Measuring Dimensions of Information Security Culture Across Industries with Situational Judgement Tests

Early stage paper

Samantha Phillips
School of Cyber Studies
College of Engineering & Computer Science
The University of Tulsa
samantha-phillips@utulsa.edu

Bradley Brummel
University of Houston
bjbrummel@uh.edu

Sal Aurigemma
University of Hawaii
The University of Tulsa
sa8@hawaii.edu

Tyler Moore
School of Cyber Studies
College of Engineering & Computer Science
The University of Tulsa
tyler-moore@utulsa.edu

ABSTRACT

The human element of an organization's information security posture is influenced by its information security culture (ISC). This paper describes the creation of an information security culture situational judgement test (ISC-SJT) used to assess the underlying basic assumptions of employees surrounding an organization's ISC to determine the type of culture and the security behavioral tendencies that are present. This research views information security culture as both being influenced by security behaviors and reflected in security behaviors. Hofstede et al.'s six organizational culture dimensions were used as part of the ISC-SJT's underlying measurement to determine the type of culture. The research platform Prolific was utilized to recruit 330 participants who work full-time in the United States to complete the ISC-SJT. The participants were equally distributed across the Technology, Government/Military, Manufacturing/Heavy, Healthcare, and Education industries to facilitate comparisons between industries within the United States. The

ISC-SJT results revealed that certain types of cultures exhibit more desirable security behavioral tendencies. Furthermore, the results showed the prominent type of culture and security behavioral tendencies for each of the five industries and identified significant differences between them.

Keywords

Information security culture, Situational judgement test, Organizational culture dimensions, Security behaviors

INTRODUCTION

The success, or failure, of an organization's information security efforts can be greatly impacted by its employees, often referred to as "the human element". According to the 2024 Verizon Data Breach Investigation Report (DBIR), the human element was involved in 68% of the 10,626 confirmed data breaches they assessed. With the human element contributing to the majority of 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 factor to consider is an organization's information security culture (ISC). Information security culture (also commonly referred to as cybersecurity culture and security culture) refers to "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).

Information security culture, and organizational culture in general, is a complex concept that is highlighted by the many unique perspectives and research endeavors focused on it within the ISC field and beyond. Typically, it builds upon foundational concepts and theories from the field of organizational psychology (Nasir et al., 2019; Uchendu et al., 2021). The research presented in

this paper is founded on the work of Edgar Schein and Geert Hofstede, both prominent culture researchers within the field of organizational psychology. Edgar Schein developed a Three-Level Model of culture based on the visibility of cultural phenomenon (Schein & Schein, 2016, p. 17). The three levels of the model are artifacts, espoused beliefs and values, and underlying basic assumptions. Hofstede et al. (2010) on the other hand, identified six dimensions of organizational culture that reflect perceived shared practices within an organization. Each of the six dimensions are comprised of two orientations that reflect opposite cultures. We build on these foundations in this paper by developing and evaluating an information security culture situational judgement test (ISC-SJT). The ISC-SJT is used to assess the underlying basic assumptions of employees to determine the type of culture, based on the dimensions from Hofstede et al., and security behavioral tendencies present within an organization.

This ISC research takes the perspective of adding information security to an organization's culture rather than viewing it as an entirely separate concept. By understanding the type of culture present within an organization, information security initiatives can be aligned with the culture, rather than against it, to improve security behavioral tendencies. The ISC-SJT aims to help an organization understand where their ISC is organically, rather than where leadership thinks the culture is, and alleviate discontinuity between information security initiatives and end-users.

The research platform Prolific was utilized to recruit 330 participants across five industries (Technology, Government/Military, Manufacturing/Heavy, Healthcare, and Education) within the United States to complete the ISC-SJT survey. ISC research is limited within the United States, so the study aims to contribute to that area of ISC research. While differences can be found between organizations within the same industry, cultural variations can be exhibited by industry (Schein &

Schein, 2016, p. 281) especially in regard to perceived shared practices (Hofstede et al., 2010). The following questions guide the research presented in this paper:

Primary Research Question:

How can a situational judgment test reveal the underlying assumptions employees have about the type of information security culture and security behavioral tendencies present within their organization?

Secondary Research Questions:

- Does one orientation, for each of the 6 organizational culture dimensions, exhibit more desirable security behavioral tendencies than its counterpart orientation?
- How do the results of the situational judgement test compare across the Education, Healthcare, Manufacturing/Heavy Industry, Technology, and Government/Military industries within the United States?
- To what extent are the situational judgement test items applicable across all identified industries?

BACKGROUND AND RELATED WORKS

The first part of this section discusses the three levels of Schein's culture model. The second part provides an overview of the six organizational culture dimensions established by Hofsted et al. (2010). The third part outlines the situational judgement test method, and the fourth part focuses on related works within the field of information security culture research.

Three-Level Model of Culture

A founding father of organizational culture research, Edgar Schein, established a three-level model of culture to classify cultural phenomenon (Schein & Schein, 2016, p. 17). The model consists of

the level's artifacts, espoused beliefs and values, and underlying basic assumptions. The term level refers to "the degree to which the cultural phenomenon is visible to you as participant or observer" (Schein & Schein, 2016, p. 17). The three levels are intertwined, build upon each other, and work together to create an organization's overall culture. Figure 1 provides a visual representation of the model along with information security examples for each level.

