awareness.

Tab. 3 presents the final selection of items comprising the LISA scale, along with the corresponding global fit statistics. Although the model χ^2 (186) = 801.79 ($p < .001$) statistic is significant, it is widely recognized as overly sensitive to sample size and deviations from multivariate normality and therefore should not be treated as the primary indicator of model fit [70], [71]. More informative fit indices demonstrated that the model achieves an acceptable to reasonable fit, with CFI = 0.986, RMSEA (90 % CI) = 0.076 [0.070–0.081], and SRMR = 0.067 [72], [73]. The German version provided in the appendix A reports comparable global fit statistics. As expected, robust fit indices from WLSMV estimation for both samples (CFI = .802 - .817, RMSEA = .124 - .125) were poorer than those from the DWLS estimator.

Finally, a closer inspection of the subscales estimated as standalone CFAs showed acceptable model fit for the attitude dimension in both languages (CFI = 0.993–0.995, RMSEA = 0.077–0.091, SRMR = 0.041–0.047). In contrast, the knowledge and behavior dimensions demonstrated acceptable CFI (0.978-0.988) and SRMR (0.059-0.072) values, but showed insufficient RMSEA values—knowledge in the German sample (0.102) and behavior in both language versions (0.119–0.121). Overall, these results support that ISA is best represented as a three-factor KAB structure rather than as three independent unidimensional scales. Nevertheless, the attitude subscale emerges as the most internally

consistent and psychometrically stable component, and it can be used on its own when a brief, single-dimensional measure is needed.

5.2.2. Summary. Factor-analytic refinement reduced the initial item pool to a concise 21-item scale with a clear three-factor KAB structure. Item selection based on standardized loadings ensured strong representation of each dimension while substantially improving parsimony. Model fit indices indicate acceptable to good fit, supporting the structural validity of LISA. Results further show that ISA is best modeled as a multidimensional construct, with the attitude dimension emerging as the most stable standalone component.

5.3. Phase III: Scale Evaluation

5.3.1. Convergent Validity and Reliabilities. A measure is considered to demonstrate convergent validity when independent assessments of the same construct are strongly correlated [74]. Factor score correlations with SeBIS and SISA supported the construct's convergent validity (see Tab. 9 in the Appendix B). As expected, the behavioral dimension of LISA showed the strongest association with SeBIS (up to r = .57 in the DACH sample), consistent with SeBIS's focus on security-related behavioral intentions. Similarly, correlations with SISA were moderate to strong across all three dimensions (r = .50–.64), confirming that LISA aligns well with existing ISA instruments while maintaining its theoretical distinction among knowledge, attitude, and behavior components.

LISA demonstrated strong convergent validity with the HAIS-Q across both language samples (see Tab. 9 in the Appendix B). Because full statistical independence between the two instruments cannot be assumed due to partial item overlap, nine overlapping items (three per dimension) were removed from the HAIS-Q to avoid artificially inflated correlations [75]. As anticipated, factor correlations with the HAIS-Q dimensions were substantial, with each corresponding LISA subdimension—knowledge, attitude, and behavior—displaying the strongest associations with its respective HAIS-Q counterpart (r = .92–.93 in the UK sample; r = .86–.91 in the DACH sample). These correlations show that LISA captures the same underlying ISA construct as the HAIS-Q while being two-thirds shorter in item count.

McDonald's ω with polychoric correlation was used to assess reliability, given its robustness to τ-inequivalence [76]. The LISA demonstrated high internal consistency across all three subdimensions in both language samples. Values ranged from .87 to .92 in the UK sample and from .88 to .91 in the DACH sample.

5.3.2. Discriminant Validity. Discriminant validity refers to the extent to which a construct is empirically distinct from other theoretically different constructs [74]. Discriminant validity was evaluated using both the Fornell–Larcker criterion [77] and the Heterotrait–Monotrait (HTMT2) ratio [78], [79]. While the AVE–SV comparison did not meet the Fornell–Larcker threshold (DACH sample AVE = .52 – .61, SV = .61 – .65; UK sample AVE = .52 - .63, SV = .70 - .75), the HTMT values among the three LISA subdimensions across the two samples ranged from .65 to .81, remaining below the conservative cutoff of .85. These results support discriminant validity under the HTMT criterion, consistent with the theoretical expectation that knowledge, attitude, and behavior are interrelated yet empirically distinguishable components of the information security awareness construct.

5.3.3. Nomological Validity. Nomological validity refers to the degree to which a measure stays in an hypothesized association with theoretically related constructs [74]. Results support the nomological validity of LISA, showing that its subdimensions behave as theoretically expected in relation to stable personality traits and self-efficacy across two linguistic and cultural contexts. Regarding the Big Five, conscientiousness and agreeableness were expected to have a positive influence, neuroticism a negative one, and extraversion and openness no effect on ISA [80] . In addition, self-efficacy was expected to have a positive effect on ISA [38], [81], [82].

In the German sample, and based on composite mean scores, conscientiousness showed expected moderate positive correlations with all three LISA dimensions (r = .18–.36, $p < .001$), indicating that organized and disciplined individuals tend to report higher knowledge, attitudes, and behaviors related to information security. Agreeableness was expected to be positively correlated but showed no relationship. Neuroticism correlated negatively with the knowledge and behavior subdimensions (r = –.13 to –.27, $p < .05$), suggesting that emotionally unstable individuals exhibit lower awareness. Openness and extraversion were, as expected, largely unrelated to LISA, except for a small positive correlation between extraversion and the behavioral dimension (r = .13, $p < .05$). Self-efficacy was positively associated with all LISA subdimensions (r = .16–.23, $p < .01$), consistent with the assumption that individuals confident in their ability to act effectively also engage more in secure behaviors.

The UK sample replicated the overall pattern of associations, though with slightly weaker and partly insignificant effect sizes. Conscientiousness showed positive correlations with the attitude and behavior dimensions of LISA (r = .14–.29, $p < .05$). Agreeableness was positively related to behavior (r = .18, $p < .001$), whereas neuroticism was negatively associated with LISA behavior (r = –.23, $p < .001$). Extraversion and openness remained unrelated, while self-efficacy showed a positive correlation with the behavioral dimension (r = .17, $p < .05$).

5.3.4. Socially desirable response bias. Socially desirable responding is a response bias in which individuals provide answers they believe are socially acceptable or favorable rather than truthful [83]. Assessing the extent to which a scale is susceptible to this bias is essential to prevent distorted results and avoid spurious effects. Overall, participants' responses to LISA measures appear to reflect genuine self-assessment. Social desirability assessed through was

modestly associated with self-reported behavior, particularly for the UK and DACH samples (LISA: $r = .28 - .30$, $p < .001$). In contrast, knowledge and attitude dimensions showed non-significant correlations across languages. Prior findings with the HAIS-Q also reported only a handful of items exceeding $r = .25$ with social desirability, primarily related to incident reporting [25]. These results support the assumption that most items elicit authentic responses, while the behavior scales may be more sensitive to small social desirability bias.

5.3.5. Measurement Invariance. Measurement invariance testing across English and German samples (see Table 10 in Appendix C) demonstrated acceptable model stability for LISA asses through a three-factor CFA. We tested configural, threshold, metric (thresholds and loadings constrained), and scalar invariance (thresholds, loadings, and intercepts constrained) using a stepwise approach [84]. Across all models with DWLS estimation, changes in fit indices remained within the recommended thresholds (ΔCFI $\geq$ –0.01, ΔRMSEA $\leq$ 0.015 [85]), supporting scalar invariance. Establishing scalar invariance enables researchers to meaningfully compare group means on the latent factors [86] across languages, thereby laying the foundation for cross-cultural research and application in multinational organizations.

5.3.6. Second-Order Factor Model. ISA is conceptualized in prior research as a multidimensional construct comprising knowledge, attitude, and behavior [23], [25]. These facets jointly represent the overarching latent construct of information security awareness. This theoretical characterization provides a direct rationale for operationalizing ISA using a hierarchical model in which a second-order factor captures the shared variance among the three first-order dimensions.

The first-order CFA with knowledge, attitude, and behavior as correlated latent variables demonstrated acceptable global model fit (see Tab. 3 and Tab. 8). Following established guidance [31], the next step is to examine the magnitude of the correlations among the first-order factors. As shown in Tab. 9, the dimensions are strongly and significantly interrelated (UK: .83–.86; DACH: .75–.81), indicating substantial shared variance consistent with a higher-order structure.

