# Measuring Dimensions of Information Security Culture Across Industries with Situational Judgment Tests

Samantha Phillips
*School of Cyber Studies, The University of Tulsa, Tulsa, Oklahoma, USA*

Bradley Brummel
*Department of Psychology, University of Houston, Houston, Texas, USA*

Sal Aurigemma
*Department of Information Technology Management*
*University of Hawai'i at Mānoa, Honolulu, Hawaii, USA*

Tyler Moore
*School of Cyber Studies, The University of Tulsa, Tulsa, Oklahoma, USA*

**Abstract**

**Purpose** – Understanding the type of information security culture (ISC) present in organizations is important because it guides how employees navigate the use of technology and information resources. This study aims to develop and evaluate a situational judgment test (SJT) designed to measure the underlying assumptions level of ISC through employee security tendencies. The goal is to determine if this approach could provide an engaging format and useful information on different types of cultures.

**Design/methodology/approach** – A novel ISC-SJT was developed to simultaneously measure cultural alignment and security behavior tendencies as a reflection of ISC. The 24-item ISC-SJT was administered to 330 employees across five U.S. industries: Technology, Government/Military, Manufacturing/Heavy, Healthcare, and Education. Analysis included correlations, ANOVA, and post-hoc comparisons. Additional questions assessed participant perspectives on the format and realism of the items.

**Findings** – Results revealed that specific cultural orientations—means-oriented, internally driven, strict work discipline, open system, and employee-oriented—are associated with more desirable security behavior tendencies. Significant U.S. industry-level differences were also identified, with Education showing an easygoing work discipline culture and the lowest overall security scores. The ISC-SJT was found to be both realistic and engaging, offering contextually grounded insights.

**Originality/value** – This research utilized a novel methodology and perspective to assess the underlying assumptions level of organizational ISC. It focused on evaluating the type of culture, rather than influencing factors of culture, through the lens of Hofstede's organizational culture dimensions and security behavior tendencies. The study investigated cultural differences between five U.S. industries and explored differences between cultural orientations.

**Keywords** Information security culture, Information security, Situational judgment test, Organizational culture, Security behavior, Underlying assumptions

Funding: Phillips and Moore gratefully acknowledge support from the US National Science Foundation (NSF) Award No. 2147505. The authors acknowledge support from Tulsa Innovation Labs via the Cyber Fellows initiative.

Samantha Phillips is also affiliated with Department of Information Systems and Security, Kennesaw State University, Kennesaw, Georgia, USA

## 1. Introduction

The success or failure of an organization's information security efforts is often significantly influenced by its employees, commonly referred to as "the human element". According to the 2025 *Verizon Data Breach Investigation Report* (DBIR), the human element was involved in 60% of the 10,798 confirmed data breaches they assessed (*Verizon Business,* 2025). With the human element contributing to many security incidents, how can organizations support and encourage their employees to be valuable assets rather than obstacles in the face of ever-evolving security threats? One key element to consider is an organization's information security culture (ISC).

Information security culture can be defined as "the accumulation of shared artifacts, beliefs, values, and underlying assumptions that a group uses to navigate the use and safeguarding of important information resources securely and effectively" (Phillips *et al.*, 2023, p.4). Put simply, ISC describes how members of a group, shaped by cultural influences, tend to behave in information security-related situations.

Foundational organizational culture models have guided ISC research and measurement approaches for decades (Nasir *et al*., 2019; Uchendu *et al*., 2021). Existing ISC measurements primarily rely on Likert scales to assess factors influencing ISC within organizations (Uchendu *et al*., 2021), focusing on culture levels (e.g., maturity or acceptability) or strength (e.g., strong vs. weak). While these measures were not designed to classify culture types, prior research has shown that different organizational culture types significantly influence security-related outcomes, such as policy compliance (Chang and Lin, 2007; Karlsson *et al*., 2022; Soloman and Brown, 2021).

We propose a novel approach using a situational judgment test (SJT) to measure the type of ISC based on employees' security tendencies. This method considers not only the desirability of security behavior but also cultural alignment. The ISC-SJT is grounded in two organizational culture frameworks, Schein's Three-Level Model of Culture (Schein and Schein, 2016) and Hofstede's organizational culture dimensions (Hofstede *et al*., 2010). By understanding the type of culture present within an organization, information security initiatives can be aligned with the culture to improve effectiveness.

## 2. Background and related works

### *2.1 Organizational Culture*

Understanding ISC begins with examining the broader construct of organizational culture, as ISC is widely recognized as a subculture within this larger framework (Alnatheer *et al*., 2012;

Da Veiga and Martins, 2017; Solomon and Brown, 2021). Drawing from organizational culture literature and applying a security-specific lens provides a theoretical foundation for ISC research. This study builds upon two well-established models from organizational culture: Hofstede's Organizational Culture Dimensions and Schein's Three-Level Model of Culture.

*Organizational Culture Dimensions.* Hofstede's work identifies six dimensions of organizational culture, each reflecting perceived shared practices within an organization (Hofstede *et al*., 2010; *The Culture Factor Group*, n.d.). These dimensions are independent of each other, with each consisting of two opposing orientations. The dimensions are organizational effectiveness (means versus goal-oriented), customer orientation (internally versus externally driven), level of control (easygoing versus strict work discipline), focus (local versus professional), approachability (open versus closed system), and management philosophy (employee- versus work-oriented).

*Three-Level Model of Culture.* Schein proposed a three-level model for categorizing cultural phenomena spanning artifacts, espoused beliefs, and underlying basic assumptions (Schein and Schein, 2016). Artifacts represent the most tangible part of an organization's culture – what one can see, hear, or feel when engaging with an organization (Schein and Schein, 2016, p.17). Espoused beliefs and values encompass the stated norms, strategies, goals, and philosophies that an organization uses to depict the culture to themselves and others (Schein and Schein, 2016, pp.19-21). Underlying basic assumptions refer to unconscious, taken-for-granted beliefs that influence perceptions, thoughts, feelings, and behaviors (Schein and Schein, 2016, p.10,18). Underlying assumptions include how employees expect others or themselves to behave when interacting with technology or how they feel and think about their organization's information security initiatives. The SJTs presented here aim to measure these underlying assumptions.

### *2.2 Information Security Culture*

ISC research has primarily focused on theoretical frameworks, with relatively few measurement tools available (Uchendu *et al*., 2021). Schein's model is widely accepted as a theoretical foundation for ISC research (Okere *et al.*, 2012; Karlsson *et al*., 2015; Nasir *et al*., 2019; Uchendu *et al*., 2021). Several researchers have adapted this model to information security contexts. For example, Schlienger and Teufel (2002) applied Schein's levels to define layers of ISC, while Kraemer and Carayon (2005) contextualized them within computer and information security. Van Niekerk and Von Solms (2010) expanded the model by adding "knowledge" as a fourth dimension, arguing that security knowledge is a prerequisite for secure behavior. Similarly,

Da Veiga and Eloff's (2010) ISC Framework (ISCF) integrates Schein's levels to examine how influencing factors shape information security behavior.

Hofstede's work is less prevalent in existing ISC research. Most ISC studies have drawn from Hofstede's national culture model (e.g., Alfawaz, 2011; Bruin, 2022; Hoffman, 2021; Stan *et al*., 2023; Zhang and Yang, 2019), but some have used his organizational culture dimensions. Tang *et al*. (2016), for instance, proposed links between Hofstede's dimensions and security policy compliance, communication, accountability, and governance. Failla (2020) used these dimensions to examine cybersecurity governance in breached organizations using publicly available data.