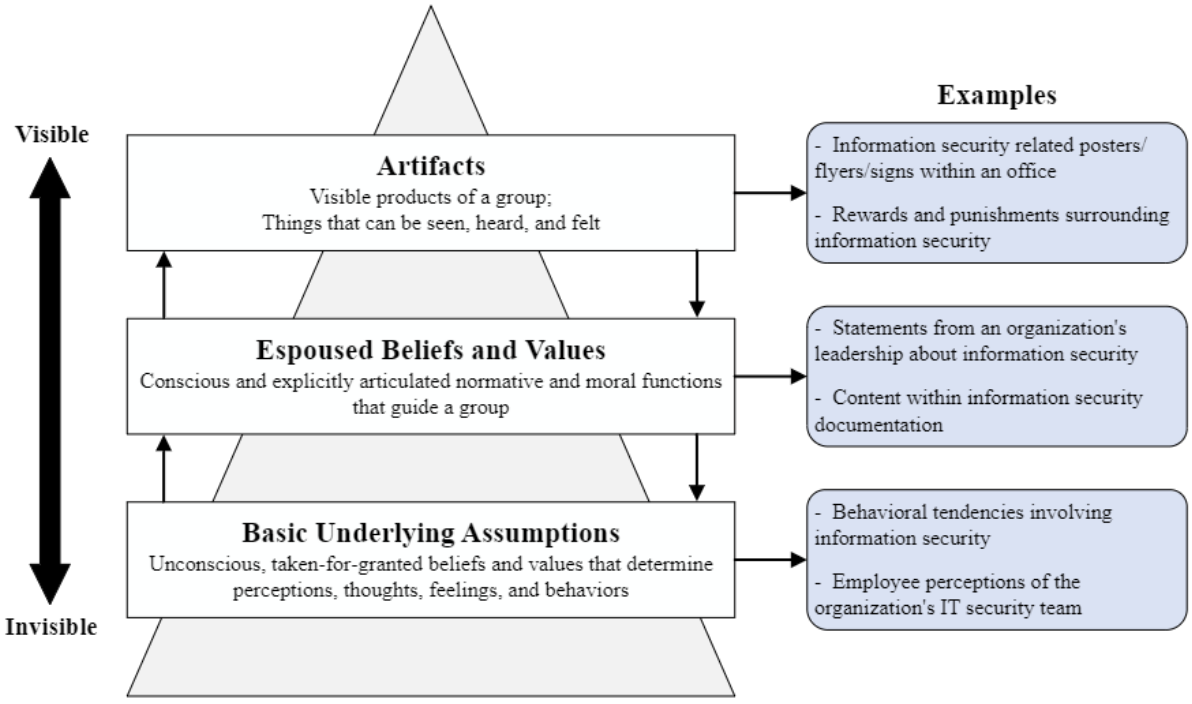

Figure 1: Schein's Three-Level Model of Culture

Artifacts. According to Schein & Schein, artifacts are thought of as "the phenomena that you would see, hear, and feel when you encounter a new group within an unfamiliar culture" (Schein & Schein, 2016, p. 17), including visible and feelable structures and processes and observed behaviors. Artifacts are the most tangible part of an organization's culture. Examples include the physical environment, technologies, products, artistic creations, styles, myths and stories, observable rituals and ceremonies, organizational charts, and published values of the organization. The language used by employees to speak to each other and about things, along with manners of

address and emotional displays, are considered artifacts as well. For example, posters/flyers/signs relating to information security displayed throughout an office building and rewards and punishment for security related behaviors could be regarded as artifacts. The artifact level is easy to observe but hard to decipher without further context (Schein & Schein, 2016, p. 18). If an observer tries to understand the underlying assumptions of an organization based solely on the observed artifacts, their interpretations may reflect projections of their own cultural background.

Espoused Beliefs and Values. Espoused beliefs and values are the second/middle level of the culture model (Schein & Schein, 2016, p. 19-21). The espoused beliefs and values level refers to how an organization's members use beliefs, values, norms, and rules of behavior to depict the culture to themselves and others. This level answers the question "why we do it that way" within an organization's culture. Examples of espoused beliefs and values include ideals, goals, aspirations, ideologies, rationalizations, moral or ethical rules, and organizational strategies and goals. The espoused beliefs and values of an organization's culture "remain conscious and are explicitly articulated because they serve the normative or moral function of guiding members of the group as to how to deal with certain key situations as well as in training new members how to behave" (Schein & Schein, 2016, p. 20). For example, statements made by an organization's leadership about security or policy documents could reflect the espoused beliefs and values of an organization's ISC. Furthermore, the espoused beliefs and values of an organization may or may not align with the underlying basic assumptions held by the members of an organization (Schein & Schein, 2016, p. 21). Therefore, when analyzing the espoused beliefs and values of an organization's culture, it must be determined if they are consistent with the underlying basic assumptions, they are part of the ideology or philosophy of the organization, or if they are aspirational.

Underlying Basic Assumptions. Espoused beliefs and values can leave areas of behavior unexplained, which is where the third level comes into play (Schein & Schein, 2016, p. 21). The third level of the model, underlying basic assumptions, is the DNA of an organization's culture (Schein & Schein, 2016, p. 7). These basic assumptions "consist of the taken-for-granted, nonnegotiable beliefs, values, and behavioral assumptions" (Schein & Schein, 2016, p. 10). Understanding the underlying basic assumptions of an organization's culture is key to deciphering patterns, correctly predicting future behavior, and obtaining an in-depth understanding of the culture (Schein & Schein, 2016, p. 21). These assumptions determine the behaviors, perceptions, thoughts, and feelings of the organization's employees (Schein & Schein, 2016, p. 18). In addition, the assumptions help define what organization members should pay attention to, what things mean, how they should emotionally react, what actions they should take in varying situations, and provides them with a sense of identity (Schein & Schein, 2016, p. 22). For example, ISC underlying basic assumptions could be reflected in security behavioral tendencies and employee perceptions of an organization's IT security team.

Organizational Culture Dimensions

While Schein focused on the levels of organizational culture, Hofstede's research focused on identifying dimensions both at the national and organizational culture levels (Hofstede et al., 2010). According to Hofstede et al., the two types of cultures, national and organizational, "are of a different nature" (2010, p. 346). The different mix of values and practices present within the two types of cultures are the basis for their differences. National cultures consist mainly of the basic values that are acquired through a person's upbringing and organizational cultures consist mainly of the practices established within an organization (Hofstede et al., 2010). Between the years of 1985 and 1987, Hofstede and colleagues conducted a research project under the Institute for

Research on Intercultural Cooperation (IRIC). The results from the IRIC research project were the foundation for establishing six organizational culture dimensions that reflect perceived shared practices within an organization. Each of the six dimensions consists of two opposite orientations, neither of which is inherently better than the other, and are independent of each other and can occur in all possible combinations. Aligning an organization's information security practices with the dimensions could provide security leadership with insights on how to successfully integrate security initiatives and improve security behaviors based on their organization's type of culture.

Organizational Effectiveness. The organizational effectiveness dimension consists of the orientations means-oriented and goal-oriented (Hofstede et al., 2010; The Culture Factor, n.d.). In a means-oriented culture, the focus is placed on how work is carried out (The Culture Factor, n.d.). In an organization that is highly associated with a means-oriented culture, employees think of themselves as avoiding risk and putting forth limited effort in their jobs (Hofstede et al., 2010; The Culture Factor, n.d.). In contrast, a goal-oriented culture is focused on achieving specific goals or results, even if there is substantial risk involved. Members of a goal-oriented culture likely perceive themselves as comfortable in unknown situations and putting in maximal effort (Hofstede et al., 2010).

Customer Orientation. The customer orientation dimension consists of the orientations internally driven and externally driven (Hofstede et al., 2010; The Culture Factor, n.d.). In an internally driven culture, there is a strong emphasis placed on business ethics, honesty, and following organizational procedures. The focus is placed on the organization's perceived relationship to the outside world with high standards of what is good for their customers and the world. In an externally driven culture, the emphasis is placed on customer requirements and the organization is market driven with results being a higher priority than correctly following procedures.