Estimating the second-order model (see Fig. 1) confirms this interpretation. The standardized loadings of the second-order ISA factor on the first-order dimensions are high (UK: .90–.92; DACH: .86–.91), explaining between 73% and 86% of the variance in the first-order constructs. This pattern indicates that a single higher-order factor effectively accounts for the associations among knowledge, attitude, and behavior.

Because a hierarchical model is a reparameterization of the correlated-factor model, its overall fit cannot exceed that of the freely correlated first-order solution [31]. The justification for the second-order specification therefore rests not on improvements in global fit but on theoretical coherence and empirical evidence that the three dimensions function as manifestations of a single, more general ISA construct.

5.3.7. Summary. LISA demonstrates strong psychometric robustness across multiple validation criteria. Convergent validity is supported by substantial correlations with established ISA measures, while high internal consistency confirms reliability across all dimensions. Discriminant validity indicates that knowledge, attitude, and behavior are empirically distinct yet related components. Nomological validity aligns with theoretical expectations, and social desirability effects are limited. Measurement invariance across languages enables meaningful cross-cultural comparisons, and the second-order model confirms that the three dimensions reflect a coherent overarching ISA construct.

6. Study II: Ecological Validation of LISA in a Time-Critical, Heterogeneous Organization

In Study II, we evaluated the LISA scale in a large university hospital in Germany to assess its performance under real-world, time-critical, and highly heterogeneous working conditions. This setting enabled us to examine the scale's functioning beyond controlled survey environments and to conduct key validation steps within an operational organization. Specifically, we assessed factorial validity and reliability, tested known-groups differentiation, evaluated criterion-related validity, and compared factor scores with simple sum scores.

6.1. Procedure and Participants

6.1.1. Survey Design and Implementation. We administered an online survey consisting of three sections. A copy of the survey instrument is available in the supplementary materials [50]. The first section presented the 21-item LISA scale. The second section assessed organizational antecedents of ISA, selected based on systematic reviews of research on information security policy (ISP) compliance [8], [9], [87], [88], [89], [90] and refined through expert interviews, focus groups, and consultations with the hospital's CISO team. From this process, we identified 11 factors that balance comprehensiveness with survey length: two individual-level enablers (self-efficacy for policy compliance and general IT knowledge), four organizational-level enablers (management commitment, policy availability and accessibility, active support and training, and sanctions for misconduct), and five organizational-level barriers (organizational laxness, policy-related work impediments, frequency of technical problems, workload and time pressure, and shadow work processes). The final section collected participants' demographic information.

Items for the 11 enablers and barriers were operationalized as multi-item scales drawn or adapted from established instruments measuring constructs such as self-efficacy and IT literacy [7], [91], top management commitment and policy access [92], [93], [94], [95], laxness and shadow work [96], workload and error frequency [97], and sanctions [7]. All items were carefully translated and back-translated between German and English and were measured

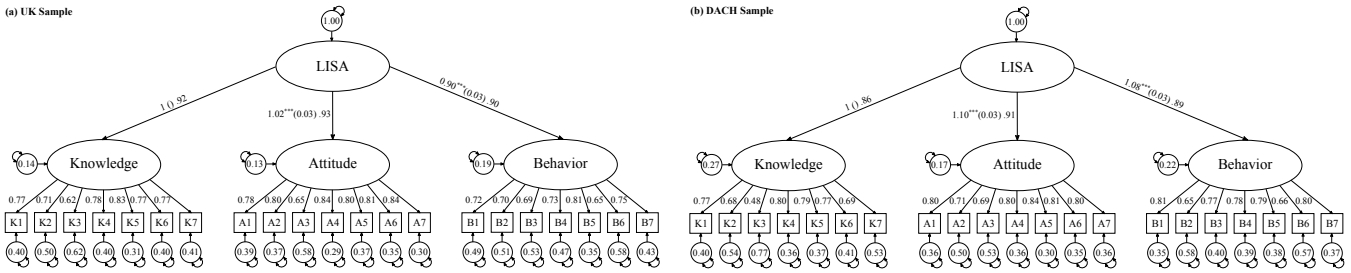

Figure 1. Second-order factor model of LISA for the (a) UK and (b) DACH sample, with the higher-order construct explained by the latent subdimensions of knowledge, attitude, and behavior. The sequence of results in regression paths: unstandardized estimates, standard errors in round brackets, and standardized estimates. Factor loadings are standardized. Values in circles with curved arrows denote error variances. Because the knowledge factor loading on the second-order LISA construct was designated as the marker (reference) indicator, its unstandardized loading was fixed at 1.0. As a consequence of this identification constraint, no standard error or significance test is reported for this parameter.

TABLE 4. DISTRIBUTION OF RESPONDENTS BY STAFF GROUP.

Staff Group	Count	Share (%)
Admin & IT	**197**	**34.0**
Administration	157	27.1
IT	40	6.9
Clinical Staff	**268**	**46.3**
Medical Services	55	9.5
Nursing & Functional Services	98	16.9
Medical Technical Services	115	19.9
Other Staff	**114**	**19.7**
Research	66	11.4
Other	37	6.4
NA	11	1.9
Total	**579**	**100.0**

on 7-point Likert scales ranging from "1 Strongly Disagree" to "7 Strongly Agree", with reversed items included to mitigate response bias.

6.1.2. Participants and Recruitment. Participants were recruited via email invitations sent to all employees of a large university hospital in Germany, distinct from the hospital involved in Study I, which employs approximately 10,000 staff. A total of 579 employees participated. Of these, 46.3% (n = 268) were healthcare-related staff, including personnel from medical services, nursing and functional services, and medical-technical services. The remaining 51.8% (n = 300) were non-healthcare staff, comprising researchers, administrative and IT personnel, and employees in supply, technical, pastoral, child care, and other auxiliary services (cf. Table 4). Among participants, 59% identified as female, 27% as male, and 14% did not report their gender. The median age group was 40–49 years, with 12.1% not reporting age.

6.2. Results

6.2.1. Factorial Validity and Reliabilities. First, we examined item-level skewness and kurtosis to determine an appropriate estimator. Most items showed moderate non-normality, with skewness (Mean = –1.99; 1st–3rd Qu. = –2.28 to –1.47; Min/Max = –4.68 to –0.46) and kurtosis (Mean = 3.90; 1st–3rd Qu. = 1.70 to 5.33; Min/Max = –0.78 to 25.16), indicating mild to occasionally pronounced skew and heavy tails. Only the German item 'Knowledge 6' exceeded liberal thresholds (skewness = –4.68, kurtosis = 25.16), suggesting a ceiling effect that may warrant reevaluation in future studies. As the majority of items remained within acceptable distributional limits [67], and given that a robust estimator in WLSMV can over-correct the χ^2 statistic in moderately sized, complex ordinal models [68], [69], the DWLS estimator was selected.

Overall, LISA demonstrated satisfactory factorial validity, with standardized factor loadings ranging from .461 to .841. Average loadings were .633 for knowledge, .769 for attitude, and .666 for behavior, indicating stable representation across dimensions. Global model fit was acceptable (χ^2 (186) = 1002.79 with $p < .001$, CFI = .965, RMSEA = .087 [90% CI: .078 – .092], SRMR = .087). As expected, robust fit indices from WLSMV estimation (CFI = .728, RMSEA = .139) were poorer than those from the DWLS estimator.

Inspecting the subdimensions as standalone CFA models largely replicated the pattern observed in Validation Study I. The knowledge subscale showed good global fit (CFI = 0.994, RMSEA = 0.031, SRMR = 0.047), and the attitude subscale demonstrated acceptable fit (CFI = 0.987, RMSEA = 0.095, SRMR = 0.062). In contrast, the behavior subscale showed insufficient model fit when estimated in isolation, with notably elevated RMSEA values (CFI = 0.933, RMSEA = 0.178, SRMR = 0.113).

McDonald's ω, computed using polychoric correlations, indicated good reliability for all LISA dimensions, with ω = .82 for knowledge, ω = .90 for attitude, and ω = .82 for behavior.

6.2.2. Comparison of Factor Scores and Sum Scores. To obtain methodologically sound estimates of latent constructs, psychometric instruments such as LISA are typically analyzed using Structural Equation Modeling (SEM). SEM specifies a measurement model that explicitly accounts for measurement error and estimates relationships between observed indicators and latent variables [53].

