

DOI: https://doi.org/10.48009/3_iis_2021_127-141

Assessing U.S. and Slovenian organizational security culture with Hofstede's national culture framework

Fred Hoffman, *Mercyhurst University*, fhoffman@mercyhurst.edu

Abstract

It is the consensus among information security professionals that it is people, rather than technology, that poses the greatest threat to information security within an organization. As government organizations and private firms alike are increasingly urged to recognize the importance of establishing an effective information security culture, the importance of understanding the security-related attitudes of the workforce becomes apparent. This study examines the role that national culture plays in influencing employee attitudes and behaviors with respect to information security. One of the most widely used frameworks for assessing national culture, and for comparing one national culture to another, Hofstede's (1980) six dimensions of national culture. This study uses Hofstede's framework and an explanatory sequential mixed methods model to examine how national culture influences the attitudes of employees in two mid-sized companies, one in Slovenia and one in the United States. Differences in national culture were found to have an impact on the attitude that participating Slovenian and U.S. employees had with respect to information security.

Keywords: National culture, organizational culture, information security

Introduction

In recent decades, Information Age businesses increasingly captured, stored, and electronically shared sensitive information in digital form. The digitization of information facilitated globalization, a worldwide trend that has resulted in significant changes to the structure, composition, and behavior of modern business. In addition to spurring globalization, the digitization of information also brought about some undesired consequences: Organizations now face serious threats not only from malicious internal and external actors seeking unauthorized access to valuable digital information, but also from non-malicious organization members whose failure to observe information security policies unintentionally puts their organization's sensitive information at risk.

Every organization in the world has its own corporate culture, a subset of which is its information security culture. In a world where organizations are increasingly interacting and sharing information with one another, information security breaches in one organization in one country can have serious negative consequences for that organization's partners, vendors, contractors, suppliers, and customers around the world; how organizations in one country address information security challenges can therefore have implications and consequences for other organizations around the world. Research has shown that national culture influences organizational culture (Ifinedo, 2014; Căpățînă & Schin, 2013; Minkov, 2012; Johnston, Warkentin, & Luo, 2009; Jais, 2007; House, Hanges, Javidan, Dorfman, & Gupta, 2004; Ralston, Holt, Terpstra, & Yu, 1997), and that an organization's information security culture is influenced by the overall organizational culture (Tang, Li, & Zhang, 2016; D'Arcy & Greene, 2014; Baggett, 2003). Given the influence of national culture on organizational culture, and the influence of organizational culture on information security culture within an organization, what influence does national culture have on employee attitudes and behaviors with respect to information security?

The purpose of this article is to describe how Hofstede's national culture framework was used to examine and compare the organizational security culture in a U.S. and a Slovenian firm. The value of this study is that it reveals the applicability of Hofstede's assessments of national culture to better understanding security-related issues in different countries. That understanding can help information security professionals understand culture-driven challenges and shortcomings and tailor security training and verification protocols accordingly. Hoffman and Skovira (2020) described how they created an organizational security index based on Hofstede's VSM methodology; that index was used in this study.

In the Introduction, this article introduces the reader to the concepts of national, organizational, and organizational security culture and describes how corporate culture can be created or modified. In Methodology, the article introduces Hofstede's Values Survey Modules and explains how they are used to evaluate and compare national cultures and also explains how other researchers have used Hofstede's methodology to look at other, non-security related aspects of information technology. The article then explains Hofstede's six dimensions of national culture, describes the two companies, and describes the explanatory mixed methods approach used in this study. In Results, the article presents findings comparing survey and interview responses from members of both the U.S. and Slovenian firms.

National and organizational culture

Culture

Culture is a term that seemingly defies standardized definition; a study by anthropologists in the early 1990s encountered no fewer than 164 different definitions in the anthropology literature for the word *culture* (Chatman & O'Reilly, 2016). While researchers may have proven unable to agree on a standard definition of culture, what they do agree upon is that culture exists, and that it merits investigation. Social anthropologist Geertz (1973) focused on that which could be observed and interpreted within a culture; not only speech and behavior, but also symbols and rituals. Geertz (1973) described culture as *semiotic*; that is, "that man is an animal suspended in webs of significance he himself has spun, I take culture to be those webs, and the analysis of it to be therefore not an experimental science in search of law but an interpretive one in search of meaning" (Geertz, 1973, p. 5).

