9-18-2020

The “Right” recipes for security culture: a competing values model perspective

Hwee-Joo Kam

Thoma Mattson
University of Richmond, tmattson@richmond.edu

Dan J. Kim

Recommended Citation

Kam, Hwee-Joo, Thomas Mattson, and Dan J. Kim. “The ‘Right’ Recipes for Security Culture: A Competing Values Model Perspective.” *Information Technology & People Online First* (September 18, 2020). https://doi.org/10.1108/ITP-08-2019-0438.

The "Right" Recipes for Security Culture: A Competing Values Model Perspective

Journal:	*Information Technology & People*
Manuscript ID	ITP-08-2019-0438.R3
Manuscript Type:	Article
Keywords:	Organisational culture < Organizational attribute < Unit attribute, Security < Theoretical concept, Information system effectiveness < IT/IS management < Practice, Culture < Theory, Information management < IT/IS management < Practice, Organizational theory < Theory

The "Right" Recipes for Security Culture: A Competing Values Model Perspective

Abstract

Purpose: This study argues that the effect of perceived organizational culture on the formation of security-related subjective norms and the level of compliance pressure will vary based on how the employees perceive their organization's cultural values. These perceptions reflect on the assumptions and principles that organizations use to guide their security-related behaviors. To make these arguments, we adopt the competing values model (CVM), which is a model used to understand the range of organizational values and resulting cultural archetypes.

Design: This study conducted a survey of working professionals in the banking and higher education industries and used Partial Least Squares (PLS)-Structural Equation Model (SEM) to analyze the data. In a series of post-hoc analyses, we ran a set of multi-group analyses to compare the perceived organizational cultural effects between the working professionals in both industries.

Findings: Our study reveals that perceived organizational cultures in favor of stability and control promoted more positive security-related behaviors. However, the different effects were more pronounced when comparing the effects between the working professionals in both industries.

Originality: This study is one of the few that examines which cultural archetypes are more effective at fostering positive security behaviors. These findings suggest that we should be cautious about generalizing the effects of organizational culture on security-related actions across different contexts and industries.

Keywords: Organizational culture, security compliance pressure, security subjective norms, competing value model

Introduction

The culture of an organization (i.e., its values and assumptions) is a key factor that affects how employees behave in an organization (Briody et al., 2018; Hartnell et al., 2019). One important action that employees take each day are voluntary and involuntary information security (InfoSec) behaviors (Posey et al., 2015). The culture of an organization helps define the appropriate InfoSec behaviors, which may create strong perceived security-related subjective norms (Hu et al., 2012). Forming an organizational culture that promotes mindful InfoSec actions is an important step in fostering employees' secure behaviors (da Veiga et al., 2020). However, many organizations have found it difficult to create such a culture, which leaves them vulnerable to threats originating from their employees (AlHogail, 2015; Chang and Lin, 2007).

A security-aware organizational environment is one that shapes attitudes that encourage employees to protect the organization's information assets by mindfully following their InfoSec policies (ISP) (da Veiga and Martins, 2017). A strong security-aware organizational environment minimizes the risks of computer misuse (AlHogail, 2015) and shapes good InfoSec practices (Chang and Lin, 2007). It is unclear, however, what values organizations should promote to create a strong security-aware environment. For instance, should an organization value flexibility and discretion over stability and control? Should an organization value integration (emphasis on the employees) over differentiation (emphasis on the organization)? The prior literature has not provided clear answers to these questions in an InfoSec context, which is problematic because organizations have many different values that it must balance when forming their organizational culture and establishing their security-aware environment (Wiley et al., 2020). As such, our paper addresses the following important research question: *How do employees' perceptions of their organizational cultures influence InfoSec related subjective norms and compliance pressures?*

To answer this research question, we draw on the competing values model (CVM), which is a values-based theoretical model used to understand and evaluate organizational culture (Quinn and Rohrbaugh, 1983). The CVM proposes that organizations balance competing values along two primary dimensions: 1) organizational structures (flexibility versus stability) and 2) primary focus (internally focused versus externally focused). We argue theoretically that how an organization balances these competing values will help determine its security-related subjective norms and its overall security compliance environment, because employees typically act based on whether their organizational culture condones or condemns specific behaviors (Schein, 2010).

To evaluate empirically how these competing values impact security-related outcomes, we surveyed working professionals in the banking and higher education industries. We found that employees (across both industry segments) who perceived that their organizations valued stability and control had strong perceived security-related subjective norms and security-related compliance pressures (i.e., pressure to comply with its organization's ISP). In a series of post hoc analyses, we found that these effects varied significantly across industries, which suggests that the effects of organizational culture on security-related outcomes may not be broadly generalizable.

Theoretical Background

Security-Related Subjective Norms and Security Compliance Pressure

The human aspect of ISP compliance in organizations has been and continues to be an important area of academic research (Jeon et al., 2020; Kim and Han, 2019; Vedadi and Warkentin, 2020). The prior literature has used many theories to explain how and why employees comply with ISPs (Bulgurcu et al., 2010; Moody et al., 2018). One consistent finding across these different theories is that subjective norms (i.e., perceived social pressures based on the shared beliefs) affect employees' propensity to perform a variety of security-related actions (Aurigemma et al., 2019;

D'Arcy et al., 2009). If channelled properly, these security-related subjective norms create a sense of social pressure to act in a secure manner (Herath and Rao, 2009a, 2009b), which may be a key factor of creating a strong security aware environment across organizations (Ifinedo, 2014).

This stream of literature has also documented the multitude of challenges that managers face convincing their employees to follow the ISPs (Moody et al., 2018; Siponen and Vance, 2010). Organizations invest significant time and energy making their employees aware of the ISPs, but employees still routinely fail to comply with those ISPs (Wiley et al., 2020). Thus, it is important for organizations to impose compliance pressures in their settings. ISP compliance pressures are built on both external (i.e., regulatory pressures) and internal (i.e., security polices and practices) factors (Hu et al., 2007). Facing external regulatory pressures, organizations will turn inward and compel its employees to stay compliant (Kam et al., 2019). We then argue that an organization's compliance pressure is reflected on its employees' perceptions toward ISPs compliance.

Competing Values Model (CVM)

Schein (2010) posits that organizational cultures embody artifacts (organizational attributes), *values* (adopted norms), and assumptions (taken-for-granted beliefs). Our study is specifically interested in *values* because values are the forces that determine what actions are deemed acceptable in an organization (Cameron and Quinn, 2011). Organizations balance a series of competing values along a variety of dimensions, which defines their cultures (Marinova et al., 2018; Quinn and Rohrbaugh, 1983). From an InfoSec perspective, if, for instance, an organization values speed over diligence, then that might adversely affect InfoSec actions because secure behaviors might consume more time and effort (Aurigemma and Mattson, 2019).

Interestingly, not all employees have the same perceptions about their organizations' cultures, because different employees have different organizational experiences that shape their perceptions

about their organizations (Chatman and O'Reilly, 2016). For instance, an employee working in the marketing department of a bank may form different perceptions of the organization's culture relative to an employee working in the information technology (IT) department based on the different projects that they work on and the different social interactions that occur in their workplaces. These various perceptions of the same organization may result in different mental schemas related to how employees believe that they should act (Schein, 2010).

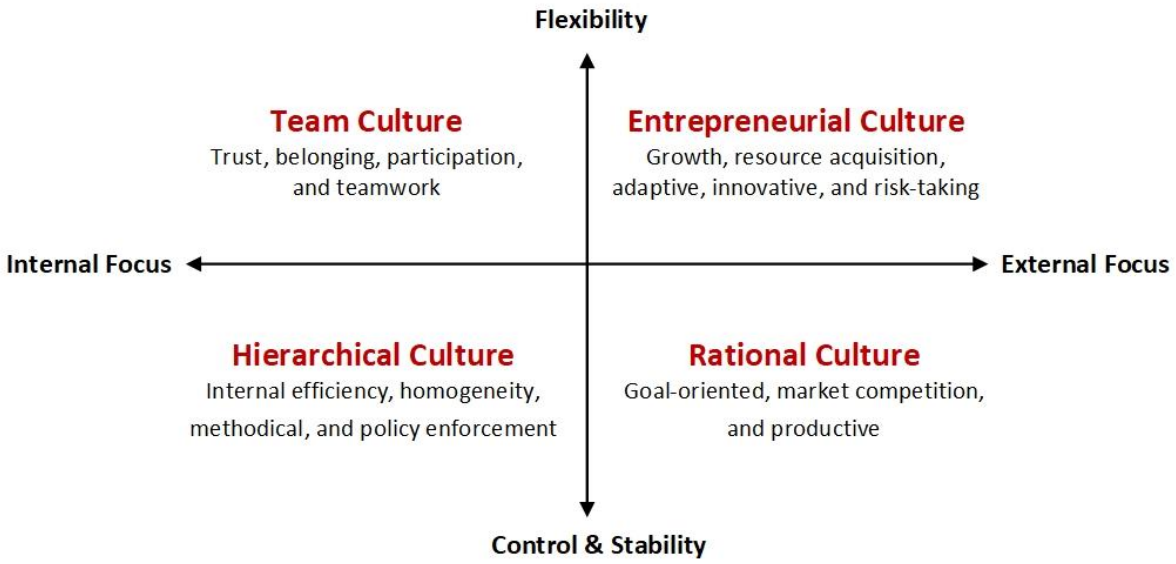

Figure 1. Cultural Archetypes (Denison and Spreitzer, 1991; Quinn and Rohrbaugh, 1983)

