Impact of Organizational Culture and Security Norms on Security Compliance Pressure: A Competing Value Model Perspective

Abstract

Most scholars generally agree that the culture of an organization influences a variety of information security related behaviors primarily through the formation of security related norms. However, determining universal effects of organizational culture on security behaviors is challenging because there are many different types of organizational cultures that get formed and promoted with varying levels of success. In this paper, we argue that the effect of organizational culture on the formation of information security norms and the level of compliance pressure will vary depending on the type of organizational culture because not all cultures promote strong security-related values and taken for granted assumptions. To make these arguments, we use the competing value model (CVM), which is an integrated model used to understand the range of values within an organization. Using the CVM, we categorize organizational cultures based on two competing values: 1) internal versus external focus and 2) flexibility versus stability. In a survey of industry professionals across the banking and higher education industries, we found that the effect of organizational culture on security related norms and general compliance pressures varied significantly depending on the type of organizational culture. We also found that the effects varied across the entire sample and between industry segments. Based on our theoretical discussion and empirical findings, we suggest that future research be cautious about proposing a universal model of organizational culture in the context of information security related behaviors.

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

Introduction

The culture of an organization (i.e., the collective values that guide behaviors) is an important factor that influences how employees formally and informally act in an organizational context [1]. One important action that employees take each day are behaviors related to voluntary and involuntary information security behaviors [2]. The culture of an organization helps define the security actions that are appropriate or inappropriate, which may create strong or weak security related norms in the organization [3]. Most organizations recognize that developing an organizational culture that promotes diligent information security actions is an important step in fostering secure behaviors from its employees [3-4]. For a variety of reasons, however, many organizations have found it difficult to create such an organizational culture, which leaves them vulnerable to threats originating from their own employees [5-6].

A security-aware organizational culture is one that encourages (through formal and informal mechanisms) individuals to protect information assets by strictly or mindfully following the information security policies and procedures of the organization [3] [6]. There are many benefits of developing this type of organizational culture. For instance, a security-aware organizational culture minimizes the risks of computer misuse [7], positively shapes information security management practices [6], enhances information security compliance behavioral intentions [3], and raises general information security awareness [8]. Moreover, a security-aware organizational culture should reduce security related risks in organizations [5].

It is unclear, however, what cultural values organizations should promote to create this type of security-aware environment in an organization. For instance, does an organizational culture that values flexibility over stability foster a stronger or weaker security-aware environment? Does an organizational culture that values rationality more than team-based decision making create a stronger or weaker security-aware environment? The literature has not provided clear answers to these questions, which is problematic because organizations have many different values that they must balance when forming their organizational culture and establishing their information security environment. As such, the purpose of our paper is to

address the following important research question: *How do different types of organizational cultures shape information security related norms and compliance pressures?*

To answer this research question, we draw on the competing values model (CVM) that is a values-based model used to understand and evaluate the effectiveness of an organization [9]. Quinn and Rohrbaugh [9] argue that organizations balance competing values along two primary dimensions: 1) the different types of organizational structures (flexibility versus stability) and 2) the primary focus of the organization (internally focused versus externally focused). How an organization balances these values (and others) shapes its organizational culture, which impacts its overall effectiveness [9-10]. We argue that these competing values will also help determine whether an organization will develop a strong or a weak security-aware organizational environment. In general, we propose that organizations that have a more internally focused value proposition along with a stable organizational structure will have a stronger security-aware organizational environment, which will (in turn) foster strong information security norms and high pressure to comply with the organization's information security policies and procedures.

To evaluate empirically how these different 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 had a flexible (as opposed to stable or rigid) organizational culture did not develop strong information security related norms but still had relatively high perceived pressure to comply with their organization's information security policies and procedures. In contrast, for employees who perceived that they worked in organizations with a stable (as opposed to flexible) organizational culture, we found that those employees perceived their organizations had strong security-related norms and strong perceived compliance pressures. In a post hoc analysis, we further found that these effects varied significantly across industries (i.e., the effects of flexibility versus stability for our sample of banking employees were different from our sample of higher education employees). However, we did not find differences based on whether the employees perceived that their organizations had an organizational culture with an internal versus an external focus. We will discuss the theoretical and practical contributions of the study at the end of this paper.

Literature Review

Encouraging employees to comply with their organization's information security policies and procedures is an important step to protect the organization's information resources [11]. As such, academics have spent significant time and attention building models to explain the variance in employees' compliance behaviors (or intentions thereof). To do so, the prior literature has used a variety of different theories to construct behavioral compliance models such as the technology acceptance model [12], health belief model [13], deterrence theory [14-15], protection motivation theory [2] [16-17], neutralization theory [11], and control balance theory [18]. Many of these theoretical models focus on individual choices. For instance, deterrence theory and rational choice theory suggest that individuals decide how punishments can be used to encourage compliance (or discourage noncompliance). However, the models from the previously published empirical and theoretical research rarely include any type of structural inhibitor or facilitator (such as the culture of the organization) as a mediator or a moderator to an individual making the choice to follow (or not to follow) the security-related policies and procedures.

The primary structural inhibitor or facilitator that scholars have found to impact compliance behaviors (or intentions thereof) is subjective norms (i.e., social pressure from others). In general, the greater the social pressure from others in the organization, the greater the likelihood that an employee will comply with the organization's policies and procedures [14]. However, organizations come in many different forms with varying norms, cultures, histories, and taken-for-granted assumptions regarding what it means to be secure [19-20]. Based on the prior literature, it is still unclear what types of organizational environments might create strong compliance-related subjective norms. Hu et al. [3] suggest that the culture of the organization (either goal-oriented or rule-oriented) has the potential to create strong or weak subjective norms, which (they propose) mediates employees' intentions to comply with their organization's security-related policies and procedures.

An organizational culture refers to the collective values, actions, and behaviors of employees that constitute an organization's climate and overall business environment [10] [21]. These collective beliefs provide a shared set of assumptions that guide how employees behave in the organizational context [22-

24]. Organizational cultures form based on (among many others) the types of employees working for the organization, the history of the organization, the corporate and business strategy of the organization, the vision and mission statement of the organization, the values promoted by top executives, and the habitual actions of the employees [10] [25]. All of these define how business gets done in a specific organization along with the specific principles and values that guide organizational decision-making [9-10].

Organizational Culture & Information Security Literature

Given that the culture of an organization impacts the overall business environment of the organization, it is not surprising that prior information security literature has theorized about the effects of organizational culture on a variety of information security-related actions. Table 1 displays relevant and selected research on organizational culture in the information security context. In general, the prior literature has revealed that a security-aware organizational culture reduces security related risks in organizations by creating an environment that is conducive to following the organization's security-related policies and procedures [3] [5] [26]. Moreover, a security-aware organizational culture creates an environment for information security compliance behaviors [3], fosters sound information security management practices [6] [27-28], reduces the likelihood that employees will misuse technology resources [7], minimizes technical disruption after a merger [29], and raises general information security awareness [8]. The overall information security environment is shaped by the organizational culture and the cultural decisions that top management make [30]. Furthermore, prior literature strongly suggests that changing the culture of the organization is one of the first places an organization should look when attempting to create a security-aware environment [31-32].

Table 1. Summary of Organizational Cultural Literature

Studies	Theories	Key Research Findings
Towards Information Security Behavioural Compliance [26]	Model of organizational culture [21]	Since it is very difficult to audit human behavior in organizations, an informal, subtle approach is necessary to change organizational culture for cultivating information security.

Cultivating an Organizational Information Security Culture [32]	Theory of Organizational Knowledge Creation [33]	Model for Information Security Shared Tacit Espoused Values (MISSTEV) suggests that management should make employees aware of their roles in information security protection and organization's vision of information security.
Exploring Organizational Culture for Information Security Management [6]	Organizational culture theories [34-35]	The control-oriented culture generates a stronger effect on ISM in comparison to the flexibility-oriented culture.
Information security culture: A Management Perspective [28]	Theory of culture [36]	A proposed conceptual model posits that interactions between management's requests (i.e., espoused values) and employees' beliefs and values (i.e., shared tacit assumptions) are important to cultivate security.
Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture [3]	Theory of Planned Behavior (TPB) [37]	Attitudes, subjective norms, and perceived behavioral control affect an individual's intention to comply with ISP. Moreover, top management can encourage positive security behavior by actively participate in security related activities and by cultivating rule and goal-oriented culture.
Information Security Policy Compliance Model in Organizations [27]	Social Bond Theory [38] and Involvement Theory [39]	Employees' involvement, commitment, and beliefs generate employees' positive attitude toward ISP compliance. Moreover, organizations can promote information security through information security knowledge sharing, collaboration, and intervention.