Additionally, in an externally driven culture, a pragmatic approach prevails over an ethical attitude to business ethics.

Level of Control. The level of control dimension consists of the orientations easygoing work discipline and strict work discipline (Hofstede et al., 2010; The Culture Factor, n.d.). This dimension is focused on the internal structure, control, and discipline present within an organization. In an easygoing work discipline culture, the internal structure is fluid, there is limited control and discipline, and there is a lack of predictability which results in improvisation and surprises (The Culture Factor, n.d.). A strict work discipline culture is the opposite, members of the organization are punctual and serious and there are formal control systems in place (Hofstede et al., 2010; The Culture Factor, n.d.).

Focus. The focus dimension consists of the orientations local and professional (Hofstede et al., 2010; The Culture Factor, n.d.). Employees within a local culture are short-term directed and identify with their boss and/or their unit due to a strong social control to be like everyone else (The Culture Factor, n.d.). In other words, their identity is derived primarily from the organization itself (Hofstede et al., 2010). In a professional culture, an employee's identity is determined by their profession and/or their job content (The Culture Factor, n.d.). Employees are long-term directed and there is not a strong desire to be like everyone else (Hofstede et al., 2010; The Culture Factor, n.d.). Furthermore, this orientation is correlated with the education level of employees within an organization (Hofstede et al., 2010). Local cultures tend to have employees with less formal education while professional cultures are the opposite.

Approachability. The approachability dimension is related to the accessibility of an organization and consists of the orientations open system and closed system (Hofstede et al., 2010; The Culture Factor, n.d.). In an open system culture, new members are immediately welcomed, the organization

is open to both insiders and outsiders, and almost anyone could fit in the organization. In a closed system culture, the employees are closed and secretive (Hofstede et al., 2010). Even among insiders' employees are closed off and secretive and it takes a long time to feel accepted. This dimension is the only one of the six that is associated with national culture.

Management Philosophy. The management philosophy dimension consists of the orientations employee-oriented and work-oriented (Hofstede et al., 2010; The Culture Factor, n.d.). In an employee-oriented culture, employees feel that the organization accounts for their personal problems and their welfare, even if it is at the expense of completing work. Additionally, important decisions are likely made by groups or committees (Hofstede et al., 2010). In a work-oriented culture, employees experience pressure to perform their work even if it is at their own expense (The Culture Factor, n.d.). Employees perceive the organization as only being interested in the work they do and not in their personal welfare (Hofstede et al., 2010). Important decisions are likely made by individuals within this type of culture.

Situational Judgement Test

The primary measurement method for this research is a situational judgement test (SJT). As discussed by Phillips et al. (2024), SJTs could provide the field of behavioral information security research with numerous benefits including contextually relevant items that enhance the practical application of survey results. SJTs have traditionally been used within the field of organizational psychology to predict employee performance and influence employment decisions (hiring, promotions, etc.) (Weekley & Ployhart, 2005; Ployhart & MacKenzie, 2011). An SJT item presents participants with a realistic job/work-related situation, known as the item stem, and potential response options. SJTs are considered a multidimensional measurement method because a variety of latent constructs can be measured simultaneously (Oostrom et al., 2015; Ployhart &

MacKenzie, 2011; Ployhart & Ward, 2013; Pollard & Cooper-Thomas, 2015). Additionally, the structure of the response instructions for an SJT determine whether it is measuring knowledge (maximal performance) or behavioral tendency (typical performance) of the respondents (McDaniel et al., 2007). Phillips et al. (2024) provide an overview of SJTs from an information security perspective and how they compare to Likert-scales and Scenario vignettes which are commonly used within the field of information security.

Related Works

Both industry and academic researchers have contributed various frameworks, dimensions, definitions, terminology, and measurement instruments to the field of ISC research, many of which build upon organizational psychology research (Uchendu et al., 2021). The previously discussed Three-Level Model of Culture established by Edgar Schein is the most prominently used foundational theory from organizational psychology within ISC research (Nasir et al., 2019; Uchendu et al., 2021). For decades the model has been used by ISC researchers in a multitude of ways (Schlienger & Teufel, 2002; Kraemer & Carayon, 2005; Van Niekerk, 2005; Van Niekerk & Von Solms, 2005; Van Niekerk & Von Solms, 2006; Da Veiga & Eloff, 2010; Van Niekerk & Von Solms, 2010; Van Niekerk & Von Solms, 2013; Reid et al., 2014; AlKalbani et al., 2015; Chen et al., 2015; Da Veiga, 2015; Da Veiga & Martins, 2015; Martins & Da Veiga, 2015; Parsons et al., 2015; Hassan et al., 2017; Nasir et al., 2017). The integration of the Three-Level Model of Culture as a theoretical foundation in ISC research is widely accepted throughout the field.

Both Hofstede's national and organizational culture research have been used within ISC research. Hofstede's national culture research has been utilized in ISC research such as Alfawaz (2011), Zhang & Yang (2019), Hoffman (2021), Bruin & Mersinas (2022), and Stan et al. (2023). Hofstede's organizational culture research has been used by ISC researchers including Tang et al.

(2016) and Failla (2020). The research conducted by Tang et al. (2016) specifically focused on how Hofstede et al.'s (2010) organizational culture dimensions could influence compliance, communication, accountability, and governance regarding information security policies (ISPs). Tang et al. (2016) provide six propositions within their paper about the relationships between the organizational culture dimensions and the four areas of interests regarding ISPs that could be explored in future research. Failla's (2020) research focused specifically on how organizational culture influences cybersecurity governance as defined by Tang et al. (2016) and Da Veiga et al. (2007) within organizations that have recently experienced security breaches. Failla (2020) used publicly available data to discover evidence surrounding governance related to Hofstede's organizational culture dimensions.

Beautement et al. (2016) developed a scenario-based survey, similar to the scenarios we developed for the SJTs, to collect data on employee behaviors and attitudes. Rather than Hofstede's dimensions, they utilized a cultural framing developed by Adams (2003). The results of their research can be used to detect differences between employee groups to inform targeted security interventions. Beautement et al.'s (2016) research is a prime example of how scenario-based surveys can be used to assess security behaviors, which is a primary focus of this research paper.

