https://doi.org/10.48009/3_iis_2020_95-104

Issues in Information Systems
Volume 21, Issue 3, pp. 95-104, 2020

THE ORGANIZATIONAL SECURITY INDEX: A TOOL FOR ASSESSING THE IMPACT OF NATIONAL CULTURE ON INFORMATION SECURITY ATTITUDES IN SLOVENIA AND THE UNITED STATES

Fred Hoffman, Mercyhurst University, fhoffman@mercyhurst.edu
Robert Joseph Skovira, Robert Morris University, skovira@rmu.edu

ABSTRACT

This study seeks to enhance understanding of the role that national culture plays in influencing employee attitudes and behaviors with respect to information security. Commercial firms and governmental organizations are increasingly dependent on a variety of relationships with foreign organizations staffed by individuals raised and socialized in their own national culture. Information security professionals agree that people, rather than technology, pose the greatest threat to information within an organization. As commercial organizations recognize the importance of establishing an effective information security culture, the importance of understanding the security-related attitudes of the workforce becomes apparent. The impact of national culture on information security attitudes and behavior has relevance not only in the commercial world, but also in the public sector, as government entities engage with foreign partners in activities ranging from information exchanges to multinational, coalition military operations. One of the most widely-used theoretical models used to assess and describe national culture, and to compare one national culture to another, is the framework developed by Hofstede (1980). This study employs an explanatory sequential mixed methods model to examine how national culture influences the attitudes of employees in an insurance company in Slovenia and a maritime industry firm in the United States. Building upon Hofstede's work, this study proposes an Organizational Security Culture Index, or OSCI, as a tool for helping gauge how national culture influences information security-related attitudes in a workforce.

Keywords: National culture, information security, dimensions of national culture

INTRODUCTION

This study was the consequence of four converging and interrelated trends: *Globalization*, *outsourcing*, *digitization*, and the evolving nature of *information security*. Levitt (1983) introduced the term *globalization* to describe companies' tendency to expand abroad in search of cheaper labor and new worldwide markets. Since the 1980s, companies have not only aggressively expanded into foreign markets, they have also seized opportunities to *outsource* certain non-core functions to foreign joint venture partners, suppliers, and contractors, a practice that has allowed companies to "shorten and flatten their organizations by concentrating their limited resources on a relatively few knowledge-based core competencies where they can develop best-in-world capabilities" (Quinn, 1994, p. 12). While such information technology advances as the internet, mobile phones, and wifi facilitated and accelerated both globalization and outsourcing, it was the *digitization* of data that made international business relationships function at the speed of business, replacing paper documents with digitized data that could be easily captured, stored, and disseminated. Unfortunately, the digitization of data also meant that sensitive corporate information and intellectual property (IP) was no longer retained on paper and secured in a safe; it was increasingly digitized, stored, manipulated, and exchanged via corporate information systems (Williamson, 1996). External and internal threats to the security of that information soon arose. As companies increasingly suffered the loss of IP and other invaluable information due to both internal and external threats, they responded by investing in technology to mitigate those threats (Hills and Anjali, 2017). However, information security professionals agree that the key to *information security* in an organization is not technology, but rather "human behavior and organizational structures and policies" (Posey, Roberts, & Lowry, 2015, p. 180).

Researchers have taken several different approaches to understanding the factors influencing the information security-related attitudes of an organization's members. As the literature review explains, the initial focus was on understanding what prompted (or constrained) individuals. More recently, researchers have also studied *cultural* influences on individuals' attitudes toward information technology. The purpose of this study was to expand and focus on the impact that a national culture has on attitudes toward information security.

After spending a lifetime studying national culture around the globe, Hofstede (2010) asserts that the culture of individual nations can be identified and assessed across six different cultural dimensions. Other research has revealed that national culture influences *organizational* culture (Ifinedo, 2014; Căpăţînă & Schin, 2013; Minkov, 2012; Johnston, Warkentin, & Luo, 2009; Jais, 2007; House, Hanges, Javidan, Dorfman, & Gupta, 2004), and that organizational culture influences an organization's *information security* culture (Tang, Li, & Zhang, 2016; D'Arcy & Greene, 2014; Baggett, 2003).