Despite all the existing research in this area, there is still a need for more research to further our understanding of the relationship between organizational culture and information security related behaviors [40]. Much of the prior information security literature uses a high level "organizational culture" construct to capture all types of organizational cultures in their theoretical models. However, there are many types of organizational cultures so it is difficult for academics to make universal claims related to organizational cultures without investigating the different types of organizational cultures. Only then will we be able to determine the effectiveness of organizational culture on information security actions. Moreover, top executives have many choices when determining how to shape the culture of an organization, but we do not know the effect that those choices have on creating a security-aware organizational environment [6] [27-28].

It is important to keep in mind that the culture of an organization is not designed specifically for information security. Instead, it is designed to instill certain values and principles to maximize the

organization's overall effectiveness (i.e., maximize shareholder value or maximize value across all stakeholders) based on its overall mission and vision statement [1] [41]. From the existing information security literature on organizational culture, however, it is unclear what principles and values will have the benefit of both maximizing effectiveness for all stakeholders and creating a security-aware environment. To investigate these values, we leverage the competing value model (CVM), which is an integrated model used to understand the range of values within an organization. We chose the CVM because it is one of the most influential models in business, is parsimonious yet insightful, and has been previously used to explain a variety of phenomena such as organizational design, effectiveness, quality, culture, and leadership [41-42].

Competing Value Model (CVM)

The CVM is a values-based model used to evaluate and predict the effectiveness of an organization [9]. Organizations ascribe to many values and principles but the empirical research using the CVM has found two consistent dimensions/values that explain the effectiveness of many organizations. The first value is related to the stability of the organization. An organization may value stability, control, and order on one end of the spectrum or flexibility and agility on the other end of the spectrum. How flexible or adaptive their managers are or are not helps define the culture of the organization. The second value is related to the focus area of the organization. An organization may have an internal (internal relationships and strong organizational processes) or an external (market niches and consumer relationships) value orientation, which also helps shape the culture of the organization [43-44]. Said differently, organizations will either focus on their organizations' social and technical systems or adapt to the external environment defined by threats, opportunities, and resources [9].

Together these values form four quadrants with each representing a distinct set of organizational, cultural, and individual values. The intersection of both value dimensions creates four organizational cultural archetypes: 1) hierarchical, 2) rational, 3) entrepreneurial, and 4) team cultures [45].

Figure 1 graphically displays the four cultural archetypes along the continuum of both value dimensions. An organizational culture may espouse one or more of these cultural archetypes due to an

organization having many subcultures (especially large organizations), which may create contradictory or competing values within and between organizations [9] [43] [44]. Each axis displayed in Figure 1 highlights opposing ends of the continuum (i.e., flexibility is the opposite of stability and internal is the opposite to external). Therefore, the values produce organizational cultures that are contradictory along each axis and diagonally.

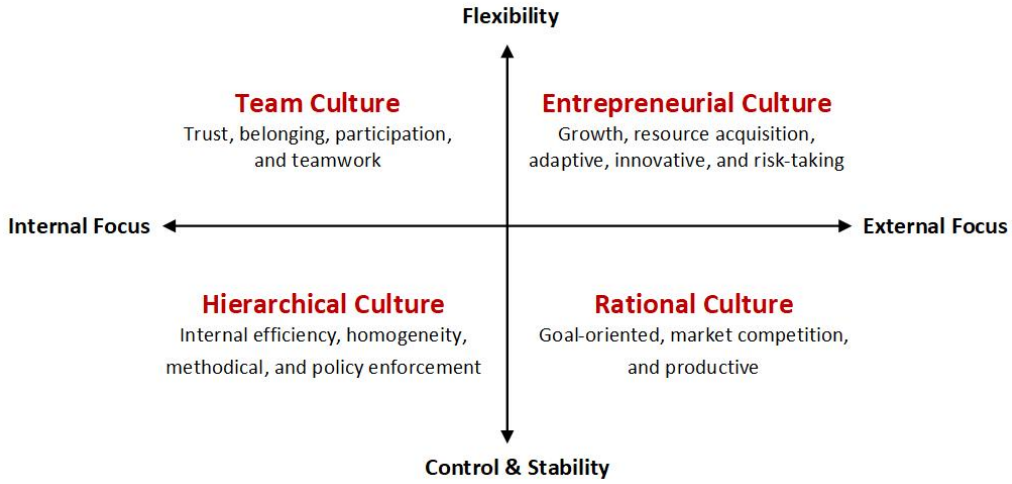

Figure 1. Competing Values Model [9] [45]

Although the CVM places organizational cultures in four quadrants, these four quadrants are not necessarily mutually exclusive, especially in large organizations that include many subcultures. For instance, a bank may primarily embrace a hierarchical organizational culture [45-46] that is inwardly focused to comply with local, regional, and national regulations, but that same bank may also have certain divisions that adopt a rational culture that is outwardly focused to adapt to market forces [47]. Hence, an organization may have contradictory values within its own organizational boundaries and between other organizations either in the same or different industries [44] [47].

The information systems literature has used the CVM to explain a variety of technology-related phenomena. For instance, the prior information systems literature has used the CVM to examine the relationship between organizational culture and the adoption of system's development methodologies [49], to investigate the impact of absorptive capacity (i.e., knowledge transfer) on technology implementations [50], and to study the influence of organizational culture on software development process improvements

[51]. In the behavioral information security literature, [6] used the CVM to examine the impact of culture on information security management practices. Overall, the CVM is appropriate for research that examines the impact of culture quantitatively in organizations [52] across a variety of technical phenomena.

Research Model

Our research model proposes relationships between the different types of organizational cultures (based on the CVM), perceived compliance pressures, and perceived security-related subjective norms. We chose to investigate perceived compliance pressures because a security-aware organizational environment is one where employees consciously and mindfully follow the organization's security-related policies and procedures [3] [6]. If the employees perceive that their organizational culture does not create a security-aware environment that strongly encourages them to follow the information security rules and regulations, then that type of organizational culture will put the organization at a greater security risk (relative to an environment that does promote or facilitate following the security-related rules and regulations).

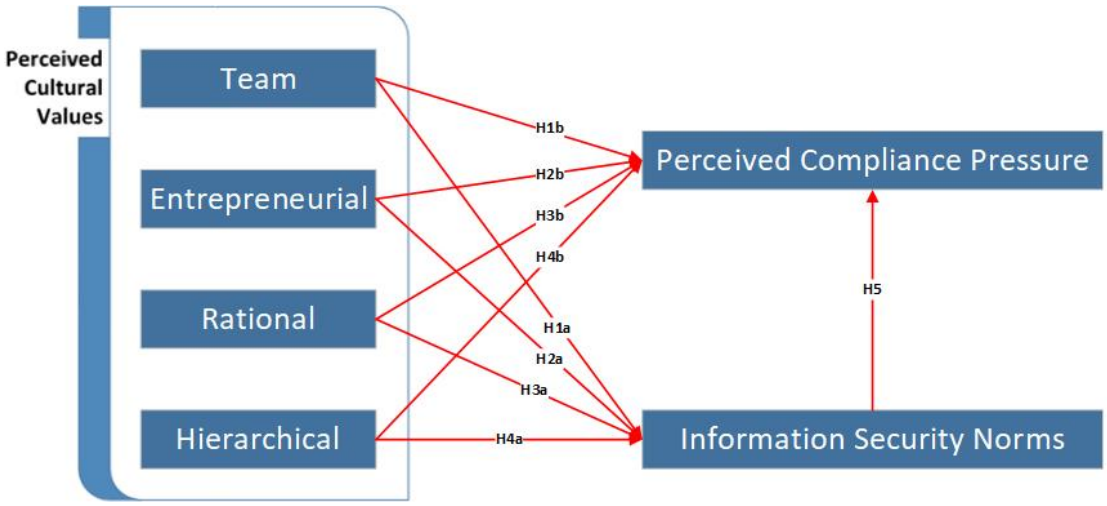

Figure 2: Proposed Research Model

We further chose to examine the role of organizational culture on the formation of security-related subjective norms because the culture of an organization influences how individuals think, feel, and act [21] [52]. Through these thoughts and actions, the culture of an organization shapes and reinforces the norms within that organization [53-54]. The organizational culture defines appropriate actions in the organizational context, which (over time) results in normative behaviors by its employees [54]. However,

certain organizational cultures create chaotic organizational environments that are constantly changing [48], which may adversely impact the creation of strong security-related subjective norms. Thus, we posit that different types of organizational cultures may have a varying effect on the formation of subjective norms within an organization. Figure 2 displays our research model, which we develop in the subsequent sections.