Latent variables (η) are not directly observed. If researchers or practitioners wish to obtain individual-level

scores, these can be derived post hoc via factor score prediction. In this study, we applied a regression-based method to compute factor scores ($\hat{\eta}$) using the `lavPredict()` function from the `lavaan` [98] package. Under this approach, factor scores correspond to model-based predictions of the latent variables given the observed responses. These predictions can be expressed as linear combinations of the observed indicators,

$$\hat{\eta} = \mathbf{W}^\top \mathbf{x},$$

where $\mathbf{x}$ denotes the vector of observed item responses and $\mathbf{W}$ is a weight matrix implied by the fitted SEM. Importantly, $\mathbf{W}$ is derived from the full model-implied covariance structure, including factor loadings, measurement error variances, and latent variable covariances. Consequently, factor score estimates represent model-based optimal linear predictions of the latent variables rather than simple loadings-based composites.

In applied research, SEM may not always be feasible due to methodological complexity or sample size requirements. Moreover, when absolute and easily interpretable score values are required for practical or reporting purposes, researchers often rely on unweighted *sum* or *mean* scores as pragmatic alternatives, which aggregate observed item responses within each factor:

$$\text{Sum score: } S_j = \sum_{i=1}^{k_j} x_{ij}, \quad \text{Mean score: } \bar{S}_j = \frac{1}{k_j} \sum_{i=1}^{k_j} x_{ij}.$$

These scores assume equal item weighting and do not explicitly account for measurement error. However, they can approximate latent constructs reasonably well when factor loadings are relatively homogeneous [99].

To assess the extent to which sum scores approximate SEM-based factor scores, we examined the correspondence between both approaches. Table 5 reports Pearson correlations between regression-based factor scores ($\hat{\eta}_j$) obtained via SEM and the corresponding sum scores (S_j), alongside Cronbach's α reliability estimates for each subscale across the three participant samples, including the hospital staff surveyed in this study.

Across all samples, correlations between factor scores and sum scores were consistently high (r = .828–.959), indicating that the unweighted sum scores closely approximate the latent constructs measured by LISA. Reliability was also acceptable to high, with Cronbach's α ranging from .65 (LISA-K, DE-Hospital) to .90 (full LISA, EN-Prolific), demonstrating that the sum scores maintain internal consistency comparable to SEM-based scores. Notably, the hospital sample showed slightly lower reliability for the knowledge subscale, likely reflecting greater heterogeneity in staff roles and backgrounds. These results suggest that, in practice, the sum or mean scores of LISA provide a valid and reliable approximation of the latent factors.

TABLE 5. CORRELATION COEFFICIENTS BETWEEN LISA FACTOR SCORES AND SUM SCORES AND CRONBACH'S α RELIABILITY SCORES FOR THE THREE PARTICIPANT SAMPLES IN THIS STUDY.

(Sub-)Scale	EN-Prolilfic		DE-Bilendi		DE-Hospital	
	r	α	r	α	r	α
LISA	.951***	.90	.959***	.90	.932***	.87
LISA-K	.890***	.79	.906***	.80	.828***	.65
LISA-A	.898***	.81	.918***	.83	.883***	.81
LISA-B	.945***	.79	.957***	.82	.939***	.74

Note. r: Pearson correlations; α: Cronbach's α for items included in the unweighted sum scale. $n = 579$; ***$p \leq .001$, **$p \leq .01$, *$p \leq .05$.

6.2.3. Differentiation by Known-Groups. Known-groups validity evaluates whether a measure can distinguish between groups expected to differ on the underlying construct. Evidence for this form of validity is typically demonstrated when mean scores vary significantly between groups that theoretically should show higher or lower levels of the measured trait [74]. Based on prior work, especially clinical staff should show lower ISA scores compared to administration and IT roles [9].

The results of multiple regression analyses, using staff group as a predictor, are presented in Table 6. Both SEM-based factor scores and unweighted sum scores were examined. Across the models, clinical staff consistently showed significantly lower LISA scores compared to the reference group (administration and IT), with standardized regression coefficients ranging from -0.19 to -0.29 for factor scores and -0.22 to -0.41 for sum scores. Other staff members without direct clinical duties also showed lower scores, though the effects were generally smaller in magnitude.

6.2.4. Criterion-related Validity. Criterion-related validity of the LISA scale was assessed by examining correlations between LISA scores and the 11 individual- and organizational-level factors hypothesized to influence ISA. Strong associations with these criterion variables support that LISA captures constructs that are both theoretically grounded and practically relevant. We specifically evaluated concurrent validity, which is demonstrated when a measure correlates substantially with established criteria assessed at the same time [74].

Construct validity of the 11 factors was assessed using a CFA measurement model estimated with DWLS. We inspected standardized factor loadings and calculated the Average Variance Extracted (AVE) for each construct to confirm convergent validity. We confirmed internal consistency reliability using McDonald's ω based on polychoric correlations. The results indicated that all constructs exhibited satisfactory internal consistency (see Tab. 7), and the pattern of factor loadings supported the hypothesized structure, providing evidence that the items adequately represent the intended latent variables.

As reported in Table 7, LISA scores show robust correlations with the 11 individual- and organizational-level antecedents of information security compliance. At the individual level, self-efficacy correlates positively with all LISA dimensions (r = .342–.622, $p < .001$), whereas general IT

TABLE 6. STAFF GROUP DIFFERENCES IN LISA AND ITS SUBDIMENSIONS.

	Factor scores				Sum scores			
	LISA	**LISA-K**	**LISA-A**	**LISA-B**	**LISA**	**LISA-K**	**LISA-A**	**LISA-B**
Intercept (Ref: Admin & IT)	0.11^{*}	0.10^{*}	0.12^{*}	0.17^{*}	0.22^{***}	0.12	0.13	0.26^{***}
	(0.04)	(0.04)	(0.05)	(0.05)	(0.03)	(0.07)	(0.03)	(0.05)
Clinical Staff	-0.20^{***}	-0.19^{**}	-0.23^{***}	-0.29^{***}	-0.35^{***}	-0.22^{*}	-0.23^{*}	-0.41^{***}
	(0.05)	(0.06)	(0.06)	(0.06)	(0.09)	(0.09	(0.09)	(0.09)
Other Staff	-0.19^{**}	-0.19^{*}	-0.22^{**}	-0.27^{***}	-0.27^{*}	-0.12	-0.14	-0.36^{**}
	(0.07)	(0.08	(0.08)	(0.08)	(0.11)	(0.12)	(0.12)	(0.12)
R^2	0.02	0.02	0.02	0.04	0.03	0.01	0.01	0.04
Adjusted R^2	0.02	0.02	0.02	0.04	0.02	0.01	0.01	0.03
F	7.15^{***}	5.6^{**}	7.14^{***}	12.03^{***}	7.34^{***}	2.71	2.92	10.55^{***}

Note. Values represent standardized regression coefficients with standard errors in parentheses. Results were obtained from multiple regressions with $n = 579$; $^{***}p \leq .001$, $^{**}p \leq .01$, $^{*}p \leq .05$.

knowledge shows negligible associations. This lack of correlation does not undermine scale validity, as LISA captures broader, multi-determined constructs that may not align with single predictors. Alternatively, general IT knowledge may not directly translate into ISA-related knowledge, attitudes, or behaviors among employees in this organization.

At the organizational level, enablers such as management commitment, policy availability, active support, training, and sanctions for misconduct show moderate to strong positive correlations ($r = .291$–$.705$, $p < .001$). Barriers, including organizational laxness, perceived work impediments, and shadow work processes, show negative associations with LISA scores ($r = -.199$–$-.621$, $p < .05$), whereas technical problems and workload exhibit weaker or inconsistent correlations.

Overall, these patterns provide evidence of criterion-related (concurrent) validity, indicating that LISA reflects both individual and organizational factors relevant for information security awareness.

6.2.5. Response Time for LISA. LISA demonstrated a short completion time. Of the 579 participants, we evaluated completion duration based on 477 responses, as extreme outliers would distort the results. These outliers likely resulted from hospital staff opening the questionnaire and completing it at a later time. Therefore, only responses within the interquartile range (IQR) after outlier removal were included in the analysis (see [66]). The average completion time for the 21-item scale was M = 2.76 minutes (SD = 0.82). When broken down by subdimensions, the mean response times were 1.11 minutes for knowledge (SD = 0.40), 0.84 minutes for attitude (SD = 0.29), and 0.82 minutes for behavior (SD = 0.27), suggesting a potential learning or response time effect as participants progressed through the scale. Overall, the ability to validly and reliably assess information security awareness in approximately one minute per subdimension highlights LISA's balance between brevity and psychometric validity, which is an important advantage for applied research and organizational practice, underscoring its suitability for large-scale assessments and use in time-critical organizational settings.

