Information Security Culture: A look Ahead at Measurement Methods

Samantha Phillips
University of Tulsa
samantha-phillips@utulsa.edu

Bradley Brummel, PhD
University of Tulsa
bradley-brummel@utulsa.edu

Sal Aurigemma, PhD
University of Tulsa
sal-aurigemma@utulsa.edu

Tyler Moore, PhD
University of Tulsa
tyler-moore@utulsa.edu

Abstract

The information security culture field is a complex research area that does not currently have a standardized term, definition, and measurement process for organizations of various sizes, industries, and locations. While information security culture is still a relatively new field, the field of organizational culture research is more established and can continue to offer theory and methods to improve information security culture development and practice. Organizational culture research has established three levels of culture that will be used to propose an information security culture definition and guide future research plans for creating a multi-method information security culture measurement process. A multi-method approach will aim to overcome the limitations of using a single method approach by capturing all aspects of an organization's information security culture. The methods introduced in this paper for future research are a situational judgment test, analysis of beliefs and values through company statements, documents, and processes, and observations by a third party.

Introduction

The focus on understanding the human elements of information security is an essential component in an effort to improve an organization's security posture and decrease the possibility of security incidents. According to the Verizon 2022 Data Breach Investigation Report, "82% of breaches involved the human element" (Data Breach Investigations Report, 2022). Other organizations such as Varonis and KnowBe4 have published percentages even higher, 95% and 88% respectively (Sobers, 2022; Sjouwerman, n.d.). Defining, measuring, and cultivating an information security culture continues to be debated in current academic and industry research. The information security culture field is complex and rapidly evolving in many different directions. There is currently not a standardized term, definition, or measurement for information security culture in organizations.

The purpose of this paper is to discuss the current state of information security culture and propose a definition and dimensions for information security culture that align with plans for future research of a multi-method approach to measuring information security culture in organizations. The multi-method approach will aim to move beyond relying solely on questionnaire/survey data to measure an organization's

information security culture and provide an easy to use and repeatable measurement process for researchers, consultants, and organizations. The first section of this paper provides background information about information security culture, the second section describes the proposed information security culture definition, the third section outlines the use of the three levels of organizational culture as dimensions for information security culture, and the fourth section discusses plans for future research based on the proposed definition and dimensions.

Background Information

The terms information security culture, cyber security culture, security culture, and various other similar terms, are used throughout current academic and industry research and literature. Some use the terms synonymously and others declare differences between them, such as Da Veiga, Astakhovam, Botha, and Herselman who stated cybersecurity culture is a subset of information security culture (Da Veiga et al., 2020). A 2021 review paper discussed the use of the term's information security culture, cyber security culture, and security culture between 2010 and 2020 (Uchendu et al., 2021). Over those ten years the term information security culture was the most commonly used term of the three. From the corpus of 58 papers in their review the term information security culture was used in 42 of the reviewed papers, cybersecurity culture was used in 10 papers, with a major increase in term usage occurring in 2019, and security culture was used in 7 papers. The various terms all reference a similar, if not the same, concept. To stay aligned with the majority of the field, the leading term information security culture will be used in this paper.

Although research about information security culture has continued over the past several decades, there is not a prominent validated tool that can be used to measure information security culture in varying organizations (Orehek & Petrič, 2021; Sas et al., 2020). Surveys and questionnaires are the most commonly used tools to measure information security culture, however there are concerns as to whether more dynamic measurement methods are required to fully assess information security culture (Uchendu et al., 2021).

In their 2020 paper, Sas et al. provided a systematic overview and analysis of six tools for measuring security culture (Sas et al., 2020). The authors identified a total of 16 tools, but ten tools were excluded from the analysis for one of the following reasons: a narrow focus on security awareness instead of security culture, the tool was created by someone other than the author of the article, a lack of sufficient information about the content of the instrument, inability to generalize the tool to other situations, or the tool was solely theoretical. Of the six analyzed tools, two focused on physical security (primarily in the context of nuclear facilities) and four focused on information security. All six tools analyzed used a self-assessment questionnaire in their measurement approach. Two of the six used a mixed-method approach which included interviews, document analyses, and observations along with a questionnaire. Of the four tools focusing on information security culture, three use a questionnaire as the sole measurement method and one uses a mixed-method approach. The one tool that uses a mixed-method approach is described as difficult to repeat in other organizations or by other researchers. The authors of the article state the exploration in their review "reveals that there is no validated and widely accepted tool that can be used in different sectors and organizations" (Sas et al., 2020, p. 340).