Research has revealed how national culture influences certain IT-related behaviors (Straub, 1994; Iivonen, Sonnenwald, Parma, & Poole-Kober, 1998; Asai & Fernando, 2011). In recent years, a number of researchers have applied one or more of Hofstede's six dimensions of national culture to compare information technology-related behaviors in two or more countries (Tang, Li, & Zhang, 2016; Ifinedo, 2014; Hovav & D'Arcy, 2012; and Dinev, Goo, Hu, & Nam, 2009). What these various researchers did not focus on, however, was how national culture impacts attitudes toward information security. The purpose of this study was to address this gap in the literature by comparing the information security-related attitudes of two groups of individuals who were socialized in distinctly different national cultures.

CULTURE AND SECURITY

Hofstede (1980), who described culture as "the collective programming of the mind which distinguishes the members of one human group from another" (p. 21), asserted that the term *culture* could be applied at the level of nations, societies, organizations, professions, and even individual families. Prompted by the pioneering work of Geertz (1973), and driven by a desire to explain the phenomenal economic success of Japanese firms during the 1980s, "academics became increasingly interested in how culture affected behavior in organizations" (Chatman & O'Reilly, 2016, p. 201). Indeed, organizational culture became the subject of many books, conferences, and scholarly research in the late 1970s and 1980s (Chatman & O'Reilly, 2016).

In their respective literature reviews on the subject of information security culture, both Karlsson, Åström, and Karlsson (2014) and Connolly and Lang (2013) found Schein's (1985) to be the most commonly-cited organizational culture model. Schein first introduced his model of organization culture and then refined it over three decades; for him, three levels of analysis for organizational culture are artifacts, espoused beliefs and values, and taken-for-granted underlying basic assumptions (Schein & Schein, 2016). Expanding beyond his well-known theoretical and research work on the subject of *national* culture, Hofstede (2010) asserts that *organizational* culture: (1) is holistic; (2) is historically determined; (3) has observable rituals and symbols; (4) is created and sustained by the individuals who form the organization, (5) is soft, and (6) is resistant to change. "Organizational culture integrates a team of professionals, offering benefits such as a common identity, shared beliefs, vocabulary, rituals, values, work style, etc," (Piwowarski, 2013, p. 43). Chmura (2016) described organizational culture in terms of its values, standards, and symbols.

An important subset of an organization's overall culture is its information security culture. The linkage between organizational culture and an organization's information security culture has been asserted by numerous researchers (Hills & Anjali, 2017; Da Veiga, 2016a; Chmura, 2016; Tang et al., 2016; D'Arcy & Greene, 2014; Lopes & Oliveira, 2014; Lacey, 2010; Chang & Lin, 2007). Lopes and Oliveira (2014) asserted that "one cannot talk about information security in an organization without addressing and understanding the information security culture of that institution" (p. 277). Specifically, an information security culture "consists of a shared pattern of values, mental models and activities that are traded among an organization's employees over time, affecting information security" (Karlsson et al, 2014, p. 247). Key components of an organization's security culture are information security, cybersecurity, and physical security (see Figure 1). The criticality of having a healthy organizational security culture was clear from analysis of statistics about security violations and incidents at Russian nuclear facilities that Geraskin, Krasnoborodko, Glebov, & Piskureva (2015) acquired from the Russian State Corporation Rosatom and Russian State Regulatory Agency *Rostekhnadzor*, which revealed that "as many as 80% of the root causes of security violations are related to human error or other culture-related issues" (p. 332).