7. Discussion

The present research introduced LISA as a concise, psychometrically valid instrument for assessing ISA across heterogeneous organizational contexts. Evidence for convergent, discriminant, ecological, and known-group validity, together with high internal consistency, measurement invariance across languages, its calculation as composite sum or mean score supports LISA as theoretically and statistically solid and practically applicable. Its brief administration time, approximately three minutes in total, demonstrates that ISA measurement can be achieved with minimal respondent burden, making the scale particularly suitable for large-scale surveys in time-critical settings.

Its criterion-related validity, known-group differences, and the similarity of summed scores and factor scores highlight LISA's practical utility. Positive associations with organizational enablers (e.g., management commitment, policy availability) and negative associations with barriers (e.g., work impediments, shadow work, technological constraints) show that the instrument is sensitive to key antecedents of security-related behavior. Administrative and IT staff also scored higher across all LISA dimensions, especially behavioral, whereas clinical and other staff scored lower. This aligns with findings from HAIS-Q, SISA, and related measures [43], [100], [101], which consistently show stronger awareness among non-clinical staff. This gap likely reflects the realities of clinical work, where time pressure and frequent interruptions often take precedence over security procedures [102].

Although LISA covers a narrower content range than comprehensive instruments such as the HAIS-Q, it targets highly relevant aspects of information security that go beyond technical or cybersecurity issues. Comparable instruments—such as CS-S [35], SeBIS [36], MISAS [40], and shorter measures like CSEC [42], the Resource Misuse and Security Carelessness Scales [34], SA-6 [38], or SISA [43]—primarily assess personal end-user or technical behavior, and many are not designed for organizational contexts. LISA, by contrast, captures core workplace practices—protecting sensitive information, following training and policy requirements, and reporting incidents—which

TABLE 7. CORRELATION COEFFICIENTS BETWEEN LISA FACTOR SCORES AND SUM SCORES WITH COMMONLY IDENTIFIED OR RESEARCHED ENABLERS AND BARRIERS TO INFORMATION SECURITY COMPLIANCE IN ORGANIZATIONAL RESEARCH.

			Factor scores				Sum scores			
	ω	AVE	**LISA**	**LISA-K**	**LISA-A**	**LISA-B**	**LISA**	**LISA-K**	**LISA-A**	**LISA-B**
Individual-Level Enablers										
Self-efficacy toward security policy compliance	.92	.80	$.622^{***}$	$.569^{***}$	$.546^{***}$	$.615^{***}$	$.486^{***}$	$.342^{***}$	$.343^{***}$	$.510^{***}$
IT knowledge & computer literacy	.87	.63	.008	.050	−.010	.004	−.002	.000	.000	.000
Organizational-Level Enablers										
Top management commitment ISP compliance	.88	.71	$.629^{***}$	$.574^{***}$	$.561^{***}$	$.616^{***}$	$.497^{***}$	$.346^{***}$	$.388^{***}$	$.498^{***}$
ISP availability and accessibility	.85	.67	$.700^{***}$	$.635^{***}$	$.622^{***}$	$.690^{***}$	$.552^{***}$	$.374^{***}$	$.421^{***}$	$.569^{***}$
Active support and training for ISP compliance	.87	.73	$.705^{***}$	$.647^{***}$	$.630^{***}$	$.694^{***}$	$.561^{***}$	$.392^{***}$	$.438^{***}$	$.562^{***}$
Sanctions for ISP misconduct	.84	.64	$.508^{***}$	$.455^{***}$	$.471^{***}$	$.497^{***}$	$.410^{***}$	$.291^{***}$	$.341^{***}$	$.392^{***}$
Organizational-Level Barriers										
Organizational laxness with ISP compliance	.79	.56	$-.621^{***}$	$-.549^{***}$	$-.576^{***}$	$-.609^{***}$	$-.505^{***}$	$-.317^{***}$	$-.421^{***}$	$-.512^{***}$
ISP being a work impediment	.89	.74	$-.416^{***}$	$-.356^{***}$	$-.399^{***}$	$-.406^{***}$	$-.345^{***}$	$-.199^{*}$	$-.308^{***}$	$-.347^{***}$
Overall experience of technical problems	.86	.62	$-.176^{**}$	$-.134^{*}$	$-.156^{**}$	$-.178^{**}$	$-.133^{*}$	.000	.000	$-.166^{**}$
Overall workload and time pressure	.83	.56	.034	.044	.032	.032	.020	.000	.000	.000
Overall presence of shadow working processes	.90	.76	$-.477^{***}$	$-.413^{***}$	$-.447^{***}$	$-.468^{***}$	$-.392^{***}$	$-.237^{**}$	$-.324^{***}$	$-.406^{***}$

Note. Regression values represent Pearson correlation coefficients. All variables represent self-reported data by $n = 579$ hospital staff; $^{***}p \leq .001$, $^{**}p \leq .01$, $^{*}p \leq .05$. ω indicates internal consistency of each scale, with values ≥ 0.70 considered acceptable [53]. AVE (Average Variance Extracted) reflects the proportion of variance in items explained by the latent construct, with values ≥ 0.50 considered adequate for convergent validity [53].

explained substantial variance in both first- and second-order ISA factors without compromising psychometric quality and remained grounded in the knowledge–attitude–behavior framework.

Moreover, LISA is designed to measure the latent dimension of ISA as a brief screener, particularly well suited for heterogeneous organizations where information security challenges extend beyond technical system use. Although it does not aim to assess all specific facets of ISA, low LISA scores reliably signal gaps in general information security awareness, as reflected in its strong correlations with the more comprehensive HAIS-Q. Such results can serve as an early indicator that more detailed or domain-specific assessment is warranted. Importantly, high LISA scores should not be interpreted as a guarantee of secure behavior but rather as an indicator of generally sound awareness.

LISA is the first psychometric ISA instrument to demonstrate scalar measurement invariance across English and German, confirming its suitability for cross-lingual use. Although measurement invariance is a core methodological standard [86], it is still often overlooked, even though language differences are a major source of non-equivalence in comparative research [103], [104]. Without testing invariance, observed cultural differences may simply reflect translation artifacts rather than true psychological variation [103], underscoring the need for rigorous translation procedures such as the TRAPD framework [55]. No existing ISA measure meets these standards, positioning LISA as a methodological benchmark for future ISA scale development.

These results indicate that the three KAB dimensions perform best as a combined three-factor structure. Only the attitude subscale demonstrated solid psychometric stability across languages and studies to be used as a standalone measure. In contrast, the behavior subscale should not be used independently, as its psychometric quality is likely influenced by contextual and organizational constraints. Further refinement is needed before it can function as a robust standalone scale.

Also, LISA is equally suitable for use in homogeneous organizational settings. Its concise structure enables efficient monitoring of overall ISA levels without imposing unnecessary respondent burden, allowing organizations—whether complex or uniform in structure—to track awareness reliably and at regular intervals.

Taking everything into account, LISA advances existing research by providing a theory grounded, psychometrically validated, and concise instrument that resolves key trade offs in prior ISA measurement. It combines full knowledge, attitude, and behavior coverage with minimal response burden, enabling reliable assessment within minutes across heterogeneous organizational contexts, including roles with limited interaction with digital systems. Supported by cross language measurement invariance between German and English and strong performance in real world settings, LISA functions as a domain general screening instrument for information security awareness. By jointly addressing brevity, validity, and multilingual applicability, it contributes a practical and methodologically robust tool for both research and organizational diagnostics.

8. Limitations

A central limitation of this work concerns the choice of estimators for model fitting. We used diagonally weighted least squares (DWLS) because item distributions met acceptable thresholds, with only a few showing pronounced nonnormality. Although the weighted least squares estimator with mean and variance adjustment (WLSMV) is typically considered more conservative, it produced markedly poorer

fit indices in both studies. Prior research indicates that WLSMV can overcorrect the robust chi square statistic in models with moderate sample sizes and higher complexity [68], [69], whereas DWLS reduces this risk. Still, the discrepancy between estimators suggests that the generalizability of our results should be interpreted with caution, and future research with larger samples may reassess the estimator choice.