Levels of culture: National, organizational, organizational security culture

Hofstede (1980) described culture as "the collective programming of the mind which distinguishes the members of one human group from another" (p. 21) and asserted that the term culture could be applied at the level of nations, societies, organizations, professions, and even individual families. Although Hofstede, Hofstede, & Minkov (2010) asserted that the word *culture* is used with respect to both nations and organizations, it is important to differentiate between the two. "Using the word culture for both nations and organizations suggests that the two kinds of culture are identical phenomena. This is incorrect: a nation is not an organization, and the two types of culture are of a different nature. The difference between national and organizational cultures is based on their different mix of values and practices" (Hofstede et al., 2010, p. 346).

In this study, culture was considered at three distinct levels: (1) national culture, (2) organizational culture, and the (3) information security culture within an organization. Of primary interest was the way in which national culture influences an organization's information security culture.

National culture

National culture is the predominant culture of a country. National culture does not start and stop at a country's borders, for example, a multi-ethnic country may have a predominant national culture and also one or more lesser cultures, and a country may have significant numbers of its population who live overseas yet subscribe to the fundamental aspects of the dominant national culture (Hofstede et al., 2010).

Organizational culture

Although the study of group culture was popularized by the work of such pioneering social anthropologists as Geertz (1973), it was only in the late 1970s and 1980s that the subject of culture at the *organizational* level became the popular subject of books, conferences, and scholarly research, driven in large measure by the desire to logically explain the phenomenal economic success of Japanese corporations during the 1980s (Chatman & O'Reilly, 2016).

Seeking to comprehend the reasons behind the success of Japanese corporations, U.S. researchers, in particular, began to study their organizational culture and practices, and "academics became increasingly interested in how culture affected behavior in organizations" (Chatman & O'Reilly, 2016, p. 201).

A healthy organizational culture provides both tangible and intangible benefits to its members.

"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.

Hofstede et al. (2010) assert 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.

How corporate culture can be created or modified

Zappos

Tony Hsieh was already a very successful businessman when he decided to create an online shoe retail firm that was built around its corporate culture (Riordan, 2013). Hsieh's corporate culture empowered, motivated, and focused Zappos employees (Sosnilo, Zorina, & Seleznev, 2018), enabling the company to become wildly successful in just a few years (Yugendhar & Ali, 2017).



Figure . Organizational security culture and its components as a subset of organizational culture.

Best Buy

Whereas Tony Hsieh proved it was possible to create a corporation in which corporate culture was a conscious, deliberate factor, Best Buy's CEO, Hubert Joly, demonstrated how to significantly change the trajectory of a company by improving its corporate culture. By 2012, Amazon's online shopping model was wreaking havoc among traditional brick-and-mortar retailers like Sears, JC Penney, Radio Shack, and Best Buy. Unlike these four competitors, Amazon sold to consumers online, and therefore did not require the hundreds of retail locations and the staff required to operate them, which enabled Amazon to sell at lower cost than its competitors (Wang, Hoffman, Lim, & Kwon, 2019). By October of 2018, Sears declared bankruptcy (Wahba, 2018), and by December 2018 industry experts were predicting that JC Penney would soon do likewise (Martin, 2018). In contrast to its peers, however, Best Buy was able to not only stave off bankruptcy, but reinvent itself (Wang, Hoffman, Lim, & Kwon, 2019). As Logan, King, & Fischer-Wright (2008) asserted, "Tribal Leaders focus their efforts on building the tribe, or, more precisely, upgrading the tribal culture. If they are successful, the tribe recognizes them as the leaders, giving them top effort, cult-like loyalty, and a track record of success" (p. 3). Best Buy's new CEO, Hubert Joly, not only changed much of the company's business model, but also invested time and effort into revamping the corporate culture by visiting Best Buy locations to speak with employees, working on-site for a week at a store, restoring an employee discount program, and improving employee training (Bariso, 2019). "Emotional intelligence is what caused Joly to recognize the importance of improving organizational culture and enabled him to become an effective tribal leader" (Wang, Hoffman, Lim, & Kwon, 2019, p. 139).

Methodology

The impact of national culture on attitudes toward information technology

As computers proliferated throughout workplaces and homes in the late 1980s and early 1990s, researchers became interested in the way culture influenced attitudes and behaviors with respect to IT. Some researchers compared the impact of national culture on workplace or information technology-related behavior in different countries. Straub (1994) examined how differences in culture influenced fax and email usage in the United States and Japan. Iivonen, Sonnenwald, Parma, & Poole-Kober (1998), who compared the attitudes towards technology of Finnish and U.S. college students collaborating through the use of electronic discussion groups, found that "cultural attitudes toward technology may influence people's beliefs and use of the technology" (p. 4). Or, as Asai & Fernando (2011) put it, "People from different cultures react in different ways in similar situations" (p. 119).