In their 2021 paper, Orehek & Petrič conducted a systematic review focused on analyzing published scales that measured information security culture (Orehek & Petrič, 2021). While the Sas et al. (2020) paper previously mentioned focused primarily on the characteristics of the tools identified, this article focused on evaluating the rigor of the reported operationalization and the reported validity and reliability of the identified scales. The information security culture tools proposed by AlHogail & Mirza (2015) and Alnather et al. (2012) are included in both systematic reviews. After identifying, screening, and assessing the eligibility of scales for the review, Orehek & Petrič included nineteen scales/studies in their paper. Eleven of the scales measured information security culture as a multidimensional concept while the other eight measured it as a unidimensional concept. The authors used twelve criteria for evaluating rigor of operationalization: Essential definition of the concept, Definition of the components of the concept (only applicable to multidimensional scales), Source of items, Expert review, Pilot test of items, Sample size, Response rate, Sample characteristics, Descriptive statistics of the items or factors, Correlations between factors/items, EFA (exploratory factor analysis), and CFA (confirmatory factor analysis). Of the nineteen scales reviewed the highest criteria met for the evaluation of rigor of operationalization was eleven out of twelve or 91.7%. For the evaluation of reported validity and reliability there were four criteria: Convergent validity, Discriminant validity, Criterion validity, and Reliability. None of the scales being evaluated met all

four criteria. Eight of the nineteen scales fulfilled the criterion for convergent validity, discriminant validity, and reliability. None of the scales fulfilled or partially fulfilled the criteria for Criterion validity.

Academia is not the only area conducting research about information security culture. The organization KnowBe4, whose primary business focus is security awareness and anti-phishing training, bought the company CLTRe in 2019 which has published a Security Culture Framework, Security Culture Survey, and most recently in March of 2022 a Security Culture Maturity Model (*KnowBe4 acquires CLTRE*, 2019; *KnowBe4 Security Culture Survey*, 2019; *Security culture framework*, n.d.; *Introducing the Security Culture Maturity Model*, 2022). Of the three items published by CLTRe and KnowBe4, the Security Culture Maturity Model has the most publicly available information about it. The maturity model is primarily developed for customers of KnowBe4's platform, but "non-KnowBe4 customers can also gain value from the model by using anecdotal evidence to best estimate their maturity" (*Introducing the Security Culture Maturity Model*, 2022, p. 8). The maturity model consists of five levels: Level 1 – Basic compliance, Level 2 – Security awareness foundation, Level 3 – Programmatic Security Awareness & Behavior, Level 4 – Security Behavior Management, and Level 5 – Sustainable security culture. The Security Culture Survey has some information published from 2019 about its validity and reliability but the actual questions and format of the survey are not publicly accessible "to ensure the integrity of the assessment" (KnowBe4 Security Culture Survey, 2019, p. 1). On the KnowBe4 website, it states the security culture survey measures seven dimensions of security culture which include: Attitudes, Behavior, Cognition, Communication, Compliance, Norms, and Responsibility (*The Security Culture Survey*). Based on this information, the security culture survey seems to fall within the category of measuring a multidimensional concept of security culture. The use of a survey to measure security culture also aligns with the pattern of questionnaires/surveys being presented in academic literature as shown by the two review articles previously discussed.

Overall, a major issue within the information security culture field is a lack of standardized and validated tools that can be applied to numerous organizations within different industries and locations. While the literature on information security culture is still relatively nascent, the field of organizational culture research is more established and can continue to offer theory and methods to improve information security culture development and practice.