Da Veiga, Eloff, and Martins have conducted extensive ISC research over the past two decades. Da Veiga and Eloff (2010), created an Information Security Culture Framework (ISCF) and used their Information Security Culture Assessment (ISCA) questionnaire (Da Viega et al., 2007) to empirically validate it. Their ISC research focuses on how seven information security components (Leadership and governance, Security management and operations, Security policies, Security program management, User security management, Technology protection and operations, and

Change) influence information security behaviors across organizational, group, and individual levels which then cultivate an information security culture (Da Veiga & Eloff, 2010). The ISCA questionnaire used in their research consisted of 85 Likert-scale questions covering the seven information security components. The Likert-scale questions are unidimensional, measuring only its associated component, and the results provide organizations with a picture of security behaviors (good vs. bad) regarding the components.

The research presented in the paper in hand provides a different perspective than that of Da Veiga, Eloff, and Martins by viewing information security culture as both being influenced by security behaviors and reflected in security behaviors. Behavior patterns that continue to be successful eventually become part of the underlying assumptions of an organization's culture (Schein & Schein, 2016, p. 8) and the assumptions then influence a group's behavior (Schein & Schein, 2016, p. 15). It is a continuously evolving lifecycle of behaviors influencing cultural assumptions which in turn influence behaviors. Another difference is that our work is explicitly tied to the organizational culture dimensions developed by Hofstede et al. (2010).

Based on the ISC and organizational culture literature, the following hypothesis were established:

Hypothesis 1: The means-oriented, internally driven, strict work discipline, professional, open system, and employee-oriented orientations will exhibit more desirable security behavioral tendencies compared to their counterparts under each of Hofstede et al.'s (2010) organizational culture dimensions.

Hypothesis 2: Healthcare, Government/Military, and Manufacturing/Heavy industries will have similar results due to the critical nature and rigorous procedures of the industries. Education and Technology industries will differ from all the other industries assessed.

RESEARCH DESIGN AND METHODS

The purpose of this research was to create a survey instrument to assess the underlying basic assumptions of employees surrounding an organization's information security culture to determine the type of culture and the security behavioral tendencies that are present. As previously discussed in section 2.1, the cultural assumptions determine the behaviors, perceptions, thoughts, and feelings of an organization's employees (Schein & Schein, 2016, p. 18), and guide the actions employees should take in varying situations (Schein & Schein, 2016, p. 22). Therefore, by using a situational judgement test, employee behavioral tendencies in relation to information security can be elicited as reflections of employee assumptions and aligned with the six organizational culture dimensions.

The final survey instrument used in this study consisted of 36 items (24 SJT items, 4 open-ended questions, 6 slider scale questions, and 2 feedback questions). The 24 SJT items are the core component of the assessment, and are referred to as the ISC-SJT (Information security culture – situational judgement test). The ISC-SJT items were created to be a multidimensional assessment to identify the type of culture present within an organization and security behavioral tendencies of employees based on their underlying basic assumptions surrounding information security.

The security behavioral tendency part of the assessment uses the classification terms desirable and undesirable to describe the security behaviors. Originally the terms secure and nonsecure were utilized when creating the ISC-SJT, however during the revision process it became evident that some of the items labeled as nonsecure were in a literal sense still secure. For example, an employee would like to use a new application that would streamline their work, but they are not sure if it is safe, so they decide to just not use it. The response in a literal sense is still secure because they didn't use the application, but it is undesirable from a business efficiency perspective.

Therefore, the terms desirable and undesirable were chosen to describe security behaviors, so behaviors that are secure but unwanted can be included in the assessment. Additionally, the security behaviors are not all based on the individual level, so the results reflect underlying assumptions about the security behavioral tendencies of the organization as a whole.

The open-ended questions included in the survey asked participants about their thoughts on common aspects of organizational information security including their organization's security policies and training, how they think they contribute to protecting their organization from security threats, and lastly soliciting any additional information the participant would like to share about their organization's information security or IT security team. The purpose of including these items was to gather additional information from participants about their organization's ISC and the results could potentially be used to assess the espoused beliefs and values level of culture in future research.

The slider scale section of the survey was used to directly receive input from participants directly about where they thought their organization fell on each of the six organizational culture dimensions. A question was included for each dimension in which the participant was provided the definitions for each of the dimension orientations and a 1 – 7 slider scale with one orientation on each end. Participants were asked to adjust the slider scale to reflect the culture within their organization and then there was an optional question asking participants to explain why they chose their answer. The purpose of including the slider scale was to collect information directly about the participants' perception of their organization's culture without an information security context. Lastly, two open-ended feedback questions were asked to gather information on the interest, enjoyability, and engagement levels of employees while taking the survey.

ISC-SJT Item Creation

The first step of developing the ISC-SJT was generating content for the SJT item-stems and response options. The goal was to develop four items for each of the six organizational culture dimensions for a total of 24 SJT items. The situations and response options were created to be generic to be applicable across all five industries. For future research, the SJT items should be customized to be directly applicable to the organization being assessed to improve the contextual relevance and practical application of the results.

The content of the SJT items is based on common information security situations (e.g. Plugging in unknown USB drives, locking the computer when walking away, etc.) and experiences the researchers have previously encountered. Each of the 24 ISC-SJT items have an underlying measurement that simultaneously assesses the security behavioral tendencies and type of culture present within an organization. This multidimensional measurement is based on the response options for each of the ISC-SJT items. The response instructions of the SJT items are structured to elicit behavioral tendency (typical performance) responses. Each SJT item consists of four response options, with each one aligning with one of the organizational culture dimensions' orientations and desirable or undesirable security behaviors. Participants were asked to choose the most likely and least likely response for a given item to provide additional details about their underlying assumptions.

ISC-SJT Revision Process

After the 24 initial ISC-SJT items were created, five SMEs (subject matter experts) from the fields of cybersecurity, information systems, and organizational psychology, completed a sorting exercise to ensure the items aligned with their underlying measurements. The SMEs were instructed to code each of the SJT items by dimension and the associated response options by

orientation and security behavior. After receiving the results from the sorting exercise and feedback from the SMEs, the ISC-SJT items were revised to improve their alignment with the underlying measurement. Next, three of the five SMEs reviewed the revised items and provided additional revision feedback. After a third round of revisions, the same three SMEs reviewed the 24 items and agreed that all appropriately reflected their underlying measurement. The rigorous revision process was utilized to ensure high content validity for the constructs being measured. Table 1 - 6 presents six of the final ISC-SJT items, one from each dimension, and its associated underlying measurement.