To examine these organizational values, we chose the CVM. As a parsimonious yet powerful values-based model (Marinova et al., 2018), the CVM it is one of the most influential models that has been used to explain organizational effectiveness, culture, and leadership (Cameron, 1986; Iivari and Huisman, 2007). Organizations ascribe to many values but the CVM empirical research has found two consistent values that explain organizational effectiveness (Quinn and Rohrbaugh, 1983). The first value pertains to stability. An organization may value stability, control, and order on one end of the continuum or flexibility and agility on the other end of the continuum (Quinn and Rohrbaugh, 1983). The second value pertains to the focus of the organization. Along this dimension, an organization may have an internal (strong organizational processes) or an external

(consumer relationships) value orientation (Denison and Spreitzer, 1991). That is, organizations will either focus internally on their organizations' social and technical systems or adapt to the external environment defined by threats and opportunities (Quinn and Rohrbaugh, 1983). Together these values form four quadrants with each signifying a distinct set of organizational, cultural, and individual values. The intersection of both value dimensions creates four organizational cultural archetypes: hierarchical, rational, entrepreneurial, and team cultures (Denison and Spreitzer, 1991; Quinn and Rohrbaugh, 1983). Figure 1 graphically displays the four cultural archetypes.

An organizational culture may espouse one or more of these cultural archetypes due to an organization having many subcultures, which may create contradictory or competing values within and between organizations (Quinn and Rohrbaugh, 1983). Each axis highlights opposing ends of the continuum (i.e., flexibility versus stability and internal versus external). Therefore, these values shape organizational cultures that are contradictory along each axis and diagonally, forming paradoxical propositions (Quinn and Rohrbaugh, 1983). That is:

> *"Because certain pairs of concepts are located at opposite poles in the spatial model, they can share no place in a consistent and convergent theory of organization. The argument might contend that, for every proposition that could be derived from such an analytical approach, its contradiction could also be derived."* (Quinn and Rohrbaugh, 1983, p. 374)

Organizational cultures in the four quadrants (see Figure 1) are not mutually exclusive. For instance, a bank may mostly espouse a hierarchical culture that is inwardly focused on complying with regulations, but that same bank may also adopt a rational culture that is outwardly focused on adapting to market forces (Paulin et al., 1999). Therefore, an organization may have contradictory values within its own organizational boundaries and between other organizations either in the same or different industries (Cooper and Quinn, 1993; Denison and Spreitzer, 1991).

The information systems literature has used the CVM to examine the relationship between organizational culture and the adoption of system's development methodologies (Iivari and Huisman, 2007), to assess the effect of knowledge transfer on IT implementations (Harrington and Guimaraes, 2005), and to study the effect of organizational culture on software development (Shih and Huang, 2010). Particularly germane to our study, Chang and Lin (2007) used the CVM in a study, which revealed that control-oriented cultures had a strong effect on InfoSec behaviors, but flexible-oriented cultures had a negative or no effect on similar behaviors. Built on their study, we argue that certain organizational cultures facilitate InfoSec behaviors via normative pressures.

Research Model and Hypotheses

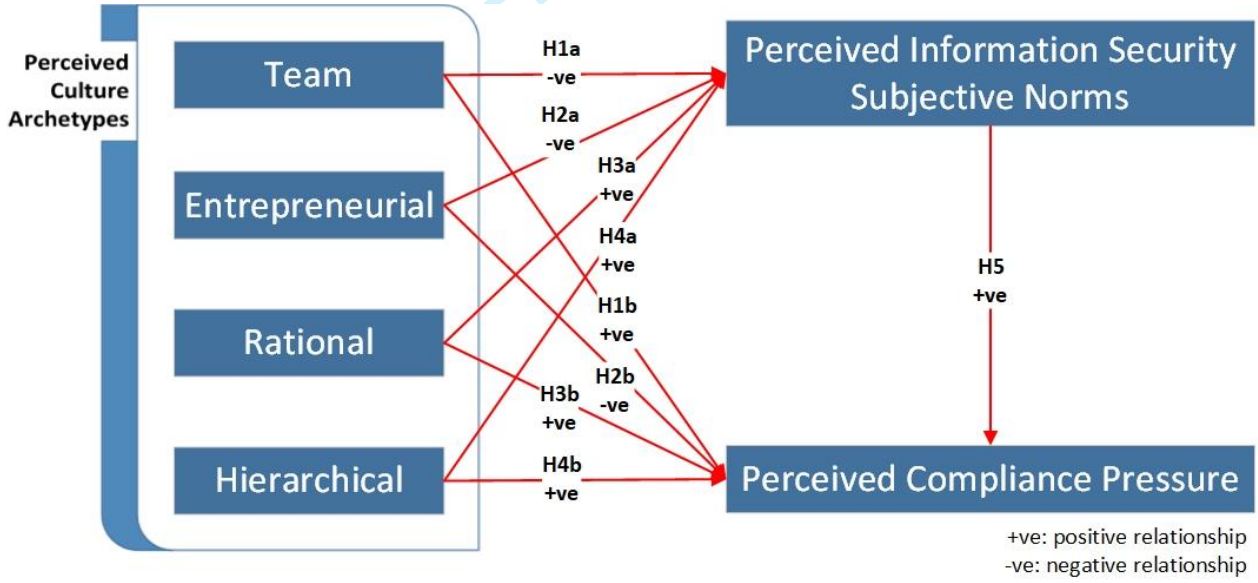

Figure 2: Proposed Research Model

Encouraging employees to comply with their organization's ISPs is one of the main problems that InfoSec managers face (Aurigemma et al., 2019; Moody et al., 2018). Organizational culture is a key element in creating a compliance centric environment (Ifinedo, 2014) and in creating positive security-related subjective norms (da Veiga et al., 2020; Wiley et al., 2020), which we argue produces significant pressure to comply with the organization's ISPs. Hence, our dependent

variables are the perceived pressure to comply with the organization's ISPs and the perceived security-related subjective norms in an organization. Figure 2 shows our proposed research model.

Perceived Entrepreneurial and Team Organizational Cultures

Perceived team and entrepreneurial organizational cultures highlight certain organizations' propensity to be flexible and adaptable (Cooper and Quinn, 1993; Denison and Spreitzer, 1991). These types of perceived organizational cultures value change and often do not have well-defined ISPs. On the one hand, being flexible, such as not having rigid policies, promotes agility, which enables organizations to respond to new threats quickly (Tallon et al., 2019). On the other hand, however, flexibility makes it difficult for organizations to develop in-depth ISPs and related training programs. Routines generally require stable or habitual actions by its employees (Dönmez et al., 2016), which can be difficult to develop if the operational procedures are in a constant state of flux. This suggests that the flexible nature of these organizational cultural archetypes may make it difficult to develop consistent routines (Karlsson et al., 2018), which may result in a lower propensity to develop strong perceived InfoSec subjective norms. Therefore, we hypothesize:

H1a: Perceived team organizational cultures are negatively associated with perceived security-related subjective norms.

H2a: Perceived entrepreneurial organizational cultures are negatively associated with perceived security-related subjective norms.

As noted earlier, the CVM creates paradoxes in organizations (Marinova et al., 2018; Quinn and Rohrbaugh, 1983). In an InfoSec context, we argue that perceived team organizational cultures instigate a paradox. While the flexibility of team organizational cultures may hinder the growth of security-related subjective norms, team collaboration may still facilitate perceived compliance pressure built on organizations' intentions to remain compliant with their ISPs. Organizations that have perceived organizational team cultures are internally oriented with clearly defined business processes (Cooper and Quinn, 1993). These processes may promote a strong security-aware

environment (assuming that the processes have a security component) within specific teams. Moreover, increased organizational commitment have been shown to be positively correlated with this cultural archetype (Goodman et al., 2001; Lee and Edmondson, 2017), which fosters teamwork and the collaborative effort of staying compliant with the organization's ISPs. Therefore, behaviors that are deemed to be damaging to the team are discouraged in this cultural archetype (Gelfand et al., 2004; Schreuder et al., 2017). One type of damaging behavior is not following the ISPs and putting the team (and later the organization) at a security risk. Thus, we propose:

H1b: Perceived team organizational cultures are positively associated with perceived compliance pressure.