Defining Information Security Culture

As previously mentioned, various terms have been used to reference the concept of information security culture. There are also a variety of definitions presented by researchers and industry for these terms, some of which are 2 short paragraphs long while others are a single sentence. Table 1 contains some prevalent definitions that can be found in current academic and industry literature. Table 1 only provides examples of definitions and terms that have been used in literature to describe information security culture.

Inconsistency and variability is found between the definitions present in current literature, even from the same source which can be seen in the KnowBe4 definitions outlined in Table 1 for security culture. However, many of the definitions have similar themes including artifacts and creations, values, norms and knowledge, and basic assumptions and beliefs (Da Veiga et al., 2020).

Table 1: Terms and Definitions

Term	Definition	Source
Information Security Culture	Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives. The behaviour over time becomes part of the way things are done, i.e. second nature, as a result of employee assumptions, values and beliefs, their knowledge and attitude towards and perception of the protection of information assets. The information security culture is directed by the vision of senior management together with management support in line with the information security policy and influenced through internal and external factors, supported by an adequate ICT	Da Veiga et al., 2020

	environment, visible in the artefacts of the organisation and behaviour exhibited by employees, thereby creating an environment of trust with stakeholders and establishing integrity.	
Information Security Culture	For the purpose of this research, an information security culture is therefore defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time	Da Veiga & Eloff, 2010
Security Culture	Security Culture is defined as the ideas, customs, and social behaviors of a group that influence its security.	KnowBe4 - *Security culture maturity model*
Security Culture	Security culture can be defined as the ideas, customs and social behaviors that impact the security of your organization.	KnowBe4 - *The Security Culture Survey*

Edgar Schein, one of the first organizational culture researchers and often considered the 'father' of the field, published the following dynamic definition of culture in 2016:

> "The culture of a group can be defined as the accumulated shared learning of that group as it solves its problems of external adaptation and internal integration; which has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, feel, and behave in relation to those problems.
>
> This accumulated learning is a pattern or system of beliefs, values, and behavioral norms that come to be taken for granted as basic assumptions and eventually drop out of awareness" (Schein & Schein, 2016, p. 6).

In an attempt to create a more concise definition for information security culture that could be used in academia and industry, and aligns with future research plans, the following definition is proposed:

> Information security culture is 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.

The proposed definition is based on Schein's dynamic definition of culture and three levels of culture (Schein & Schein, 2016). Many information security culture definitions and dimensions in academic literature have been built upon Schein's work in organizational culture with the addition of diverse concepts (Nasir et al., 2019). The proposed definition stands apart by being directly tied to Schein's definition and levels of culture, therefore the components of the definition can be further explained and supported using organizational culture concepts.

Information Security Culture Dimensions

Schein's three levels of culture, which are incorporated in the previously proposed definition, are artifacts, espoused beliefs and values, and basic underlying assumptions (Schein & Schein, 2016). The three levels of culture have been used to support and influence numerous information security culture dimensions in academic research (Nasir et al., 2019). However, based on a 2019 review of information security culture dimensions, the sole use of the three levels of culture as dimensions had only been used in 1 out of the 48

articles analyzed (Nasir et al., 2019; Chen et al., 2015). Another research team used the three levels in addition to information security knowledge as a fourth dimension (Nasir et al., 2019; Niekerk & Solms, 2005). Many of the analyzed articles used Schein's organizational culture research, and other works influenced by it, to establish information security culture dimensions that were not the three levels of culture. For the purpose of this article and future research, the three levels of culture will be used as the dimensions of information security culture. The purpose of using Schein's three levels of culture is that they are generic, yet detailed enough, to be applied to any organization and there is organizational culture research supporting their use of classifying different aspects of culture.

Artifacts are things that can be seen, heard, and felt when interacting with a new group in an unfamiliar culture (Schein & Schein, 2016). In other words, artifacts are the visible products of the group. Visible products of a group include its physical environment, language, technology and products, artistic creations, style, myths and stories about the organization, published values, and observable rituals, routines, and ceremonies. The artifacts of an organization should not be used alone to determine the culture, as the espoused beliefs and values and underlying assumptions behind them can cause the same artifact to have different meanings depending on the organization/group.