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

Table 1. Organizational Effectiveness ISC-SJT Items

Item Stem: Your organization discovers they have experienced a recent data breach that exposed the personal information of customers. What do you think your organization would most likely and least likely do?		
Response Options	**Orientation**	**Security Behavior**
A. They would promptly notify affected customers about the data breach, take responsibility, and outline steps taken to address the issue, emphasizing the organization's commitment to data security and ethical handling of the situation.	Internally driven	Desirable
B. They would attempt to downplay the severity of the breach, delay customer notification, and prioritize internal discussions over taking immediate action to secure affected individuals' data.	Internally Driven	Undesirable
C. They would focus on meeting legal obligations, promptly inform affected customers, and assure them that the situation is under control while emphasizing compliance with data protection regulations and working towards rebuilding trust.	Externally driven	Desirable
D. They would ignore or minimize the breach, prioritize business as usual, and avoid taking responsibility. Downplaying the impact on customers and focusing on maintaining a positive external image.	Externally driven	Undesirable

Table 2. Customer Orientation ISC-SJT Items

Item Stem: The employees in your organization receive an email from IT Security stating that access to the organization's Enterprise Resource Planning (ERP) system will be unavailable for 48 hours due to a critical security update. How do you think the majority of the employees at your organization would most likely and least likely react?		
Response Options	**Orientation**	**Security Behavior**
A. They would accept the inconvenience with a positive attitude, understanding that the security update is crucial. Employees may find alternative ways to work or take the opportunity for a short break, maintaining a fluid and easygoing perspective.	Easygoing work discipline	Desirable
B. They would dismiss the security update as unnecessary, potentially trying to find workarounds to access the ERP system during the update.	Easygoing work discipline	Undesirable
C. They would respond by diligently planning their work around the scheduled downtime, demonstrating discipline and adherence to protocols.	Strict work discipline	Desirable
D. They would react with frustration and anxiety due to the disruption, potentially ignoring security warnings and attempting to access the ERP system despite the update.	Strict work discipline	Undesirable

Table 3. Level of Control ISC-SJT Items

Item Stem: You are working on a tight deadline when you receive an email from an unfamiliar address claiming to be a survey from your company's HR department. It asks for your feedback on workplace culture and includes a link to complete the survey. What would you most likely and least likely do?

Response Options	Orientation	Security Behavior
A. I would double-check with colleagues if they received a similar email, then report it to IT Security for verification.	Local	Desirable
B. I would open the link to complete the survey because I wouldn't want to be the only person to not complete it.	Local	Undesirable
C. I would immediately report the email to IT Security and then continue working.	Professional	Desirable
D. I would ignore the email and continue working because the email is irrelevant to my current tasks.	Professional	Undesirable

Table 4. Focus ISC-SJT Items

Item Stem: As you are entering your office building, someone you don't know asks you to hold the door open for them because they are visiting someone in the building. What would you most likely and least likely do?

Response Options	Orientation	Security Behavior
A. I would hold the door open for them and then walk them to the visitor check-in location before heading to my office.	Open system	Desirable
B. I would hold the door open for them and then give them directions to the visitor check-in location before heading to my office.	Open system	Undesirable
C. I would tell them they need to contact the person they are visiting to let them into the building and then close the door, so they do not follow me into the building.	Closed system	Desirable
D. I would ignore them and hope the door closes behind me before they can make it inside the building.	Closed system	Undesirable

Table 5. Approachability ISC-SJT Items

Item Stem: Your organization's IT Security team recently conducted a mandatory security training session, which you had to miss due to other commitments. Curious about what was covered, you ask a coworker for a recap of the training. How do you think your coworker would most likely and least likely describe the training?

Response Options	Orientation	Security Behavior
A. They would say the training was insightful, introducing new security practices tailored to our specific roles and extending to cover security habits that could protect us outside work too.	Employee-oriented	Desirable
B. They would say the training was pretty basic, going over basic security steps for both at work and at home. It was the same as last year, the training didn't introduce anything new to them.	Employee-oriented	Undesirable
C. They would say the training was targeted and practical, focusing on security information that's directly applicable to our job functions, aiming to help us do our work efficiently in a safe way.	Work-oriented	Desirable
D. They would say the training was a general rundown of basic security measures for the workplace. It was a generic overview, the kind of stuff we've all heard in previous sessions.	Work-oriented	Undesirable

Table 6. Management Philosophy ISC-SJT Items

ISC-SJT Scoring

Situational judgement tests can be scored in a variety of ways depending on the type of data being collected and statistical analysis being conducted. The responses to each ISC-SJT item were scored in three different ways to assess both the type of culture and security behavioral tendencies.

The first scoring method, referred to as the dimension score, was dimension focused to assess the type of culture within the industries. For the dimension scoring method, if the response option selected aligned with the hypothesized orientation to exhibit more desirable security behavioral tendencies the item received a score of "1", else it was scored "0" for the most likely response option. The reverse is true for the least likely response option. Dimension subscale scores were calculated for each dimension by adding together the scores of the four items for each dimension.

The second scoring method, referred to as the security score, was security focused to assess the security behavioral tendencies per dimension and obtain an overall security score for each participant. For this second method, if the response option aligned with a desirable security behavior the item received a score of "1", else it was scored "0" for the most likely response option. The reverse is true for the least likely response option. An overall security score was calculated for each participant by adding up the scores across all items and subscale security scores were calculated for each dimension.

The third scoring method, referred to as the dimension & security score, focused on a combination of both dimensions and security behaviors. For this third method, a most likely response only received a "1" if the response option selected aligned with the hypothesized orientation and desirable security behavior. The reverse is true for the least likely response option, the non-hypothesized orientation and undesirable security behavior response was scored a "1". Table 7

provides examples of participant response patterns for each scoring method based on the underlying measurement of the response options for the ISC-SJT items.

Participant Response Pattern	Response Type	Orientation	Security behavior	Dimension Score	Security Score	Dimension & Security Score
1	Most likely	Orientation 1	Desirable	1	1	1
	Least likely	Orientation 2	Undesirable	1	1	1
2	Most likely	Orientation 1	Undesirable	1	0	0
	Least likely	Orientation 2	Desirable	1	0	0
3	Most likely	Orientation 2	Desirable	0	1	0
	Least likely	Orientation 1	Undesirable	0	1	0
4	Most likely	Orientation 2	Undesirable	0	0	0
	Least likely	Orientation 1	Desirable	0	0	0

Note. Orientation 1 is representative of the hypothesized orientation to exhibit more desirable security behavioral tendencies.

Table 7. ISC-SJT Scoring Methods

Data Collection

The final survey was completed by 330 participants across five industries (Technology, Government/Military, Healthcare, Manufacturing/Heavy industry, and Education) within the United States (66 participants per industry). The online research platform Prolific was used to recruit participants to complete the survey. For a participant to be eligible to complete the survey, they had to be 18 years of age or older, work within the United States, and be a full-time employee within one of the five industries. Table 8 provides an overview of participant demographics across the industries. Participant data provided through Prolific included their current U.S. state of residence, which is represented by the category "# of unique U.S. states" to reflect the location diversity of participants within the United States. This study was determined to be exempt and approved by the university IRB Protocol No. 24-37.