The results of Validation Study I are based on access panel data, which, while cost efficient, are prone to selection bias, unverifiable participant identities, and undetected multiple participation [105], [106]. Nevertheless, such panels are suitable for initial instrument validation, especially since no representative inferences were drawn and the findings are interpreted with appropriate caution. Importantly, LISA's ecological validity and reliability were confirmed in a second real world sample, reinforcing the robustness of the initial validation.

In addition, both studies relied on self-administered online surveys, limiting control over the survey environment and completion conditions [105]. Participation in the hospital sample was voluntary, so the results may not be fully representative. The study also relies on self-reported rather than observed behavior, which may diverge from actual practices and thus only approximate participants' real actions.

To date, LISA is available only in English and German, and only the German version has been tested in a heterogeneous, time-critical organizational environment. Nevertheless, because the English version performed similarly to the German one and demonstrated measurement invariance in the initial validation study, we expect comparable performance in practice. Moreover, the translation and validation procedure documented in this paper provides a clear guideline for extending LISA to additional languages in the future.

Finally, we tested the German version of LISA in a single hospital, which limits generalizability. However, the hospital included a broad range of professional roles and work activities, offering a diverse setting for examining information security awareness. Still, future studies should evaluate LISA in additional organizational contexts to further establish its robustness.

9. Conclusions

Human factors play a critical role in organizational information security, yet existing measures of Information Security Awareness (ISA) often lack theoretical grounding, psychometric rigor, and practical usability. This paper presents the Lightweight Information Security Awareness (LISA) scale—the first theory-based, psychometrically validated, cross-language tool designed to efficiently assess ISA in diverse organizational settings. Validated with 1,182 panel participants and 579 employees of a German university hospital, LISA shows strong internal consistency, English–German measurement invariance, and robust construct and ecological validity. By correlating LISA with 11 organizational enablers and barriers and demonstrating its applicability across a heterogeneous workforce, the study shows that LISA enables both scientific research and practical assessments, offering a reliable, concise, and accessible solution for measuring ISA.

Acknowledgements

We sincerely thank all participants and the participating hospitals for their time, openness, and commitment. We are grateful for the substantial support provided by the hospitals' (C)ISO teams throughout the project. We thank the translators for their engagement in the iterative translation process, as well as the former and current members of the Data and Application Security Group who assisted with screening the candidate items. We thank Christoph Frohn for his advice and feedback on the statistical analysis. We further thank the reviewers for their thoughtful and constructive feedback, which helped to improve this paper. We also acknowledge the support of German taxpayers in enabling publicly funded research. This research was supported by the German Federal Ministry of Health under grant number ZMI1-2521FSB801.

References

[1] M. T. Siponen, "Five dimensions of information security awareness," *ACM SIGCAS Computers and Society*, vol. 31, no. 2, pp. 24–29, 2001.

[2] L. Jaeger, "Information Security Awareness: Literature Review and Integrative Framework," in *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)*, 2018, pp. 4703–4712.

[3] A. Tsohou, K. , Maria, K. , Spyros, , and E. Kiountouzis, "Managing the introduction of information security awareness programmes in organisations," *European Journal of Information Systems*, vol. 24, no. 1, pp. 38–58, 2015.

[4] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014.

[5] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 2014, pp. 248–252.

[6] European Parliament & Council of the European Union, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)," 2022.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010.

[8] W. A. Cram, J. D'Arcy, and J. G. Proudfoot, "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly*, vol. 43, no. 2, pp. 525–554, 2019.

[9] P. K. Sari, P. W. Handayani, A. N. Hidayanto, S. Yazid, and R. F. Aji, "Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors," *Healthcare*, vol. 10, no. 12, p. 2531, 2022.

[10] H. Kruger and W. Kearney, "A prototype for assessing information security awareness," *Computers & Security*, vol. 25, no. 4, pp. 289–296, 2006.

[11] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology - Behaviour & IT*, vol. 33, pp. 1–12, 2012.

[12] E. H. Schein, *Organizational culture and leadership*, 3rd ed. Jossey-Bass, 2004.

[13] T. Schlienger and S. Teufel, "Information Security Culture," in *Security in the Information Society*, M. A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan, Eds., 2017, vol. 86, pp. 191–201.

[14] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Computers & Security*, vol. 29, no. 4, pp. 476–486, 2010.

[15] E. P. Bettinghaus, "Health promotion and the knowledge-attitude-behavior continuum," *Preventive Medicine*, vol. 15, no. 5, pp. 475–491, 1986.

[16] T. E. Miller, C. D. Booraem, J. V. Flowers, and A. E. Iversen, "Changes in knowledge, attitudes, and behavior as a result of a community-based AIDS prevention program," *AIDS Education and Prevention*, vol. 2, no. 1, pp. 12–23, 1990.

[17] Q. Yi and N. Hohashi, "Comparison of perceptions of domestic elder abuse among healthcare workers based on the Knowledge-Attitude-Behavior (KAB) model," *PLOS ONE*, vol. 13, no. 11, p. e0206640, 2018.

[18] F. Bogner, "The Influence of Short-Term Outdoor Ecology Education on Long-Term Variables of Environmental Perspective," *The Journal of Environmental Education*, vol. 29, pp. 17–29, 1998.

[19] A. Kollmuss and J. Agyeman, "Mind the Gap: Why do people act environmentally and what are the barriers to pro-environmental behavior?" *Environmental Education Research*, vol. 8, no. 3, pp. 239–260, 2002.

[20] T. Kizildeniz and F. Bozkurt, "Evaluating Climate Change Knowledge, Attitudes, and Behaviors (KAB) in Agricultural Sciences and Technologies Education," *Karadeniz Fen Bilimleri Dergisi*, vol. 14, pp. 619–633, 2024.

[21] S. van der Linden, "Towards a new model for communicating climate change," *Understanding and governing sustainable tourism mobility: Psychological and behavioural approaches*, pp. 243–275, 2014.

[22] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2013, pp. 286–290.

[23] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165–176, 2014.

[24] P. Schrader and K. Lawless, "The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments," *Performance Improvement*, vol. 43, pp. 8–15, 2004.

[25] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Computers & Security*, vol. 66, pp. 40–51, 2017.

[26] I. Ajzen, *Attitudes, personality, and behavior*, 2nd ed. Open University Press, 2005.

[27] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, p. e14234, 2023.

[28] J. D. Wasserman and B. A. Bracken, "Fundamental Psychometric Considerations in Assessment," in *Handbook of Psychology, Second Edition*, 2012, ch. 3.

[29] G. O. Boateng, T. B. Neilands, E. A. Frongillo, H. R. Melgar-Quiñonez, and S. L. Young, "Best Practices for Developing and Validating Scales for Health, Social, and Behavioral Research: A Primer," *Frontiers in Public Health*, vol. 6, 2018.

[30] M. W. Watkins, "Exploratory Factor Analysis: A Guide to Best Practice," *Journal of Black Psychology*, vol. 44, no. 3, pp. 219–246, 2018.

[31] T. A. Brown, *Confirmatory factor analysis for applied research*, 2nd ed. The Guilford Press, 2015.

[32] K. Swan, R. Speyer, M. Scharitzer, D. Farneti, T. Brown, V. Woisard, and R. Cordier, "Measuring what matters in healthcare: a practical guide to psychometric principles and instrument development," *Frontiers in Psychology*, vol. 14, p. 1225850, 2023.

[33] H. K. Mohajan, "Two criteria for good measurements in research: Validity and reliability," *Annals of Spiru Haret University. Economic Series*, vol. 17, no. 4, pp. 59–82, 2017.

[34] A. M. Chu and P. Y. Chau, "Development and validation of instruments of information security deviant behavior," *Decision Support Systems*, vol. 66, pp. 93–101, 2014.

[35] I. Arpaci and K. Sevinc, "Development of the cybersecurity scale (CS-S): Evidence of validity and reliability," *Information Development*, vol. 38, no. 2, pp. 218–226, 2022.

[36] S. Egelman, M. Harbach, and E. Peer, "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*, 2016, pp. 5257–5261.

[37] Y. Sawaya, S. Lu, T. Isohara, and M. Sharif, "A High Coverage Cybersecurity Scale Predictive of User Behavior," in *Proceedings of the 33rd USENIX Security Symposium (USENIX 24)*, 2024, pp. 5503–5520.

[38] C. Faklaris, L. Dabbish, and J. I. Hong, "A Self-Report Measure of End-User Security Attitudes (SA-6)," *Proceedings of the Fifteenth Symposium on Usable Privacy and Security.*, 2019.