Espoused beliefs and values are conscious and explicitly articulated normative or moral functions that guide members of a group on how to deal with certain key situations and train new members on how to behave (Schein & Schein, 2016). Beliefs and values can become a part of an organization's philosophy or ideology which is used as a guide to handle uncontrollable or difficult events. Espoused beliefs and values can sometimes reflect an organization's desired behavior while not being reflected in the observed behavior. Therefore, when analyzing this level of culture, a distinction must be made between beliefs and values aligned with underlying assumptions that guide performance, that are part of the organization's ideology or philosophy, and those that are rationalization or organizational aspirations. Beliefs and values that can be empirically tested and continue to reliably solve a problem will become transformed into assumptions.

Basic underlying assumptions are unconscious, taken-for-granted beliefs and values (Schein & Schein, 2016). The basic assumptions of an organization determine the behaviors, perceptions, thoughts, and feelings of employees. The assumptions also define what to pay attention to, what things mean, how to react emotionally to a situation, and what actions to take. There is very little variation found in a social unit's basic assumptions.

Table 2 provides a few examples for artifacts, espoused beliefs and values, and basic underlying assumptions in the context of information security culture.

Table 2: Information Security Culture Dimensions Examples

Information Security Culture Dimension	Examples
Artifacts	- The presence of a security awareness training program - Communication platforms - Using encrypted USBs - The language employees use to speak about information security
Espoused Beliefs and Values	- Organization stating "Information security is a top priority" - Content in IT Procedures and Policies
Basic Underlying Assumptions	- Non-security employees think information security is not their responsibility - Employees think security training is a waste of time - Employees feel they are an important part of preventing information security incidents

Future Research

As discussed in the background information section, the majority of the proposed information security culture measurement tools are surveys. Surveys can measure part of an organization's information security culture, but often fall short of capturing the entire picture (Corritore et al., 2019). To address this issue and attempt to create a reliable and validated information security culture measurement tool, future research plans include establishing a multi-method approach to measuring information security culture based on the proposed definition and three dimensions presented in this paper. A multi-method approach will likely allow for a deeper analysis and understanding of an organization's information security culture. The goal of creating a multi-method approach is to enable an organization to have someone, similar to an auditor or consultant, come into their organization and measure their information security culture and track progress over time. Each method will aim to measure, at a minimum, part of a dimension. Potential methods to be addressed in future research include the creation and use of a situational judgment test, analysis of espoused beliefs and values through company statements, documents, and processes, and organizational observations by a third party.

Additional research steps that will be explored to help gather information to create a multi-method measurement process include the use of interviews and a case-study. Interviews will be conducted with chief information security officers (CISO), and other potential positions, from various industries and organizational sizes to help shape the information security culture measurement process. Interviews are a common research method in cybersecurity, especially when researching organizational aspects of cybersecurity (Fujs et al., 2019).

A case study would be an intensive and systematic investigation of an organization to examine in-depth data related to the organization's information security culture (Heale & Twycross, 2018). The results of a case-study designed to evaluate organizations that are deemed to have weak or strong information security cultures could be used to help build the multi-method measurement process. The analysis of organizations through case-studies could reveal common characteristics of organizations with information security cultures that exist on the spectrum from weak to strong. A challenge that will need to be addressed when designing the case-study is how an organization is determined to have a weak or strong information security culture. For example, does the organization claim it has a strong culture or has another source stated the organization has a strong or weak culture.

The first potential method to be addressed in future research is the use of Situational Judgement Tests (SJTs). SJTs are commonly used to simulate work situations to evaluate whether someone would be a good fit for a job position, however that is not their only purpose. According to the U.S. Office of Personnel Management (OPM), "SJTs measure effectiveness in social functioning dimensions such as conflict management, interpersonal skills, problem solving, negotiation skills, facilitating teamwork, and cultural awareness" (Situational Judgment Tests, para. 2). The measurement focus of a SJT would be basic underlying assumptions related to information security culture. An analysis of whether using open-ended or answer choices is more effective will need to be conducted. Some potential SJT scenarios and answer options are provided in table 3.