If understanding organizational culture is necessary to comprehend an organization's information security culture, then understanding national culture is essential for understanding organizational culture, because organizations in a given society are predominantly formed by individuals whose attitudes are shaped by the larger society in which they live (Hofstede, 2010). Like Geertz (1973), Hofstede (2010) also acknowledged the importance of symbols, heroes, ritual, and values, which he labeled the "four manifestations of culture" (p 7). One of the most widely-used models for describing national culture, and to compare one national culture to another, is the theoretical framework developed by Hofstede (1980). Using survey data collected twice from 40 different countries, first in 1968 and then again in 1972, Hofstede analyzed the results of over 116,000 usable surveys to develop his framework (Hofstede, 1980). Hofstede asserted his research identified "four main dimensions along which dominant value systems in the 40 countries can be ordered and which affect human thinking, organizations, and institutions in predictable ways" (Hofstede, 1980, p. 11). Hofstede's original dimensions of national culture consisted of four indices: Power Distance Index (PDI), Uncertainty Avoidance Index (UAI), Individualism Index (IDV), and Masculinity Index (MAS). Hofstede later added a fifth dimension, Long-Term Orientation (LTO) (Hofstede, 1991), and subsequently a sixth, Indulgence Versus Restraint (IVR) (Hofstede, 2010).

Figure 1. Organizational Security Culture and its components as a subset of Organizational Culture.

As globalization, outsourcing, digitization, and Internet access proliferated around the world in the 1980s and 1990s, researchers became increasingly interested in the ways that culture influenced attitudes and behavior towards information technology. As Asai & Fernando (2011) found, "People from different cultures react in different ways in similar situations" (p. 119). A common method for comparing attitudes toward information technology was the application of Hofstede's dimensions of national culture. Some of the researchers who applied one or more of Hofstede's six dimensions of national culture to compare information technology-related behaviors in two or more countries include Tang, Li & Zhang (2016), Ifinedo (2014), Hovav & D'Arcy (2012), and Dinev, Goo, Hu, & Nam (2009).

Although a number of researchers have applied Hofstede's dimensions of national culture to an examination of IT-related attitudes, very few explicitly focused on comparing how national culture might impact information security-related attitudes within organizations in different countries. The aim of this study, then, was twofold: First, to address this gap in the literature; second, to develop and test an Organizational Security Culture Index (OSCI) that could be used to consistently assess and compare organizational cultures by adapting Hofstede's (2010) Values Survey Model collection methodology and his six dimensions of national culture to specifically address participants' attitudes toward organizational security culture. The research question was, "How does national culture influence information security-related attitudes within an organization?" To answer this question, this researcher examined how Hofstede (2013) studied national culture across six different dimensions, and adapted Hofstede's (2013) approach to specifically focus on attitudes toward information security.

ADAPTING HOFSTEDE'S VALUES SURVEY MODULE

Values Survey Module (VSM) 2013

Over a period of four decades starting in the mid-1960s, Hofstede (2013) developed a succession of Values Survey Modules (VSM), which he described as instruments for comparing "culturally-influenced values and sentiments of similar respondents from two or more countries" (Hofstede, 2013, p. 2). Four indices comprised Hofstede's original dimensions of national culture; these were the Power Distance Index (PDI), Uncertainty Avoidance Index (UAI), Individualism Index (IDV), and Masculinity Index (MAS). Later, Hofstede added a fifth dimension, Long-Term Orientation (LTO) (Hofstede, 1991), and then a sixth, Indulgence versus restraint (IVR) (Hofstede, 2011). The current iteration of Hofstede's VSM is VSM 2013, which includes the four original dimensions of national culture first

conceptualized in VSM 82, along with the more recently-developed dimensions of LTO and IVR. Throughout this paper, references to Hofstede's Six Dimensions of National Culture (6DNC) refer to descriptions of those dimensions provided by Hofstede and contained in VSM 2013.

Organizational Security Culture Index (OSCI)

Whereas Hofstede's VSM were developed to assess and characterize countries across six different cultural dimensions, this researcher developed the Organizational Security Culture Index (OSCI) to be more narrowly-focused, as a tool for assessing information security attitudes within an organization through the prism of Hofstede's six national culture dimensions. This researcher did not use a pre-existing survey instrument because of the need to ask survey participants information security attitude-related survey questions that aligned with each of Hofstede's (2010) six dimensions of national culture. Therefore, this researcher developed 13 survey questions related to information security that were each rooted in definitions of one of the six current dimensions of national culture as described by Hofstede in *Cultures and Organizations: Software of the Mind* (Hofstede, 2010) and the VSM 2013 manual. This researcher employed fewer questions in the OSCI survey than Hofstede used in his VSM 2013 to avoid survey fatigue and also due to the narrower focus of the OSCI survey.