In contrast, perceived entrepreneurial organizational cultures have an external instead of an internal focus. Organizations with entrepreneurial cultures tend to take risk, adapt to their external environments (Denison and Spreitzer, 1991), and maintain fewer formal procedures due to its outward value proposition (Wang, 2010). These types of organizational cultures seek external legitimacy based on their product or service offerings as opposed to seeking legitimacy based on their internal work processes (Navis and Glynn, 2010; Vaast et al., 2013). Often these types of organizational cultures foster technology-mediated work practices (Hargadon and Douglas, 2001; Ratten, 2019), but those practices may not have a strong focus on the security risks due to their often-fleeting nature. Also, organizations with entrepreneurial cultures tend to have chaotic work environments (Ahmetoglu et al., 2018), giving the appearance of making their policies up "on the fly". This may be problematic for security-related behaviors. We then propose:

H2b: Perceived entrepreneurial organizational cultures are negatively associated with perceived compliance pressure.

Perceived Rational and Hierarchical Organizational Cultures

Rational and hierarchical organizational cultures highlight certain organizations' desire to have stable environments (Cooper and Quinn, 1993). Organizations with these types of perceived

organizational cultures often have well-defined objectives, are goal-oriented, and are somewhat bureaucratic (Denison and Spreitzer, 1991; Scheibe and Gupta, 2017). From a compliance perspective, stability is probably preferable over flexibility because it is easier to train employees on ISPs that do not constantly evolve (Dhillon et al., 2016). Stable organizational structures also make it easier to identify roles, responsibilities, and accountability for InfoSec matters. Moreover, employees are subject to peer pressure when perceived security-related norms are well-defined (Chen et al., 2019), which will tend to be the case in more stable organizational cultures.

We propose that employees working for organizations with a perceived rational organizational culture will weigh the costs associated with establishing sound internal controls with the benefits of reducing their risk exposure when making InfoSec related decisions (D'Arcy and Lowry, 2019). Thus, a perceived rational organizational culture should offer an environment that fosters effective security controls for preventing security breaches because it makes economic sense to do so (i.e., benefit of stakeholders' trust is larger than the cost of applying security controls). As such, we argue that employees working in this cultural archetype will form strong norms and routines surrounding InfoSec actions due to economic reasons. We then theorize:

H3a: Perceived rational organizational cultures are positively associated with perceived security-related subjective norms.

H3b: Perceived rational organizational cultures are positively associated with perceived compliance pressure.

Hierarchical organizational cultures are methodical and rules driven with a focus on structured internal processes (Denison and Spreitzer, 1991). Iivari and Huisman (2007) established that this cultural archetype enables management to enforce mandatory actions for system implementations. We then posit that a hierarchical organizational culture may drive compliance behaviors and create perceived security-related subjective norms through a top-down approach, because this cultural archetype enforces the rules through a command and control organizational environment (Denison

and Spreitzer, 1991). This environment may effectively increase compliance pressure and create perceived subjective norms (Yazdanmehr et al., 2020). Thus, we propose:

H4a: Perceived hierarchical organizational cultures are positively associated with perceived security-related subjective norms.

H4b: Perceived hierarchical organizational cultures are positively associated with perceived compliance pressure.

Perceived Security-Related Subjective Norms

Our final prediction is related to the link between perceived security-related subjective norms and the perceived pressure to comply with the organization's ISPs. This link has been well established in a variety of disciplines including InfoSec. The greater the perceived subjective norms to perform a security action, the greater the likelihood that an individual will perform that security action (Herath and Rao, 2009a; Ifinedo, 2014). We have no reason to believe that these prior results will not hold in our model of the different cultural archetypes. Thus, we propose:

H5: Perceived security-related subjective norms are positively associated with perceived compliance pressure (irrespective of cultural archetype).

Research Methods

Research Design

To investigate our research model empirically, we surveyed working professionals in the banking and higher education industries. We selected employees in these two industries due to their contrasting (both real and perceived) cultural characteristics and compliance environments. For instance, the higher education industry is subject to the regulations established by the Family Education and Privacy Act (FERPA) but the penalties for FERPA violations are not particularly severe. In the banking industry, however, banks must comply with a series of regulations established by Sarbanes-Oxley Act (SOX) and the Gramm Leach Bliley Act (GLBA) with major fines for not complying with these mandatory regulations. With such notable differences between

both industries, we expected to have enough variation and contrasting values to examine the distinctive organizational cultural effects across the four cultural archetypes.

To determine the organizational culture of the organizations where our subjects worked, we used their perceived organizational values. We decided to measure each subject's perceptions of their organizations instead of attempting to subjectively categorize each of their organizations based on the four cultural archetypes for two main reasons. First, in the same organization, employees share different experiences, which shape their perceived organizational cultures (Harrison et al., 2019). For instance, an employee who works primarily in collaborative teams with supportive colleagues will have much different perceptions of their organizations' culture relative to an employee in the same organization who works in a bureaucratic department with unsupportive colleagues. These socialization differences may create dramatically different cultural perceptions about their organizations' values. For this reason, many scholars argue that culture must be measured and analyzed at the individual level (Bochner and Hesketh, 1994).

Second, the perceptions of our research subjects' organizations are more valuable than our subjective classification of their organizations. For instance, if an employee who works in an IT department at a bank perceives that their organizational culture is entrepreneurial, then that employee works under the assumption that their bank has an organizational culture that is somewhat entrepreneurial. The perceptions of the employees represent their reality related to their organizational cultures, which guides their behaviors in the organization (Harrison et al., 2019).

Measurement Items and Instrument Validation

We used existing measurement items from pre-validated multi-item scales for several of our latent constructs (Helfrich et al., 2007; Herath and Rao, 2009a). For other latent constructs that did not contain pre-validated multi-item scales, we used the items from Hu et al. (2007) as our starting

point to build our own measurement items. To build these items, we first used a panel of expert InfoSec researchers to provide an initial content validity of our adapted and new items. We then had four Certified Information Systems Security Professional's (CISSP) review our items. After an iterative process of getting feedback and refining our measurement items, we finalized our items and designed our survey instrument using best practices related to instruction wording and question order as advocated by Dillman et al. (2014). On our final survey instrument, all measurement items used 7-point Likert scales. Finally, to remedy potential common method bias procedurally via our survey instrument, we used best practices suggested by Podsakoff et al. (2012), particularly related to the proximal separation of the measurement items used to capture our independent and dependent variables. After that, we ran a pilot study with 51 InfoSec professionals. As a result of our participants' feedback, we refined our items to rectify identified ambiguities. On our final survey instrument (see Appendix A), all measurement items were randomized to reduce the adverse effect of question ordering on our results (Podsakoff et al., 2012).

Data Collection

We sent our survey electronically to managers and IT professionals who worked in the banking and higher education industries in the United States. In our data, we did not permit entry-level employees to participate because entry-level employees may be so new that they might not realize their organizations' culture, ISPs, and values. We identified research subjects in these two industries based on alumni networks from two public universities in the United States. Originally, 200 participants were invited to participate in our survey. We received 40 responses, which gave us a response rate of 25%. We removed 3 subjects from the sample because they did not complete the entire survey instrument, which made those data points not usable. We then recruited additional participants in a second round of data collection using Qualtrics. After both rounds of data

collection, we had a final sample size of 125 in the banking industry and 135 in the higher education industry. All of our participants had more than 5-years professional work experience but not necessarily at the same organization. The average age of our participants was 38 for the banking subjects and 46 for the higher education subjects (see Table 1).

[Insert Table 1]

To assess the potential adverse impact of non-response bias on our results, we ran a series of ANOVAs (Analysis of Variance) comparing early and late responders on our key constructs. These ANOVAs showed no statistically significant differences between the two groups of respondents, which suggests that non-response bias was not a major issue with our study.

Data Analysis and Results

We used Partial Least Squares (PLS)-Structural Equation Model (SEM) with SmartPLS version 3.2. to analyze our survey data. The key advantages of using PLS-SEM are (1) it relaxes the normal distribution assumptions required by the maximum likelihood method and (2) it is better at estimating complex models with relatively small sample sizes (Gefen et al., 2011; Hair et al., 2019). Using PLS-SEM, we first assessed the validity and the reliability of our measures and then tested our hypotheses using the standard bootstrapping method (with 1000 resampling).