Existing literature has established a wide range of dimensions associated with information security culture (Nasir *et al*. 2019). Typically, the dimensions are evaluated for how they influence ISC, rather than how differences in values lead to varying ISC. For example, the ISCF and Information Security Culture Assessment (ISCA) evaluate how various dimensions impact behavior (Da Veiga, 2015; Da Veiga and Eloff, 2010; Martins and Da Veiga, 2015). Several studies have examined the factors influencing organizational ISC. Sherif *et al*. (2015) explored the variables influencing the establishment of ISC. Nasir *et al*. (2017) conducted a study on the development of an ISC model that is based on dimensions that guide information security behavior. Uchendu *et al*. (2021) conducted a literature review of current cybersecurity culture practices and identified factors regarded as important to cybersecurity culture. Booker and Rebman (2023) extended this line of research by examining how intentional ISC interventions correlate with cyberattack frequency. A recent example of a study focusing on top management influence on ISC is Grill *et al*. (2025), which targeted ISC improvements through information security behavior training at both the employee and managerial level.

Alongside culture-level approaches, recent research has examined information security behaviors using established individual-level behavioral models and validated instruments, such as the Human Aspects of Information Security Questionnaire (HAIS-Q) developed by Parsons *et al*. (2014) to assess cybersecurity awareness, attitudes, and self-reported practices. Studies grounded in Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and Self-Determination Theory (SDT) have been used to explore how individual motivations, perceptions, and intentions relate to security behavior. For example, Gangire *et al*. (2021) developed an information security compliance questionnaire based on SDT and HAIS-Q, Sommestad *et al*. (2019) synthesized TPB-based research on information security policy compliance, and Doge *et*

*al*. (2023) examined PMT-based predictors of intentions to adopt cybersecurity practices. While these approaches provide valuable insight into individual-level predictors of security behavior, they primarily emphasize intentions and motivations rather than the shared cultural assumptions and behavioral tendencies that this study is designed to uncover. Taken together, these individual-level approaches have advanced the understanding of security behavior but remain limited in their ability to assess information security culture as a shared organizational construct.

Despite decades of ISC research, there is still not a widely adopted, validated tool for assessing ISC across diverse organizational contexts (Orehek and Petrič, 2021; Sas *et al*., 2020; Uchendu *et al*., 2021). The dominant measurement approach has been Likert-scale-based surveys and questionnaires. Sas *et al*. (2020) reviewed six tools, noting that all ISC-focused instruments relied on questionnaires, with only Schlienger and Teufel (2002) incorporating additional methods. A separate review by Orehek and Petrič (2021) evaluated the operational rigor and psychometric quality of ISC scales, though some included instruments, like Parson's HAIS-Q (2014), were not originally designed to measure culture. In summary, while existing ISC measurements have contributed valuable insights, they largely assess influencing factors rather than identifying distinct types of ISC. This gap highlights the need for alternative assessment methods that can uncover the implicit assumptions and cultural tendencies shaping security behavior.

### *2.3 Relationship between Organizational Culture and Information Security Culture*

An organization's overarching cultural environment directly influences how individuals perceive, interpret, and act on information security expectations. Chang and Lin (2007), Karlsson *et al*. (2022), and Solomon and Brown (2021) each investigated the relationship between organizational culture and information security aspects, such as policy compliance. All three studies examined the organizational culture and information security relationships using the Competing Values Framework (CVF), which categorizes organizational culture along two axes: flexibility vs. control and internal vs. external focus (Cameron, 2009).

Chang and Lin (2007) used this framework to explore how cultural traits such as cooperativeness, innovativeness (flexibility-oriented), and effectiveness, consistency (control-oriented) affect the implementation of information security management principles. Their findings indicated that control-oriented traits were more conducive to success, while flexibility-oriented traits were less favorable. Similarly, Karlsson *et al*. (2022) found that internal cultural orientations were positively associated with employees' compliance with security policies. Solomon and

Brown (2021) concluded that both organizational culture and ISC significantly influence employee compliance, with control-oriented cultures exerting a particularly strong impact.

These studies underscore the importance of considering the type of culture—not just the presence or strength of security factors—when designing and implementing security initiatives. However, they do not apply an information security lens directly to organizational culture but rather look at the relationship between organizational culture and information security components.

### *2.4 Situational Judgment Tests (SJTs)*

While existing information security culture assessments heavily rely on self-report questionnaires using Likert-scale items, such tools often assess perceptions or attitudes in isolation rather than capturing context-driven behavioral tendencies. Situational judgment tests (SJTs) have traditionally been used within the field of organizational psychology to predict employee performance and influence employment decisions (Ployhart and MacKenzie, 2011; Weekley and Ployhart, 2005). An SJT item presents participants with a realistic work-related situation followed by a set of possible response options. SJTs are considered multidimensional, as they can assess a variety of latent constructs simultaneously (Oostrom *et al*., 2015; Ployhart and MacKenzie, 2011; Ployhart and Ward, 2013; Pollard and Cooper-Thomas, 2015). Moreover, the way response instructions are structured—such as asking what respondents *would do* versus *should do*—determines whether the SJT measures behavioral tendency or knowledge (McDaniel *et al*., 2007). Phillips *et al*. (2024) provides a detailed comparison of SJTs with commonly used information systems measurement approaches, including Likert-scale assessments and scenario-based vignettes.

In a similar vein, Beautement *et al*. (2016) developed a scenario-based survey to assess employee behaviors and attitudes in relation to security practices. Rather than using Hofstede's framework, their study applied a cultural lens developed by Adams (2003) to interpret group-level behavioral tendencies. The results demonstrated how scenario-based assessments can uncover behavioral differences across employee groups and inform the design of more tailored security interventions. Their research illustrates the potential of scenario-based instruments to capture security behavior in context, supporting a more nuanced understanding of the cultural factors influencing secure or insecure practices.

Building on this foundation, the present study introduces the Information Security Culture Situational Judgment Test (ISC-SJT) to assess employee's underlying basic assumptions by evaluating behavioral tendencies in security-relevant situations. Unlike previous scenario-based tools, the ISC-SJT is explicitly grounded in Hofstede's organizational culture dimensions and Schein's three-level model of culture, enabling the classification of ISC types based on behavioral tendencies rather than inferred attitudes or maturity levels. As previously discussed in Section 2.1, the underlying assumptions level of culture determines the behaviors, perceptions, thoughts, and feelings of an organization's members and guides the actions employees should take in varying situations (Schein and Schein, 2016, p.18-22). Therefore, by using the capabilities of a situational judgment test, security behavior tendencies can be elicited as reflections of the underlying assumptions that shape how employees perceive, interpret, and respond to information security situations.

## 3. Research design and methodology

This section outlines the development, format, and scoring of the ISC-SJT, as well as the data collection procedures for the research study. The final survey consisted of 24 SJT items, demographic items, and feedback questions.

### *3.1 Research questions and hypotheses*

In this study, we examine ISC dimensions across a range of U.S. industries. Although cultural differences exist between organizations within the same industry, industries themselves can exhibit shared cultural characteristics, particularly regarding perceived shared practices (Schein & Schein, 2016, p.28; Hofstede *et al*., 2010, pp.347–348). Therefore, cross-industry data collection was deemed appropriate. In addition to detailing the ISC-SJT development process, this study is guided by the following research questions:

- *RQ1: Does one orientation within each of Hofstede's six organizational culture dimensions exhibit more desirable security behavior tendencies than its counterpart?*
- *RQ2: How do ISC-SJT results compare across all observed industries?*
- *RQ3: To what extent are the ISC-SJT items applicable across all observed industries?*

The following hypothesis were established in relation to research question RQ1:

- *H1:* For the Organizational Effectiveness dimension, the means-oriented orientation will exhibit more desirable security behavior tendencies than the goal-oriented orientation.