This researcher sought to ascertain: (1) whether responses to information security-related questions based on Hofstede's 6DNC would reflect the cultural characteristics Hofstede associated with those DNC, (2) how OSCI survey scores for a particular national culture dimension would compare with Hofstede's dimension score for that particular culture, and (3) how OSCI scores for one national culture would compare with the OSCI scores for a second national culture. Alignment between OSCI scores and Hofstede's 6DNC country scores could indicate that national culture does, in fact, influence organizational security culture.

This researcher developed a survey instrument in which each of 13 substantive questions was based on characteristics associated with a particular dimension of Hofstede's 6DNC (see Table 1). For example, this researcher included in the study three information security-related questions that were based upon Hofstede's definition of PDI, and scored them (as Hofstede did in his VSM) using the same 100-point index. Spatial considerations prevent a thorough discussion of how the entire OSCI was developed; this will be the subject of a separate article. However, one example should illustrate this researcher's approach.

Table 1. Mapping of survey questions to Hofstede's six dimensions and the Organizational Security Culture Index.

Survey Questions	Hofstede National Culture Dimension	Organizational Security Culture Index
1,2,3	PDI	PDI-OSCI
4,5	IDV	IDV-OSCI
6,7	MAS	MAS-OSCI
8,9	UAI	UAI-OSCI
10,11	LTO	LTO-OSCI
12,13	IVR	IVR-OSCI

Hofstede (2013) describes his Power Distance dimension as "the extent to which the less powerful members of institutions and organizations with a society expect and accept that power is distributed unequally" (p. 7). According to Hofstede (2010), individuals from a higher Power Distance culture are more likely to accept authority, and do what their superiors tell them to do, than their counterparts in a lower power distance culture. Hofstede (2010) rates Slovenia as a *high* power distance culture (71 out of 100), and the U.S. as a *low* power distance culture (40 out of 100). For example, survey question 1 asked participants to choose a Likert scale response to the statement, "If a manager instructed me to violate an information security rule in order to complete a critical project more quickly, I would ignore the manager's instruction and comply with that information security rule." Extrapolating from Hofstede's characterization of high and low power distance cultures, this researcher anticipated that employees in a

higher power distance culture (Slovenia, 71) would be more likely than their counterparts in a low power distance culture (U.S., 40) to accept that sanctions imposed on violators of company information security policies will not necessarily be applied evenly, but instead be influenced by the person's position within the company.

THE STUDY

Research orientation and method

The study was based on a post-positivist research orientation, which according to Creswell (2018) disputes the positivist belief in the absolute truth of knowledge, especially with respect to human behavior. An explanatory sequential mixed methods design was used in two phases: Phase I was quantitative (online surveys), and Phase II was qualitative (semi-structured interviews). Following statistical analysis of Phase I data, semi-structured interview questions were then developed and posed to interview subjects from each company. As Creswell (2018) explains, "The overall intent of this design is to have the qualitative data help explain in more detail the initial quantitative results" (p. 222).

Phase 1 (survey)

This researcher examined the questions used by Hofstede in his VSM survey tool and created the OSCI survey, a truncated version of Hofstede's (2013) VSM, containing questions that were specifically focused on information security and aligned with each of Hofstede's (2010) six dimensions of national culture. The OSCI survey consisted of 23 substantive and demographic questions.

A Slovenian company (approximately 1,200 employees) and a U.S. company (approximately 250 employees) both agreed to participate. Because the purpose of the survey was to gather respondent attitudes about IT security from a very specific population, the study involved *purposive* (also known as judgmental, selective, or subjective) sampling, which "involves designating a group of people for selection because you know they have some traits you want to study" (Nardi, 2014, p. 125).

Data collection was accomplished via a 23-question, anonymous, online survey administered via the Internet, with possible answers on a five-point Likert scale ranging from *Strongly Disagree* to *Strongly Agree*. The first 14 content questions addressed participant attitudes towards information security-related behavior, and the following nine questions were demographic. This researcher developed 13 of the 14 substantive questions as part of his Organizational Security Culture Index; the 14th question was a substantive one that had been requested for inclusion in the survey by the Slovenian company, and which was asked of both Slovenian and U.S. survey participants.