[39] F. Di Nocera, G. Tempestini, and F. Presaghi, "Reliability and validity of the Cybersecurity Awareness INventory (CAIN)," *Behaviour & Information Technology*, vol. 44, no. 7, pp. 1417–1428, 2025.

[40] F. Erdoğdu, S. Gökoğlu, and M. Kara, ""What about users?": Development and validation of the mobile information security awareness scale (MISAS)," *Online Information Review*, vol. 45, no. 2, pp. 406–421, 2021.

[41] Y. Gangire, A. Da Veiga, and M. Herselman, "Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory," in *Human Aspects of Information Security and Assurance*, N. Clarke and S. Furnell, Eds., 2020, pp. 144–157.

[42] J. R. Schoenherr and R. Thomson, "The Cybersecurity (CSEC) Questionnaire: Individual Differences in Unintentional Insider Threat Behaviours," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, pp. 1–8.

[43] T. Schmidt, C. Nøhr, and R. Koppel, "A simple assessment of information security awareness in hospital staff across five Danish regions," in *Studies in health technology and informatics*, 2021, vol. 281.

[44] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Computers & Security*, vol. 56, pp. 83–93, 2016.

[45] H.-Y. Huang, S. Demetriou, M. Hassan, G. S. Tuncay, C. A. Gunter, and M. Bashir, "Evaluating user behavior in smartphone security: A psychometric perspective," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 509–524.

[46] J. Kang and G. Seomun, "Development and validation of the information security attitude questionnaire (ISA-Q) for nurses," *Nursing Open*, vol. 10, no. 2, pp. 850–860, 2023.

[47] Š. Orehek and G. Petrič, "A systematic review of scales for measuring information security culture," *Information & Computer Security*, vol. 29, no. 1, pp. 133–158, 2020.

[48] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI)*, 2017, pp. 2202–2214.

[49] E. Davidov, B. Muthen, and P. Schmidt, "Measurement invariance in cross-national studies," *Sociological Methods & Research*, 2018.

[50] D. Langer, J. Tolsdorf, and L. Lo Iacono, "Supplementary Materials for "LISA: A Scale-Optimized and Psychometrically-Validated Instrument for the Lightweight Assessment of Organizational Information Security Awareness in Heterogeneous Organizations"," OSF repository, 2026. [Online]. Available: https://doi.org/10.17605/OSF.IO/KYMC2

[51] R. F. DeVellis, *Scale development: Theory and applications*, 4th ed. Los Angeles: SAGE, 2017.

[52] S. Carpenter, "Ten Steps in Scale Development and Reporting: A Guide for Researchers," *Communication Methods and Measures*, vol. 12, no. 1, pp. 25–44, 2018.

[53] J. F. Hair, *Multivariate data analysis*, 8th ed. Cengage, 2019.

[54] J. Tolsdorf and L. Lo Iacono, "Expert Perspectives on Information Security Awareness Programs in Medical Care Institutions in Germany," in *Proceedings of the 6th International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT)*, 2024, pp. 98–117.

[55] J. Harkness, "Questionnaire Translation," in *Cross-cultural survey methods*, J. A. Harkness, F. J. R. v. d. Vijver, and P. P. Mohler, Eds., 2003, pp. 35–56.

[56] B. Dorer, "ESS Round 9 Translation Guidelines," 2018.

[57] S. Egelman and E. Peer, "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*, 2015, pp. 2873–2882.

[58] C. Beierlein, A. Kovaleva, C. J. Kemper, and B. Rammstedt, "Allgemeine Selbstwirksamkeit Kurzskala (ASKU)," *Zusammenstellung sozialwissenschaftlicher Items und Skalen (ZIS)*, 2014.

[59] E. S. Doll, D. Nießen, I. Schmidt, B. Rammstedt, and C. M. Lechner, "General self-efficacy short scale-3 (GSE-3)," *ZIS - The Collection of Items and Scales for the Social Sciences*, 2021.

[60] B. Rammstedt, C. J. Kemper, M. C. Klein, C. Beierlein, and A. Kovaleva, "Big five inventory (bfi-10)," *Zusammenstellung sozialwissenschaftlicher Items und Skalen (ZIS)*, 2014.

[61] B. Rammstedt and O. P. John, "Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German," *Journal of Research in Personality*, vol. 41, no. 1, pp. 203–212, 2007.

[62] D. Crowne and D. Marlowe, "A new scale of social desirability independent of psychopathology," *Journal of consulting psychology*, vol. 24, no. 4, pp. 349–354, 1960.

[63] H. Lück and E. Timaeus, "Soziale Erwünschtheit SDS-CM," *Zusammenstellung sozialwissenschaftlicher Items und Skalen (ZIS)*, 1997.

[64] H. Breitsohl and C. Steidelmüller, "The impact of insufficient effort responding detection methods on substantive responses: results from an experiment testing parameter invariance," *Applied Psychology*, vol. 67, no. 2, pp. 284–308, 2018.

[65] A. M. Dunn, E. D. Heggestad, L. R. Shanock, and N. Theilgard, "Intra-individual response variability as an indicator of insufficient effort responding: comparison to other indicators and relationships with individual differences," *Journal of Business and Psychology*, vol. 33, no. 1, pp. 105–121, 2018.

[66] F. Marmolejo-Ramos and S. T. Tian, "The shifting boxplot. A boxplot based on essential summary statistics around the mean," *International Journal of Psychological Research*, vol. 3, no. 1, 2010.

[67] S. J. Finney and C. DiStefano, "Nonnormal and categorical data in structural equation modeling," in *Structural equation modeling: A second course, 2nd ed*, 2013, pp. 439–492.

[68] C.-H. Li, "Confirmatory factor analysis with ordinal data: Comparing robust maximum likelihood and diagonally weighted least squares," *Behavior Research Methods*, vol. 48, no. 3, pp. 936–949, 2016.

[69] D. Shi, C. DiStefano, H. L. McDaniel, and Z. Jiang, "Examining Chi-Square Test Statistics Under Conditions of Large Model Size and Ordinal Data," *Structural Equation Modeling: A Multidisciplinary Journal*, vol. 25, no. 6, pp. 924–945, 2018.

[70] S. G. West, A. B. Taylor, and W. Wei, "Model Fit and Model Selection in Structural equation Modeling," in *Handbook of Structural Equation Modeling*, R. H. Hoyle, Ed., 2012.

[71] R. B. Kline, *Principles and practice of structural equation modeling*, 4th ed. The Guilford Press, 2016.

[72] L. Hu and P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal*, vol. 6, no. 1, pp. 1–55, 1999.

[73] M. W. Browne and R. Cudeck, "Alternative ways of assessing model fit," in *Testing structural equation models*, K. A. Bollen and J. S. Long, Eds., 1993, no. 154, pp. 136–162.

[74] R. G. Netemeyer, W. O. Bearden, and S. Sharma, *Scaling Procedures: Issues and Applications*. SAGE, 2003.

[75] G. T. Smith, D. M. McCarthy, and K. G. Anderson, "On the sins of short-form development." *Psychological Assessment*, vol. 12, no. 1, pp. 102–111, 2000.

[76] I. Trizano-Hermosilla and J. M. Alvarado, "Best alternatives to Cronbach's alpha reliability in realistic conditions: Congeneric and asymmetrical measurements," *Frontiers in Psychology*, vol. 7, 2016.

[77] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, vol. 18, no. 1, p. 39, 1981.

[78] E. Roemer, F. Schuberth, and J. Henseler, "HTMT2–an improved criterion for assessing discriminant validity in structural equation modeling," *Industrial Management & Data Systems*, vol. 121, no. 12, pp. 2637–2650, 2021.

[79] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, vol. 43, no. 1, pp. 115–135, 2015.

[80] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Computers in Human Behavior*, vol. 69, pp. 151–156, 2017.

[81] D. Branley-Bell, L. Coventry, E. Sillence, S. Magalini, P. Mari, A. Magkanaraki, and K. Anastasopoulou, "Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff," *Annals of Disaster Risk Sciences*, vol. 3, no. 1, 2020.

[82] J. Ryan, "Information security awareness: An evaluation among business students with regard to computer self-efficacy and personal innovation," *AMCIS Proceedings*, 2007.

[83] A. J. Nederhof, "Methods of coping with social desirability bias: A review," *European Journal of Social Psychology*, vol. 15, no. 3, pp. 263–280, 1985.