Measurement Model

We evaluated convergent validity using the average variance extracted (AVE), Cronbach's alpha (CA), and composite reliability (CR) values (see Table 2). AVE values greater than 0.5 and CA and CR values greater than 0.7 are considered acceptable thresholds for establishing convergent validity (Chin, 1998; Fornell and Larcker, 1981). Our values met these thresholds.

[Insert Table 2]

We then analyzed the square root of the AVE for each construct to establish discriminant validity. Tables 3 and 4 display these values. When the square root of the AVE for each construct

is larger than the correlations between that construct and all of the other constructs in the model, then that is evidence of discriminant validity (Chin, 1998). In our data, we met these criteria.

[Insert Table 3]

[Insert Table 4]

Moreover, we analyzed the factor loadings of each measurement item on its intended construct (see Appendix B). All of our items loaded greater than the recommended threshold of 0.7 (Chin, 1998). The factor loadings also showed that the difference between the loading on the intended construct and the loading on any other construct was greater than 0.1. Therefore, we have strong evidence of both convergent and discriminant validity in our data (Gefen and Straub, 2005).

[Insert Table 5]

Perceived compliance pressure (COMP) was the only formative construct in our research model. Table 5 displays the item weights for each indicator variable in this formative construct. The variance inflation factors (VIF) for each measurement item were below 3.3, which suggests adequate construct reliability for this formative construct (Diamantopoulos and Siguaw, 2006). All of the other construct measurement items met the requirements to be considered reflective indicators of their respective latent constructs based on the criteria set forth by Petter et al. (2007). Finally, we tested for the presence of common method variance of the measurement model using the unmeasured latent method factor approach outlined by Podsakoff et al. (2012). In our data, adding a first-order method factor whose only measures were the indicators of the theoretical constructs of interest that share a common method did not reveal any major issues.

Structural Models for Hypothesis Testing

[Insert Table 6]

Using PLS-SEM, we assessed both the effect size (F^2) and the null-hypothesis significance test for all models and paths. An F^2 larger than 0.02, 0.15, and 0.35 signifies small, medium, and large

effect sizes (respectively) (Cohen, 1977). Table 6 shows the results of structural models. We found that perceived entrepreneurial ($\beta = 0.167$, $p < 0.05$), team ($\beta = 0.129$, $p < 0.05$), and hierarchical ($\beta = 0.185$, $p < 0.001$) cultures fostered perceived compliance pressure, but perceived rational culture ($\beta = 0.093$, $p > 0.05$) did not. While perceived entrepreneurial cultures predicted perceived compliance pressure, it was in the opposite direction of our hypothesis (i.e., positive instead of negative path coefficient). Thus, H1b and H4b were supported but H2b and H3b were not.

The perceived cultural archetypes that valued control and stability were significant predictors of perceived security-related subjective norms (hierarchical: $\beta = 0.193$, $p < 0.001$ and rational: $\beta = 0.306$, $p < 0.001$), but perceived entrepreneurial ($\beta = 0.077$, $p > 0.05$) and perceived team ($\beta = 0.041$, $p > 0.05$) cultures were not. Since both perceived entrepreneurial and team cultures valued flexibility over control and stability, these cultural archetypes did not support subjective norms that usually grew in a stable organizational setting. Of the significant paths, the effect sizes were relatively small. Overall, we find support for H3a and H4a but no support for H1a and H2a.

Next, we found that perceived security-related subjective norms fostered perceived compliance pressure ($\beta = 0.437$, $p < 0.001$) with a moderate effect size ($F^2 = 0.276$), which supported our H5 prediction. Our results also show that perceived security-related subjective norms fully mediated the relationship between perceived rational culture and perceived compliance pressure.

Cross Industry Post-hoc Analyses

Next, we ran a set of multi-group analyses (MGA) to compare the perceived cultural archetypes between our banking (n=125) and our higher education (n=135) participants. The prior literature proposes that there could be a general industry effect due to varying values among employees working across different industry segments (Chiasson and Davidson, 2005; Kam et al., 2019). To make our results meaningful, we assessed measurement invariance of our measurement items

between the two different industry groups. To do this, we ran the three-step process outlined by Henseler et al. (2016) using the built-in Measurement Invariance of Composite Models (MICOM) procedure in SmartPLS. Our data satisfied the criteria for compositional measurement invariance (see Appendix C). Table 7 and Figure 3 show the results of our MGA.

[Insert Table 7]

We found a few noteworthy differences. First, perceived hierarchical culture fostered perceived compliance pressures ($\beta = 0.408$, $p < 0.001$) and perceived security-related subjective norms ($\beta = 0.368$, $p < 0.001$) with our banking sample, but not with higher education sample. These path coefficient differences for perceived hierarchical cultures were statistically significant for perceived security-related subjective norms (β difference = 0.281, $p < 0.01$) and perceived compliance pressure (β difference = 0.301, $p < 0.05$). Thus, perceived hierarchical culture created security-aware settings *only* in our sample of banking employees.

Second, perceived team cultures had a positive effect on perceived security-related subjective norms among our higher education employees ($\beta = 0.220$, $p < 0.05$), but had no such effect ($\beta = -0.044$, $p > 0.05$) among their banking counterparts. These path coefficients were significantly different (β difference = 0.264, $p < 0.05$). This effect, however, was positive and not negative as we predicted in H1a. This is probably because higher education institutions tend to espouse team-oriented culture (Kezar et al., 2020; Smart and St. John, 1996) but team-oriented culture may not be common in the banking industry, which might have affected our respondents' perceptions.

Third, perceived entrepreneurial culture created perceived compliance pressure ($\beta = 0.319$, $p < 0.001$) with our higher education sample but not with our banking sample ($\beta = 0.037$, $p > 0.05$). This difference was statistically significant between both groups (β difference= 0.282, $p < 0.05$). Again, this finding may be due to not many banks having an entrepreneurial culture.

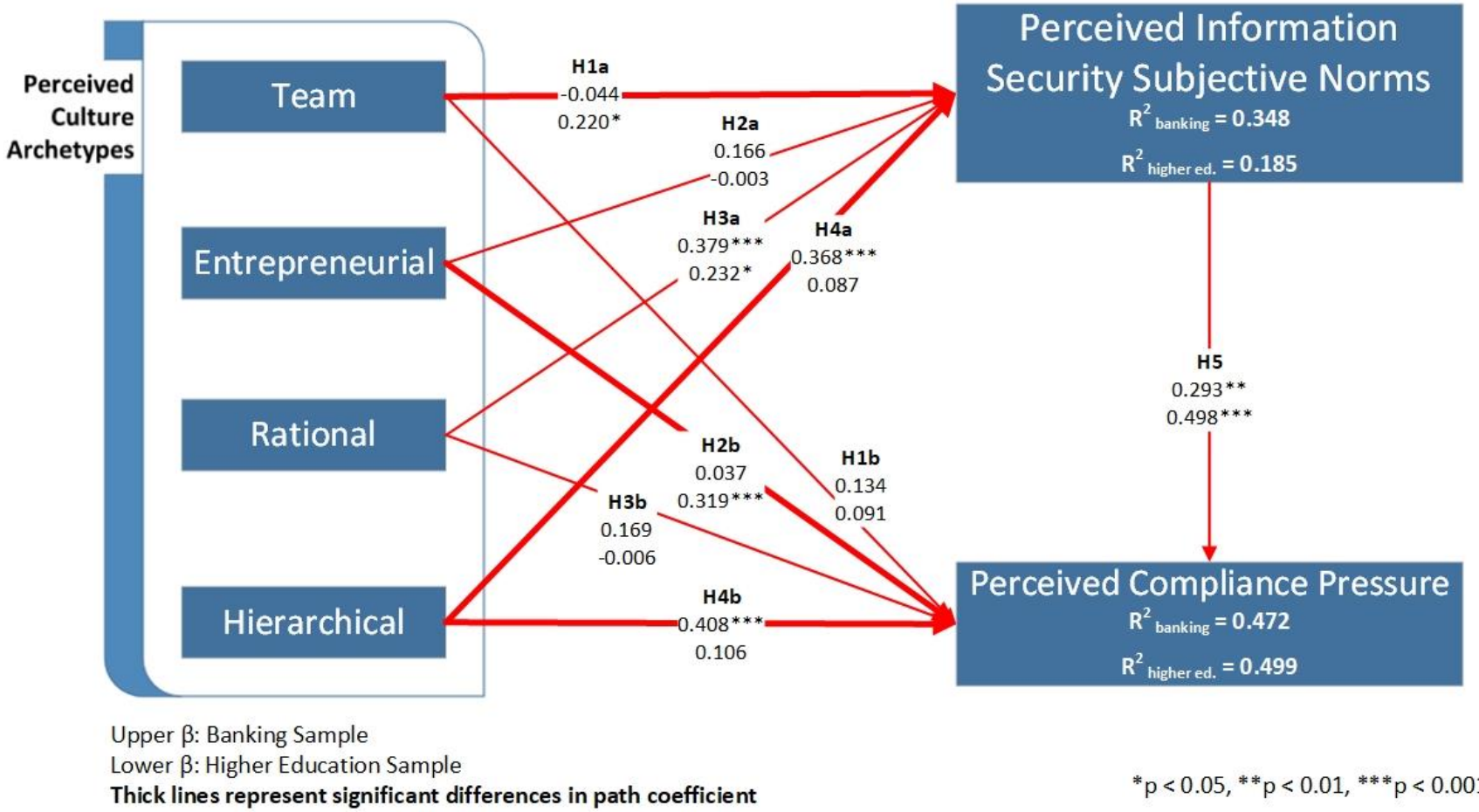

Figure 3: Structural Model Testing Results

Finally, we found the same fully mediated effect of perceived rational organizational cultures across both industry samples. In both industry groups, perceived rational cultures only affected perceived compliance pressures via perceived subjective norms. However, we found no statistically significant differences between the path coefficients between both groups.