The participant population was limited to male and female adults (18 years of age or older) who were full-time employees of the same company, whose country of origin was Slovenia (in the case of the Slovenian company) or the U.S. (in the case of the U.S. company), and who had access to their employer's computer network and data as part of their daily work duties. Using the *QuestionPro* online survey tool, this researcher obtained completed surveys from 168 respondents from the Slovenian company and 62 completed surveys from U.S. company employees. All 168 Slovenian surveys were usable, but only 55 of the U.S. surveys were because seven U.S. participants indicated they had been born and raised outside the U.S.

Of the 873 Slovenian employees to whom their employer had emailed survey participation solicitation emails, 168 respondents opted to fill out the survey, resulting in a response rate of more than 19%. When examining for outliers in the Slovenian survey data file, this researcher identified 12 mild and 36 extreme outliers; the 36 extreme outliers were Winsorized to mitigate the effect of outliers on the data set.

After collection, data was downloaded from *QuestionPro* and entered into an SPSS data file, and a code book was created that explains the data file entries. Collected data was statistically analyzed using SPSS software.

Phase II (semi-structured interviews)

This researcher coordinated with the participating Slovenian firm to conduct thirteen, face-to-face, semi-structured interviews of company employees at corporate headquarters in Slovenia. This researcher also coordinated with the U.S. firm to conduct interviews of fifteen of its employees by phone, rather than in person, because some of the U.S. interview participants were located around the United States. There are three different types of interviews: Structured,

unstructured, or semi-structured (Berg, 1989). Semi-structured interviews employ a series of previously-prepared questions that are posed to the interview subject in a logical, predetermined order, while affording an interviewer the latitude to interject probing or follow-up questions in response to interviewee responses. Consistent with the semi-structured interview style, the same core questions were asked of both Slovenian and U.S. interviewees, along with various probing questions as appropriate.

This researcher asked the CEO of each participating company to nominate a mix of interview candidates including senior company managers, IT managers, mid-level (non-IT) managers, and non-supervisory employees, and a mix of males and females in different age groups. This was accomplished. All interviews were conducted in English. In the case of Slovenia, all interviewees demonstrated full professional competency in English.

Interviews lasted between 30 minutes and two and a half hours; all were recorded, transcribed, and subjected to content analysis, starting with coding. In qualitative research, a *code* is "a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data" (Saldaña, 2015, p. 3). This researcher then noted when certain codes reoccurred in the same or multiple interviews and thematically clustered them.

LIMITATIONS

One significant challenge associated with studying this topic was obtaining corporate concurrence for the study. This researcher initially approached the Chief Information Security Officer (CISO) of six large, multinational corporations to pitch the proposed study. In all six cases, the CISO was immediately supportive and enthusiastically pitched the concept to the corporate board of directors. Unfortunately, CISO enthusiasm was not shared by the human resources and/or general counsel, which resulted in all six companies declining to participate out of fear the findings could reflect negatively on the company. Fortunately, this researcher was able to secure approval from the two companies that ultimately participated in this study through a combination of personal/professional relationships and face-to-face meetings with corporate leadership. Both companies were in the process of rethinking their approach to information security training, which made the study timely and beneficial to them.

This researcher acknowledges that, by virtue of their education, experience, and the nature of their jobs, study participants represented a targeted segment, and not a diverse cross-section, of either the Slovenian or U.S. population. However, because the focus of this research was on the impact of national culture on information security-related attitudes within a particular organizational culture, the two samples were proved suitable for the purpose of this study.

In addition to being limited to one company in each of the two countries studied, the study was also limited to Slovenia and the U.S. Verification of the OSCI tool would necessitate its use in many more countries.

One acknowledged limitation of this study is its sample size. In his 2013 Values Survey Module Manual, Hofstede asserted, "An ideal size for a homogeneous sample is 50 respondents" (Hofstede, 2013, p. 2). Given the admittedly modest objectives of this limited-scope study, having only 55 usable surveys from the U.S. company, and 168 usable surveys from the Slovenian company, was adequate. However, in order to achieve greater confidence about what to deduce from OSCI scores within a particular national culture, additional research should be conducted in multiple organizations in a given country, and over time.