Industry	Male	Female	Age Range	# of unique U.S. States
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**

Table 8. Participant Demographics

RESULTS

Table 9 is a correlation coefficient matrix using the dimension scores and security scores for each participant to facilitate the comparison of relationships between organizational culture dimensions and security behavioral tendencies. Correlation coefficients measure the strength and direction of a linear relationship between two variables (Schober at el., 2018). Based on Cohen's (1977, p. 115) guidelines, the strength of the correlation coefficients 0.1, 0.3, and 0.5 are described as small, medium, and large respectively. All the security behavior subscales (S1 – S6) have large positive relationships with the overall security scale. Also, all the security behavior subscales positively correlate with each other as expected. The organizational effectiveness dimension subscale, customer orientation dimensions subscale, and management philosophy subscale have a medium positive correlation with overall security scores. The level of control dimensions subscale and management philosophy dimensions subscale have a large positive correlation with overall security scores. Lastly, the focus dimension subscale correlation with overall security is below 0.1, which means there is a negligible relationship between them.

To address the research question, how the ISC-SJT results compare across industries, the first thing to look at is the average dimension scores and security scores for each industry. Comparisons can be assessed from two perspectives, by types of culture and security behavioral tendencies. Table 10 provides the overall security score, dimension subscale scores, and security subscale scores for

each industry. The maximum score for overall security is 48 and the maximum score for all subscales is 8. For the security scores, higher scores are associated with more desirable security behavioral tendencies.

The dimension scores on the other hand are a bit more complex, each end of the score (less than 4 and greater than 4) represents an orientation for the associated dimension. The orientations above 4 align with those hypothesized to exhibit more desirable security behavioral tendencies due to the scoring method. Therefore, for the organizational effectiveness dimension scores greater than 4 reflect a means-oriented culture and scores less than 4 reflect a goal-oriented culture. For the customer orientation dimension scores greater than 4 reflect an internally driven culture and scores less than 4 reflect an externally driven culture. For the level of control dimension scores greater than 4 reflect a strict work discipline and scores less than 4 reflect an easygoing work discipline. For the focus dimension scores greater than 4 reflect a professional culture and scores less than 4 reflect a local culture. For the approachability dimension scores greater than 4 reflect an open system culture and scores less than 4 reflect a closed system. Lastly, for the management philosophy dimension scores greater than 4 reflect an employee- oriented culture and scores less than 4 reflect a work-oriented culture.

As shown by the scores in Table 10, some of the scores between industries are quite close. Therefore, analysis of variance (ANOVA) tests were conducted to identify significant differences across the industries based on their scores. The individual scores for all participants were used to conduct one-way ANOVA tests for each subscale, the results of which can be found in Table 11. The one-way ANOVA tests revealed that there are statistically significance differences in scores between at least two industries for seven of the scales. Post-hoc analysis using Bonferroni's method was conducted for the seven scales to identify the specific differences between industries,

the results are shown in Table 12. In this study, statistical analysis was performed using the built-in capabilities of R (2021.04.01) and the `psych` package (Revelle, 2007) for advanced psychometric testing.

After each of the SJT items were presented, participants were asked to respond yes or no to the question "Do you find this situation to be reasonable for something that could actually happen within your organization?". The purpose of asking the question was to determine the relevancy of the items across the five industries. Percentages ranged from 64% to 91% with an average of 79% of the participants agreeing the situations presented in the SJT items were reasonable for something that could happen within their organization.

According to the SJT literature, there are several reasons that estimating the reliability of an SJT is problematic (Whetzel & McDaniel, 2009). Due to the multidimensionality of SJTs and the construct heterogeneous at the item level, Cronbach's alpha is not the most appropriate reliability index. Although coefficient alpha underestimates the internal reliability it is still widely reported in SJT research due to better-suited alternatives such as test-retest and parallel form reliability being more complex and resource intensive. Therefore, coefficient alpha was calculated for each of the organizational culture dimensions and the overall scale using the dimension & security score, which assigns one "correct" answer to each most likely and least likely response, with the expectation of low internal reliability due to the small number of questions per dimension and their heterogeneity. The coefficient alpha results are as follows: Overall scale – 0.73, Organizational effectiveness – 0.28, Customer orientation – 0.34, Level of control – 0.29, Focus – 0.36, Approachability – 0.38, and Management philosophy – 0.54. In addition, the security scores for all participants were used to calculate coefficient alpha for the overall security scale aspect of the ISC-SJT resulting in an alpha of 0.81.

	Mean	SD	Range	S	D1	D2	D3	D4	D5	D6	S1	S2	S3	S4	S5	S6
Overall Security Score (S)	35.95	7.31	39	1.00												
Organizational Effectiveness Dimension Score (D1)	4.16	1.56	8	.255	1.00											
Customer Orientation Dimension Score (D2)	4.38	1.55	8	.275	.046	1.00										
Level of Control Dimension Score (D3)	4.37	1.58	8	.301	.109	.038	1.00									
Focus Dimension Score (D4)	4.89	1.56	8	.043	.061	.050	.001	1.00								
Approachability Dimension Score (D5)	5.83	1.55	6	.397	.040	.126	.051	-.028	1.00							
Management Philosophy Dimension Score (D6)	4.33	2.00	8	.276	-.007	.145	.091	-.122	.268	1.00						
Organizational Effectiveness Security Score (S1)	6.03	1.77	8	.692	.221	.151	.193	.153	.158	.071	1.00					
Customer Orientation Security Score (S2)	6.85	1.65	7	.712	.162	.169	.222	.120	.363	.119	.401	1.00				
Level of Control Security Score (S3)	6.58	1.58	6	.758	.191	.209	.222	.030	.342	.182	.469	.550	1.00			
Focus Security Score (S4)	5.96	1.96	8	.765	.195	.224	.264	-.085	.275	.222	.427	.403	.527	1.00		
Approachability Security Score (S5)	6.13	1.60	7	.700	.209	.213	.196	.132	.272	.076	.439	.431	.432	.448	1.00	
Management Philosophy Security Score (S6)	4.40	1.91	8	.547	.092	.177	.159	-.133	.257	.444	.169	.245	.248	.333	.207	1.00