Some of the researchers who applied one or more of Hofstede's six dimensions of national culture to compare information technology-related attitudes and behaviors (but not information *security*-related attitudes and behaviors) in two or more countries include Tang, Li & Zhang (2016), Ifinedo (2014), Hovav & D'Arcy (2012), Dinev, Goo, Hu, & Nam (2009), Yoon (2009), Johnson et al. (2009), Schmidt, Johnston, Arnett, Chen, & Xi'an (2008), Chen, Medlin, & Shaw (2008), Waarts & van Everdingen (2005), Veiga, Floyd, & Dechant (2001), Milberg, Smith, & Burke (2000), Ralston, Holt, Terpstra, & Yu (1997).

Although researchers studied the impact of national culture on IT-related behavior, in many instances using Hofstede et al.'s (2010) dimensions of national culture, an identified gap in the literature was that there was no known study where Hofstede et al.'s (2010) dimensions of national culture model was used to compare information security attitudes in two or more countries.

Hofstede's approach to evaluating and comparing national cultures

Hofstede's Values Survey Modules (VSM)

Between 1966 and 1973, as an IBM employee, Hofstede (1980) conducted surveys around the world to learn about and compare the work-related values of IBM employees. Because the IBM survey questions used for those surveys “had not really been composed for the purpose of reflecting international differences in value patterns” (Hofstede et al., 2013, p. 10), over the subsequent four decades Hofstede developed his own 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 et al., 2013, p. 2). Hofstede's initial value survey instrument was VSM 80, which employed some of the content questions contained in earlier IBM employee. Two years later, Hofstede produced VSM 82, which he first publicly used in 1982, to survey IBM employees in 40 countries. Like the later iterations of the survey instruments that would succeed it, VSM 82 was comprised of both demographic and content questions, with the content questions in VSM 82 addressing the then-four cultural dimensions of Hofstede's dimensions of national culture theory: Power Distance Index (PDI), Individualism Index (IDV), Masculinity Index (MAS), and Uncertainty Avoidance Index (UAI). Although VSM 82 contained six demographic questions and 47 content questions, Hofstede asserted that only 13 of the content questions were actually needed to compute scores on his four dimensions of national culture. VSM 82 was widely used for 12 years (Hofstede et al., 2013). 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.

Hofstede's Six Dimensions of National Culture

One of the most widely used models used to describe 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, Neujen, Ohayy, & Sanders, 1990), and subsequently a sixth, Indulgence Versus Restraint (IVR) (Hofstede et al., 2010). Hofstede's six dimensions of national culture are briefly described below.

Table 1. Hofstede's Six Dimensions of National Culture.

Hofstede's Six Dimensions of National Culture	
Power distance (PDI)	Power distance describes the dependence relationships in a country. “Power distance can therefore be defined as the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally” (Hofstede et al., 2010, p. 61).
Uncertainty Avoidance (UAI)	Uncertainty avoidance addresses the way individuals in a particular national culture handle uncertainty, and the degree to which uncertainty causes anxiety (Hofstede et al., 2010). Characteristics of cultures that score high on this scale include a preference for strict rules, rigid laws, and norms of conduct. Risk taking is generally avoided, traditions are respected and maintained, and change is slow (Hofstede et al., 2010).
Individualism-Collectivism (IDV)	The individualism index concerns the role (and importance) of the individual as compared to the group. Hofstede’s (2010) individualism index contrasts collectivist societies with individualist ones.
Masculinity-Feminism (MAS)	This dimension rates a national culture in terms of it being more masculine or feminine with respect to work-related goals. “A society is called masculine when emotional gender roles are clearly distinct: men are supposed to be assertive, tough, and focused on material success, whereas women are supposed to be more modest, tender, and concerned with the quality of life. A society is called feminine when emotional gender roles overlap: both men and women are supposed to be modest, tender, and concerned with the quality of life” (Hofstede et al., 2010, p. 140).
Long-term vs short-term orientation (LTO)	Hofstede’s fifth dimension of national culture “stands for the fostering of virtues oriented toward future rewards—in particular, perseverance and thrift. Its opposite pole, short-term orientation, stands for the fostering of virtues related to the past and present—in particular, respect for tradition, preservation of ‘face,’ and fulfilling social obligations” (Hofstede et al., 2010, p. 239).
Indulgence vs Restraint (IVR)	“Indulgence stands for a tendency to allow relatively free gratification of basic and natural human desires related to enjoying life and having fun. Its opposite pole, restraint, reflects a conviction that such gratification needs to be curbed and regulated by strict social norms” (Hofstede et al., 2010, p. 281). In addition, “Indulgence versus restraint shows the conflict between a need for freedom of speech versus a need for order” (Hofstede et al., 2010, p. 413).