Another acknowledged limitation of the OSCI tool was the number of survey questions asked. With respect to his VSM 82, which was widely used as a values survey tool for 12 years, Hofstede asserted that only 13 of the content questions were actually needed to compute scores on his four dimensions of national culture (Hofstede, 2013). Asking more survey questions would increase confidence, but also raise the risk of participant fatigue.

Even with only 23 questions, it is not possible to verify the truthfulness of respondents (Emerson, Felce, & Stancliffe, 2013; Gonyea, 2005). Despite being assured of anonymity, respondents might still fear their responses could be held against them, which could influence their answers (Knapp & Kirk, 2003). Finally, the limitations associated with self-reporting data also create certain risks to validity, to include: a desire to be viewed positively, issues with accuracy, self-selection biases, and the participants' desire to be viewed in a positive light (Rosenbaum, Rabenhorst, Reddy, Fleming, & Howells, 2006).

FINDINGS

Analysis of the quantitative and qualitative data gathered during this study revealed that national culture did, in fact, impact the information security-related attitudes of the Slovenian and U.S. populations, and in ways that were consistent with Hofstede's multi-faceted characterization of each culture: For each of Hofstede's six cultural dimensions, the country with the higher DNC score also had a higher OSCI score than the other country. However, the differences between Hofstede's DNC scores (Figure 2) were more pronounced than the differences between the OSCI scores for each cultural dimension (Figure 3). As will be discussed, there are a number of possible reasons for this.

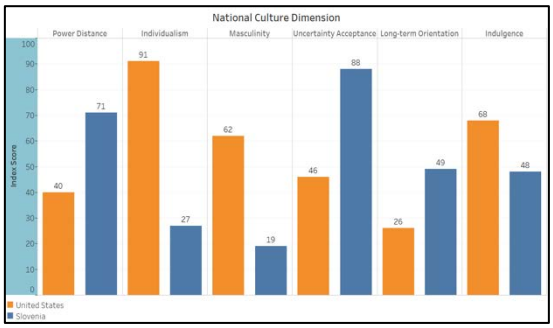

Figure 2. Comparison of country scores for the U.S. and Slovenia for each of Hofstede's (2010) six dimensions of national culture.

Identifying how national culture impacts the information security-related attitudes of members of an organization is useful because this knowledge enables organizational leadership to not only better understand how employees think about information security, but also gain insight as to what factors may be contributing to their employees' information security-related attitudes. That knowledge, in turn, enables recognition of needs concerning information security training and information system policy.

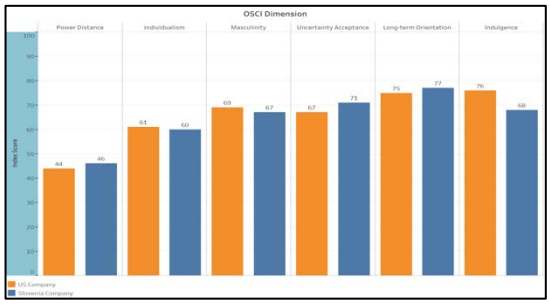

Figure 3. Comparison of Organizational Security Culture Index (OSCI) scores for the Slovenian

National culture is not static; in some ways, it is a moving target. In countries with very traditional cultures, the pace of change may be glacial; in others, significant changes can occur far more quickly (Hofstede, 2010). For example, during interviews for this study, adult Slovenians socialized in Tito's Yugoslavia consistently evidenced certain attitudes about information security that were rather different from those of their younger colleagues who had been born and raised after Yugoslavia collapsed. A 55-year-old male who grew up without a television set in the former Yugoslavia and a 25-year-old female who has had a cell phone and a computer for more than half of her young life may both be from the same town, work for the same company, and be products of the same national culture, but their life experiences *within that same national culture* may have been radically different, cause them to respond to OSCI scenario-based questions in very different ways, and reflect very different attitudes they may have with respect to certain aspects of information security. Such revelations make clear that while national culture is useful for identifying general tendencies within a population, a more nuanced understanding of differences *within* a culture, the reasons for those differences and their potential attitudinal implications, remains necessary.