Table 9. Correlations Across Industry Types

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

Table 10. ISC-SJT Average Scores by Industry

Dependent Variable	**F-ratio**	**p-value**
Overall Security Score (S)	**4.321**	**.002**
Organizational Effectiveness Dimension Score (D1)	0.415	.798
Customer Orientation Dimension Score (D2)	0.543	.705
Level of Control Dimension Score (D3)	**4.608**	**.001**
Focus Dimension Score (D4)	2.247	.064
Approachability Dimension Score (D5)	1.507	.200
Management Philosophy Dimension Score (D6)	1.372	.243
Organizational Effectiveness Security Score (S1)	**6.110**	**.000**
Customer Orientation Security Score (S2)	**2.652**	**.033**
Level of Control Security Score (S3)	**2.445**	**.047**
Focus Security Score (S4)	**3.563**	**.007**
Approachability Security Score (S5)	1.203	.309
Management Philosophy Security Score (S6)	**5.168**	**.000**

Predictor variable for all tests = Industry type

Table 11. Summary of One-way ANOVA Tests

		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
	Manufacturing/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**
	Manufacturing/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	Manufacturing/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
Manufacturing/Heavy	Healthcare	0.09	0.22	0.37	-0.23	0.47	-0.14	0.11

Note: Bolded mean differences have a p-value < 0.05

Table 12. Post-hoc Analysis

DISCUSSION

The correlation matrix shown in Table 9, provides the information necessary to determine which orientation for each dimension is predictive of higher overall security scores, which represents more desirable security behavioral tendencies. The organizational effectiveness dimension has a small positive correlation with overall security, therefore being more means-oriented is predictive of a higher overall security score. Means-oriented cultures are more risk averse than goal-oriented cultures which aligns with this finding. The customer orientation dimension has a small positive correlation with overall security, so being more internally driven is predictive of a higher overall security score. The level of control dimension has a medium positive correlation with overall security, which means the strict work discipline is more predictive of a higher overall security score. The focus dimension has a positive but negligible correlation with overall security and is therefore not a strong predictor of the overall security score, so neither the local nor the professional orientation is important for influencing overall security score. The approachability dimension has a medium positive correlation with overall security, so the open system orientation is more predictive of a higher overall security score. Lastly, the management philosophy dimension

has a small positive correlation with overall security, therefore being more employee-oriented is predictive of a higher overall security score.

In other words, hypothesis 1 was partially supported. The results confirmed that the means-oriented, internally driven, strict work discipline, open system, and employee-oriented orientations exhibit more desirable security behavioral tendencies compared to their counterparts. However, the hypothesis that the professional orientation for the focus dimension would exhibit more desirable security behavioral tendencies was not supported by the results. Neither orientation for the focus dimension has a significant influence on predicting more desirable security behavioral tendencies. These results could be used to support organization culture change initiatives to improve security behaviors. However, changing a culture is quite difficult, so at the very least by knowing the type of culture an organization has, initiatives to promote desirable security behaviors can be aligned with the culture versus fighting against it.

The results of the ISC-SJT revealed the prominent type of culture and security behavioral tendencies present within the Technology, Government/Military, Manufacturing/Heavy, Healthcare, and Education industries within the United States. Based on the one-way ANOVA tests and post-hoc analysis, statistically significant differences were identified for both the type of culture and security behavioral tendencies of the industries. Hypothesis 2 which stated the Government/Military, Manufacturing/Heavy, and Healthcare industries would not differ from each other while the Technology and Education industries would differ from all other industries is partially supported by the results of the survey. The Education industry has statistically significant differences from all the industries. The Technology industry has statistically significant differences from the Education, Government/Military, and Healthcare industries. Lastly, the Government/Military, Manufacturing/Heavy, and Healthcare industries do not have any

statistically significant differences identified between them. Hypothesis 2 is considered partially supported because results did not reveal any significant differences between the Technology and Manufacturing/Heavy industries.

For the type of culture, the level of control dimension was the only one to display significant differences between industries. The post-hoc analysis for the dimension revealed significant differences between the Education industry and the Government/Military, Manufacturing/Heavy, and Healthcare industries. The p-value for Education versus Technology industries for this dimension's post-hoc analysis was 0.052, slightly above the 0.05 threshold. Based on the dimension scores, the Education industry exhibits an easygoing work discipline culture, and the other four industries exhibit a strict work discipline culture. The Education industry was the only industry of the five to fall on the easygoing side of the level of control dimension and consistently scored low on security behavior. The overall security score for Education is the lowest of all five industries at 33.21, which is more than a standard deviation below the highest scoring industry (Technology). According to Tang et al.'s (2016) propositions, the level of control dimension "is important and dangerous for information security management compared to the other dimensions of organizational culture" (p. 185). Furthermore, the level of control dimension has the second highest correlation coefficient with overall security.

Based on the analysis results, overall security scores significantly varied between the Education industry and the Technology and Government/Military industries. The Education industry had the lowest overall security score while Technology and Government/Military had the top two scores. The Education dimension-based security scores significantly varied from that of the Technology industry for the dimensions organizational effectiveness, focus, and management philosophy. Also, the Education industry dimensions-based security scores significantly varied from the

Government/Military industry scores for the dimensions organizational effectiveness, customer orientation, and management philosophy. The Manufacturing/Heavy industry security score also significantly varied from that of the Education industry along the organizational effectiveness dimension. Other significant differences in dimension security scores occurred between Technology and Healthcare for organizational effectiveness and management philosophy, and between Technology and Government/Military for the management philosophy dimension. Lastly, the one-way ANOVA tests revealed overall variability between the industries along the level of control security score, however there were no significant differences found between any of the industries based on post-hoc analysis. These industry results could be used as a baseline when assessing a single organization within one of the five industries to address the question "How does our organization compare to others within the industry?".

As shown in Table 10, all five industries score highest on approachability of the dimension scores, reflecting an open-system culture. According to Hofstede et al. (2010), the approachability dimension is closely related to the Uncertainty Avoidance dimension of National Culture. Based on their research, the United States is classified as having a weak uncertainty avoidance, which aligns with an Open-system orientation in organizational culture. This is shown in the results of the ISC-SJT survey, as the open system responses were selected at a much higher rate across all 5 industries than any other orientation. Therefore, assessments of organizations outside the United States may be needed to receive a closed system result.

LIMITATIONS & FUTURE RESEARCH

In the limitations section of Hofstede et al. (2010), the authors acknowledge that the research conducted to identify the six organizational culture dimensions was limited to two countries (Denmark and Netherlands), therefore additional dimensions may be applicable in other countries.

However, the six organizational culture dimensions provide ISC research with a strong foundation to build upon. Another limitation identified is the length of the ISC-SJT, of the 330 participants the average completion time was around 38 minutes. The length of the survey in its current state could influence whether organizations would want to use it on a wide scale. However, the non-SJT item questions could potentially be removed in future survey iterations which would decrease the completion time and required level of effort to complete.