The difference between U.S. and Slovenian country scores on each of Hofstede et al.’s (2010) six dimensions of national culture is depicted in Figure 2. Based on Hofstede et al.’s (2010) country scores, Slovenia and the United States are very different cultures. “Slovenia is a highly collectivistic, feminine society, characterized by high uncertainty avoidance and power distance. The United States is quite the opposite: very individualistic, quite masculine, and a little below average on uncertainty avoidance and power distance” (Zagorsek, Jaklic, & Stough, 2004, p. 20).

The companies

The Slovenian firm is publicly owned business with over 1,000 employees; the U.S. firm is a family-owned company in the maritime industry with approximately 150 full-time employees and around 200

contract employees. Whereas the Slovenian firm has a highly educated workforce and (according to interviewees) relatively high personnel turnover, most employees of the U.S. firm have high school educations and stay with the company for many, many years. For both companies, a key inclusion criterion was that survey participants and interview subjects had to have been born, raised, and socialized in that country.

From an information security perspective, one important similarity between the two companies was the considerable value of the customer and company data that employees acquire, manipulate and manage, as well as the potentially catastrophic consequences for the company if that data were to be denied, degraded, damaged, destroyed, disclosed to unauthorized third parties, or stolen.

Salaries are low in both workforces, according to interviewees from both companies. Both companies have a corporate headquarters and a large number of small field offices, mostly manned by just a couple of employees; this organizational dispersion makes cultivating and sustaining an enterprise-wide organizational security culture challenging for both companies.

The study

The purpose of this study was to assess and compare how national culture impacts information security-related attitudes within two different organizations in the United States and Slovenia. This study employed an explanatory sequential mixed method design, with Phase I (quantitative) consisting of an anonymous, online survey taken in November 2018 by 168 Slovenian employees and 62 U.S. employees. Researcher used SPSS software to statistically analyze the participants' responses. Phase II (qualitative) consisted of semi-structured, face-to-face interviews of 13 Slovenian and 15 U.S. employees of the two companies studied. This research design enabled researcher to "have the qualitative data help explain in more detail the initial quantitative results" (Creswell, 2018, p. 222).

Because of the desire to ask questions that aligned with each of Hofstede et al.'s (2010) six dimensions of national culture, researcher did not use a pre-existing survey instrument, but instead developed an online survey that focused on information security matters. To encourage maximum participation while also mitigating the risk of survey participant fatigue, the researcher only asked 23 questions: 14 questions about information security (each based on a five-point Likert score), plus nine demographic questions. For each of the 14 information security-related questions researcher developed, two to three related to each of Hofstede et al.'s (2010) six national culture dimensions as described by Hofstede in *Cultures and Organizations: Software of the Mind* (Hofstede et al., 2010) and his Values Survey Module (VSM) 2013 manual. Despite asking only 23 questions, researcher drew confidence from Hofstede's assertion that with VSM 82, an instrument he widely used for 12 years, he only needed 13 of his content questions to compute scores for his dimensions of national culture (Hofstede et al., 2013).