CONCLUSIONS

Trends in globalization, outsourcing, digitization, and information security revealed the need to better identify and understand factors influencing the information security-related attitudes and behaviors of organizational members. This study represents one small methodological contribution to that growing body of literature by examining not only *whether* national culture can influence information security, but also by offering a potential methodology for *how* to conduct a meaningful assessment of specific cultural impacts.

A second methodological contribution was the use of an explanatory sequential mixed methods approach for this study. While the quantitative data from surveys was essential for identifying national culture impacts, the qualitative

data from semi-structured interviews proved invaluable for understanding the *reasons* for those various impacts. Surveys revealed the *what*, while interviews revealed the *why*. For example, U.S. firm interviewees consistently described how their company possesses a stable, positive, communicative workforce with a longstanding culture of physical security. Such knowledge is highly useful for crafting the delivery methods, selecting suitable training content, and choosing feedback and verification techniques that will be well-received by the workforce, thereby maximize the prospects of success.

This researcher fully acknowledges that the OSCI survey questions themselves represented an admittedly crude, initial attempt to craft information security-related questions aligned to each of Hofstede's six dimensions of national culture. As a proof-of-concept, the OSCI survey was adequate; however, future researchers might consider crafting better (and maybe more) questions to more accurately gauge the impact of national culture on participants' information security attitudes.

This study sought to address an identified gap in the literature by examining how national culture impacts the information security-related attitudes and behaviors of organizational members in two different companies in two different national cultures. Rather than simply measure how national culture impacts attitudes in two different organizations and national cultures, this study also introduced the Organizational Security Culture Index as a rudimentary tool for assessing specific ways in which the influence of national culture manifests itself in the attitudes of organizational members. The research findings were encouraging in that they revealed national culture does, in fact, influence attitudes toward information security.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2): 179–211. doi:10.1016/0749-5978(91)90020-T.

Asai, T. & Fernando, S. (2011). Human-related problems in information security in Thai cross-cultural environments. *Contemporary Management Research, 7*(2): 117-141.

Baggett, W. O. (2003). Creating a Culture of Security. *Internal Auditor, 60*(3), 37-41.

Berg, B. L. (1989). *Qualitative Research Methods for the Social Sciences.* Allyn and Bacon, Needham Heights, Massachusetts.

Căpăţînă, A., & Schin. G. (2013). Minding the cultural gaps between different countries - A real challenge for the international managers. Review of International Comparative Management / Revista de Management Comparat International, *14*(5), 704-712.

Chatman, J., & O'Reilly, C. (2016). Paradigm lost: Reinvigorating the study of organizational culture. *Research in Organizational Behavior, 36***,** 199-224.

Chmura, J. (2016). The impact of positive organizational culture values on information security management in the company. *Journal of Positive Management, 7*(1), 87-98. doi:10.12775/JPM.2016.006

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3): 438-458.

Connolly, Y., Lang, M., Gathegi, J., & Tygar, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: a qualitative study. *Information and Computer Security, 25*(2): 1-24. doi: 10.1108/ICS-03-2017-0013

Connolly, L., & Lang, M. (2012). Investigation of cultural aspects within information systems security research. *The 7th International Conference for Internet Technology and Secured Transactions* (ICITST 2012). London: IEEE Digital Library, 105-111.

Creswell, J. (2018). *Research design*: *Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, CA: Sage.

D'Arcy, J., and Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474-489. doi:10.1108/IMCS-08-2013-0057

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *Proceedings of the 2016 SAI Computing Conference* (SAI): 1006-1015.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information and Computer Security*, *24*(2), 139-151. doi:doi:10.1108/ICS-12-2015-0048

Dinev, T., Goo, J., Hu, Q. & Nam, K. (2009). User behavior towards protective information technologies: The role of national cultural differences, *Information Systems Journal*, *19*(4), 391-412.