Ideally all employees would take the situational judgment test to gather as much information as possible about the organization's information security culture. Since the test will be the same for all employees and can be taken individually as time permits there shouldn't be a major increase in cost in having all employees take the test versus a subset of employees. However, the reality of all employees completing the test is unlikely, so at a minimum having participants at each hierarchy and department in a company complete the test could be adequate.

A first step in creating the SJT will be to determine attributes of information security culture to use to organize the scenarios and the assumptions they aim to measure. Two approaches that could be used to help determine the attributes for the SJT include interviewing security professionals, particularly CISOs from various organizations, and using findings in current information security culture literature. For example, Tolah, Furnell, and Papadaki proposed an information security culture framework in 2017 that consists of influencing factors and organizational behavior factors that impact information security culture in an organization (Tolah et al., 2017). The influencing factors are top management, security policy, information security education and training, risk assessment, and ethical conduct. The

organizational behavior factors are job satisfactions and personality traits. The authors build upon this framework in their 2019 and 2021 papers as well (Tolah et al., 2019; Tolah et al., 2021).

Table 3: Potential SJT Scenarios

Scenarios	Answer Options
You get a phone call while at work from someone claiming to be from the IT Helpdesk. They say they need your password to verify some information and that you will need to approve your 2-factor authentication momentarily after providing the password. You would…	a. Provide the person your password and approve the MFA b. Don't provide your password and take no further action. c. Don't provide your password and report the incident to IT Security d. Provide the person your password and approve the MFA and then report the incident to IT Security.
You are browsing through your organization's file system and notice you have access to files and information that are not necessary for you to complete your job. You would…	a. Keep browsing to see what you information you can find b. Stop looking at the files and take no further action c. Stop looking at the files and report your finding to IT Security d. Keep browsing to see what information you can find and then report your finding to IT Security
You received an email from a customer with an attached pdf file. After opening the pdf file your computer starts to act strange. You would…	a. Restart your computer and then continue working. b. Continue working and ignore anything strange happening. c. Disconnect your computer from the Internet and immediately notify IT Security. d. Restart your computer and immediately notify IT Security.
You get a phone call while at work from someone claiming to be from the IT Helpdesk. They say they need your password to verify some information and that you will need to approve your 2-factor authentication momentarily after providing the password.	a. Provide the person your password and approve the MFA b. Don't provide your password and take no further action. c. Don't provide your password and report the incident to IT Security

The second potential method to be addressed in future research is a an analysis of an organization's espoused beliefs and values through company statements, documents, and processes. Organization ideologies that are expressed as statements from the organization and in documents such as IT or security policies and procedures can potentially be used to assess the espoused beliefs and values of an organization. Further analysis and planning will be needed to establish this method for testing purposes. Some considerations include how to collect and analyze the information, setting a benchmark or standard for measurement classification, and determining the specific information that needs to be collected from the organization. Machine learning models may also prove useful in helping to analyze collected data.

The third potential method to be addressed in future research is organizational observations by a third party. The purpose of this method will be to identify the information security culture artifacts present in an organization. Schein & Schein state that artifacts are thought of "as the phenomena that you would see, hear, and feel when you encounter a new group with an unfamiliar culture" (Schein & Schein, 2016, p. 17). Based on this statement, having an individual unfamiliar with an organization observe aspects of the organization related to information security would allow for the identification and assessment of artifacts. A formal observation process will need to be established and some considerations include determining what is a priority to observe, how long observations will occur, and how the presence or absence of an artifact influences the organization's information security culture. Some of the information security culture measurement tools that have been proposed in academic research over the years use observations as part of their process, future research plans can therefore build upon existing methods and lessons learned.

The use of a multi-method approach is the focus of future research because each single measurement method has its own limitations, so by combining methods the goal is to obtain a more accurate and detailed analysis and measurement of an organization's information security culture. The three methods discussed plan to be addressed in future research studies with the hopes of combining them, or other methods, to create a resource for consultants, organizations, and potentially others to measure information security culture.