Discussion

We demonstrated empirically that the different perceived cultural archetypes have important ramifications for, but different impacts on, perceived security-related subjective norms and compliance pressures. When we analyzed our entire sample together in a single model, we found that only the organizational cultures that favored control and stability (i.e., perceived rational and hierarchical cultures) had a positive effect on the formation of perceived security-related subjective norms. We found no such effect for organizational cultures that valued flexibility (i.e., perceived entrepreneurial and team cultures).

The different effects of the four perceived cultural archetypes became even more pronounced when we split our sample between the banking and higher education samples. Our findings disclose that many banking organizations are heavily influenced by perceived hierarchical culture, whereas most of the colleges and universities appear to be driven by perceived team and entrepreneurial cultures. We assert that these differences may be due to: 1) different industries tend to attract different types of employees and 2) organizations with specific organizational cultures tend to attract different types of employees (within and between industries) (Kam et al., 2019; Schneider et al., 1998). For instance, a perceived team culture in the higher education industry may attract a different type of employee relative to a perceived hierarchical culture in that same industry. Moreover, the types of employees interested in pursuing careers in the banking industry are probably different from those interested in pursuing careers in higher education. These

different personality will shape the culture of the organizations across industries (Schneider et al., 1998), which will affect the formation of perceived subjective norms.

We found that perceived rational cultures had similar effects across both industries. This similarity might be due to the fact that performing a security action by rationally calculating its benefits and its costs are somewhat industry agnostic (Bulgurcu et al., 2010). Therefore, on some level, most organizations have some elements of rationality (but with varying degrees) embedded in their organizational cultures and in their normative routines, which includes security-related subjective norms. Although organizations may define rationality differently, the idea of performing a cost-benefit analysis in relation to performing important daily tasks (including security-related tasks) is done consistently across organizations and industries.

We predicted a negative effect of perceived team and entrepreneurial cultural archetypes (H1a and H2a) on perceived security-related subjective norms but found no effect for either. The flexible nature of these cultural archetypes might not be conducive to creating subjective norms in these types of organizational cultures. Subjective norms take time and procedural consistency to develop in an organization (Cabrera and Bonache, 1999; Herath and Rao, 2009b). This development might not be possible if the policies, procedures, and routines constantly change, which is more likely in these perceived cultural archetypes (Karlsson et al., 2018). Therefore, a null relationship between these two perceived cultural archetypes might be a more logical prediction.

We predicted a negative effect of the perceived entrepreneurial cultural archetype on perceived compliance pressure (H2b) but we found a positive effect. Conceptually, this type of organizational culture fosters an open system of information sharing (Cooper and Quinn, 1993). Information sharing supports fast response to emerging security-related threats (Maitlo et al., 2019; Pérez-González et al., 2019), leading to a positive effect on an organization's compliance environment.

Procedurally, we tested this hypothesis using employees in higher education and banking, which are mature industries. If we were to test this proposed effect with a sample of employees working in Silicon Valley, we might have a result that is more consistent with our prediction.

We predicted a partially mediated effect for the perceived rational cultural archetype and perceived compliance pressure through perceived security-related subjective norms (H3b), but we found the effect to be fully mediated with no direct effect between perceived rational culture and perceived compliance pressure. Because perceived rational cultures value efficiency (Denison and Spreitzer, 1991), we argue that promoting security-related subjective norms such as embracing a shared belief of non-disclosure to protect data confidentiality may foster efficiency of InfoSec behaviors. However, perceived compliance pressure entails perceived organizational expectations of ISP compliance. ISPs outline the overall security objectives, but they do not necessarily share the operational details (Chapple et al., 2018) that suggest the efficiency of an InfoSec safeguard.

Research Implications and Limitations

Theoretical Contributions

Our study contributes to the behavioral InfoSec literature in two important ways. First, the core theories that scholars used in the extant literature have generally not included the possible mediating, moderating, or direct effect of organizational culture on InfoSec related behaviors. The core behavioral InfoSec theories mostly assume the effects of those theories will be the same regardless of the organizational environment. Our results suggest that this might not be the case based on how they balance competing values. Future studies could investigate the role of different organizational cultures in (for instance) protection motivation theory to determine if the type of organizational environment might strengthen or weaken those theorized effects.

Second, our results suggest that there might not be a universal effect of organizational culture on security-related behaviors (Tams, 2013). We established empirically that the different cultural archetypes create conflicting values within organizations (Quinn and Rohrbaugh, 1983), which either inhibit or enable the formation of perceived security-related subjective norms and perceived compliance pressures. Given these differences, it is hard to say definitively that one specific cultural archetype will always create a heightened sense of security awareness across all industries. Thus, another interesting area of future research could build from our results by investigating the conditions under which each of the four cultural archetypes create or do not create strong security-aware settings. Our post-hoc analyses examined a potential industry effect, but other contextual conditions might mediate or moderate our proposed relationships.

Practical Implications

Our paper suggests that there is no one-size-fits-all approach to manage an organization's ISPs. InfoSec managers must know their organizational culture and manage accordingly. For instance, our results suggest that perceived team and entrepreneurial cultures do not promote the formation of strong perceived security-related subjective norms. However, strong perceived security-related subjective norms are still an important mechanism to protect an organization's information assets. Thus, InfoSec managers may need to find an alternative way to create strong perceived security-related subjective norms in team and entrepreneurial organizational cultures.

The culture of an organization is not developed specifically for InfoSec. Instead, the organizational culture is shaped by the mission, strategy, and values of the organization (Briody et al., 2018). We suggest that it is important for senior-level managers to understand that the overall organizational culture could positively or negatively shape the InfoSec environment. Therefore, although we are not suggesting that senior-level managers create an organizational culture

specifically for security purposes, we propose that senior-level managers be mindful of the indirect effects that high-level strategic decisions might have on the security environment. By doing so, they can then manage InfoSec in the context of the espoused organizational culture.

We did not test specific managerial interventions related to security-related behaviors in our study, but our results do suggest that different managerial approaches might work better or worse in certain organizational cultures. For instance, in perceived team cultures, InfoSec managers may want to cultivate strong security-related subjective norms through shared governance instead of through a top-down approach given the collaborative nature of this cultural archetype. Conversely, a top-down approach might work effectively in perceived rational and hierarchical organizational cultures given their internal and process-oriented value orientation. Thus, our key message to practitioners is to make security-related decisions in the context of their organizational culture. What works in one organizational culture may not work effectively in a different setting.

Limitations and Future Directions

Like all research, our paper has several limitations. First, organizational culture evolves over time, but our study took a snapshot of each of our subject's perceptions of their current organizational settings. We cannot offer any insights into what might happen when employees' perceptions of their organizational cultures change over time. Thus, scholars should be cautious about referencing our findings in organizations that have undergone several organizational culture changes. An interesting future study might examine organizational culture change and how that amplifies or nullifies our theorized relationships. Second, our measurement items did not include any context specificity or clear domain specification, which was suggested by Siponen and Vance (2014). Future research could extend or validate our findings by using scenario vignettes to contextualize specific security-related actions. Third, our sample only included two industries.

These two industries provided a sufficient variance along the four cultural archetypes to examine our proposed theoretical relationships both within and between industry groups, but we make no claims that both industries represent all industries. Future research could investigate theoretically and empirically how our proposed relationships might vary across additional industries.