Entrepreneurial & Team Organizational Cultures

Team and entrepreneurial organizational cultures highlight certain organizations' propensity to be flexible and adaptable [44] [47]. These types of organizational cultures focus on change and often do not have well-documented policies and procedures (i.e., possibly not having formal data governance documents or well-defined information security-related policy documents). On the one hand, being flexible and adaptable is beneficial for information security practices because the threat landscape is constantly changing. Not having rigid policies and procedures may allow these organizations to quickly respond to new threats as they arise. On the other hand, however, flexibility makes it difficult for organizations to develop in-depth policies and related training programs, for organizations to develop routines, and for organizations to formalize their security-related policies and procedures. Routines generally require stable or habitual actions by its employees, which can be difficult to develop if the policies and procedures of the organization are in a constant state of flux. Therefore, the flexible nature of these organizational environments may make it difficult to develop strong security-related norms, which may result in a significantly lower propensity to develop strong subjective norms (related to security) in these organizational cultures.

Organizations that have a team organizational culture have a more internal orientation whereby managers focus most of their attention on the internal processes (as opposed to responding to the external environment) necessary for their teams to be successful [48]. An internal value orientation focuses on clearly defining and optimizing internal organizational processes. These clearly defined processes may promote a strong security-aware environment (assuming that the internal processes include a security component). To conceptualize a team organizational culture, let's consider an organizational structure, which organizes staff in temporary project teams to accomplish specific (albeit temporary) objectives. In

this cultural environment, each team may form its own norms that may vary significantly from team-to-team. The subjective norms and compliance pressure to comply may come from the other team members (due to a desire to not let the other team members down), which can have powerful effects on all types of behaviors in the organization [56]. As such, we hypothesize the following:

H1a: Team organizational culture is positively associated with security-related subjective norms.
H1b: Team organizational culture is positively associated with perceived compliance pressure.

In contrast, an entrepreneurial organizational culture (while still valuing flexibility as opposed to stability) has an external focus instead of an internal focus. Organizations with an entrepreneurial culture tend to be risk takers and seek to adapt to the external environment [45], but this tends to not be the case for team organizational cultures. Entrepreneurial organizational cultures tend to not have many documented policies because they have more of an outward (instead of an inward) value proposition [57]. These types of organizations tend to seek external legitimacy based on their product or service offerings [57] as opposed to seeking legitimacy based on their internal work processes [57-58]. Often these types of entrepreneurial cultures tend to have technology-mediated work practices [59-60], but those technology-mediated work practices may not have a strong focus on the security risks associated with those work practices due to the often-fleeting nature of the work practices.

Organizations with an entrepreneurial culture tend to be newer and have chaotic work environments. On the one hand, chaotic internal work environments often have the appearance (perception) of making the policies and procedures up "on the fly" because the environment is constantly evolving, which may be problematic for security-related behaviors. On the other hand, however, an entrepreneurial organizational culture promotes an open system for information sharing due (in part) to these under-developed organizational work processes [44] [47] [49], which can have the benefit of responding to emerging security-related threats. This tension may create an environment that still provides some pressure to act in a secure manner, because part of establishing external legitimacy is not having the negative media exposure associated with a data breach. For instance, firms such as Uber, Lyft, or Tesla who have an entrepreneurial organizational culture and who espouse to have a technology savvy reputation would (more likely than not)

see a negative hit to their reputations if their information systems were compromised. Thus, we hypothesize the following:

H2a: Entrepreneurial organizational culture is positively associated with security-related subjective norms.

H2b: Entrepreneurial organizational cultures is positively associated with perceived compliance pressure.

Although the wording of our first two hypotheses might suggest that we are proposing the same effect for team and entrepreneurial organizational cultures, this is not the case. We are not suggesting that the magnitude of our two proposed effects will be the same across the two types of organizational cultures (even though we do posit that both cultural archetypes will result in some degree of security-related subjective norms and compliance pressures). From the above discussion, we are proposing that the security-related subjective norms and compliance pressures will be stronger in team organizational cultures relative to entrepreneurial organizational cultures due to team organizational cultures having more well-defined internal processes (i.e., effect of H1a and H1b will be stronger than the effect of H2a and H2b).

Rational & Hierarchical Organizational Cultures

Rational and hierarchical organizational cultures highlight certain organizations' desire to have stable or rigid environments [45] [48]. Organizations with these types of organizational cultures tend to have well-defined objectives, are goal-oriented, and are somewhat bureaucratic [45]. Organizations in more mature industries tend to value stability over the flexibility that might come from an entrepreneurial or a team organizational culture. From a compliance perspective, stability is more preferable than flexibility because it is easier to train employees on policies and procedures that do not constantly evolve. Stable organizational structures also make it easier to clearly identify roles, responsibilities, and accountability for matters of information security in more stable organizational environments. Furthermore, employees may be more susceptible to the peer pressure from employees when security-related norms are more well-defined, which will tend to be the case in more stable organizational cultures.

In general, for-profit organizations are rational entities (with an external as opposed to an internal focus) that make decisions based primarily on a rational calculation of costs and benefits [62-63]. However, not

all organizations are for-profit and not all for-profit organizations have a strictly rational culture. For instance, Grameen Danone (the social business formed to curb the nutrition crisis in Bangladesh) makes decisions based on social value (as opposed to based economic rationality) and institutions of higher education often make decisions based on the pursuit of knowledge (as opposed to purely based on economic rationality). Having said this, many organizations such as banks and accounting firms make decisions mainly based on economic rationality, which leads to a rational organizational culture.

We propose that employees working for organizations with a rational organizational culture tend to weigh the costs associated with establishing sound internal controls with the benefits of reducing their risk exposure when making information security-related decisions. Therefore, a rational organizational culture should provide an environment that encourages organizations to build effective security controls for preventing security breaches because it makes economic sense to do so (i.e., benefit of greater stakeholder trust outweighs the cost of implementing security controls). As such, we argue that employees working in a rational organizational culture will understand the economic reasons behind complying with the organization's information security policies and procedures. Accordingly, we hypothesize:

H3a: Rational organizational culture is positively associated with security-related subjective norms.
H3b: Rational organizational culture is positively associated with perceived compliance pressure.

A hierarchical organizational culture tends to have more of an inward focus whereas a rational culture tends to have more of an outward focus (but both still favoring stability over flexibility) [48]. As we argued with a team oriented inward focused organizational culture, a hierarchical organizational culture focuses on internal processes as well as policies and procedures that should promote a security-aware environment. Hierarchical organizational cultures are methodical, conservative, and rule driven [48]. [49] demonstrated empirically that hierarchical organizational cultures empower management to impose and enforce mandatory actions (as related to system implementations). In the context of behavioral information security, we posit that a hierarchical organizational culture may drive compliance behaviors and establish security-related norms through a top-down (bureaucratic) approach. A hierarchical organizational culture is highly structured (similar to a team organizational culture but even more formalized). As such, a

hierarchical organizational culture enforces the rules and policies through a command and control organizational environment [45], which can be a very effective way to increase compliance pressure and create security-related norms. Therefore, we hypothesize:

H4a: Hierarchical organizational culture is positively associated with security-related subjective norms.