- *H2:* For the Customer Orientation dimension, the internally driven orientation will exhibit more desirable security behavior tendencies than the externally driven orientation.
- *H3:* For the Level of Control dimension, the strict work discipline orientation will exhibit more desirable security behavior tendencies than the easygoing work discipline orientation.
- *H4:* For the Focus dimension, the professional orientation will exhibit more desirable security behavior tendencies than the local orientation.
- *H5:* For the Approachability dimension, the open system orientation will exhibit more desirable security behavior tendencies than the closed system orientation.
- *H6:* For the Management Philosophy dimension, the employee-oriented orientation will exhibit more desirable security behavior tendencies than the work-oriented orientation.

Five of the six hypotheses align with the orientation Tang *et al*. (2016) theorizes is more likely to comply with information security policies. H4 is the exception in that the professional orientation is hypothesized to exhibit more desirable security behavior tendencies over the local orientation. The professional orientation was chosen because although Tang *et al*. propose that in a local culture employees are more likely to comply with policies, in a professional culture information security would be placed in a more important position since it would be a profession for the organization. Since the ISC-SJT does not focus solely on compliance related behaviors, but also how individuals perceive the security of others, such as the IT security team, it is hypothesized that professional cultures in this context will exhibit more desirable security behavior tendencies overall compared to local cultures.

### *3.2 Creating the ISC-SJT*

We sought to make the ISC-SJT items generic and cover a broad range of security concepts. Each item is multidimensional in that it simultaneously assesses a cultural dimension and security behavior tendency. Hofstede's six organizational culture dimensions were used as the foundation for classifying the type of culture present within an organization. Table 1 illustrates one ISC-SJT item that assesses the "Organizational Effectiveness" culture dimension. All 24 ISC-SJT items can be found in Appendix 1.

**Table 1. Organizational Effectiveness ISC-SJT Item**

| **Item Stem:** Your organization uses a "Report Phish" feature on their email system, where users can press a button to send suspicious emails to be reviewed by IT Security. How would you most likely and least likely use this feature? | | |
|---|---|---|
| **Response Options** | **Orientation** | **Security Behavior** |
| A. I would immediately report any emails that I think might be phishing after a quick glance to avoid slowing down my work. | Goal-oriented | Desirable |
| B. I would just avoid interacting with any emails that look suspicious and not worry about reporting them to avoid slowing down my work. | Goal-oriented | Undesirable |
| C. I would carefully check each email to determine if I think it might be phishing before submitting the email to IT Security for review. | Means-oriented | Desirable |
| D. I would report all emails from new or unknown senders just to be on the safe side, even if the email looks safe. | Means-oriented | Undesirable |

Source: Authors own work.

Each ISC-SJT item consists of an item stem and four response options. Each response option aligns with an orientation of the culture dimension being assessed and a desirable or undesirable security behavior. Furthermore, to capture results that reflect the underlying assumptions of the organization's ISC, the items include both self-expected and other-expected behavior tendency responses. For example, some items ask the participants what they would do, while other items ask the participants what they think someone else would do in the presented situation. The mixed approach also helps reduce bias in self-report and peer-report assessments.

We first generated content for the SJT item stems and response options. We developed four items for each of the six organization culture dimensions, for a total of 24 items. The content of the ISC-SJT items is based on common information security situations (e.g. plugging in unknown USB drives, locking a computer when walking away). Each item was designed to reflect decision contexts associated with a specific cultural dimension, with response options representing contrasting orientations within that dimension. The second step was to adjust the item stems and response option ideas based on Hofstede's dimension definitions to align with the underlying measurement structure.

Next, we developed the instruction format. Since the goal of the ISC-SJT is to elicit responses that reflect the participant's underlying assumptions of their organization's ISC, we utilized a behavioral tendency instruction format. Each item uses the term "would" and prompts participants to select the most likely and least likely response options, consistent with behavior tendency measurement in SJT design. This was done to gather more context for the culture type and behavior expectations. If the instructions instead used the term "should," the items would be designed to assess knowledge of expected or ideal behaviors, potentially shifting responses toward

socially desirable or normatively correct answers rather than those reflecting typical organizational practice.

### *3.3 ISC-SJT Revision Process*

We undertook an extensive iterative revision process to ensure high content validity for the constructs being measured. After the initial development of 24 ISC-SJT items, five subject matter experts (SMEs) from cybersecurity, information systems, and organizational psychology completed a sorting exercise to evaluate alignment between the items and their intended underlying measurements. The SMEs were provided with definitions for each culture dimension and orientation and were instructed to code each item by dimension and to code the associated response options by orientation and security behavior.

Initial agreement among SMEs was high for the security behavior classification, with 19 of the 24 items (79%) receiving agreement from at least four of the five SMEs, including 10 items with unanimous agreement. Agreement on the intended culture dimension was more moderate, with 16 items (67%) receiving agreement from at least three SMEs, including 8 items with agreement from at least four SMEs, prior to item revision.

Based on the results of the sorting exercise and qualitative feedback from the SMEs, the ISC-SJT items were revised to improve their alignment with the underlying constructs. During this initial revision phase, the security behavior classification terminology was also refined. Originally, the terms secure and non-secure were used; however, it became evident that some behaviors classified as non-secure were technically secure but undesirable from a business efficiency perspective (e.g., avoiding a productivity-enhancing tool due to uncertainty about its security rather than requesting a formal security review). As a result, the terms desirable and undesirable were adopted to more accurately capture security behavior tendencies.

Following these revisions, three of the five SMEs reviewed the updated ISC-SJT items and provided additional feedback. After a third round of revisions, the same three SMEs reviewed the final set of 24 items and agreed that all items appropriately reflected their intended underlying measurements. This sorting exercise, along with multiple rounds of expert review and revision, was conducted to establish the content validity of the ISC-SJT items. The SME sorting protocol is included in Appendix 2.

### *3.4 Scoring the ISC-SJT*

The responses to each ISC-SJT item can be scored in a variety of ways to assess both the type of culture and security behavior tendencies. The three scoring methods used are referred to as Dimension Score, Security Score, and Dimension & Security Score. Table 2 presents response types and their associated score for each scoring method. Each ISC-SJT item can receive a maximum score of "2" per scoring method. Item scores are summed to calculate subscale scores that reflect each participant's cultural dimension profile and security behavior tendencies. For the Dimension Score and Dimension & Security Score methods, one orientation must be selected as the reference orientation for each culture dimension to serve as the scoring baseline. This choice is made solely for analytical convenience. For this study, the reference orientation for each dimension is the orientation hypothesized to exhibit more desirable security behavior tendencies (means-oriented, internally driven, easygoing work discipline, professional, open system, and employee-oriented). Appendix 1 provides the scoring key for each ISC-SJT item using these reference orientations. Reversing the reference orientation inverts the numerical scores but yields the same interpretations, as demonstrated in Appendix 3.

**Table 2. ISC-SJT Scoring Methods**

| Response Type | Orientation | Security behavior | Dimension Score | Security Score | Dimension & Security Score |
|---|---|---|---|---|---|
| Most Likely | Orientation 1 | Desirable | 1 | 1 | 1 |
| | Orientation 1 | Undesirable | 1 | 0 | 0 |
| | Orientation 2 | Desirable | 0 | 1 | 0 |
| | Orientation 2 | Undesirable | 0 | 0 | 0 |
| Least Likely | Orientation 1 | Desirable | 0 | 0 | 0 |
| | Orientation 1 | Undesirable | 0 | 1 | 0 |
| | Orientation 2 | Desirable | 1 | 0 | 0 |
| | Orientation 2 | Undesirable | 1 | 1 | 1 |

Note. Orientation 1 is representative of the reference orientation chosen for scoring purposes.
Source: Authors own work.