References

Ahmetoglu, G., Akhtar, R., Tsivrikos, D. and Chamorro-Premuzic, T. (2018), "The Entrepreneurial Organization: The Effects of Organizational Culture on Innovation Output", *Consulting Psychology Journal: Practice and Research*, Vol. 70 No. 4, pp. 318–338.

AlHogail, A. (2015), "Design and Validation of Information Security Culture Framework", *Computers in Human Behavior*, Vol. 49, pp. 567–575.

Aurigemma, S. and Mattson, T. (2019), "Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research", *Journal of the Association for Information Systems*, Vol. 20 No. 12.

Aurigemma, S., Mattson, T. and Leonard, L.N.K. (2019), "Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications", *AIS Transactions on Replication Research*, Vol. 5 No. 1.

Bochner, S. and Hesketh, B. (1994), "Power Distance, Individualism/Collectivism, and Job-Related Attitudes in a Culturally Diverse Work Group", *Journal of Cross-Cultural Psychology*, Vol. 25 No. 2, pp. 233–257.

Briody, E.K., Berger, E.J., Wirtz, E., Ramos, A., Guruprasad, G. and Morrison, E.F. (2018), "Ritual as Work Strategy: A Window into Organizational Culture", *Human Organization*, Vol. 77 No. 3, pp. 189–201.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523–548.

Cabrera, E.F. and Bonache, J. (1999), "An Expert HR System for Aligning Organizational Culture and Strategy", *Human Resource Planning*, Vol. 22 No. 1, p. 51.

Cameron, K.S. (1986), "Effectiveness as Paradox: Consensus and Conflict in Conceptions of Organizational Effectiveness", *Management Science*, Vol. 32 No. 5, pp. 539–553.

Cameron, K.S. and Quinn, R.E. (2011), Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework, 3rd Ed., John Wiley & Sons, San Francisco, CA.

Chang, E.S. and Lin, C. (2007), "Exploring Organizational Culture for Information Security Management", *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438–458.

Chapple, M., Stewart, J.M. and Gibson, D. (2018), *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide*, 8 Ed., Sybex, Indianapolis, Indiana.

Chatman, J.A. and O'Reilly, C.A. (2016), "Paradigm Lost: Reinvigorating the Study of Organizational Culture", *Research in Organizational Behavior*, Vol. 36, pp. 199–224.

Chen, H., Chau, P.Y.K. and Li, W. (2019), "The Effects of Moral Disengagement and Organizational Ethical Climate on Insiders' Information Security Policy Violation Behavior", *Information Technology & People*, Vol. 32 No. 4, pp. 973–992.

Chiasson, M.W. and Davidson, E. (2005), "Taking Industry Seriously in Information Systems Research", *MIS Quarterly*, Vol. 29 No. 4, pp. 591–605.

Chin, W.W. (1998), "The Partial Least Squares Approach to Structural Equation Modeling", *Modern Methods for Business Research*, Vol. 295 No. 2, pp. 295–336.

Cohen, J. (1977), Statistical Power Analysis for the Behavioral Sciences, Academic Press, NY.

Cooper, R.B. and Quinn, R.E. (1993), "Implications of the Competing Values Framework for Management Information Systems", *Human Resource Management*, Vol. 32 No. 1, pp. 175–201.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79–98.

D'Arcy, J. and Lowry, P. (2019), "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study", *Information Systems Journal*, Vol. 29, pp. 43–69.

Denison, D.R. and Spreitzer, G.M. (1991), "Organizational Culture and Organizational Development: A Competing Values Approach", *Research in Organizational Change and Development*, Vol. 5 No. 1, pp. 1–21.

Dhillon, G., Syed, R. and Pedron, C. (2016), "Interpreting Information Security Culture: An Organizational Transformation Case Study", *Computers & Security*, Vol. 56, pp. 63–69.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration. *British Journal of Management*, *17*(4), 263–282.

Dillman, D.A., Smyth, J.D. and Christian, L.M. (2014), *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 4th edition., Wiley, Hoboken.

Dönmez, D., Grote, G. and Brusoni, S. (2016), "Routine Interdependencies as a Source of Stability and Flexibility. A Study of Agile Software Development Teams", *Information and Organization*, Vol. 26 No. 3, pp. 63–83.

Fornell, C. and Larcker, D.F. (1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Gefen, D., Rigdon, E.E. and Straub, D. (2011), "Editor's Comments: An Update and Extension to SEM Guidelines for Administrative and Social Science Research", *MIS Quarterly*, Vol. 35 No. 2, pp. iii–xiv.

Gefen, D. and Straub, D. (2005), "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example", *Communications of the Association for Information Systems*, Vol. 16 No. 1.

Gelfand, M.J., Lim, B.-C. and Raver, J.L. (2004), "Culture and Accountability in Organizations: Variations in Forms of Social Control across Cultures", *Human Resource Management Review*, Vol. 14 No. 1, pp. 135–160.

Goodman, E.A., Zammuto, R.F. and Gifford, B.D. (2001), "The Competing Values Framework: Understanding the Impact of Organizational Culture on the Quality of Work Life", *Organization Development Journal*, Vol. 19 No. 3, pp. 58–68.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to Use and How to Report the Results of PLS-SEM", *European Business Review*, available at:https://doi.org/10.1108/EBR-11-2018-0203.

Hargadon, A.B. and Douglas, Y. (2001), "When Innovations Meet Institutions: Edison and the Design of the Electric Light", *Administrative Science Quarterly*, Vol. 46 No. 3, pp. 476–501.

Harrington, S.J. and Guimaraes, T. (2005), "Corporate Culture, Absorptive Capacity and IT Success", *Information and Organization*, Vol. 15 No. 1, pp. 39–63.

Harrison, J., Thurgood, G.R., Boivie, S. and Pfarrer, M. (2019), "Perception Is Reality: How CEOs' Observed Personality Influences Market Perceptions of Firm Risk and Shareholder Returns", *Academy of Management Journal*, available at:https://doi.org/10.5465/amj.2018.0626.

Hartnell, C.A., Ou, A.Y., Kinicki, A.J., Choi, D. and Karam, E.P. (2019), "A Meta-Analytic Test of Organizational Culture's Association with Elements of an Organization's System and its Relative Predictive Validity on Organizational Outcomes", *Journal of Applied Psychology*, Vol. 104 No. 6, pp. 832–850.

Helfrich, C.D., Li, Y.-F., Mohr, D.C., Meterko, M. and Sales, A.E. (2007), "Assessing an Organizational Culture Instrument based on the Competing Values Framework: Exploratory and Confirmatory Factor Analyses", *Implementation Science*, Vol. 2 No. 1, p. 13.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2016), "Testing Measurement Invariance of Composites Using Partial Least Squares", *International Marketing Review*, Vol. 33 No. 3, pp. 405–431.

Herath, T. and Rao, H.R. (2009a), "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154–165.

Herath, T. and Rao, H.R. (2009b), "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106–125.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660.

Hu, Q., Hart, P. and Cooke, D. (2007), "The Role of External and Internal Influences on Information Systems Security–A Neo-Institutional Perspective", *The Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153–172.

Ifinedo, P. (2014), "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition", *Information & Management*, Vol. 51 No. 1, pp. 69–79.

Iivari, J. and Huisman, M. (2007), "The Relationship between Organizational Culture and the Deployment of Systems Development Methodologies", *MIS Quarterly*, Vol. 31 No. 1, pp. 35–58.

Kam, H.-J., Mattson, T. and Goel, S. (2019), "A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness", *Information Systems Frontiers*, available at:https://doi.org/10.1007/s10796-019-09927-9.

Karlsson, M., Denk, T. and Åström, J. (2018), "Perceptions of organizational Culture and Value Conflicts in Information Security Management", *Information & Computer Security*, Vol. 26 No. 2, pp. 213–229.

Kezar, A., Dizon, J.P.M. and Scott, D. (2020), "Senior Leadership Teams in Higher Education: What We Know and What We Need to Know", *Innovative Higher Education*, Vol. 45 No. 2, pp. 103–120.

Kim, H.L. and Han, J. (2019), "Do Employees in a 'Good' Company Comply Better with Information Security Policy? A Corporate Social Responsibility Perspective", *Information Technology & People*, Vol. 32 No. 4, pp. 858–875.

Lee, M.Y. and Edmondson, A.C. (2017), "Self-Managing Organizations: Exploring the Limits of Less-Hierarchical Organizing", *Research in Organizational Behavior*, Vol. 37, pp. 35–58.

Maitlo, A., Ameen, N., Peikari, H.R. and Shah, M. (2019), "Preventing Identity Theft: Identifying Major Barriers to Knowledge-Sharing in Online Retail Organisations", *Information Technology & People*, Vol. 32 No. 5, pp. 1184–1214.