H4b: Hierarchical organizational culture is positively associated with perceived compliance pressure.

Again, we are not suggesting that the effects of a rational and hierarchical organizational culture will have the same effects across our third and fourth hypotheses. From the above discussion, we are suggesting that the magnitude of the effects for rational organizational cultures will be less than the effects for hierarchical organizational cultures due to the inward versus external focus (i.e., effect of H4a and H4b will be stronger than the effect of H3a and H3b). Furthermore, we are also not suggesting that the effects across all four hypotheses will be the same. Instead, it would seem logical that the effects of rational organizational cultures would be stronger than those of entrepreneurial organizational cultures because the former values stability and control more than the latter (i.e., effect of H3a and H3b will be stronger than the effect of H2a and H2b). Similarly, the internal focus and rigidity associated with a hierarchical organizational culture should amplify those proposed effects relative to the effects of a team organizational culture (i.e., effect of H4a and H4b will be stronger than the effect of H1a and H1b).

Security-Related Subjective Norms

Our (a) hypotheses predict whether each cultural archetype will impact security-related subjective norms (and we posit that each cultural archetype will have such an effect with varying magnitudes). Our final prediction is related to the link between security-related subjective norms and the pressure to comply with the organization's security-related policies and procedures. This link has been well established in a variety of disciplines including information security. The greater the subjective norms to perform a security action, the greater the likelihood that an individual will perform (or intend to perform) that security action [64-68]. Hence, we propose:

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

Research Design and Methods

To investigate this research model empirically, we surveyed working professionals across two industries: 1) banking and 2) higher education. We choose these two industries due to their contrasting cultural characteristics. Organizations (or institutions) in the higher education industry may have open, team-based, or innovative (entrepreneurial) organizational cultures [69-70], whereas organizations in the banking industry may have hierarchical or rational organizational cultures [46]. Moreover, the compliance environments across organizations in these two industries have clear differences. The higher education industry is subject to certain federal regulations particularly regarding FERPA but the penalties for FERPA violations are not particularly severe. In the banking industry, however, banks must comply with a series of regulations such as Sarbanes-Oxley Act (SOX) and the Gramm Leach Bliley Act (GLBA). Furthermore, banks face significant fines for not complying with these mandatory rules and regulations. With such notable differences across these two industries, we should 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 research subjects worked, we used their perceptions about their organizations. 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. The perceptions of our research subjects' organizations are more valuable than our subjective classification of their organizations. For instance, if a banking employee who works in a technology division at their bank perceives that their organizational culture is entrepreneurial (at least partially), then that employee works under the assumption that their bank has an organizational culture that is partially entrepreneurial (even if we would have probably classified the bank as a whole as having hierarchical or rational organizational culture). This approach is similar to the approach taken by other researchers who investigated organizational or industry effects (see [6] and [71]).

Measurement Items and Instrument Validation

We used existing measurement items from pre-validated multi-item scales for the measures for several of our latent constructs [65] [72]. For other latent constructs that did not contain previously published pre-

validated multi-item scales, we used the items from [71] as our starting point to construct our own measurement items. To do this scale development, we first used a panel of expert information security researchers and scale developers to provide an initial content validity of our adapted measurement items and our new measurement items. We then had four information security professionals who had the Certified Information Systems Security Professional (CISSP) designation review our measurement items. After our measurement items were developed and/or adapted to fit our research context (see Appendix A), we designed our survey instrument using best practices related to instruction wording and question order as advocated by [73]. On our final survey instrument, all measurement items used 7-point Likert scales with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree. Finally, in order to remedy potential common method bias procedurally via our survey instrument, we used best practices by [74] particularly related to the proximal separation between the measures of the independent and dependent variables.

After we developed our initial survey instrument, we ran a pilot study with information security professionals. Our pilot study had 51 usable data points. As a result of the pilot study (and our discussion of the survey instrument with our participants), we refined our measurement items and modified the survey instructions to rectify identified ambiguities. On our final survey instrument, all measurement items were randomized to reduce the adverse impact of question ordering on our results [75].

Sample & Data Collection

We sent our survey electronically to technology professionals and middle/upper-level managers who worked in the banking industry and in the higher education industry in the United States. For our study, we did not include entry-level employees because entry-level staff members may be so new that they might not be knowledgeable about the culture of their organizations and they might not know the information security policies and procedures in their organizations. For our sample, we identified organizations in these industries based on personal contacts and alumni networks from two public Midwestern universities in the United States. To assess the potential adverse impact of non-response bias, we ran a series of ANOVAs comparing early and late responders on our key constructs. These ANOVAs did not show any material differences.

Data Analysis & Results

We used Partial Least Squares (PLS) with SmartPLS 3.2 to analyze our survey data. PLS is appropriate for evaluating path coefficients in structural models [76].[1] We evaluated our models in two steps. We first assessed the validity and the reliability of our measures with a measurement model. We then tested our research model using bootstrapping method to assess our hypothesized relationships.

Measurement Model

We assessed our measurement models in terms of convergent and discriminant validity of all of our constructs. We evaluated convergent validity using the average variance extracted (AVE), Cronbach's alpha, and composite reliability values. AVE values greater than 0.5 and Cronbach's alpha (CA) and composite reliability (CR) values greater than 0.7 are considered acceptable thresholds for establishing convergent validity [77-78]. In our data, all of our values met these recommended thresholds (see Table 2). Therefore, our survey data proved convergent validity.

Table 2. Construct Validity and Reliability

	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

We then analyzed the square root of the AVE for each construct to establish discriminant validity in our survey data. 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 (see Table 3 and Table 4), then that is evidence of discriminant validity [78]. In our data, we met or exceeded these criteria so we have evidence for discriminant validity.

Table 3. Discriminant Validity & Inter-Construct Correlations (All Samples)

	ENT	HIE	NORM	RAT	TEAM
ENT	0.968				
HIE	-0.094	0.925			

[1] Before running any of our PLS models, we first successfully screened our data for potentially problematic issues such as collinearity, outliers, and non-normality [77].

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

Note: Shaded cell represents square root of AVE

Table 4. Discriminant Validity & Inter-Construct Correlations

	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

Note: Shaded cell represents square root of AVE

To evaluate our measurement model further, we analyzed the factor loading of each measurement item on its intended construct (see Appendix B). All of our items loaded greater than the recommended threshold of 0.7 [78]. The factor loadings also show that the difference between the loading on the intended construct and the loading on any other construct was greater than 0.1. Thus, we have strong evidence of both convergent and discriminant validity in our data [80].

Table 5. Formative Construct Validity and Reliability

	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)*

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

Perceived compliance pressure (COMP) is the only formative construct in our research model. Table 5 displays the item weights (which are statistically significant) for each indicator variable in this formative construct. Additionally, the variance inflation factor (VIF) for each measurement item is below 3.3, which suggests adequate construct reliability for this formative construct [81]. All of the other construct measures met the requirements to be considered reflective indicators of their respective latent constructs based on the criteria set forth by [82]. In addition, although we used measurement items that had been approved from previous studies, the common method variances of the measurement model were tested by using the unmeasured latent method factor approach discussed by [74]. In our data, adding this 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

Using a series of structural PLS models to tease out the effects of each of the four cultural archetypes we tested hypotheses. Especially, we check the effect size (F^2) along with null-hypothesis significance testing (NHST) for all models because the NHST may be sensitive to sample size [81-82]. The effect size statistic (F^2), however, is not sensitive to sample size so it produces a better measure of the degree of the effect between two variables [81] [83]. An F^2 larger than 0.02, 0.15, and 0.35 signifies small, medium, and large effect size, respectively [86]. Table 6 summarizes the results of structural models. The R^2 values for information security subjective norms (NORM) and perceived compliance pressures (COMP) were 0.208 and 0.459 respectively. The lower R^2 for subjective norms makes sense because there are inevitably more factors that go into the formation of subjective norms than just the culture of the organization.