Future research endeavors plan to use the results from this research to improve the ISC-SJT for future use when assessing an organization's ISC. Additionally, future research is needed on how to best assess the other two levels (artifacts and espoused beliefs and values) of an organization's ISC. Espoused beliefs and values could potentially be gathered from employees through open-ended questions such as those asked within the overall survey for this research. Statements and documents published externally or internally by an organization may be able to reveal reflections of espoused beliefs and values as well as artifacts of ISC. Artifacts could also potentially be identified through organizational observations and interviews.

CONCLUSION

In conclusion, the ISC-SJT was able to assess the underlying assumptions of employees across five industries within the United States and the results revealed the type of culture and security behavioral tendencies present in the industries. Additionally, one orientation for five of the six dimensions promotes more desirable security behaviors over its opposite orientation. The results of this ISC-SJT data collection could be used as an industry baseline for future research and support to initiate culture changes. Furthermore, the results of the ISC-SJT for a specific industry could be used to identify specific areas for information security improvements and provide guidance on how to align security efforts with the culture.

ACKNOWLEDGEMENTS

The authors acknowledge support from Tulsa Innovation Labs via the Cyber Fellows initiative.

REFERENCES

2024 Data Breach Investigations Report. 2024. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Adams, J. 2003. "Risk and Morality: Three framing devices," *Risk and Morality*, pp. 87–106.

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

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

Bruin, M., & Mersinas, K. 2022. Individual and Contextual Variables of Cyber Security Behaviour -- An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour. (thesis). University of London.

Chen Y., Ramamurthy K., Wen K. 2015. "Impacts of Comprehensive Information Security Programs on Information Security Culture," *Journal of Computer Information Systems* (55:3), pp. 11-19.

Cohen, J. 1977. "Statistical power analysis for the behavioral sciences," *Elsevier Science & Technology*.

Da Veiga, A. 2015. "An Information Security Training and Awareness Approach (ISTAAP) to Instill an Information Security-Positive Culture," *Human Aspects of Information Security & Assurance*, pp. 95-107.

Da Veiga, A., & Eloff, J. H. P. 2010. "A framework and assessment Instrument for information security culture," *Computers & Security* (29:2), pp. 196–207.

Da Veiga, A., & Martins, N. 2015. "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security* (49), pp. 162–176.

Da Veiga, A., Martins, N., & Eloff, J. H. P. 2007. "Information security culture – validation of an assessment instrument," *Southern African Business Review* (11:1), pp. 147–168.

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

Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. 2017. "Information security culture in health informatics environment: A qualitative approach," *2017 International Conference on Research and Innovation in Information Systems (ICRIIS).*

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.

Hofstede, G., Hofstede, G. J., & Minkov, M. 2010. Cultures and organizations: Software of the mind: intercultural cooperation and its importance for survival (Revised and expanded third edition). McGraw-Hill.

Kraemer, S., & Carayon, P. 2005. "Computer and Information Security Culture: Findings from two studies," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (49:16), pp. 1483–1488.

McDaniel, M. A., Hartman, N. S., Whetzel, D. L., & Grubb, W. L. 2007. "Situational Judgment Tests, Response Instructions, and Validity: A Meta-analysis," *Personnel Psychology* (60:1), pp. 63-91.

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*.

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.

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.

Reid, R., Van Niekerk, J., & Renaud, K. 2014. "Information security culture: A general living systems theory perspective," *2014 Information Security for South Africa*.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. 2015. "The influence of Organizational Information Security Culture on Information Security Decision making," *Journal of Cognitive Engineering and Decision Making* (9:2), pp. 117–129.

Phillips, S., Brummel, B., Aurigemma, S., & Moore, T. 2023. "Information Security Culture: A look Ahead at Measurement Methods," in *Proceedings of the Annual Information Institute Conference*, G. Dhillon, S. Furnell, and D. Demetis (eds.), Las Vegas, NV.

Phillips, S., Aurigemma, S., Brummel, B., & Moore, T. 2024. "Leveraging Situational Judgment Tests to Measure Behavioral Information Security," *in Proceedings of the 57th Hawaii International Conference on System Sciences.*

Ployhart, R. E., & 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.

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., & Cooper-Thomas, H. D. 2015. "Best practice recommendations for Situational Judgment tests," *Australasian Journal of Organisational Psychology* (8).

Revelle, W. 2007. Psych: Procedures for psychological, psychometric, and Personality Research. CRAN: Contributed Packages. https://doi.org/10.32614/cran.package.psych

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

Schlienger, T. & Teufel, S. 2002. "Information Security Culture: The Socio-Cultural Dimension," *Information Security Management*, pp. 191-202.

Schober, P., Boer, C., & Schwarte, L. A. 2018. "Correlation coefficients: Appropriate use and interpretation," *Anesthesia & Analgesia* (126:5), pp. 1763–1768.

Stan, Bianca-Elena, Staiculescu, Ana Rodica, & Predoana, Marius-Razvan. 2023. "Security Culture from Communism to Democracy," *Romanian Intelligence Studies Review* (30), pp. 112-129.

Tang, M., Li, M., & Zhang, T. 2016. "The impacts of organizational culture on information security culture: A case study," *Information Technology and Management* (17:2), pp. 179–186.

The Culture Factor. n.d. *Organisational culture: What you need to know*. Hofstede Insights. https://www.hofstede-insights.com/organisational-culture

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. 2021. "Developing a cyber security culture: Current practices and future needs," *Computers & Security* (109).

Van Niekerk, J. F. 2005. Establishing an information security culture in organizations: an outcomes based education approach (dissertation), Nelson Mandela Metropolitan University.

Van Niekerk, J., & Von Solms, R. 2005. "A holistic framework for the fostering of an information security sub-culture in organizations," *ISSA*, pp. 1–13.

Van Niekerk, J., & Von Solms, R. 2013. "A theory based approach to information security culture change," *Information (Japan)* (16:6B), pp. 3907-3930.

Van Niekerk, J., & Von Solms, R. 2010. "Information security culture: A management perspective," *Computers & Security* (29:4), pp. 476–486.

Van Niekerk, J., & Von Solms, R. 2006. "Understanding Information Security Culture: A Conceptual Framework," *ISSA*, pp. 1-10.

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

Whetzel, D. L., & McDaniel, M. A. 2009. "Situational judgment tests: An overview of current research," *Human Resource Management Review* (19:3), pp. 188–202.

Zhang, X., & Yang, H. 2019. "Impact of Cross-Culture on Behavioral Information Security," *Journal of Integrated Design and Process Science* (22:2), pp. 63–80.