Marinova, S., Cao, X. and Park, H.S. (2018), "Constructive Organizational Values Climate and Organizational Citizenship Behaviors: A Configurational View", *Journal of Management*, p. 014920631875530.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a Unified Model of Information Security Policy Compliance", *MIS Quarterly*, Vol. 42 No. 1, pp. 285–311.

Navis, C. and Glynn, M.A. (2010), "How New Market Categories Emerge: Temporal Dynamics of Legitimacy, Identity, and Entrepreneurship in Satellite Radio, 1990–2005", *Administrative Science Quarterly*, Vol. 55 No. 3, pp. 439–471.

Paulin, M., Ferguson, R.J. and Alvarez Salazar, A.M. (1999), "External Effectiveness of Service Management A Study of Business-to-Business Relationships in Mexico, Canada and the USA", *International Journal of Service Industry Management*, Vol. 10 No. 5, pp. 409–429.

Pérez-González, D., Preciado, S.T. and Solana-Gonzalez, P. (2019), "Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation", *Information Technology & People*, Vol. 32 No. 5, pp. 1262–1275.

Petter, S., Straub, D. and Rai, A. (2007), "Specifying Formative Constructs in Information Systems Research", *MIS Quarterly*, Vol. 31 No. 4, pp. 623–656.

Podsakoff, P.M., MacKenzie, S.B. and Podsakoff, N.P. (2012), "Sources of Method Bias in Social Science Research and Recommendations on How to Control It", *Annual Review of Psychology*, Vol. 63 No. 1, pp. 539–569.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets", *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179–214.

Quinn, R.E. and Rohrbaugh, J. (1983c), "A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis", *Management Science*, Vol. 29 No. 3, pp. 363–377.

Ratten, V. (2019), "The Effect of Cybercrime on Open Innovation Policies in Technology Firms", *Information Technology & People*, Emerald Publishing Limited, Vol. 32 No. 5, pp. 1301–1317.

Scheibe, K. and Gupta, M. (2017), "The Effect of Socializing via Computer-mediated Communication on the Relationship between Organizational Culture and Organizational Creativity", *Communications of the Association for Information Systems*, Vol. 40 No. 1.

Schein, E.H. (2010), *Organizational Culture and Leadership*, 4th Ed., John Wiley & Sons, San Francisco.

Schneider, B., Smith, D.B., Taylor, S. and Fleenor, J. (1998), "Personality and Organizations: A Test of the Homogeneity of Personality Hypothesis.", *Journal of Applied Psychology*, Vol. 83 No. 3, pp. 462-470.

Schreuder, F., Schalk, R. and de Jong, J. (2017), "Psychological Contracts in Self-Directed Work Teams: Development of a Validated Scale and its Effects on Team Commitment", *Team Performance Management: An International Journal*, Vol. 23 No. 3, pp. 136–155.

Shih, C.-C. and Huang, S.-J. (2010), "Exploring the Relationship between Organizational Culture and Software Process Improvement Deployment", *Information & Management*, Vol. 47 No. 5, pp. 271–281.

Siponen, M. and Vance, A. (2010), "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487–502.

Siponen, M. and Vance, A. (2014), "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations", *European Journal of Information Systems*, Vol. 23 No. 3, pp. 289–305.

Smart, J.C. and St. John, E.P. (1996), "Organizational Culture and Effectiveness in Higher Education: A Test of the 'Culture Type' and 'Strong Culture' Hypotheses", *Educational Evaluation and Policy Analysis*, Vol. 18 No. 3, pp. 219–241.

Tallon, P.P., Queiroz, M., Coltman, T. and Sharma, R. (2019), "Information Technology and the Search for Organizational Agility: A Systematic Review with Future Research Possibilities", *The Journal of Strategic Information Systems*, Vol. 28 No. 2, pp. 218–237.

Tams, S. (2013), "Moving Cultural Information Systems Research toward Maturity: A Review of Definitions of the Culture Construct", *Information Technology & People*, Vol. 26 No. 4, pp. 383–400.

Vaast, E., Davidson, E. J., & Mattson, T. (2013). Talking about Technology: The Emergence of a New Actor Category through New Media. *MIS Quarterly*, *37*(4), 1069–1092.

Vedadi, A. and Warkentin, M. (2020), "Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions", *Journal of the Association for Information Systems*, Vol. 21 No. 2.

da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020), "Defining Organisational Information Security Culture-Perspectives from Academia and Industry", *Computers & Security*, Vol. 92, p. 101713.

da Veiga, A. and Martins, N. (2017), "Defining and Identifying Dominant Information Security Cultures and Subcultures", *Computers & Security*, Vol. 70, pp. 72–94.

Wang, P. (2010), "Chasing the Hottest IT: Effects of Information Technology Fashion on Organizations", *MIS Quarterly*, Vol. 34 No. 1, pp. 63–85.

Wiley, A., McCormac, A. and Calic, D. (2020), "More than the Individual: Examining the Relationship between Culture and Information Security Awareness", *Computers & Security*, Vol. 88, p. 101640.

Yazdanmehr, A., Wang, J. and Yang, Z. (2020), "Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance", *Information Systems Journal*, available at:https://doi.org/10.1111/isj.12271.

	Banking		Higher Education	
18-29	26	20.80%	16	11.86%
30-44	50	40.00%	19	14.07%
45-60	49	39.20%	100	74.07%
> 60	0	0	0	0%
Total	125	100%	135	100%
Male	60	48.00%	73	54.07%
Female	65	52.00%	62	45.93%
Total	125	100%	135	100%
Faculty	0	0	43	31.85%
Middle Mgmt.	106	84.80%	60	44.44%
Upper Mgmt.	13	10.40%	7	5.19%
IT Professional	57	15.60%	25	18.52%
Total	125	100%	135	100%

Table 1. Demographic

	All Samples			Banking Sample			Higher Education Sample		
	CA	**CR**	**AVE**	**CA**	**CR**	**AVE**	**CA**	**CR**	**AVE**
ENT	0.943	0.972	0.946	0.947	0.945	0.973	0.937	0.933	0.968
HIE	0.911	0.943	0.846	0.840	0.905	0.940	0.855	0.919	0.947
NORM	0.930	0.956	0.878	0.926	0.960	0.974	0.825	0.894	0.934
RAT	0.909	0.942	0.845	0.859	0.918	0.948	0.790	0.869	0.919
TEAM	0.924	0.952	0.868	0.869	0.925	0.952	0.864	0.922	0.950

Table 2. Construct Validity and Reliability

	ENT	**HIE**	**NORM**	**RAT**	**TEAM**
ENT	0.968				
HIE	-0.094	0.925			
NORM	0.175	0.204	0.908		
RAT	0.352	0.383	0.384	0.889	
TEAM	0.476	0.128	0.356	0.544	0.930

Table 3. Discriminant Validity & Inter-Construct Correlations (All Samples)
Note: Shaded cell are square root of AVE

	Banking Sample					Higher Education Sample				
	ENT	**HIE**	**NORM**	**RAT**	**TEAM**	**ENT**	**HIE**	**NORM**	**RAT**	**TEAM**
ENT	0.973					0.968				
HIE	-0.218	0.917				-0.094	0.925			
NORM	0.142	0.406	0.962			0.175	0.204	0.908		
RAT	0.184	0.184	0.468	0.927		0.352	0.383	0.384	0.889	
TEAM	0.308	-0.096	0.045	0.193	0.932	0.476	0.128	0.356	0.544	0.930

Table 4. Discriminant Validity & Inter-Construct Correlations
Note: Shaded cells are square root of AVE

	All Samples		Banking Sample		Higher Education Sample	
	VIF	**Item Weight**	**VIF**	**Item Weight**	**VIF**	**Item Weight**
COMP1	2.463	0.260 (2.053)*	2.206	0.410 (2.306)*	2.597	0.054 (0.329)
COMP2	2.374	0.508 (3.757)***	1.820	0.230 (1.009)	2.883	0.683 (4.087)***
COMP3	2.392	0.339 (3.577)***	1.965	0.499 (4.397)***	2.497	0.334 (2.522)*

Table 5. Formative Construct Validity and Reliability
Note: *p < 0.05, **p < 0.01, ***p < 0.001