Table 6. Results of Hypothesis Testing

Hypotheses		β (t-value)	SD of β	Mean of β	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	***Yes***
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***

Note: SD – Standard Deviation, *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

We find that perceived entrepreneurial ($\beta = 0.167$, $p < 0.05$), team ($\beta = 0.129$, $p < 0.05$), and hierarchical ($\beta = 0.185$, $p < 0.01$) organizational cultures foster greater perceived compliance pressure, but perceived rational organizational cultures ($\beta = 0.093$, $p > 0.05$) do not. Thus, H1a, H2a, and H4 were supported but H3a was not. Of the significant paths, the effect sizes were small (see Table 6). Thus, we do not see a definitive pattern between organizational cultures with an internal value orientation versus an external value orientation or a flexible versus stable structure. Entrepreneurial ($\beta = 0.077$, $p > 0.05$) and team ($\beta = 0.041$, $p > 0.05$) organizational cultures do not foster information security subjective norms, but hierarchical ($\beta =$

0.193, $p < 0.001$) and rational organizational cultures ($\beta = 0.306$, $p < 0.001$) do. Accordingly, H3b and H4b were supported, but H1b and H2b were not. Our results also reveal that the effect sizes for all the said significant paths were small (see Table 6).

Consistent with the prior literature, we also find that information security subjective norms fostered greater perceived compliance pressure ($\beta = 0.437$, $p < 0.001$), which supports our H5 prediction. Our data also suggest that information security subjective norms was a full mediator between rational organizational cultures and perceived compliance pressure. Our data show that rational organizational cultures did not facilitate perceived compliance pressure (with security-related subjective norms in the model), but it did foster strong information security subjective norms, which (in turn) generated higher perceived compliance pressure.

Cross Industry Post-hoc Analysis

To further analyze our data, we conducted a set of multi-group analyses to compare the organizational cultural effects between our banking (n=125) and our higher education (n=135) survey participants. To make the results of our multi-group analyses meaningful, we first had to assess measurement invariance (i.e., the same construct was measured similarly across the different collectives) between the measurement items among the two different groups of survey participants across the two industries. To do this, we followed the three-step process outlined by [87] using the built in MICOM procedure in SmartPLS version 3.2. This process required analyzing configural invariance, compositional invariance, and the equality of mean values and variances. Our data met the criteria for full compositional invariance and configural invariance along with partial invariance for the equality of mean values and variances, which enabled us to run and interpret the results from our multi-group analyses. Appendix C contains the statistical details concerning these invariance tests.

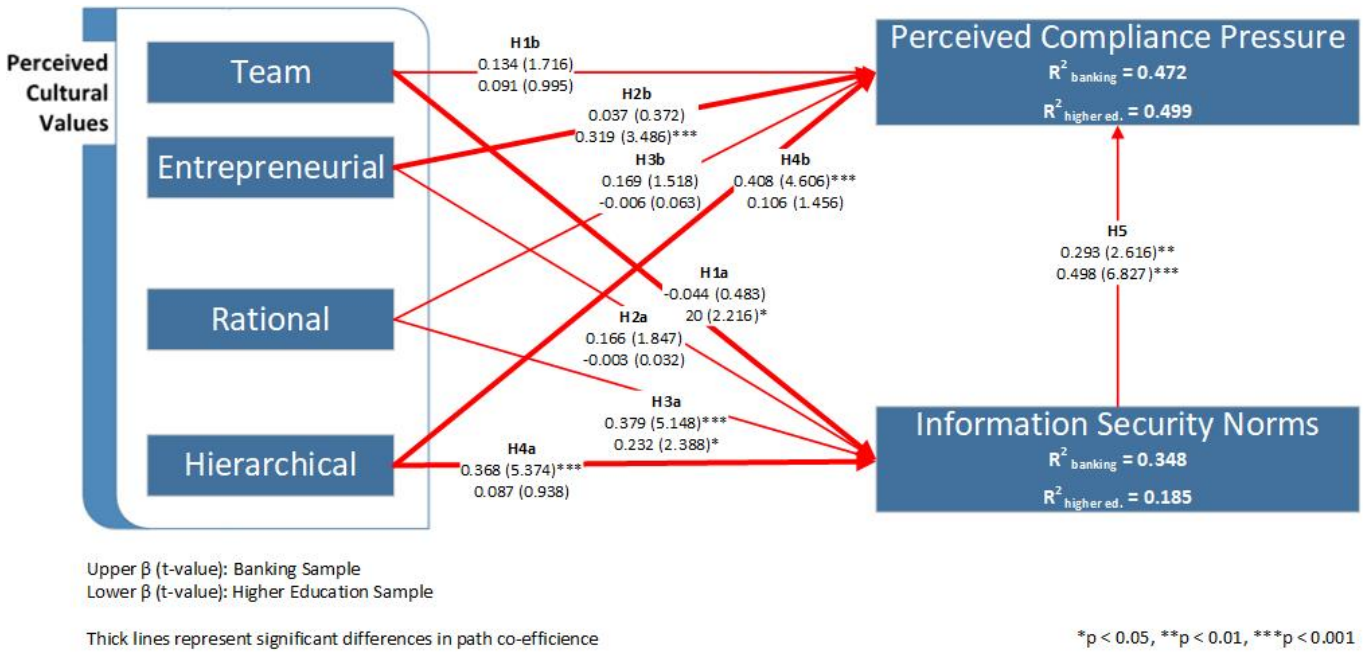

Figure 3: Structural Model Testing Results

Table 7 and Figure 3 displays the results of our multi-group analyses. In general, we find a few significant differences between the organizational cultural archetypes across both industries. For example, we find that hierarchical organizational cultures foster greater perceived compliance pressures ($\beta = 0.408$, $p < 0.001$) and information security subjective norms ($\beta = 0.368$, $p < 0.001$) among the banking employees, but hierarchical organizational cultures had no effect on those among their higher education counterparts (see Table 7). These path coefficient differences for hierarchical organizational cultures were statistically significant (information security subjective norms (β difference = 0.281, $p < 0.01$) and perceived compliance pressure (β difference = 0.301, $p < 0.05$)). Therefore, we find that hierarchical organizational cultures create a security-aware organizational environment in banking but not in higher education.

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

Hypotheses	β (t-value)		Mean of β		Differences	Effect Size (F^2)	
	Banking	Higher Ed.	Banking	Higher Ed.	β (t-value)	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

Indirect Effect (Banking vs. Higher Education)					
Indirect Path	β (t-value)		Mean of β		β Differences (t-value)
	Banking	Higher Ed.	Banking	Higher Ed.	
TEAM → COMP	-0.013 (0.448)	0.110 (2.292)*	-0.011	0.106	**0.123 (2.203)***
ENT → COMP	0.049 (1.459)	-0.002 (0.030)	0.045	-0.001	0.050 (0.811)
RAT → COMP	0.111 (2.173)*	0.116 (1.989)*	0.111	0.121	0.005 (0.059)
HIE → COMP	0.108 (2.331)*	0.043 (0.938)	0.107	0.046	0.065 (0.995)

R^2 Values (Banking vs. Higher Education)			
Endogenous Variable	Banking R^2 (t-value)	Higher Education R^2 (t-value)	R^2 Differences (t-value)
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)

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

Additionally, we find that team organizational cultures generate a positive effect on information security subjective norms among our higher education employees ($\beta = 0.220$, $p < 0.05$), but we found no such effect ($\beta = -0.044$, $p > 0.05$) among their banking counterparts. These path coefficients were significantly different (β difference = 0.264, $p < 0.05$). We further found that a team organizational culture produced an indirect effect on perceived compliance pressure in our sample of higher education employees ($\beta = 0.110$, $p < 0.05$) but not in our sample of banking employees. This indirect effect was statistically different across the two groups of employees in our sample (β difference = 0.123, $p < 0.05$). This differential effect is interesting. Logically, one might expect an institution in the higher education industry to have more team oriented organizational cultures whereas as team oriented organizational culture may not be a common cultural archetype in the banking industry.