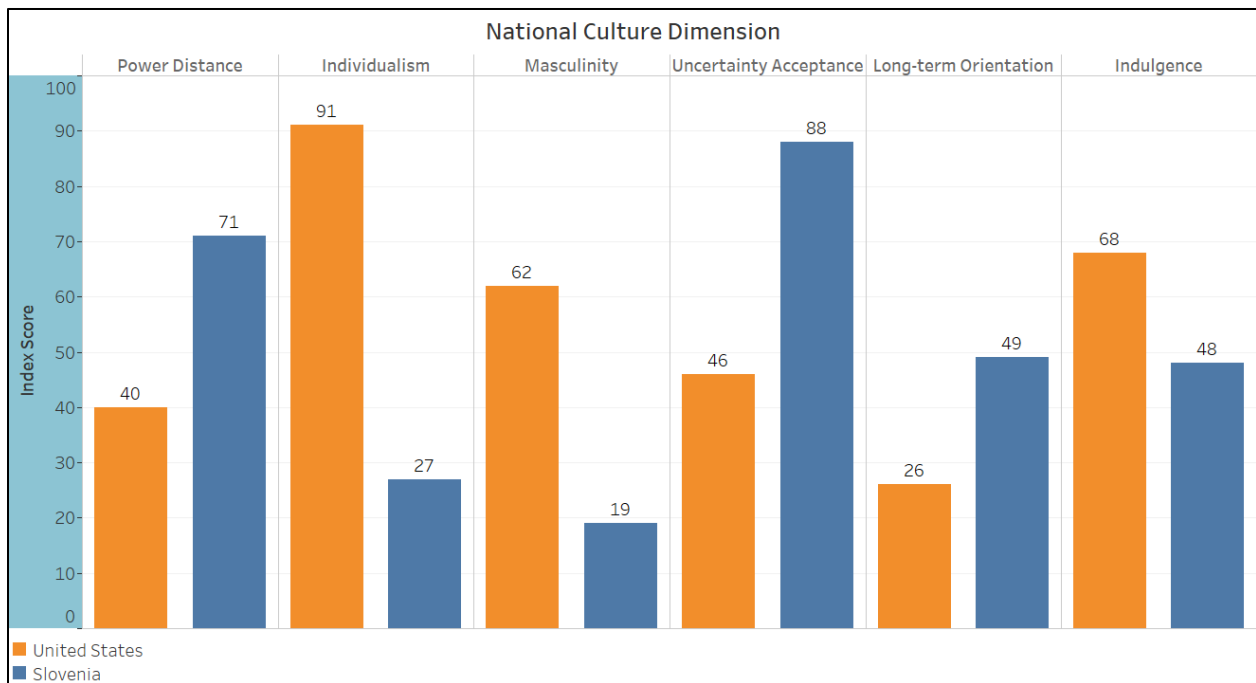


Figure 2. Comparison of country scores for the U.S. and Slovenia for each of Hofstede's (2010) six dimensions of national culture.

Results

Power distance (PDI)

PDI – Slovenian firm

One of the interesting findings in the case of Slovenia was the existence of generational differences between company employees who were raised and socialized in the former Yugoslavia, and younger employees who had no such life experience. While younger Slovenian employees consistently expressed a willingness to confront a senior manager who appeared to be on the verge of committing a security violation, older employees were more hesitant. Several older Slovenian interviewees explained that this hesitancy was a holdover from living in a communist country (Yugoslavia).

PDI – U.S. firm

According to Hofstede et al. (2010), members of an organization in a low power-distance culture like the U.S. will have fewer trepidations about confronting a superior in the workplace than do counterparts in a high power-distance culture like Slovenia. One would therefore expect that a greater percentage of American than Slovenian workers would express a willingness to confront a superior who instructed them to do something that would violate an information security rule. Instead, 26% of both Americans and Slovenians surveyed said they would comply with the supervisor's instruction and violate the information security rule. During the interviews, though, it became clear that while the percentages might be the same across cultures, the *reasons* weren't: Slovenians who said they'd go along with a supervisor's guidance to

violate a security policy did so because they assumed the boss had a good reason for asking them to do so and because, well, *he was the boss*. Americans who were interviewed, by contrast, said they had no qualms at all about confronting, or even reporting, a supervisor. However, if a supervisor told them to do something in violation of security policy, they assumed the violation was probably necessary for mission accomplishment.

Individualism-collectivism (IDV)

IDV – Slovenian firm

Consistent with Hofstede et al.'s (2010) description of Slovenia as being a collectivist culture, Slovenian employees see the head of the company as a father figure, or patriarch. As one survey participant said, the head of the company “leads us in a way like family”, in turn expecting family members will comply with the paternal leader's wishes. Compliance is also a component of collectivist culture, according to Hofstede et al. (2010).

IDV – U.S. firm

Hofstede et al. (2010) described the U.S. as an individualist culture, and Slovenia as a collectivist culture. Given this, one might therefore expect compliant and consensus-oriented Slovenians to be more likely than Americans to agree with the survey statement, “I will always comply with an information security rule, even if that rule makes no sense to me, or makes me less efficient.” Surprisingly, though, 73% of Americans surveyed agreed with this statement. On the other hand, 27% of American employees surveyed did not agree with the statement, meaning that more than a quarter of U.S. employees might disregard an information security rule if it did not make sense to them or they regarded it as detrimental to their efficiency.