Hypotheses	**β (t-value)**	**SD of β**	**Mean of β**	**Effect Size (F^2)**	**Supported**
H1a TEAM → NORM	0.041 (0.602)	0.067	0.042	0.001	No
H1b TEAM → COMP	0.129 (2.130)*	0.061	0.126	0.022	***Yes***
H2a ENT → NORM	0.077 (1.098)	0.070	0.078	0.006	No
H2b ENT → COMP	0.167 (2.477)*	0.067	0.167	0.038	No
H3a RAT → NORM	0.306 (4.500)***	0.068	0.305	0.077	***Yes***
H3b RAT → COMP	0.093 (1.336)	0.070	0.095	0.010	No
H4a HIE → NORM	0.193 (3.365)***	0.057	0.196	0.039	***Yes***
H4b HIE → COMP	0.185 (3.361)***	0.055	0.187	0.050	***Yes***
H5 NORM → COMP	0.434 (7.656)***	0.057	0.439	0.276	***Yes***
Endogenous Variable	**R^2 Value**	**SD of R^2**		**Mean of R^2**	
COMP	0.202	0.045		0.216	
NORM	0.458	0.051		0.471	

Table 6. Results of Hypothesis Testing
Note: SD – Standard Deviation, *p < 0.05, **p < 0.01, ***p < 0.001

Hypotheses	β (t-Value)		Mean of β		Differences of β β (t-value)	Effect Size (F^2)	
	Banking	Higher Ed.	Banking	Higher Ed.		Banking	Higher Ed.
H1a: TEAM → NORM	-0.044 (0.483)	0.220 (2.216)*	-0.035	0.220	0.264 (2.008)*	0.003	0.036
H1b: TEAM → COMP	0.134 (1.716)	0.091 (0.995)	0.139	0.097	0.043 (0.346)	0.030	0.010
H2a: ENT → NORM	0.166 (1.847)	-0.003 (0.032)	0.163	-0.005	0.169 (1.213)	0.035	0.000
H2b: ENT → COMP	0.037 (0.372)	0.319 (3.486)***	0.027	0.310	0.282 (2.083)*	0.002	0.145
H3a: RAT → NORM	0.379 (5.148)***	0.232 (2.388)*	0.378	0.235	0.147 (1.204)	0.196	0.038
H3b: RAT → COMP	0.169 (1.518)	-0.006 (0.063)	0.171	-0.005	0.175 (1.159)	0.040	0.000
H4a: HIE → NORM	0.368 (5.374)***	0.087 (0.938)	0.373	0.096	0.281 (2.498)*	0.186	0.007
H4b: HIE → COMP	0.408 (4.606)***	0.106 (1.456)	0.399	0.106	0.301 (2.667)**	0.238	0.018
H5: NORM → COMP	0.293 (2.616)**	0.498 (6.827)***	0.301	0.501	0.205 (1.486)	0.106	0.404
R^2 Values							
Endogenous Variable	**R^2 (t-value)**				**R^2 Differences (t-value)**		
	Banking	**Higher Ed.**					
COMP	0.472 (6.560)***	0.499 (8.026)***			0.026 (0.276)		
NORM	0.348 (5.059)***	0.185 (3.370)***			0.163 (1.864)		

Table 7. Results of Multi-group Analyses (Banking vs. Higher Education)

Note: *p < 0.05, **p < 0.01, ***p < 0.001

Appendix A – Measurement Items

Construct	Measurement Items	Reference
COMP*	COMP1: If my organization experienced a data breach, the authority would take legal action against us.	Self-developed by referencing (Hu et al., 2007)
	COMP2: The authorized parties (e.g., external auditors) expect us to protect sensitive data using standardized procedures and controls.	
	COMP3: If my organization experienced a data breach and news of the breach became public, it would have a very bad impact on my organization's image.	
TEAM	TEAM1: Managers in my organization are warm and caring. They seek to develop employees' full potential and act as their mentors or guides.	Adapted from (Helfrich et al., 2007)
	TEAM2: My organization emphasizes human resources. High cohesion and morale are important.	
	TEAM3: The glue that holds my organization together is loyalty and tradition. Commitment to this organization runs high.	
ENT	ENT1: My organization is a very dynamic and entrepreneurial place. People are willing to stick their necks out and take risks.	
	ENT2: Managers in my organization are risk-takers. They encourage employees to take risks and be innovative.	
RAT	RAT1: Managers in my organization are coordinators and coaches. They help employees meet the organization's goals and objectives.	
	RAT2: My organization emphasizes competitive actions and achievement. Measurable goals are important.	
	RAT3: The glue that holds my organization together is the emphasis on tasks and goal accomplishment. A production orientation is commonly shared.	
HIE	HIE1: My organization is a very formalized and structured place. Bureaucratic procedures generally govern what people do.	
	HIE2: Managers in my organization are rule-enforcers. They expect employees to follow established policies and procedures.	
	HIE3: The glue that holds my organization together is formal rules and policies. People feel that following the rules is important.	
NORM	NORM1: In my organization, our top management think that we should follow ISP.	Adapted from (Herath and Rao, 2009a)
	NORM2: In my organization, our bosses think that we should follow ISP.	
	NORM3: In my organization, our colleagues think that we should follow ISP.	

Table A-1: Measurement Items (Note: * Formative)

Appendix B – Factor Loading

	COMP	ENT	HIE	NORM	RAT	TEAM
COMP1	**0.873**	0.190	0.318	0.526	0.431	0.316
COMP2	**0.935**	0.337	0.301	0.547	0.387	0.335
COMP3	**0.882**	0.278	0.306	0.511	0.433	0.302
ENT1	0.303	**0.972**	-0.077	0.181	0.340	0.407
ENT2	0.309	**0.973**	-0.115	0.171	0.332	0.422
HIE1	0.208	-0.209	**0.876**	0.217	0.210	-0.051
HIE2	0.292	-0.112	**0.941**	0.241	0.274	0.073
HIE3	0.391	-0.007	**0.941**	0.328	0.423	0.140
NORM1	0.547	0.134	0.309	**0.946**	0.411	0.171
NORM2	0.571	0.189	0.261	**0.960**	0.378	0.211
NORM3	0.533	0.188	0.258	**0.905**	0.388	0.255
RAT1	0.471	0.359	0.303	0.409	**0.921**	0.516
RAT2	0.393	0.305	0.334	0.395	**0.929**	0.346
RAT3	0.382	0.282	0.325	0.344	**0.907**	0.363
TEAM1	0.316	0.410	0.084	0.236	0.452	**0.931**
TEAM2	0.314	0.369	0.077	0.227	0.382	**0.930**
TEAM3	0.360	0.413	0.054	0.170	0.422	**0.934**

Table B-1: Factor Loading

Appendix C - 3-step Measurement Invariance Testing

We used the MICOM three-step procedure for measurement invariance testing (Henseler et al., 2016). We first assessed configural invariance by ensuring that (1) the same indicator variables were used in each group, (2) all the data were treated equally across groups, and (3) the same variance-based estimations were used for all the groups (Henseler et al., 2016). We then evaluated compositional invariance by determining whether the correlational values were close to 1 and within the range of the confident intervals. Finally, we assessed invariance for means (Step 3a) and variances (Step 3b). If a mean difference or a variance difference between two groups falls within the range of the confident intervals, then equal mean value or equal invariance has been attained, respectively. We found that for a pair of group comparison, the criteria for compositional invariance was satisfied in the second step of MICOM. With compositional invariance, although the mean value equal and the variance equal were not fully attained in the third step, it is still possible to compare the standardized coefficients of the structural model across groups (Henseler et al., 2016). Thus, we conclude that our Multi-Group Analysis (MGA) produced meaningful statistical results.

Construct	Step 1	Step 2			Step 3a			Step 3b			Invariance
	Configural Invariance	Corr.	Confident Intervals	Comp. Inv.	Mean Diff.	Confident Intervals	Equal Mean	Variance Diff.	Confident Intervals	Equal Variance	
ENT	Yes	0.999	[0.999, 1.000]	Yes	0.493	[-0.220, 0.246]	No	0.222	[-0.234, 0.256]	Yes	Partial
COMP	Yes	0.998	[0.998, 1.000]	Yes	0.687	[-0.247, 0.244]	No	-0.436	[-0.460, 0.435]	No	Partial
HIE	Yes	0.999	[0.995, 1.000]	Yes	0.280	[-0.237, 0.251]	No	-0.680	[-0.344, 0.331]	No	Partial
NORM	Yes	0.999	[0.998, 1.000]	Yes	0.254	[-0.253, 0.254]	Yes	0.268	[-0.411, 0.365]	Yes	Full
RAT	Yes	0.998	[0.998, 1.000]	Yes	0.834	[-0.244, 0.235]	No	-0.568	[-0.385, 0.340]	No	Partial
TEAM	Yes	0.999	[0.997, 1.000]	Yes	0.481	[-0.243, 0.251]	No	-0.292	[-0.295, 0.288]	Yes	Partial

Table C-1: Measurement Invariance Testing

Note: Corr. (Correlation), Comp. Inv. (Compositional Invariance), Mean Diff. (Mean Difference), Variance Diff. (Variance Difference)