We found another interesting difference between both groups of employees related to entrepreneurial organizational cultures. An entrepreneurial organizational culture cultivated greater perceived compliance pressure ($\beta = 0.319$, $p < 0.001$) with our sample of higher education employees, but we found no such effect with our sample of banking employees ($\beta = 0.055$, $p > 0.05$). This difference was statistically significant between the two industry groups (β difference= 0.263, $p < 0.05$). Similar to the multi-group effect we found with team-based organizational cultures, this finding may be due to not many banks having an

entrepreneurial organizational culture. Interestingly, perceived entrepreneurial organizational cultures generated no effect on information security norms in both industry groups. This finding is consistent with our hypothesis that entrepreneurial cultures are too chaotic to develop strong security-related norms.

We found the same fully mediated effect of rational organizational cultures across our sample of banking employees and higher education employees. In both industry groups, perceived rational organizational cultures only impacted compliance pressures through the formation of security-related subjective norms. We found no statistically significant differences between the path coefficients between the two industry groups.

Discussion & Conclusion

In this study, we discussed theoretically and demonstrated empirically that organizational culture has important ramifications for security-related actions (particularly security-related subjective norms and compliance pressures). However, we found that not all organizational cultures had the same effects on the formation of security-related subjective norms and compliance pressures. For instance, when we analyzed our entire sample together, we found that only the organizational cultures that favored control and stability (i.e., rational and hierarchical cultures) had a positive effect on the formation of security-related subjective norms. We found no such effect for organizational cultures that valued flexibility (i.e., entrepreneurial and team organizational cultures). This finding poses a bit of conundrum for organizations because some of the best organizations in the world can attribute their long-term success to their ability to change their organizational processes to meet evolving market demands [88]. Yet, this same flexibility that greatly contributes to their success might make them more susceptible to a data breach, which would have negative implications for their long-term success [89].

The different effects of the four cultural archetypes became even more pronounced when we split our sample between the two industries (banking and higher education). We assert that these differences may be due to the following: 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). For instance, a bank with an entrepreneurial organizational culture (albeit probably a

rare occurrence) might attract a different type of employee relative to a more traditional bank with a rational or a hierarchical organizational culture. Similarly, a team-based organizational culture in the higher education industry may attract a different type of employee relative to a hierarchical organizational culture in that same industry. Also, the types of employees interested in pursuing careers in the banking industry are probably different from the types of employees interested in pursuing careers in higher education. The different personality types (and educational backgrounds) of the employees will shape the culture of the organizations in these different industries, which will (we assert) impact the formation and usefulness of subjective norms in creating a security-aware organizational environment.

We did find that rational organizational cultures had similar effects across both industries. This similarity might be due to the fact that performing security actions by rationally calculating the benefits and the costs of performing that action are somewhat industry agnostic [90]. Thus, on some level, most organizations have some element of rationality (but with varying degrees) embedded in their organizational cultures and in their normative routines, which includes security-related subjective norms. We are not saying that all industries and all organizations define rationality in the same manner, but the idea of performing a cost-benefit (irrespective of whether that is monetary, social, or other costs-benefits) analysis in relation to performing important daily tasks (including security-related tasks) is done consistently across organizations and industries.

Theoretical Contributions

Our study contributes to the behavioral information security literature in two important ways. First, the core theories that scholars have used in the behavioral information security literature have generally not incorporated the possible mediating, moderating, or direct impact of organizational culture on information security-related behaviors. In ISS, the core behavioral information security theories are generally individual-level theoretical perspectives that assume (either implicitly or explicitly) the effects of those theories will be more or less the same regardless of the organizational environment. Our results suggest that this might not be the case. A fruitful area of future research could investigate the role of different

organizational cultures in (for instance) deterrence theory or 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. We discussed and established empirically that the different cultural archetypes create conflicting values within organizations [9], which either inhibit or facilitate the formation of security-related subjective norms and the pressure to comply with their organization's security policies. Given these differences, it is difficult to say definitively that one specific cultural archetype will always create a heightened sense of security awareness across all industries or all groups of employees. Thus, another interesting area of future research could build off our results by investigating the conditions under which each of the four cultural archetypes create or do not create strong security-aware environments. Our post-hoc analysis investigated a potential industry effect but other contextual conditions might mediate or moderate our proposed relationships.

Practical Implications

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

The culture of an organization is not developed specifically for information security. Instead, the organizational culture forms as a result of the mission, strategy, and values of the organization [1] [89]. Our paper suggests that it is important for senior level managers and executives to understand that the overall culture of the organization does have the ability to positively or negatively shape the security environment. Thus, although we are not suggesting that senior level managers create an organizational culture specifically for security purposes, we are suggesting that senior level managers and executives be mindful of the indirect

effect that high-level strategic decisions might have on the security environment. By doing so, they can then manage the information security of the organization 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 but not in others. For instance, a top down managerial approach to creating security-related subjective norms (or increasing compliance pressures) may not be a viable solution in some organizational settings because of their cultural values. For instance, in team-based organizational cultures, security managers may want to cultivate strong security-related subjective norms through shared governance or shared accountability instead of through a top-down approach. Conversely, a top-down approach might work better in rational and hierarchical organizational cultures. Therefore, our primary message to practitioners is to make security-related decisions in the context of their organizational culture. What works in one organizational culture and in one industry may not work effectively in a different setting.

Limitations and Future Directions

Like all research, our paper has several limitations. First, the culture of an organization evolves over time, but our study took a snapshot of each of our subject's current organizational environment. We can't offer any insights into what might happen when an organizational culture changes from one cultural archetype to a different cultural archetype over time. Therefore, scholars should be cautious about referencing our findings in organizations that have undergone one or more organizational culture changes. An interesting future study might investigate organizational culture change and how that amplifies or nullifies our theorized relationships.

Second, our measurement items did not include any context specificity and a clear domain specification [91], which was suggested by [92]. Said differently, the measurement of our constructs did not offer any type of scenario to contextualize our subject's responses. Future research could extend or validate our findings by using scenario vignettes to contextualize specific security-related actions instead of using static (point in time) behavioral items (like we used in our study). Third, our sample only included two industries.

These two industries provided a sufficient sample size to investigate our proposed theoretical relationships but we make no claims that these two industries represent all industries. Future research could investigate theoretically and empirically how our proposed relationships might vary across different industries (similar to our post-hoc analyses but across a broader spectrum of industries).

Finally, this study measured organizational values by an individual-level viewpoint. We measured each employees' perceptions of their organizational cultures. It is possible that their perceptions may not represent the reality. We argued that the employees' perceptions are better than our subjective interpretation of their 'real' organizational culture because the perceptions of the employees represent their reality (even if different employees have different realities!). Future research might extend our findings by a different way to measure the four cultural archetypes beyond using individual-level perceptions.

Reference

[1] E. K. Briody, E. J. Berger, E. Wirtz, A. Ramos, G. Guruprasad, and E. F. Morrison, "Ritual as Work Strategy: A Window into Organizational Culture," *Human Organization*, vol. 77, no. 3, pp. 189–201, Sep. 2018.

[2] C. Posey, T. L. Roberts, and P. B. Lowry, "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, Oct. 2015.

[3] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences*, vol. 43, no. 4, pp. 615–660, Aug. 2012.

[4] Ponemon Institute, "Managing Insider Risk through Training & Culture," Ponemon Institute Research Report, 2016.

[5] A. AlHogail, "Design and Validation of Information Security Culture Framework," *Computers in Human Behavior*, vol. 49, pp. 567–575, Aug. 2015.

[6] E. S. Chang and C. Lin, "Exploring Organizational Culture for Information Security Management," *Industr Mgmt. & Data Systems*, vol. 107, no. 3, pp. 438–458, Apr. 2007.

[7] A. Da Veiga and J. H. P. Eloff, "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[8] M. T. Siponen, "A Conceptual Foundation for Organizational Information Security Awareness," *Info Mgmt. & Comp Security*, vol. 8, no. 1, pp. 31–41, Mar. 2000.

[9] R. E. Quinn and J. Rohrbaugh, "A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis," *Management Science*, vol. 29, no. 3, pp. 363–377, Mar. 1983.