References

AlHogail, A., & Mirza, A. (2015). *Organizational Information Security Culture Assessment*. Retrieved February 23, 2023, from http://www.worldcomp-proceedings.com/proc/p2015/SAM6057.pdf

Alnatheer, M., Chan, T., & Nelson, K. (2012). *Understanding And Measuring Information Security Culture*. Retrieved February 23, 2023, from https://core.ac.uk/download/pdf/301358212.pdf

Chen, Y., Ramamurthy, K. (R., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Corritore, M., Goldberg, A., & Srivastava, S. (2019, December 17). *The New Analytics of Culture*. Harvard Business Review. Retrieved February 21, 2023, from https://hbr.org/2020/01/the-new-analytics-of-culture

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—perspectives from academia and industry. *Computers & Security*, *92*. https://doi.org/10.1016/j.cose.2020.101713

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

Data Breach Investigations Report. Verizon Business. (2022). Retrieved February 6, 2023, from https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-not-the-human-element/

Fujs, D., Mihelič, A., & Vrhovec, S. L. (2019). The power of interpretation: Qualitative methods in cybersecurity research. *Proceedings of the 14th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3339252.3341479

KnowBe4. (2022). *Introducing the Security Culture Maturity Model*. KnowBe4. Retrieved February 18, 2023, from https://www.knowbe4.com/hubfs/Security-Culture-Maturity-Model-WP_EN-US.pdf?hsCtaTracking=24c36a2c-2f58-4838-83ca-66e1ad0a6bb6%7Cdbfdab2f-9660-4073-ac88-e93fd6e37fbf model

KnowBe4. (2019, May 21). *KnowBe4 acquires CLTRE; shines spotlight on Security Culture Measurement*. KnowBe4 Press Releases. Retrieved February 21, 2023, from https://www.knowbe4.com/press/knowbe4-acquires-cltre-shines-spotlight-on-security-culture-measurement

KnowBe4. (2019, October). *KnowBe4 Security Culture Survey*. Retrieved from https://helpimg.s3.amazonaws.com/KMSAT/assessments/KB4_SecurityCultureSurvey.pdf

KnowBe4. (n.d.). *Security culture framework*. KnowBe4 Research. Retrieved February 18, 2023, from https://research.knowbe4.com/security-culture-framework

KnowBe4. (n.d.). *The Security Culture Survey*. KnowBe4 Research. Retrieved February 18, 2023, from https://research.knowbe4.com/security-culture-survey

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

Niekerk, J. V., & Solms, R. V. (2005). A holistic framework for the fostering of an information security sub-culture in organizations, 1–13.

Orehek, Š., & Petrič, G. (2021). A systematic review of scales for measuring information security culture. *Information & Computer Security*, *29*(1), 133–158. https://doi.org/10.1108/ics-12-2019-0140

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2020). Measuring the security culture in organizations: A systematic overview of existing tools. *Security Journal*, *34*(2), 340–357. https://doi.org/10.1057/s41284-020-00228-4

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

Sjouwerman, S. (n.d.). *Stanford Research: 88% of data breaches are caused by human error*. Security Awareness Training Blog. Retrieved February 19, 2023, from https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

Sobers, R. (2022, August 3). *166 cybersecurity statistics and trends [updated 2022]*. Varonis. Retrieved February 19, 2023, from https://www.varonis.com/blog/cybersecurity-statistics

Tolah, A., Furnell, S. M., & Papadaki, M. (2017). A Comprehensive Framework for Cultivating and Assessing Information Security Culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance*, 52–64.

Tolah, A., Furnell, S. M., & Papadaki, M. (2019). A Comprehensive Framework for Understanding Security Culture in Organizations. *12th IFIP World Conference on Information Security Education (WISE)*, 143–156. https://doi.org/10.1007/978-3-030-23451-5_11

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the Information Security Culture Key Factors Framework. *Computers & Security*, *108*, 102354. https://doi.org/10.1016/j.cose.2021.102354

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

U.S. Office of Personnel Management. (n.d.). *Situational Judgment Tests*. U.S. Office of Personnel Management. Retrieved February 20, 2023, from https://www.opm.gov/policy-data-oversight/assessment-and-selection/other-assessment-methods/situational-judgment-tests/#:~:text=Situational%20judgment%20tests%20(SJTs)%20present,how%20they%20would%20handle%20it