### *3.5 Supplementary Measures*

In addition to the ISC-SJT items, participants completed measures intended to provide supplementary information. These included slider scales and feedback questions, which are provided in Appendix 4. The slider scales were included after the ISC-SJT items to provide preliminary external indicators aligned with each ISC-SJT dimension. Each slider asked participants to indicate, on a 7-point scale, which orientation for each of the six dimensions they believed best reflected the culture within their organization. The feedback questions were included to assess the applicability of the ISC-SJT items across the five industries and to capture participants'

perspectives on their survey experience. After each ISC-SJT item, participants were asked whether they believed the situation could reasonably occur within their organization. Two open-ended questions at the end of the survey asked participants to reflect on their experience completing the survey, including interest, enjoyability, and engagement.

### *3.6 Data collection*

A total of 330 U.S.-based full-time employees across five sectors (66 each) —Technology, Government/Military, Healthcare, Manufacturing/Heavy Industry, and Education—were recruited to complete the survey through the platform Prolific. Eligibility criteria included being 18 years or older, employed full-time, working within one of the specified industries, and having an approval rate greater than 95% on Prolific. Both the ISC-SJT items and response options were randomized for each participant. Table 3 provides an overview of participant demographics. The study was reviewed and approved as exempt by The University of Tulsa IRB (Protocol No. 24-37), data collection was anonymous, and informed consent was obtained from all participants.

**Table 3. Participant Demographics**

| Industry | Male | Female | Age Range | States Represented |
|---|---|---|---|---|
| Technology | 42 | 24 | 21 – 71 | 28 |
| Government & Military | 33 | 33 | 23 – 65 | 23 |
| Manufacturing & Heavy industry | 44 | 22 | 21 – 67 | 25 |
| Healthcare | 21 | 45 | 22 – 65 | 28 |
| Education | 22 | 44 | 23 – 76 | 28 |
| **Totals** | **162** | **168** | **21 – 76** | **43** |

Source: Authors own work.

## 4. Results

This section presents the results of the ISC-SJT, beginning with correlations among dimension and security scores, followed by analyses of differences across industry types using analysis of variance (ANOVA) and post-hoc comparisons. The measurement properties of the ISC-SJT are then reported, including internal reliability and preliminary convergent validity. Finally, results from the feedback items are presented.

### *4.1 ISC-SJT Results*

This subsection presents the analysis of participants' ISC-SJT responses using dimension scores and security scores. For each organizational culture dimension, participants received a subscale score reflecting alignment with the reference orientation. Similarly, security subscale

scores represent the extent to which participants' responses aligned with desirable security behaviors.

The correlation coefficient matrix (Table 4) presents relationships between participants' dimension scores and security scores. Correlation coefficients indicate the strength and direction of linear relationships, with 0.1, 0.3, and 0.5 representing small, medium, and large effects, respectively (Cohen, 1977, p.115). All security score sub-scales (S1–S6) show large positive correlations with the overall security score (S). Positive correlations were also observed among the security subscales themselves, as expected, given that all items are designed to measure the same underlying construct of security behavior tendencies.

Among the cultural dimensions, Level of Control (D3; r = .30, 95% CI [.12, .46]) and Approachability (D5; r = .40, 95% CI [.23, .54]) showed the strongest positive associations with overall security. Organizational Effectiveness (D1; r = .26, 95% CI [.07, .42]), Customer Orientation (D2; r = .27, 95% CI [.09, .44]), and Management Philosophy (D6; r = .28, 95% CI [.09, .44]) demonstrated moderate positive relationships with overall security. In contrast, Focus (D4; r = .04, 95% CI [−.14, .23]) showed a negligible association, indicating no meaningful relationship with overall security.

These results address RQ1 by identifying which orientations within each dimension are linked to more desirable security behavior tendencies. A positive correlation between a dimension subscale (D1-D6) and overall security (S) indicates that the reference orientation for that dimension aligns with higher overall security scores. As such, the findings support hypotheses H1, H2, H3, H5, and H6, indicating that the means-oriented, internally driven, strict work discipline, open system, and employee-oriented orientations are associated with more desirable security behaviors than their counterparts. Hypothesis H4 is not supported, as D4's correlation with S (r = 0.04) is negligible, suggesting no difference between professional and local orientations in terms of security behavior tendencies.

**Table 4. Correlations Across Industry Types**

| | Mean | SD | Range | S | D1 | D2 | D3 | D4 | D5 | D6 | S1 | S2 | S3 | S4 | S5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Overall Security (S)** | 35.95 | 7.31 | 39 | | | | | | | | | | | | |
| **Organizational Effectiveness Dimension (D1)** | 4.16 | 1.56 | 8 | .26 | | | | | | | | | | | |
| **Customer Orientation Dimension (D2)** | 4.38 | 1.55 | 8 | .28 | .05 | | | | | | | | | | |
| **Level of Control Dimension (D3)** | 4.37 | 1.58 | 8 | .30 | .11 | .04 | | | | | | | | | |
| **Focus Dimension (D4)** | 4.89 | 1.56 | 8 | .04 | .06 | .05 | .00 | | | | | | | | |
| **Approachability Dimension (D5)** | 5.83 | 1.55 | 6 | .40 | .04 | .13 | .05 | -.03 | | | | | | | |
| **Management Philosophy Dimension (D6)** | 4.33 | 2.00 | 8 | .28 | -.01 | .15 | .09 | -.12 | .27 | | | | | | |
| **Organizational Effectiveness Security (S1)** | 6.03 | 1.77 | 8 | .70 | .22 | .15 | .19 | .15 | .16 | .07 | | | | | |
| **Customer Orientation Security (S2)** | 6.85 | 1.65 | 7 | .71 | .16 | .17 | .22 | .12 | .36 | .12 | .40 | | | | |
| **Level of Control Security (S3)** | 6.58 | 1.58 | 6 | .76 | .19 | .21 | .22 | .03 | .34 | .18 | .47 | .55 | | | |
| **Focus Security (S4)** | 5.96 | 1.96 | 8 | .77 | .20 | .22 | .26 | -.09 | .28 | .22 | .42 | .40 | .53 | | |
| **Approachability Security (S5)** | 6.13 | 1.68 | 7 | .70 | .21 | .21 | .20 | .13 | .27 | .08 | .44 | .43 | .43 | .45 | |
| **Management Philosophy Security (S6)** | 4.40 | 1.91 | 8 | .55 | .09 | .18 | .16 | -.13 | .26 | .44 | .17 | .25 | .25 | .33 | .21 |

Source: Authors own work.

To address RQ2, how the ISC-SJT results compare across the U.S. industries, the first step was to examine the average dimension and security scores by industry. These comparisons can be interpreted in terms of cultural orientations and security behavior tendencies. Table 5 displays the average overall security score, dimension sub-scale scores, and security sub-scale scores for each sector. The maximum possible score is 48 for the overall security scale and 8 for each sub-scale, with higher security scores reflecting more desirable behavior tendencies.

Dimension scores require a more nuanced interpretation. Each score reflects alignment with one of two orientations: scores above 4 correspond to the reference orientation (hypothesized to exhibit more desirable behavior), while scores below 4 align with the opposite. Specifically:

- D1 > 4 = means-oriented; < 4 = goal-oriented
- D2 > 4 = internally driven; < 4 = externally driven
- D3 > 4 = strict discipline; < 4 = easygoing discipline
- D4 > 4 = professional; < 4 = local
- D5 > 4 = open system; < 4 = closed system
- D6 > 4 = employee-oriented; < 4 = work-oriented

As shown in Table 5, industry averages are often close. To assess whether these differences are statistically meaningful, one-way ANOVA tests were conducted using individual participant

scores (Table 6). Assumptions for ANOVA were evaluated using Shapiro–Wilk tests of residual normality and Levene's tests of homogeneity of variance. Although some deviations from normality were observed, homogeneity of variance was generally supported, and given the large sample size, ANOVA and Tukey post-hoc tests were considered appropriate for the analyses. Significant differences were found across industries for seven of the scales (S, D3, S1, S2, S3, S4, S6). Post-hoc analysis using Tukey's method (Table 7) identified the specific industry pairings responsible for these differences.