[10] H. M. Trice and J. M. Beyer, *The Cultures of Work Organizations*. Englewood Cliffs, NJ, US: Prentice-Hall, Inc, 1993.

[11] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly*, vol. 34, no. 3, pp. 487–502, 2010.

[12] D. J. Kim, D. L. Ferrin, and H. R. Rao, "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents," *Decision Support Systems*, vol. 44, no. 2, pp. 544–564, Jan. 2008.

[13] B.-Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, Mar. 2009.
[14] J. D'Arcy, A. Hovav, and D. Galletta, "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, 2009.
[15] T. Herath and H. R. Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, Apr. 2009.
[16] S. Boss, D. Galletta, P. Lowry, G. Moody, and P. Polak, "What do Users have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly*, vol. 39, no. 4, pp. 837–864, 2015.
[17] M. Warkentin, A. C. Johnston, J. Shropshire, and W. D. Barnett, "Continuance of Protective Security Behavior: A Longitudinal Study," *Decision Support Systems*, vol. 92, pp. 25–35, Dec. 2016.
[18] G. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly*, vol. 42, no. 1, pp. 285–311, Mar. 2018.
[19] R. Goffee and R. Scase, *Corporate Realities (Routledge Revivals): The Dynamics of Large and Small Organisations*, 1st ed. New York, NY: Routledge, 2015.
[20] E. H. Schein, *Organizational Culture and Leadership*, 4th ed. San Francisco, CA: John Wiley & Sons, 2010.
[21] E. H. Schein, "Coming to A New Awareness of Organizational Culture," *Sloan Management Review*, vol. 25, no. 2, pp. 3–16, 1984.
[22] J. A. Chatman and K. A. Jehn, "Assessing the Relationship between Industry Characteristics and Organizational Culture: How Different Can You Be," *Academy of Management Journal*, vol. 37, no. 3, pp. 522–553, 1994.
[23] W. Ke and K. K. Wei, "Organizational Culture and Leadership in ERP Implementation," *Decision Support Systems*, vol. 45, no. 2, pp. 208–218, May 2008.
[24] D. Ravasi and M. Schultz, "Responding to Organizational Identity Threats: Exploring the Role of Organizational Culture," *AMJ*, vol. 49, no. 3, pp. 433–458, Jun. 2006.
[25] E. H. Schein, "How Can Organizations Learn faster? The Problem of Entering the Green Room," Massachusetts Institute of Technology (MIT), Sloan School of Management, WP 3409-92., 1992.
[26] C. Vroom and R. von Solms, "Towards Information Security Behavioural Compliance," *Computers & Security*, vol. 23, no. 3, pp. 191–198, May 2004.
[27] N. S. Safa, R. Von Solms, and S. Furnell, "Information Security Policy Compliance Model in Organizations," *Computers & Security*, vol. 56, pp. 70–82, Feb. 2016.
[28] J. F. Van Niekerk and R. Von Solms, "Information security culture: A Management Perspective," *Computers & Security*, vol. 29, no. 4, pp. 476–486, Jun. 2010.
[29] G. Dhillon, R. Syed, and C. Pedron, "Interpreting Information Security Culture: An Organizational Transformation Case Study," *Computers & Security*, vol. 56, pp. 63–69, Feb. 2016.
[30] K. J. Knapp, T. E. Marshall, K. R. Rainer, and N. F. Ford, "Information Security: Management's Effect on Culture and Policy," *Info Mgmt. & Comp Security*, vol. 14, no. 1, pp. 24–36, Jan. 2006.
[31] T. Schlienger and S. Teufel, "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture," in *14th International Workshop on Database and Expert Systems Applications, 2003 Proceedings*, 2003, pp. 405–409.
[32] K.-L. Thomson, R. von Solms, and L. Louw, "Cultivating an Organizational Information Security Culture," *Computer Fraud & Security*, vol. 2006, no. 10, pp. 7–11, Oct. 2006.
[33] I. Nonaka, "A Dynamic Theory of Organizational Knowledge Creation," *Organization Science*, vol. 5, no. 1, pp. 14–37, Feb. 1994.
[34] D. R. Denison, S. Haaland, and P. Goelzer, "Corporate Culture and Organizational Effectiveness: is there a Similar Pattern around the World?," in *Advances in Global Leadership*, vol. 3, 0 vols., Emerald Group Publishing Limited, 2003, pp. 205–227.

[35] R. E. Quinn, “The Psychometrics of the Competing Values Culture Instrument and an Analysis of the Impact of Organizational Culture on Quality of Life,” *Research in Organizational Change and Development*, vol. 1, no. 5, pp. 115–142, 1991.
[36] E. H. Schein, *The Corporate Culture Survival Guide: Sense and Nonsense About Culture Change*. San Francisco, CA: Wiley, 1999.
[37] I. Ajzen, “The Theory of Planned Behavior,” *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, Dec. 1991.
[38] T. Hirschi, *Causes of Delinquency*. Berkeley, CA: University of California Press, 1969.
[39] S. M. Lee, S.-G. Lee, and S. Yoo, “An Integrative Model of Computer Abuse based on Social Control and General Deterrence Theories,” *Information & Management*, vol. 41, no. 6, pp. 707–718, Jul. 2004.
[40] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, “Future Directions for Behavioral Information Security Research,” *Computers & Security*, vol. 32, pp. 90–101, Feb. 2013.
[41] M. E. B. Herrera, “Creating competitive advantage by Institutionalizing Corporate Social Innovation,” *Journal of Business Research*, vol. 68, no. 7, pp. 1468–1474, Jul. 2015.
[42] K. S. Cameron, “Effectiveness as Paradox: Consensus and Conflict in Conceptions of Organizational Effectiveness,” *Management science*, vol. 32, no. 5, pp. 539–553, 1986.
[43] M. Tian, P. Deng, Y. Zhang, and M. P. Salmador, “How does Culture Influence Innovation? A systematic Literature Review. Management Decision,” *Management Decision*, vol. 56, no. 5, pp. 1088–1107, Feb. 2018.
[44] B. Adkins and D. Caldwell, “Firm or Subgroup Culture: Where does Fitting in Matter Most?,” *Journal of Organizational Behavior*, vol. 25, no. 8, pp. 969–978, 2004.
[45] D. R. Denison and G. M. Spreitzer, “Organizational Culture and Organizational Development: A Competing Values Approach,” *Research in Organizational Change and Development*, vol. 5, no. 1, pp. 1–21, 1991.
[46] R. Claessens, *Corporate Culture in Banking*. UK: AuthorHouse, 2012.
[47] M. Paulin, R. J. Ferguson, and A. M. Alvarez Salazar, “External Effectiveness of Service Management A Study of Business-to-Business Relationships in Mexico, Canada and the USA,” *Int J of Service Industry Mgmt*, vol. 10, no. 5, pp. 409–429, Dec. 1999.
[48] R. B. Cooper and R. E. Quinn, “Implications of the Competing Values Framework for Management Information Systems,” *Human Resource Management*, vol. 32, no. 1, pp. 175–201, Spring 1993.
[49] J. Iivari and M. Huisman, “The Relationship between Organizational Culture and the Deployment of Systems Development Methodologies,” *MIS Quarterly*, vol. 31, no. 1, pp. 35–58, 2007.
[50] S. J. Harrington and T. Guimaraes, “Corporate Culture, Absorptive Capacity and IT Success,” *Information and Organization*, vol. 15, no. 1, pp. 39–63, Jan. 2005.
[51] C.-C. Shih and S.-J. Huang, “Exploring the Relationship between Organizational Culture and Software Process Improvement Deployment,” *Information & Management*, vol. 47, no. 5, pp. 271–281, Aug. 2010.
[52] T. Scott, R. Mannion, H. Davies, and M. Marshall, “The Quantitative Measurement of Organizational Culture in Health Care: A Review of the Available Instruments,” *Health Service Res*, vol. 38, no. 3, pp. 923–945, Jun. 2003.
[53] T. Kostova, “Transnational Transfer of Strategic Organizational Practices: A Contextual Perspective,” *Academy of Management Review*, vol. 24, no. 2, pp. 308–324, 1999.
[54] E. F. Cabrera and J. Bonache, “An Expert HR System for Aligning Organizational Culture and Strategy,” *Human Resource Planning*, vol. 22, no. 1, p. 51, Mar. 1999.
[55] W. R. Scott, *Institutions and Organizations: Ideas, Interests, and Identities*. Thousand Oaks, CA: Sage Publications, 2008.
[56] K. Tasa, S. Taggar, and G. H. Seijts, “The Development of Collective Efficacy in Teams: A Multilevel and Longitudinal Perspective,” *Journal of Applied Psychology*, vol. 92, no. 1, pp. 17–27, Jan. 2007.