Masculinity-Femininity (MAS)

MAS – Slovenian firm

Hofstede et al. (2010) asserts that in feminine cultures like Slovenia, people work in order to live, in contrast to masculine countries like the U.S., where people *live to work*. Another feature of a feminine culture concerns attitudes about size. “The idea that small is beautiful is a feminine value” (Hofstede et al., 2010, p. 167). Several Slovenian interviewees commented that Slovenia, a small country, was an unlikely target for hackers. Several Slovenian interviewees acknowledged that this widely shared notion that “we're-too-small-to-be-interesting” could make it hard for Slovenian information security professionals to persuade employees of the need to comply with information security requirements.

Another feature of feminine cultures is that colleagues are regarded much like family members. Hofstede notes that, “In feminine cultures, a humanized job should give more opportunities for mutual help and social contacts” (Hofstede et al., 2010, p. 169). That a workplace would be a family-environment might explain why not a single Slovenian interview participant recognized the term *disgruntled employee*, or thought disgruntled employees posted a threat, either to their company or elsewhere in the country.

MAS – U.S. firm

One survey question asked about the willingness of the participant to “accept without question any restrictions the company places on my personal use of the Internet at work, or on my personal use of company IT equipment.” The number of American survey respondents who disagreed with this statement was three times higher for U.S. (29%) than Slovenian (10%) respondents. Another distinction was the

number of Slovenian interview subjects who, unlike their U.S. counterparts, emphasized the need for the company to convince them that such a policy change was truly necessary. This was consistent with Hofstede's characterization of the workplace environment in masculine cultures (like that of the U.S.) where people live in order to work, conflicts are resolved "by letting the strongest win", and management is "decisive and aggressive" (Hofstede et al., 2010, p. 170). Several U.S. interviewees expressed the sentiment (expressed in slightly different language) that: *This is a workplace, and the company makes the rules. If you don't like the rules, go find a job elsewhere.*

Uncertainty avoidance (UAI)

UAI – Slovenian firm

Given that Slovenia has a very high preference for avoiding uncertainty, it was not surprising that both Slovenian survey and interview participants expressed a clear preference for precise, highly detailed information security policies that cover all conceivable contingencies and leave little room for interpretation. At the same time, a Slovenian interviewee confessed that, in advance of the researcher's interviews with them, a number of his colleagues approached him, asking where the company's information security policies were located. "The need for rules in a society with a strong uncertainty-avoidance culture is emotional" (Hofstede et al., 2010, p. 209), and even "ineffective rules can also satisfy people's emotional need for formal structure" (p. 209).

Another Hofstede et al. (2010) assertion about high uncertainty avoiding cultures is that their members are more likely to turn to specialists than generalists for assistance. Consistent with this, Slovenian interviewees demonstrated a clear preference for seeking out specialists, rather than colleagues, for dealing with information security-related issues.

UAI – U.S. firm

Two survey questions addressed different aspects of Hofstede et al.'s (2010) uncertainty avoidance dimension. Members of uncertainty avoiding cultures (like Slovenia) favor having far more detailed written policies, whereas uncertainty accepting cultures (like the U.S.) do not. Also, in uncertainty-accepting cultures, one is likely to seek guidance from a peer, rather than from a specialist; this is the opposite of what occurs in uncertainty-avoiding cultures. Indeed, 83% of Slovenians agreed with the statement, "In order to be effective, company information security policy must address all possible situations, be very detailed, and not allow room for individual interpretation." 74% of Americans also agreed with this statement.

In contrast to Slovenian interview subjects, most of whom expressed low confidence in their colleagues' understanding of information security policy, U.S. interviewees expressed satisfaction with their colleagues' understanding of information security policies. One of the interview questions was, "If you encountered an unfamiliar information security situation, and were unsure about what the information security policy was, what would you do?" Not one of the U.S. interviewees even mentioned information security policies in their response; instead, all of them identified the person, or people, they would consult for guidance.

"If an IT security specialist is not readily available, it is equally acceptable to consult a colleague for immediate guidance regarding an information security question." Consistent with Hofstede et al.'s (2010) findings, 41% of Slovenian survey respondents said it would not be acceptable to seek guidance from a colleague on an information security question; by comparison, only 31% of U.S. survey respondents "strongly agreed" or "agreed" with this statement. Turning to a colleague, rather than a specialist, was

acceptable for workers at the U.S. company because, as one U.S. interviewee explained, “information security basically just common sense.”