Among the cultural dimensions, only Level of Control (D3) showed significant variation. Education leaned toward an easygoing culture, while other sectors leaned toward a strict culture. On the security side, significant differences were observed for five of the six sub-scales and the overall security score. Education exhibited the lowest overall security score, while Technology had the highest. Education differed significantly from Technology on S, S1, S4, and S6, and from Government/Military on S1, S2, and S6. Mfg./Heavy Industry also differed from Education on S1. Additional differences were observed between Technology and Healthcare (S1, S6) and between Technology and Gov./Military (S6). While ANOVA indicated overall variability in S3 scores across sectors, post-hoc analysis did not reveal significant pairwise differences. Formal tests of measurement invariance across industries were not conducted. Therefore, industry comparisons should be interpreted cautiously given the absence of formal measurement invariance testing across industries and the internal reliability considerations discussed in Section 4.2.

**Table 5. Average Scores by Industry**

| Industry | Technology | Gov./Military | Manufacturing/Heavy | Healthcare | Education |
|---|---|---|---|---|---|
| **Overall Security (S)** | 38.29 | 36.62 | 35.85 | 35.76 | 33.21 |
| **Organizational Effectiveness Dimension (D1)** | 4.23 | 4.30 | 4.00 | 4.20 | 4.06 |
| **Customer Orientation Dimension (D2)** | 4.42 | 4.50 | 4.20 | 4.26 | 4.50 |
| **Level of Control Dimension (D3)** | 4.42 | 4.49 | 4.74 | 4.52 | 3.67 |
| **Focus Dimension (D4)** | 4.79 | 5.35 | 4.82 | 4.58 | 4.91 |
| **Approachability Dimension (D5)** | 5.88 | 5.89 | 5.56 | 6.17 | 5.67 |
| **Management Philosophy Dimension (D6)** | 4.38 | 3.99 | 4.62 | 4.09 | 4.59 |
| **Organizational Effectiveness Security (S1)** | 6.65 | 6.30 | 6.14 | 5.77 | 5.29 |
| **Customer Orientation Security (S2)** | 7.00 | 7.23 | 6.71 | 6.94 | 6.36 |
| **Level of Control Security (S3)** | 6.79 | 6.80 | 6.79 | 6.32 | 6.18 |
| **Focus Security (S4)** | 6.52 | 5.94 | 5.97 | 6.11 | 5.27 |
| **Approachability Security (S5)** | 6.06 | 6.39 | 5.83 | 6.32 | 6.05 |
| **Management Philosophy Security (S6)** | 5.27 | 3.95 | 4.41 | 4.30 | 4.06 |

Source: Authors own work.

**Table 6. Summary of One-way ANOVA Tests**

| Dependent Variable | F-ratio | p-value | $\eta^2$ [95% CI] | $\omega^2$ [95% CI] |
|---|---|---|---|---|
| **Overall Security (S)** | **4.321** | **.002** | **.05 [.02, .12]** | **.04 [.01, .11]** |
| Organizational Effectiveness Dimension (D1) | 0.415 | .798 | .01 [.00, .05] | .00 [.00, .03] |
| Customer Orientation Dimension (D2) | 0.543 | .705 | .01 [.00, .05] | .00 [.00, .04] |
| **Level of Control Dimension (D3)** | **4.608** | **.001** | **.05 [.02, .12]** | **.04 [.01, .11]** |
| Focus Dimension (D4) | 2.247 | .064 | .03 [.01, .08] | .01 [.00, .07] |
| Approachability Dimension (D5) | 1.507 | .200 | .02 [.01, .07] | .01 [.00, .06] |
| Management Philosophy Dimension (D6) | 1.372 | .243 | .02 [.01, .07] | .00 [.00, .06] |
| **Organizational Effectiveness Security (S1)** | **6.110** | **.000** | **.07 [.03, .15]** | **.06 [.02, .13]** |
| **Customer Orientation Security (S2)** | **2.652** | **.033** | **.03 [.01, .09]** | **.02 [.00, .08]** |
| **Level of Control Security (S3)** | **2.445** | **.047** | **.03 [.01, .09]** | **.02 [.00, .08]** |
| **Focus Security (S4)** | **3.563** | **.007** | **.04 [.02, .10]** | **.03 [.00, .09]** |
| Approachability Security (S5) | 1.203 | .309 | .01 [.00, .06] | .00 [.00, .05] |
| **Management Philosophy Security (S6)** | **5.168** | **.000** | **.06 [.03, .13]** | **.05 [.05, .12]** |

Predictor variable for all tests = Industry type
Source: Authors own work.

**Table 7. Post-hoc Analysis**

| | | Mean Differences (Industry 1 – Industry 2) | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Industry 1** | **Industry 2** | **S** | **D3** | **S1** | **S2** | **S3** | **S4** | **S6** |
| Education | Technology | **-5.08*** ** | **-0.75*** | **-1.36*** ** | -0.64 | -0.61 | **-1.25**** | **-1.21**** |
| | Gov./Military | -3.41 | **-0.82*** | **-1.01**** | **-0.87*** | -0.62 | -0.67 | 0.11 |
| | Mfg./Heavy | -2.64 | **-1.07*** ** | **-0.85*** | -0.35 | -0.61 | -0.7 | -0.35 |
| | Healthcare | -2.55 | **-0.85*** | -0.48 | -0.58 | -0.14 | -0.84 | -0.24 |
| Technology | Gov./Military | 1.67 | -0.07 | 0.35 | -0.23 | -0.01 | 0.58 | **1.32*** ** |
| | Mfg./Heavy | 2.44 | -0.32 | 0.51 | 0.29 | 0.00 | 0.55 | 0.86 |
| | Healthcare | 2.53 | -0.1 | **0.88*** | 0.06 | 0.47 | 0.41 | **0.97*** |
| Gov./Military | Mfg./Heavy | 0.77 | -0.25 | 0.16 | 0.52 | 0.01 | -0.03 | -0.46 |
| | Healthcare | 0.86 | -0.03 | 0.53 | 0.29 | 0.48 | -0.17 | -0.35 |
| Mfg./Heavy | Healthcare | 0.09 | 0.22 | 0.37 | -0.23 | 0.47 | -0.14 | 0.11 |

Note: Asterisks denote statistically significant differences based on Tukey's HSD post-hoc tests following significant omnibus ANOVAs ($p < .05$*, $p < .01$**, $p < .001$***). Effect sizes and 95% confidence intervals are reported at the omnibus level (see Table 6).

Source: Authors own work.

### *4.2 Measurement Properties*

This subsection evaluates the measurement properties of the ISC-SJT, including its internal reliability and initial convergent validity. Analyses focused on the dimension & security score for examining internal reliability. Dimension scores were used for analyses involving convergent validity, consistent with their intended interpretive use. For initial Exploratory Factor Analysis see Appendix 5.

Internal reliability was evaluated using both Cronbach's alpha and McDonald's omega. Alpha is included because it is a commonly reported internal reliability measure. However, it may underestimate internal reliability for situational judgment tests due to their heterogeneous content and multidimensional structure (Whetzel and McDaniel, 2009). McDonald's omega was therefore also calculated, as it provides a reliability estimate that allows items to differ in their relationships with the underlying dimensions and is well suited for complex, multidimensional measures (Revelle and Zinbarg, 2009). Omega was computed for the overall ISC-SJT and for each dimension separately based on the dimension & security score. Reliability estimates for each scale are reported in Table 8.