[84] H. Wu and R. Estabrook, "Identification of Confirmatory Factor Analysis Models of Different Levels of Invariance for Ordered Categorical Outcomes," *Psychometrika*, vol. 81, no. 4, pp. 1014–1045, 2016.

[85] F. F. Chen, "Sensitivity of Goodness of Fit Indexes to Lack of Measurement Invariance," *Structural Equation Modeling: A Multidisciplinary Journal*, vol. 14, no. 3, pp. 464–504, 2007.

[86] D. L. Putnick and M. H. Bornstein, "Measurement invariance conventions and reporting: The state of the art and future directions for psychological research," *Developmental review : DR*, vol. 41, pp. 71–90, 2016.

[87] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, "Organizational information security policies: a review and research framework," *European Journal of Information Systems*, vol. 26, no. 6, pp. 605–641, 2017.

[88] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance," *Applied Sciences*, vol. 11, no. 8, pp. 3383 (1–38), 2021.

[89] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & Security*, vol. 106, p. 102267, 2021.

[90] M. A. Fauzi, P. Yeng, B. Yang, and D. Rachmayani, "Examining the Link Between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–8.

[91] J.-B. Son, T. Robb, and I. Charismiadji, "Computer Literacy and Competency: A Survey of Indonesian Teachers of English as a Foreign Language," *Computer-Assisted Language Learning Electronic Journal*, vol. 12, no. 1, pp. 26–42, 2011.

[92] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *Journal of Enterprise Information Management*, vol. 34, no. 4, pp. 1203–1228, 2020.

[93] S. Mishra, D. J. Caputo, G. J. Leone, F. G. Kohun, and P. J. Draus, "The Role Of Awareness And Communications In Information Security Management: A Health Care Information Systems Perspective," *International Journal of Management & Information Systems (IJMIS)*, vol. 18, no. 2, pp. 139–148, 2014.

[94] H. Shahbaznezhad, F. Kolini, and M. Rashidirad, "Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?" *Journal of Computer Information Systems*, vol. 61, no. 6, pp. 539–550, 2021.

[95] Venkatesh, Morris, Davis, and Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, vol. 27, no. 3, p. 425, 2003.

[96] S. R. Kessler, S. Pindek, G. Kleinman, S. A. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," *Health Informatics Journal*, vol. 26, no. 1, pp. 461–473, 2020.

[97] J. Siegrist, R. Shackelton, C. Link, L. Marceau, O. Von Dem Knesebeck, and J. McKinlay, "Work stress of primary care physicians in the US, UK and German health care systems," *Social Science & Medicine*, vol. 71, no. 2, pp. 298–304, 2010.

[98] Y. Rosseel, "lavaan: An R Package for Structural Equation Modeling," *Journal of Statistical Software*, vol. 48, no. 2, pp. 1–36, 2012.

[99] K. F. Widaman and W. Revelle, "Thinking thrice about sum scores, and then some more about measurement and analysis," *Behavior Research Methods*, vol. 55, no. 2, pp. 788–806, 2022.

[100] K. Hore, M. Hoi Tan, A. Kehoe, A. Beegan, S. Mason, N. Al Mane, D. Hughes, C. Kelly, J. Wells, and C. Magner, "Cybersecurity and critical care staff: A mixed methods study," *International Journal of Medical Informatics*, vol. 185, p. 105412, 2024.

[101] D. Alhuwail, E. Al-Jafar, Y. Abdulsalam, and S. AlDuaij, "Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities," *Applied Clinical Informatics*, vol. 12, no. 04, pp. 924–932, 2021.

[102] J. L. Fernández-Alemán, A. Sánchez-Henarejos, A. Toval, A. B. Sánchez-García, I. Hernández-Hernández, and L. Fernandez-Luque, "Analysis of health professional security behaviors in a real clinical setting: An empirical study," *International Journal of Medical Informatics*, vol. 84, no. 6, pp. 454–467, 2015.

[103] S. Jeong and Y. Lee, "Consequences of Not Conducting Measurement Invariance Tests in Cross-Cultural Studies: A Review of Current Research Practices and Recommendations," *Advances in Developing Human Resources*, vol. 21, no. 4, pp. 466–483, 2019.

[104] C. Roberts, O. Sarrasin, and M. Ernst Stähli, "Investigating the Relative Impact of Different Sources of Measurement Non-Equivalence in Comparative Surveys," *Survey Research Methods*, pp. 399–415 Pages, 2020.

[105] R. Schnell, *Survey-Interviews: Methoden standardisierter Befragungen*. Springer Fachmedien Wiesbaden, 2019.

[106] R. Rosenthal and R. L. Rosnow, *Artifacts in behavioral research: Robert Rosenthal and Ralph L. Rosnow's classic books: a re-issue of Artifact in behavioral research, Experimenter effects in behavioral research and The volunteer subject*. Oxford University Press, 2009.

[107] Deutsche Gesellschaft für Psychologie, Ed., *Ethisches Handeln in der psychologischen Forschung: Empfehlungen der Deutschen Gesellschaft für Psychologie für Forschende und Ethikkommissionen*, 1st ed. Hogrefe, 2018.

[108] American Psychological Association, "Ethical principles of psychologist and code of conduct," 2017.

Ethics considerations

In the absence of a formal ethics committee at our institution, we adhered to the ethical guidelines of the German Psychological Society (DGPS) [107], which align with those of the American Psychological Association (APA) [108]. As our research institution is located in Germany, our processing of personal data is also subject to the strict rules of the General Data Protection Regulation. Our study was reviewed and approved by our institution's data protection officer. The hospital survey was also reviewed and approved by the hospital's CISO team and management. The workshop was reviewed and approved by the hospital's CISO team, data protection officer, works councils, and management.

All participants provided informed consent for data elicitation and use in the study. Participation was voluntary for all participants, including employees.

Prolific survey participants were compensated at the German minimum wage (£11.49/hour). For Bilendi survey participants, compensation was treated as a tax-free expense allowance under the provider's internal policies. Researchers have no control over the exact compensation amount. In the hospital setting, employees participated in the survey and the workshops during regular working hours and received their normal salaries from the hospital, but received no additional compensation from the researchers.

All survey responses were anonymous to the extent possible. Prolific and Bilendi provided the researchers with an alphanumeric pseudonym that was used for approval of responses and to process compensation. In the hospital survey, no identifiers were used, and no other means of identifying information, such as IP addresses, were collected. Neither the researchers nor the employer could identify individual employees. Invitations to the survey and the workshops

were sent via email and newsletters with general-purpose hyperlinks to our own university-owned infrastructure.

For workshops, the researchers had access to a dedicated room on the hospital's property for participants to speak and act freely. Researchers did not record attendance lists or report who took part. Workshop materials with participants' writings (e.g., moderation cards) were digitized and analyzed without any possibility of linking content to specific individuals. For workshop scheduling, we relied on GDPR-compliant software hosted by the Deutsches Forschungsnetz and on our university's email accounts. To protect participant confidentiality, contact data and any email correspondence were deleted after the workshop study was completed. Furthermore, employees were not scheduled to attend workshops with their direct superiors.

At no time did the researchers share unprocessed response data or participant data with the hospital or other entities. After the hospital studies were completed, the researchers shared aggregated data with the hospitals' CISO teams in study reports. All data were stored and processed on our own university-owned infrastructure secured through encryption and restricted access controls.

LLM usage considerations

LLMs were used for editorial purposes in this manuscript, and all outputs were inspected by the authors to ensure accuracy and originality.

Competing interests

Large parts of this research were conducted while all authors had affiliations with the H-BRS Bonn-Rhein-Sieg University of Applied Sciences in Germany. This research was supported by the German Federal Ministry of Health with grant number ZMI1-2521FSB801.

Appendix A. German Items

TABLE 8. GERMAN ITEMS OF THE LISA SCALE WITH CORRESPONDING STANDARDIZED FACTOR LOADINGS. ITEMS ARE GROUPED INTO KNOWLEDGE (K), ATTITUDE (A), AND BEHAVIOR (B) SUBSCALES.