Long-term vs short-term orientation

LTO – Slovenian firm

Slovenians are rule followers, which might explain why 81% of survey participants agreed with the statement, “It would never be acceptable to violate an information security rule, even if that appears necessary to ensure our company completes a critical project on schedule for a potentially lucrative, long-term client.” On the other hand, Slovenian interviewees asserted that their coworkers possessed a low level of information security threat awareness.

Several Slovenian interviewees took pride in Slovenians’ ability to cut corners and get the job done, regardless of protocols.

LTO – U.S. firm

According to Hofstede et al. (2010), the U.S. is assessed as having a short-term orientation. This could pose a problem, because investing in information security requires the acceptance of short-term resource and opportunity costs in exchange for (hoped-for) longer-term gains in the form of improved information security. For example, employee interviews revealed that while praise for the company’s IT department’s expertise was consistently high, several interviewees noted that information security training was incident-driven and reactive, rather than proactive. As one interviewee explained, “We just kind of do a yearly reminder of best practices, stuff like that, and as issues come up, we might send out a company-wide email to just remind people what to look for, what to watch out for, that kind of stuff.”

Indulgence vs Restraint (IVR)

IVR – Slovenian firm

Like most other Slovenian interviewees, one interviewee agreed that insiders, rather than outsiders, posed the greatest threat to information security, saying, “90% of the threats are internal.” Another Slovenian interviewee also expressed concern about the threat posed by unwitting insiders, colleagues who lacked knowledge of, and indifference toward, information security, saying, “They have to get the job done, and they don't care about protocols.”

Cyberloafing is a term that describes the excessive use of company computer resources for personal use. According to Ugrin, Pearson, & Nickle (2018), “Cyberloafing was strongest in feminine cultures” (p. 19). Using work computers for email, online shopping, and visiting questionable websites could increase the company’s susceptibility to phishing attacks or exposure to other online hazards. While Slovenian interview subjects would accept the company restricting their online activities, most said they would expect the company to provide an explanation and justification for this change.

IVR – U.S. firm

Hofstede et al. (2010) asserts that a positive attitude and optimism are two characteristics typically demonstrated by members of an indulgent culture (like that of the U.S.). Indeed, a positive attitude, self-confidence, and optimism were consistently expressed by U.S. company interviewees in response to information security-related questions. The U.S. company has a very low turnover rate, and as a result, colleagues know each other extremely well. One interviewee subject opined that this familiarity positively influences employee reactions to security issues that arise. Whereas Slovenian interviewees said their

corporate colleagues had a low understanding of information security, U.S. interviewees assessed their colleagues' information security competence was satisfactory.

Limitations

This study only looked at two distinct companies in two different countries that had significantly different national culture value scores. Although the findings aligned with what one would expect based on Hofstede's framework, it is not possible to draw conclusions about the entire population in either country, or about the applicability of Hofstede's framework generally. For generalizability, more companies in each country should be studied and compared, and additional countries should be compared as well. The findings from this study will hopefully encourage future researchers to replicate and expand on the work described in this study.

Discussion

The purpose of this study was to examine how national culture impacts the information security-related attitudes of members of two commercial organizations, one in the United States and one in Slovenia. The explanatory mixed methods approach used in this study made it possible for researcher to identify some of the ways that national culture manifests itself in the attitudes of organizational members. The quantitative and qualitative research performed in this study not only suggests that national culture impacts attitudes toward information security but does so in different ways in different national cultures, and in general alignment with Hofstede et al.'s (2010) VSM-based characterization of national culture along six different dimensions.

People comprise an organization and also determine the organization's culture. Effective organizational leaders can create and modify organizational culture. In order to mitigate risk of cybercrime that could be perpetrated by both insiders and outsiders, it is essential for an organization to have an effective information security culture. Leaders who understand attitudinal tendencies that derive from national culture, and also from organizational culture, are best equipped to both recognize potential problem areas and the cultural changes that may need to be made to address them.

References

- 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.
- Bariso, J. (2019, 4 March). Amazon almost killed Best Buy. Then, Best Buy did something completely brilliant. Retrieved from <https://www.inc.com/justin-bariso/amazon-almost-killed-best-buy-then-best-buy-did-something-completely-brilliant.html>
- Căpășină, 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.