Overall, reliability estimates indicated acceptable internal consistency for the full scale, with variation across dimensions reflecting differences in the consistency of items within each dimension. Lower reliability estimates for individual dimensions were expected given the small number of items per dimension and the variation in item content. As a result, findings at the dimension level should be interpreted cautiously, and the subscale dimension scores are best viewed as exploratory indicators of cultural tendencies.

**Table 8. Summary of Internal Reliability**

| Dimension | $\omega_t$ | α |
|---|---|---|
| Overall | .77 | .73 |
| Organizational Effectiveness | .31 | .29 |
| Customer Orientation | .39 | .35 |
| Level of Control | .33 | .29 |
| Focus | .38 | .37 |
| Approachability | .42 | .39 |
| Management Philosophy | .56 | .54 |

Source: Authors own work.

To explore preliminary convergent validity, ISC-SJT dimension scores were compared with participants' responses to the slider scale items described in Section 3.5, which asked participants to indicate the cultural orientation they believed best reflected their organization. These slider items were designed to capture broad organizational culture orientations and provide an initial check of whether participants' ISC-SJT responses aligned with the orientations they selected on the sliders. Table 9 presents correlations between the ISC-SJT dimension scores and the corresponding slider ratings.

**Table 9. Correlations Across Dimension Scores and Slider Scales**

| | Mean | SD | Range | D1 | D2 | D3 | D4 | D5 | D6 |
|---|---|---|---|---|---|---|---|---|---|
| **Organizational Effectiveness Slider** | 3.19 | 1.78 | 7 | .004 | -.013 | -.060 | .077 | -.073 | -.141 |
| **Customer Orientation Slider** | 3.96 | 2.02 | 7 | .124 | .089 | .010 | .118 | .101 | -.027 |
| **Level of Control Slider** | 4.35 | 1.88 | 7 | .068 | .035 | .239 | -.053 | -.036 | .093 |
| **Focus Slider** | 4.92 | 1.73 | 7 | .051 | -.032 | .045 | -.097 | .077 | .117 |
| **Approachability Slider** | 5.21 | 1.86 | 7 | .061 | .151 | .097 | .013 | .172 | -.004 |
| **Management Philosophy Slider** | 4.02 | 2.00 | 7 | .055 | .222 | -.004 | -.034 | .182 | .020 |

Source: Authors own work.

As shown in Table 9, correlations between the ISC-SJT dimension scores and the slider scale ratings were generally small in magnitude. This pattern is expected given that the slider items

were brief, single-item indicators intended to broadly capture organizational culture orientations. Despite their simplicity, several dimensions showed positive associations with their conceptually corresponding slider items. For example, Level of Control slider ratings were positively related to the Level of Control ISC-SJT dimension (D3), and Approachability slider ratings showed positive associations with the Approachability dimension (D5). Other associations were weaker or inconsistent, which is also expected given the coarse nature of the slider measures and the format of the ISC-SJT. Overall, these results provide exploratory evidence that ISC-SJT dimension scores vary in ways that are broadly consistent with participants' self-reported organizational culture orientations. Because the slider measures were single-item indicators designed only to capture broad organizational culture perceptions, these results should be interpreted as an initial validation step rather than definitive evidence of convergent validity.

### *4.3 Feedback Results*

Following each ISC-SJT item, participants were asked whether they found the situation "reasonable for something that could actually happen within your organization." This question aimed to assess item relevancy across the five sectors and addresses RQ3. Agreement ranged from 64% to 91%, with an average of 79% of participants affirming the scenarios were realistic within their organizational context.

Participants also responded to two general feedback questions regarding their experience with the ISC-SJT and its format. Over 70% provided positive feedback about their interest and enjoyment in completing the survey. One participant from the Manufacturing/Heavy sector noted, "[The survey] definitely made me think more than other surveys... It was fun, interesting, and thought-provoking." Approximately 80% agreed that the SJT format was engaging. A participant from the Education sector commented, "I liked the 4 options and picking the most likely and least likely. It seems way more realistic than just picking what would happen... or going on an arbitrary scale from 1–7." Common themes across responses highlighted that participants found the ISC-SJT to be a unique format compared to other surveys they have taken, and the situations were relatable and thought-provoking.

## 5. Discussion

This study demonstrates the potential of the ISC-SJT for assessing the underlying assumptions that shape information security culture and related behavior tendencies within organizations. Unlike traditional assessments that often rely on abstract Likert-scale ratings, the

ISC-SJT leverages realistic, situationally grounded items to elicit participant responses that reflect actual security reasoning and cultural alignment. By capturing both the type of cultural orientation and the desirability of security behaviors, the ISC-SJT offers an insightful lens through which organizations can evaluate how their employees perceive, interpret, and respond to information security situations. The following discussion highlights the key insights of the study, contributions, and considerations for future research and application.

### *5.1 Key Findings and Interpretations*

The results generally support hypotheses H1, H2, H3, H5, and H6, suggesting that means-oriented, internally driven, strict work discipline, open system, and employee-oriented cultural orientations tend to be associated with more desirable security behavior tendencies than their counterpart orientations. However, given the modest internal reliability estimates for the dimension subscales, these relationships should be interpreted cautiously and considered preliminary. For the Focus dimension, however, neither the local nor professional orientation was predictive of a higher overall security score, suggesting no clear relationship with security behavior tendencies. These findings offer practical value for organizations seeking to influence security behaviors through cultural alignment. Although organizational culture is difficult to change, identifying the existing culture type allows security initiatives to be designed in ways that work with, rather than against, the culture. For example, training could be customized to reinforce desirable security behaviors based on the culture type.

The results also provide industry-specific insights into information security culture. As shown in Table 10, each industry exhibits a predominant culture type across the six dimensions with varying overall security scores. These results can serve as a reference point for U.S. organizations evaluating their own cultural alignment and security posture.

Among the six cultural dimensions, Level of Control (D3) was the only one to show statistically significant differences across industries. The Education sector was the only industry that leaned toward an easygoing work discipline, and it also had the lowest overall security score, more than a standard deviation below the highest-scoring industry. Additionally, Level of Control had the second-highest correlation with the overall security score. While the data does not support a definitive causal link, the relationship between an easygoing culture and lower security scores in the Education sector warrants further investigation in future research.

**Table 10. Overall Security Score and Type of Culture by Industry**

| Industry | Technology | Gov./Military | Mfg./Heavy | Healthcare | Education |
|---|---|---|---|---|---|
| **Overall Security (S)** | 38.29 | 36.62 | 35.85 | 35.76 | 33.21 |
| **Organizational Effectiveness (D1)** | Means-oriented | Means-oriented | *Neutral* | Means-oriented | Means-oriented |
| **Customer Orientation (D2)** | Internally driven | Internally driven | Internally driven | Internally driven | Internally driven |
| **Level of Control (D3)** | Strict | Strict | Strict | Strict | Easygoing |
| **Focus (D4)** | Professional | Professional | Professional | Professional | Professional |
| **Approachability (D5)** | Open system | Open system | Open system | Open system | Open system |
| **Management Philosophy (D6)** | Employee-oriented | *Neutral* | Employee-oriented | Employee-oriented | Employee-oriented |

Source: Authors own work.

As shown in Table 5, Approachability (D5) was the highest-scoring cultural dimension across all five industries, indicating that an open system culture is prominent within the industries. According to Hofstede *et al*. (2010), this dimension maps closely to the Uncertainty Avoidance dimension in national culture. The U.S. is characterized by weak uncertainty avoidance, which aligns with an open system orientation in organizational culture. This alignment is reflected in the ISC-SJT results, where open system responses were selected at much higher rates across all industries. Therefore, assessments of organizations or industries outside the United States may be needed to receive a closed system result.