[57] P. Wang, "Chasing the Hottest IT: Effects of Information Technology Fashion on Organizations," *MIS Quarterly*, vol. 34, no. 1, pp. 63–85, Mar. 2010.
[58] C. Navis and M. A. Glynn, "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, Sep. 2010.
[59] E. Vaast, E. J. Davidson, and T. Mattson, "Talking about Technology: The Emergence of a New Actor Category through New Media," *MIS Quarterly*, vol. 37, no. 4, pp. 1069–1092, 2013.
[60] A. B. Hargadon and Y. Douglas, "When Innovations Meet Institutions: Edison and the Design of the Electric Light," *Administrative Science Quarterly*, vol. 46, no. 3, pp. 476–501, Sep. 2001.
[61] S. S. Rao, "Role of ICTs in India's Rural Community Information Systems," *INFO*, vol. 6, no. 4, pp. 261–269, Aug. 2004.
[62] C. A. Hartnell, A. Y. Ou, and A. Kinicki, "Organizational Culture and Organizational Effectiveness: A Meta-Analytic Investigation of the Competing Values Framework's Theoretical Suppositions," *Journal of Applied Psychology*, vol. 96, no. 4, pp. 694–694, 2011.
[63] H. Liu, W. Ke, K. K. Wei, J. Gu, and H. Chen, "The Role of Institutional Pressures and Organizational Culture in the Firm's Intention to Adopt Internet-Enabled Supply Chain Management Systems," *Journal of Operations Mgmt.*, vol. 28, no. 5, pp. 372–384, Sep. 2010.
[64] M. Grimes and J. Marquardson, "Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions," *Decision Support Systems*, vol. 119, pp. 23–34, Apr. 2019.
[65] T. Herath and H. R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, May 2009.
[66] P. Ifinedo, "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, Jan. 2014.
[67] H. Li, J. Zhang, and R. Sarathy, "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems*, vol. 48, no. 4, pp. 635–645, Mar. 2010.
[68] A. Yazdanmehr and J. Wang, "Employees' Information Security Policy Compliance: A Norm Activation Perspective," *Decision Support Systems*, vol. 92, pp. 36–46, Dec. 2016.
[69] Y. Rezgui and A. Marks, "Information Security Awareness in Higher Education: An Exploratory Study," *Computers & Security*, vol. 27, no. 7, pp. 241–253, 2008.
[70] J. C. Smart and E. P. St. John, "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, Sep. 1996.
[71] Q. Hu, P. Hart, and D. Cooke, "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, 2007.
[72] C. D. Helfrich, Y.-F. Li, D. C. Mohr, M. Meterko, and A. E. Sales, "Assessing an Organizational Culture Instrument based on the Competing Values Framework: Exploratory and Confirmatory Factor Analyses," *Implementation Science*, vol. 2, no. 1, p. 13, Apr. 2007.
[73] D. A. Dillman, J. D. Smyth, L. M. Christian, and D. A. Dillman, *Internet, mail, and mixed-mode surveys: the tailored design method*, 3rd ed. Hoboken, N.J: Wiley & Sons, 2014.
[74] P. M. Podsakoff, S. B. MacKenzie, and N. P. Podsakoff, "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, 2012.
[75] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common Method Biases in Behavioural Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology*, vol. 88, no. 5, pp. 879–903, 2003.

[76] S. B. MacKenzie, P. M. Podsakoff, and N. P. Podsakoff, "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly*, vol. 35, no. 2, pp. 293–334, 2011.
[77] C. Fornell and F. L. Bookstein, "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory," *Journal of Marketing R.*, vol. 19, no. 4, pp. 440–452, 1982.
[78] W. W. Chin, "The Partial Least Squares Approach to Structural Equation Modeling," *Modern Methods for Business Research*, vol. 295, no. 2, pp. 295–336, 1998.
[79] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *J. of Marketing Research*, vol. 18, no. 1, pp. 39–50, 1981.
[80] D. Gefen and D. Straub, "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of the Association for Information Systems*, vol. 16, no. 1, Jul. 2005.
[81] A. Diamantopoulos and J. A. Siguaw, "Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration," *British Journal of Management*, vol. 17, no. 4, pp. 263–282, 2006.
[82] S. Petter, D. Straub, and A. Rai, "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly*, vol. 31, no. 4, pp. 623–656, 2007.
[83] C. J. Ferguson, "An Effect Size Primer: A Guide for Clinicians and Researchers," *Professional Psychology: Research and Practice*, vol. 40, no. 5, p. 532, 2009.
[84] L. Wilkinson, "Statistical Methods in Psychology Journals: Guidelines and Explanations," *American Psychologist*, vol. 54, no. 8, pp. 594–604, 1999.
[85] J. Cohen, "A Power Primer," *Psychological Bulletin*, vol. 112, no. 1, p. 155, 1992.
[86] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. New York, NY: Academic Press, 1977.
[87] J. Henseler, C. M. Ringle, and M. Sarstedt, "Testing Measurement Invariance of Composites Using Partial Least Squares," *International Marketing Review*, vol. 33, no. 3, pp. 405–431, May 2016.
[88] M. Sabatino, "Economic Crisis and Resilience: Resilient Capacity and Competitiveness of the Enterprises," *Journal of Business Research*, vol. 69, no. 5, pp. 1924–1927, May 2016.
[89] S. Kashmiri, C. D. Nicol, and L. Hsu, "Birds of a Feather: Intra-Industry Spillover of the Target Customer Data Breach and the Shielding Role of IT, Marketing, and CSR," *J. of the Acad. Mark. Sci.*, vol. 45, no. 2, pp. 208–228, Mar. 2017.
[90] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, Sep. 2010.
[91] A. M. Y. Chu and P. Y. K. Chau, "Development and Validation of Instruments of Information Security Deviant Behavior," *Decision Support Systems*, vol. 66, pp. 93–101, Oct. 2014.
[92] M. Siponen and A. Vance, "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, 2014.

Appendix A – Measurement Items

Construct	Measurement Items	Reference
COMP*	COMP1: If my organization experienced a data security breach, the authority will take legal action against us. *(Conformance to regulatory requirements)*	Self-developed by referencing [71]
	COMP2: The authorized parties (e.g., external auditors, government agents etc.) expect us to protect sensitive data using standardized procedures and controls. *(Conformance to stakeholders' expectations of security controls)*	

	COMP3: If my organization experienced a data security breach and news of the breach became public, it would have a very negative impact on my organization's image. *(Conformance to stakeholders' tolerance of security breaches)*	
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 [72]
	TEAM2: My organization emphasizes human resources. High cohesion and morale in the organization 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 rules, 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 [65]
	NORM2: In my organization, our bosses think that we should follow ISP.	
	NORM3: In my organization, our colleagues think that we should follow ISP.	

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**

Appendix C - 3-step Measurement Invariance Testing using Permutation

We used the MICOM three-step procedure for measurement invariance testing [87]. 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 [87]. 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.

The following table (Table D-1) displays the results for our invariance tests for our sample of banking versus higher education employees. 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 [87]. Therefore, we conclude that our Multi-Group Analysis (MGA) produced meaningful statistical results to appropriately interpret the results of our multi-group comparisons.

Table C-1: Invariance Test

Construct	Step 1	Step 2			Step 3a			Step 3b			Invariance
	Configural Invariance	Corr.	Confident Intervals	Comp. Invari.	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

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