Issues in Information Systems

Volume 22, Issue 3, pp. 114-128, 2021

- Chen, C., Medlin, B., & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, 16(4): 360-376. doi.org/10.1108/09685220810908787
- 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
- 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
- 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.
- Geertz, Clifford (1973). *The interpretation of cultures*. New York: Basic Books.
- Hoffman, F., & Skovira, R. J. (2020). The organizational security index: A tool for assessing the impact of national culture on information security attitudes in Slovenia and the United States. *Issues in Information Systems*, 21(3), 95-104.
- 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.
- 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.
- Hofstede, G., Neuijen, B., Ohayv, D. & Sanders, G. (1990) Measuring organizational cultures: a qualitative & quantitative study across twenty cases. *Administrative Science Quarterly*, 35(2), 286-316.
- 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. (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management*, 12(2), 75-89.
- 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>
- Johnston, A., Warkentin, M., and Luo, X. (2009). National culture and information privacy: the influential effects of individualism and collectivism on privacy concerns and organizational commitment, in *Proceedings of the International Federation of Information Processing (IFIP), International Workshop on Information Systems Security Research*, Cape Town, South Africa, pp. 88-104.
- Logan, D. C., King, J. P., & Fischer-Wright, H. (2008). *Tribal leadership: Leveraging natural groups to build a thriving organization*. New York, NY: Collins.
- Martin, V. (2018, 10 December). JCPenney stock is a bet on a turnaround that isn't coming. Retrieved from <https://investorplace.com/2018/12/jcpenney-stock-bet-turnaround-coming/>
- Milberg, S., Smith, H. J. & Burke, S. (2000). Information privacy: corporate management and national regulation, *Organization Science*, 11(1), 35-57.
- Minkov, M. (2012). *Cross-cultural analysis: the science and art of comparing the world's modern societies and their cultures*. Thousand Oaks, CA: Sage.
- Piowowski, J. (2013). Ethics of organizational culture as an existing condition of security culture. *Science & Military Journal*, 8(1), 41-46.
- Ralston, D. A., Holt, D. H., Terpstra, R. H., & Kai-Cheng, Y. (1997). The impact of national culture and economic ideology on managerial work values: A study of the United States, Russia, Japan, and China. *Journal of International Business Studies*, 177-207.
- Riordan, C. M. (2013). We all need friends at work. *Harvard Business Review*, 3.
- Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q. & Xi'an, S. L. (2008). A cross-cultural comparison of US and Chinese computer security awareness. *Journal of Global Information Management*, 16(2), 91-103.
- Sosnilo, A. I., Zorina, E. E., & Seleznev, P. S. (2018, November). Corporate Culture as a Framework of Training Employees. In 2018 XVII Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES) (pp. 235-238). IEEE.
- 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.
- Ugrin, J. C., Pearson, J. M., Nickle, S. M. (2018). An Examination of the Relationship between Culture and Cyberloafing Using the Hofstede Model. *Journal of Internet Commerce*, 17(1), 46-63. DOI: 10.1080/15332861.2018.1424395

- Veiga, J. F., Floyd, S., & Dechant, K. (2001). Towards modelling the effects of national culture on IT implementation and acceptance. *Journal of Information Technology*, 16(3), 145-158.
- Wang, C., Hoffman, F., Lim, A., & Kwon, J. (2019). From artificial to emotional intelligence: Integrating five types of intelligence to achieve organizational excellence. *International Journal of Management, Knowledge and Learning*, 8(2), 125-144.
- Wahba, P. (2018, 15 October). Sears has only itself to blame for its decline. Retrieved from <http://fortune.com/2018/10/10/sears-bankruptcy-eddie-lampert/>
- Waarts, E., & Van Everdingen, Y. (2005). The influence of national culture on the adoption status of innovations: An empirical study of firms across Europe. *European Management Journal*, 25(6), 601-610.
- Yugendhar, A., & Ali, S. M. (2017). Evaluation of implementing holacracy, a comprehensive study on zappos. *International Journal of Engineering and Management Research (IJEMR)*, 7(5), 163-171.
- Yoon, C. (2009). The effects of national culture values on consumer acceptance of e-commerce: Online shoppers in China. *Information & Management*, 46(5), 294-301.
- Zagorsek, H., Jaklic, M., & Stough, S. J. (2004). Comparing leadership practices between the United States, Nigeria, and Slovenia: Does culture matter? *Cross Cultural Management: An International Journal*, 11(2), 16-34. <https://doi.org/10.1108/13527600410797774>