Participant feedback further supports the relevance and realism of the ISC-SJT. On average, 79% of participants agreed that the situations presented could reasonably occur within their organization, addressing RQ3. This reinforces one of the primary reasons for using the SJT format: its ability to present contextually meaningful and realistic scenarios. Open-ended feedback also highlighted the engaging and relatable nature of the ISC-SJT format, validating its potential to increase participant engagement while producing more meaningful insights.

### *5.2 Contributions*

This study offers several key contributions to both theoretical understanding and practical assessment of ISC, as well as the methodology used to evaluate it. It builds directly upon well-established organizational culture research rather than incorporating it superficially. It expands on existing ISC research around Hofstede's organizational culture dimensions to support the idea that certain cultural orientations promote desirable security behaviors. This research uses SJTs to

evaluate complex, multi-dimensional constructs like ISC. While SJTs are commonly used in organizational psychology and personnel selection, this study presents a novel application for assessing ISC. The ISC-SJT engages participants with realistic, contextually relevant situations that mirror workplace decision-making, enhancing result relevance and offering leadership actionable insights to guide security efforts.

### *5.3 Limitations and Future Research*

This study has several limitations that suggest directions for future research and refinement of the ISC-SJT. First, the instrument is relatively long. Among the 330 participants, the average completion time was approximately 38 minutes. Although participant feedback indicated strong engagement with the SJT format, the length may limit feasibility in applied organizational settings due to other priorities. Future versions could reduce administration time by removing demographic and feedback items or developing shorter versions tailored to specific assessment goals.

A related limitation concerns reliability at the subscale level. Each dimension was assessed using a small number of items, which constrains internal consistency estimates and limits the precision of individual subscale scores. As a result, conclusions drawn from individual cultural dimensions should be interpreted with care. In addition, exposure to multiple SJT items may contribute to scenario fatigue. Future research should evaluate test–retest and parallel-forms reliability, as these forms of reliability were beyond the scope of the present study.

Another limitation relates to the structural features of the ISC-SJT scoring approach. Because both the cultural dimension scores and security behavior scores are derived from the same forced-choice item structure, observed correlations between cultural dimensions and security outcomes should be interpreted with appropriate caution.

This study focused on establishing content validity through theory-driven item development and expert review. Preliminary convergent validity was also explored. While this provides an important foundation, additional validation work is needed to support broader application. Future research should examine convergent and discriminant validity using established organizational culture and information security measures, such as the HAIS-Q or ISCA. Predictive validity should also be explored by linking ISC-SJT scores to outcomes such as policy compliance, observable security behaviors, or training effectiveness. These efforts would strengthen the instrument's usefulness for benchmarking, tailoring security interventions, and informing organizational training efforts.

Interpretation of industry-level findings should also be tempered by the characteristics of the sample. Participants were recruited from a U.S.-based Prolific quota sample, which limits generalizability beyond this context. Dimensions closely tied to national culture, such as Approachability (D5), may reflect broader U.S. cultural norms rather than industry-specific effects. Future research should replicate this study across national contexts to better disentangle organizational and national cultural influences on information security behavior.

Finally, this study did not assess measurement invariance across groups. Given the flexible and context-dependent nature of situational judgment tests, future work should evaluate measurement invariance when the ISC-SJT is adapted for different populations or research objectives. Rather than treating the ISC-SJT as a fixed instrument, future research may intentionally modify or develop items aligned with specific organizational contexts, positioning the ISC-SJT as a configurable assessment framework rather than a static scale.

## 6. Conclusion

This study developed and evaluated the ISC-SJT as a theory-driven tool for assessing the underlying assumptions that shape information security culture. By applying a situational judgment test approach to the ISC domain, this work introduces a novel method for capturing how employees perceive and tend to respond to security-related situations. Using the ISC-SJT, data was collected from employees across five U.S. industries—Technology, Government/Military, Manufacturing/Heavy, Healthcare, and Education—revealing the type of culture and security behavior tendencies in each sector. The results indicate that means-oriented, internally driven, strict work discipline, open system, and employee-oriented cultures are associated with more desirable security behaviors than their counterparts. The Education sector stood out by exhibiting an easygoing work discipline culture, which may explain its lower overall security score.

Taken together, these findings demonstrate the ISC-SJT's potential for organizational use and provide an initial industry baseline for future research. With further refinement and validation, the ISC-SJT may support organizations in benchmarking their information security culture, identifying areas for improvement, and aligning security initiatives with cultural assumptions. More broadly, this work positions situational judgment testing as a promising approach for advancing both research and practice in information security culture.

## Acknowledgements

Phillips and Moore gratefully acknowledge support from the US National Science Foundation (NSF) Award No. 2147505. The authors acknowledge support from Tulsa Innovation Labs via the Cyber Fellows initiative.

**References**

Adams, J. (2003), "Risk and Morality: Three Framing Devices", Ericson R.V. and Doyle A. (Ed.), *Risk and Morality,* University of Toronto Press, Canada, pp.87-106.

Alfawaz, S.M. (2011), "Information security management: A case study of an information security culture", Thesis, Queensland University of Technology.

Alnatheer, M., Chan, T., and Nelson, K. (2012), "Understanding and Measuring Information Security Culture", in *Pacific Asia Conference on Information Systems (PACIS) 2012 Proceedings*.

Beautement, A., Becker, I., Parkin, S., Krol, K., and Sasse, A. (2016), "Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours," in *Proceedings of the Twelfth Symposium on Usable Privacy and Security*, USENIX Associations, Denver, CO.

Booker, Q. and Rebman Jr., C.M. (2023), "Factors influencing the development of a successful cybersecurity culture", *Issues in Information Systems*, 24, 4, pp.51-65, available at: https://doi.org/10.48009/4_iis_2023_105.

Bruin, M. (2022), "Individual and Contextual Variables of Cyber Security Behavior", Thesis, University of London.

Cameron, K. (n.d.), "An Introduction to the Competing Values Framework", available at: https://www.thercfgroup.com/files/resources/an_introduction_to_the_competing_values_framework_white_paper-pdf-28512.pdf.

Chang, S.E. and Lin, C.-S. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, 107, 3, pp.438-458, available at: https://doi.org/10.1108/02635570710734316.

Cohen, J. (1977), *Statistical Power Analysis for the Behavioral Sciences*, Elsevier, available at: https://doi.org/10.1016/C2013-0-10517-X.

Da Veiga, A. (2015), "An Information Security Training and Awareness Approach (ISTAAP) to Instill an Information Security-Positive Culture", in Clarke, N. and Furnell, S. (Ed.), *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, Plymouth University, Plymouth, UK, pp.95-107.

Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, 29, 2, pp.196-207, available at: https://doi.org/10.1016/j.cose.2009.09.002.

Da Veiga, A. and Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers & Security*, 49, pp.162-176, available at: https://doi.org/10.1016/j.cose.2014.12.006.

Dodge, C.E, Fisk, N., Burruss, G.W., Moule Jr., R.K. and Jaynes, C.M. (2023), "What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory", *Criminology & Public Policy*, 22, 4, pp. 849-868, available at: https://doi.org/10.1111/1745-9133.12641

Failla, R.J. (2020), "The influence of organizational culture on cybersecurity governance in breach organizations", Thesis, Capitol Technology University.

Gangire, Y., Da Veiga, A. and Herselman, M. (2021), "Assessing information security behaviour: a self-determination theory perspective", *Information & Computer Security*, available at: https://doi.org/10.1108/ICS-11-2020-0179.

Grill, M., Sommestad, T., Karlzén, H., Pousette, A. (2025), "Training for improved information security culture: a longitudinal randomized controlled trial", *Information & Computer Security*, available at: https://doi.org/10.1108/ICS-08-2024-0189.