Emerson, E., Felce, D., and Stancliffe, R. (2013). Issues concerning self-report data and population-based data sets involving people with intellectual disabilities. *Intellectual and Developmental Disabilities*, *51*(5), 333-348. doi:10.1352/1934-9556-51.5.333

Geertz, Clifford (1973). *The interpretation of cultures*. New York: Basic Books.

Geraskin, N. I., Krasnoborodko, A. A., Glebov, V. B., & Piskureva, T. A. (2015). Nuclear security culture enhancement: the role of culture coordinators at Russian nuclear sites. *Defense & Security Analysis*, *31*(4), 330-345. doi:10.1080/14751798.2015.1087103

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal*, *30*(1), 142-152. doi:10.1057/sj.2015.36

Hirschi, T. (1969). *Causes of Delinquency*. Berkeley, CA: University of California.

Hofstede, G. (1980). *Culture's consequences: International differences in work-related values*. London: Sage.

Hofstede, G., Hofstede, G., & Minkov, M. (2010). *Cultures and organizations: Software of the mind*. London: McGraw-Hill.

Hofstede, G., & Minkov, M. (2013). VSM 2013: Values Survey Module 2013 Manual.

Hofstede, G., & Minkov, M. (2013). VSM 2013: Values Survey Module 2013 Questionnaire (English language version).

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (Eds.). (2004). *Culture, leadership, and organizations: The GLOBE study of 62 societies*. Thousand Oaks, CA: Sage publications.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99-110. doi:https://doi.org/10.1016/j.im.2011.12.005

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1): 83-95.

Iivonen, M., Sonnenwald, D. H., Parma, M., & Poole-Kober, E. (1998). Analyzing and understanding cultural differences: Experiences from education in library and information studies. *64th IFLA General Conference*, 16-21 August 1998, 1-10.

Jais, S. D. (2007). *The Successful Use of Information in Multinational Companies: An exploratory study of individual outcomes and the influence of national culture*. Springer Science & Business Media. http://dx.doi.org/10.1007/978-3-8350-9371-3

Karlsson, F., Åström, J., and Karlsson, M. (2015). Information security culture -- state-of-the-art review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246-285.

Knapp, H., & Kirk, S. A. (2003). Using pencil and paper, Internet and touch-tone phones for self-administered surveys: does methodology matter? *Computers in Human Behavior*, *19*(1), 117-134.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4-13. doi:10.1108/09685221011035223

Lopes, I. & Oliveira, P. (2014). Understanding information security culture: A survey in small and medium sized enterprises. In Á. Rocha, A. M. Correia, F. B. Tan & K. A. Stroetmann (eds). *New Perspectives in Information Systems and Technologies, Volume 1*. Springer International Publishing, 277-286.

Minkov, M. (2012). *Cross-cultural analysis: the science and art of comparing the world's modern societies and their cultures*. Thousand Oaks, CA: Sage.

Nardi, P. M. (2014). *Doing survey research*. London: Routledge.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, p. 1-11.

Piwowarski, J. (2013). Ethics of organizational culture as an existing condition of security culture. *Science & Military Journal*, *8*(1), 41-46.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214. doi:10.1080/07421222.2015.1138374

Quinn, J. B., & Hilmer, F. G. (1994). Strategic outsourcing. *Sloan management review*, *35*(4), 43.

Rosenbaum, A., Rabenhorst, M. M., Reddy, M. K., Fleming, M. T., & Howells, N. L. (2006). A comparison of methods for collecting self-report data on sensitive topics. *Violence and victims*, *21*(4), 461-471.

Saldaña, J. (2015). *The coding manual for qualitative researchers.* Sage.

Schein, E. H. (1985). Defining organizational culture. *Classics of organization theory*, *3*(1), 490-502.

Schein, E., and Schein, P. (2016). *Organizational culture and leadership*. New York: John Wiley & Sons.

Straub, D. W. (1994). The effect of culture on IT diffusion: E-mail and fax in Japan and the U.S. *Information Systems Research*, *5*(1), 23-47.

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

Williamson, J. G. (1996). Globalization, convergence, and history. *The Journal of Economic History*, *56*(2), 277-306.