#	German Item	λ
K1	Wenn ich an einem vertraulichen Dokument arbeite, muss ich den Bildschirm von Laptop oder Tablet vor fremden Blicken schützen.*	.774
K2	Ich darf Ausdrucke mit sensiblen Informationen auf dem Schreibtisch liegen lassen, wenn ich mich davon entferne.*	.680
K3	Die Meldung von Sicherheitsvorfällen ist freiwillig.*	.476
K4	Das Personal muss regelmäßig an Schulungen oder Fortbildungen in Sachen Informationssicherheit teilnehmen.	.799
K5	Das Personal muss sich regelmäßig über Vorschriften und Richtlinien der Organisation zur Informationssicherheit auf dem Laufenden halten.	.792
K6	Wenn man über vertrauliche Informationen spricht, muss sichergestellt sein, dass Unbefugte nicht mithören können.	.770
K7	Die versehentliche Preisgabe sensibler Informationen an Unbefugte muss gemeldet werden.	.687
A1	Es ist riskant, vertrauliche Dokumente auf mobilen Geräten wie Laptop oder Tablet zu öffnen, wenn Fremde den Bildschirm einsehen können.*	.800
A2	Es ist riskant, Ausdrucke mit sensiblen Informationen unbeaufsichtigt auf dem Schreibtisch liegen zu lassen.*	.705
A3	Es ist riskant, Sicherheitsvorfälle zu ignorieren, auch wenn ich sie für unerheblich halte.*	.689
A4	Es ist sinnvoll, dass das Personal regelmäßig an Schulungen oder Fortbildungen in Sachen Informationssicherheit teilnimmt.	.798
A5	Es ist angemessen, sich regelmäßig über Vorschriften und Richtlinien der Organisation zur Informationssicherheit auf dem Laufenden zu halten.	.838
A6	Es ist riskant, über vertrauliche Informationen zu sprechen, wenn Unbefugte mithören können.	.806
A7	Es ist wichtig zu melden, falls sensible Informationen versehentlich an Unbefugte preisgegeben werden.	.803
B1	Wenn ich an einem vertraulichen Dokument arbeite, stelle ich sicher, dass Fremde den Bildschirm des mobilen Geräts wie Laptop oder Tablet nicht einsehen können.*	.807
B2	Ich lasse Ausdrucke mit sensiblen Informationen auf dem Schreibtisch liegen, wenn ich nicht vor Ort bin.*	.646
B3	Wenn ich einen Sicherheitsvorfall bemerke, würde ich ihn melden.*	.773
B4	Ich nehme regelmäßig an Schulungen oder Fortbildungen in Sachen Informationssicherheit teil.	.783
B5	Ich informiere mich regelmäßig über die Vorschriften und Richtlinien zur Informationssicherheit in meiner Organisation.	.789
B6	Manchmal spreche ich über vertrauliche Informationen, obwohl andere mithören können.	.656
B7	Falls ich sensible Informationen versehentlich an Unbefugte preisgebe, werde ich dies melden.	.795

Note. German entails $n = 601$. LISA was estimated by employing a three-factor Confirmatory Factor Analysis with DWLS estimator. Loadings are standardized. Global fit measures: $\chi^2(186) = 992.70$, $p < .001$, CFI = 0.980, RMSEA (90% CI) = 0.085 [0.080–0.090], SRMR = 0.073. K = Knowledge, A = Attitude, B = Behavior. Items with * were translated to German from the English items of the HAIS-Q [25], with K1, A1, and B1 adjusted by adding 'tablet' as an additional device.

Appendix B.
Convergent Validity and and Reliabilities for LISA

TABLE 9. LISA CONVERGENT LATENT CORRELATIONS AND RELIABILITIES FROM CFA MODEL FOR THE ENGLISH (UK) AND GERMAN (DACH) SAMPLES.

Variable	1	2	3	4	5	6	7	8	9	10	11
English (UK sample)											
1. LISA (Knowledge)	*(.89)*										
2. LISA (Attitude)	.86	*(.92)*									
3. LISA (Behavior)	.83	.84	*(.87)*								
4. HAIS-Q (Knowledge, no overlap)	.92	.78	.69	*(.91)*							
5. HAIS-Q (Attitude, no overlap)	.76	.92	.73	.85	*(.94)*						
6. HAIS-Q (Behavior, no overlap)	.76	.79	.93	.89	.91	*(.90)*					
7. SeBIS (Device Securement)	.42	.40	.50	.37	.35	.51	*(.68)*				
8. SeBIS (Password Generation)	.28	.36	.54	.35	.38	.57	.60	*(.81)*			
9. SeBIS (Proactive Awareness)	.30	.37	.51	.37	.45	.59	.50	.69	*(.67)*		
10. SeBIS (Updating)	.38	.45	.59	.36	.42	.57	.57	.72	.61	*(.79)*	
11. SISA	.57	.65	.76	.54	.67	.77	.50	.54	.59	.65	*(.74)*
German (DACH sample)											
1. LISA (Knowledge)	*(.88)*										
2. LISA (Attitude)	.78	*(.91)*									
3. LISA (Behavior)	.75	.81	*(.89)*								
4. HAIS-Q (Knowledge, no overlap)	.91	.72	.60	*(.90)*							
5. HAIS-Q (Attitude, no overlap)	.69	.89	.67	.86	*(.93)*						
6. HAIS-Q (Behavior, no overlap)	.70	.81	.86	.84	.92	*(.91)*					
7. SeBIS (Device Securement)	.36	.46	.50	.38	.42	.50	*(.73)*				
8. SeBIS (Password Generation)	.33	.45	.62	.34	.42	.63	.53	*(.78)*			
9. SeBIS (Proactive Awareness)	.37	.48	.63	.44	.55	.73	.52	.75	*(.69)*		
10. SeBIS (Updating)	.43	.52	.62	.35	.48	.57	.48	.69	.63	*(.76)*	
11. SISA	.65	.74	.80	.61	.71	.82	.48	.63	.72	.67	*(.76)*

Note: Values are factor correlations below the diagonal. All factor correlations are Pearson correlations of the first-order latent variables from one CFA model. All correlations are significant at $p < .001$. Italic values in parentheses on the diagonal indicate McDonald's ω, estimated with polychoric correlations. Abbreviations: CFA = Confirmatory Factor Analysis, LISA = Lightweight Information Security Awareness Scale, HAIS-Q = Human Aspects of Information Security Questionnaire, SeBIS = Security Behavior Intentions Scale, SISA = Simplified Information Security Awareness Scale. "No overlap" indicates that three items were removed from the HAIS-Q dimension to avoid inflated correlations with LISA.

Appendix C.
Measurement Invariance Testing and Global Fit Indices

TABLE 10. LISA MODEL FIT INFORMATION FOR TESTING CROSS-LINGUAL MEASUREMENT INVARIANCE BETWEEN GERMAN AND ENGLISH.

Model: LISA (3 Factor Model)	χ^2	df	CFI	RMSEA	SRMR	$\Delta\chi^2$	Δdf	ΔCFI	ΔRMSEA	ΔSRMR
Configural Invariance	1790.08	372	.983	.080	.070					
Thresholds constrained	1811.08	413	.984	.076	.070	20.99	41	0.000	–.005	0.000
Thresholds and loadings constrained	1841.88^{*}	431	.983	.074	.070	30.80	18	0.000	–.001	0.000
Thresholds, loadings, and intercepts constrained	1897.43^{***}	449	.983	.074	.070	55.55	18	0.000	–.001	0.000

Note. $^{***}p \leq .001$, $^{**}p \leq .01$, $^{*}p \leq .05$. English sample: $n = 581$; German sample: $n = 601$. Estimates are based on a three-factor CFA using the DWLS estimator and by following the guidelines of Wu and Estabrook [84].

Appendix D.
Meta-Review

The following meta-review was prepared by the program committee for the 2026 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

D.1. Summary

This research aims to provide a way to measure information security awareness (ISA) through the development of the Lightweight Information Security Awareness (LISA) scale. LISA is short, psychometrically validated, and usable across multiple languages. It also measures behaviors and attitudes beyond just technical security. LISA was created and refined through interviews with experts and a survey with $\sim$1100 adults in both English and German, resulting in a 21-item scale measuring knowledge, attitude, and behavior. For further validation, LISA was deployed in a German hospital with 579 participants where the internal consistencies matched original validation results. Finally, LISA was validated by comparing scores against established constructs.

D.2. Scientific Contributions

1) Creates a New Tool to Enable Future Science.
2) Addresses a Long-Known Issue.
3) Provides a Valuable Step Forward in an Established Field.

D.3. Reasons for Acceptance

1) The paper provides a strong motivation, explaining why existing scales and measures are not sufficient, namely that they may be too long, not validated, or not specific to organizations.
2) Use of stakeholders in item generation and real-world validation lends validity to the scale

D.4. Noteworthy Concerns

Scale is validated in a hospital setting, which possibly limits its generalizability.