Hoffman, F. (2021), "Assessing U.S. and Slovenian organizational security culture with Hofstede's national culture framework", *Issues in Information Systems*, 22, 3, pp.114-128, available at: https://doi.org/10.48009/3_iis_2021_127-141.

Hofstede, G., Hofstede, G.J., and Minkov, M. (2010), *Cultures and Organizations: Software of the Mind, Third Edition*, McGraw Hill.

Karlsson, F., Åström, J. and Karlsson, M. (2015), "Information security culture – state-of-the-art review between 2000 and 2013", *Information & Computer Security*, 23, 3, pp.246-285, available at: https://doi.org/10.1108/ICS-05-2014-0033.

Karlsson, M., Karlsson, F., Åström, J. and Denk, T. (2022), "The effect of perceived organizational culture on employee's information security compliance", *Information & Computer Securit*y, 30, 3, pp.382-401, available at: https://doi.org/10.1108/ICS-06-2021-0073.

Kraemer, S. and Carayon, P. (2005), "Computer and Information Security Culture: Findings from two studies," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* pp.1483–1488.

Martins, N. and Da Veiga, A. (2015), "An Information Security Culture Model Validated with Structural Equation Modelling", in Clarke, N. and Furnell, S. (Ed.), *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, Plymouth University, Plymouth, UK, pp.11-21.

McDaniel, M.A., Hartman, N.S., Whetzel, D.L., and Grubb, W.L. (2007), "Situational Judgement Tests, Response Instructions, and Validity: A Meta-analysis", *Personnel Psychology*, 60, 1, pp.63-91, available at: https://doi.org/10.1111/j.1744-6570.2007.00065.x.

Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017), "Information security policy compliance behavior based on comprehensive dimensions of information security culture," in *Proceedings of the 2017 International Conference on Information System and Data Mining*, pp.56-60, available at: https://doi.org/10.1145/3077584.3077593.

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019), "An analysis on the dimensions of information security culture concept: A review", *Journal of Information Security and Applications*, 44, pp. 12–22, available at: https://doi.org/10.1016/j.jisa.2018.11.003

Okere, I., Van Niekerk, J. and Mariana, C. (2012), "Assessing information security culture" A critical analysis of current approaches", in *2012 Information Security for South Asia*, pp.1-8, doi: 10.1109/ISSA.2012.6320442.

Oostrom, J. K., De Soete, B., & Lievens, F. 2015. "Situational Judgment Testing: A review and some new developments," *Employee Recruitment, Selection, and Assessment: Contemporary Issues for Theory and Practice*, pp. 172–189.

Orehek, S. and Petrič, G. (2021), "A systematic review of scales for measuring information security culture", *Information & Computer Security*, 29, 1, pp.133-158, doi: 10.1108/ICS-12-2019-0140.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security*, 42, pp.165-176, available at: http://dx.doi.org/10.1016/j.cose.2013.12.003.

Phillips, S., Brummel, B., Aurigemma, S., and Moore, T. (2023), "Information Security Culture: A look Ahead at Measurement Methods," in Dhillon, G. Furnell, S. and Demetis, D. (Ed.s), *Proceedings of the 22nd Annual Information Institute Conference*, Las Vegas, NV, available at: http://029e2c6.netsolhost.com/II-Proceedings/2023/15.pdf.

Phillips, S., Aurigemma, S., Brummel, B., and Moore, T. (2024), "Leveraging Situational Judgment Tests to Measure Behavioral Information Security," in *Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS)*, pp.4714- 4723, available at: https://hdl.handle.net/10125/106951.

Ployhart, R.E., and MacKenzie, W.I. (2011), "Situational judgment tests: A critical review and agenda for the future," *APA Handbook of Industrial and Organizational Psychology, Vol 2: Selecting and Developing Members for the Organization*, pp. 237–252, available at: https://psycnet.apa.org/doi/10.1037/12170-008.

Ployhart, R. E., & Ward, A. K. 2013. "Situational Judgment Measures," APA Handbook of Testing and Assessment in Psychology Vol. 1: Test Theory and Testing and Assessment in Industrial and Organizational Psychology, pp. 551–564.

Pollard, S. and Cooper-Thomas, H.D. (2015), "Best practice recommendations for Situational Judgment tests," *Australasian Journal of Organisational Psychology*, 8, available at: https://doi.org/10.1017/orp.2015.6.

Revelle, W. and Zinbarg, R.E. (2009), "Coefficients Alpha, Beta, Omega, and the glb: Comments on Sijtsma" *Psychometrika*, 74, pp. 145-154, available at: https://doi.org/10.1007/s11336-008-9102-z.

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., and Ponnet, K. (2020), "Measuring the security culture in organizations: a systematic overview of existing tools", *Security Journal*, 34, pp.340-357, available at: https://doi.org/10.1057/s41284-020-00228-4.

Schein, E.H. and Schein, P. (2016), *Organizational Culture and Leadership*, 5, John Wiley & Sons.

Schlienger, T. and Teufel, S. (2002), "Information Security Culture: The Socio-Cultural Dimension," in *IFIP TC11 International Conference on Information Security (Sec2002),* Kluwer Academic Publishers, Cairo, Egypt.

Sherif, E., Furnell, S. and Clarke, N. (2015), "An Identification of Variables Influencing the Establishment of Information Security Culture", in Tryfonas, T. and Askoxylakis (Ed.s),

*Human Aspects of Information Security, Privacy and Trust (HAS 2025)*, pp.436-448, available at: https://doi.org/10.1007%2F978-3-319-20376-8_39.

Solomon, G. and Brown, I. (2021), "The influence of organisational culture and information security culture on employee compliance behavior", *Journal of Enterprise Information Management*, 34, 4, 99.1203-1228, available at: https://doi.org/10.1108/JEIM-08-2019-0217.

Sommestad, T., Karlzén, H. and Hallberg, J. (2019), "The Theory of Planned Behavior and Information Security Policy Compliance," *Journal of Computer Information Systems*, 59, 4, pp.344-353, available at: https://doi.org/10.1080/08874417.2017.1368421.

Stan, B.E., Staiculescu, A.R. and Predoana, M.-R. (2023), "Security Culture from Communism to Democracy," *Romanian Intelligence Studies Review*, 30, pp.112-129.

Tang, M., Li, M. and Zhang, T. (2016), "The impacts of organizational culture on information security culture: A case study," *Information Technology and Management*, 17, 2, pp.179–186, available at: https://doi.org/10.1007%2Fs10799-015-0252-2.

*The Culture Factor Group* (n.d.), *Organisational culture: What you need to know*, available at: https://www.theculturefactor.com/organisational-culture (accessed 18 July 2025).

Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S. (2021), "Developing a cyber security culture: Current practices and future needs," *Computers & Security*, 109, available at: https://doi.org/10.1016/j.cose.2021.102387.

Van Niekerk, J. and Von Solms, R. (2010), "Information security culture: A management perspective," *Computers & Security*, 29, 4, pp. 476–486, available at: https://doi.org/10.1016/j.cose.2009.10.005.

*Verizon Business* (2025), "2025 Data Breach Investigations Report", available at: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf (accessed 16 July 2025).

Weekley, J.A. and Ployhart, R.E. (2005), "An Introduction to Situational Judgment Testing. Situational judgment tests: Theory, Measurement and Application," *Psychology Press*, Taylor & Francis Group, pp.1-10.

Whetzel, D.L. and McDaniel, M.A. (2009), "Situational judgment tests: An overview of current research," *Human Resource Management Review*, 19, 3, pp.188–202, available at: http://dx.doi.org/10.1016/j.hrmr.2009.03.007.

Zhang, X. and Yang, H. (2019), “Impact of Cross-Culture on Behavioral Information Security,” *Journal of Integrated Design and Process Science*, 22, 2, pp.63–80, available at: https://doi.org/10.3233%2FJID180003.