Information Systems Frontiers (2020) 22:1241–1264
https://doi.org/10.1007/s10796-019-09927-9

A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness

Hwee-Joo Kam[1] · Thomas Mattson[2] · Sanjay Goel[3]

Published online: 27 May 2019

Abstract
In this paper, we conceptually and empirically investigate the relationship between industry and information security awareness (ISA). Different industries have unique security related norms, rules, and values, which we propose promotes different levels of organizational effort to raise their employees' general ISA. To examine these potential industry effects, we draw on Neo-Institutional Theory (NIT) because different industries operate in unique institutional environments. We specifically theorize that the pressures from the three institutional pillars (regulative, normative, and cultural-cognitive) will affect employees across all industries but the magnitude of those effects will vary across industries, because different industries have institutionalized security practices in unique ways. To evaluate our theorized relationships empirically, we surveyed employees in the banking, healthcare, retail, and higher education industries. We found that our subjects' perceptions of the pressures from the three institutional pillars positively affected their perceptions of how much effort their organizations exerted to raise their general ISA. However, we also found that these effects were not consistent across our surveyed employees in the different industries, especially related to the direct and moderating effect of perceived normative institutional pressures. The implication of our paper is that future behavioral information security research should consider how industry and their corresponding institutional structures might affect (positively or negatively) the relationships in our core theoretical models.

Keywords Neo-institutional theory (NIT) · Cross industry · Industry effects · Information security awareness · Organizational effort

1 Introduction

The weakest link in an organization's information security defense systems is its employees (Crossler et al. 2017; Warkentin and Willison 2009). A small fraction of employees may maliciously intend to harm their organizations but most employees are non-malicious in their information security related actions (Guo et al. 2011; Workman et al. 2008). Informing these non-malicious employees about the current threats and mitigating controls is an ongoing challenge facing modern organizations (Chang and Wang 2011). As such, the information security literature has devoted significant time explicating how these non-malicious employees become aware of the existing threat landscape and why they perform a variety of different security related actions. To do this, the prior literature has utilized a variety of theoretical perspectives such as general deterrence theory (D'Arcy and Herath 2011; Herath and Rao 2009), the theory of planned behavior (D'Arcy et al. 2009), protection motivation theory (Boss et al. 2015; Posey et al. 2015; Warkentin et al. 2016), neutralization theory (Siponen and Vance 2010), and control balance theory (Moody et al. 2018). Whether these theorized relationships are consistent for individuals who work in different industries remains an open theoretical and empirical question because very few studies have investigated how these theoretical relationships vary across employees who work in different industry segments.

✉ Hwee-Joo Kam
hkam@ut.edu

Thomas Mattson
tmattson@richmond.edu

Sanjay Goel
goel@albany.edu

[1] University of Tampa, 401 W. Kennedy Blvd., Tampa, FL 33606, USA

[2] University of Richmond, 410 Westhampton Way, Richmond, VA 23173, USA

[3] University at Albany, SUNY, Business Building 311. 1400 Washington Ave., Albany, NY 12222, USA

However, we argue that industry may have a significant impact on how much effort an organization exerts to raise their employees' general information security awareness (ISA), because different industries have different security related norms, regulations, standards, and values related to digital data, security, and privacy (Stahl et al. 2012; Yeh and Chang 2007).[1] For instance, an organization in the oil and gas industry might exert a different level of effort to raise their employees' general ISA relative to an organization in the banking industry because the former industry is much less digital intensive than the latter. Therefore, contextualizing information security issues in relation to an employee's or an organization's industry environment might reveal that a one-size fits all approach to information security awareness, education, and training is not be the best approach. For instance, the tactics that work for employees and organizations in the social media industry may not work as well in the higher education industry because the different industries have different security-related values, norms, and histories.

The purpose of our paper is to investigate the following research question*: how does industry affect the amount of effort organizations exert (or perceptions thereof) to inform their employees about general information security issues?* To answer this question, we draw on Neo-Institutional Theory (NIT) because organizations across industries operate in different institutional and technical environments with unique institutional pressures (Chiasson and Davidson 2005; DiMaggio and Powell 1983; Meyer and Rowan 1977; Scott 2008). NIT posits that the normative (informal rules), cultural-cognitive (shared beliefs), and regulative (formal rules) institutional pillars affect organizational structures as well as how employees in those organizations learn, organize, and behave (Tolbert and Zucker 1983; Zucker 1987). We argue that the normative, cultural-cognitive, and regulative institutional pillars will also affect how much effort an organization exerts to raise their employees' general ISA because institutional pressures legitimate certain types of security behaviors more in certain industries relative to other industries. That is, the institutional pillars determine the taken-for-granted beliefs surrounding how employees in a specific industry understand and deal with risk, uncertainty, or ambiguity (Alexander 2012), which we assert guides how organizations and employees treat matters of information security.

To investigate empirically how NIT affects organizational effort (or perceptions thereof) to raise their employees' ISA, we surveyed employees in four different industries – banking, health care, higher education, and retail. In our survey, we assessed employees' perceptions of the three pillars of institutions in their respective industries and their perceptions of how well or poorly their organizations made them aware of general information security related issues. In our sample, we found that employees' perceptions of the institutional pressures from the three institutional pillars positively affected their perceptions of how much effort their organizations exerted to raise their general ISA. However, we also found that these effects were not consistent across our surveyed employees in the different industries. Based on our findings, we suggest that future behavioral information security research consider how industry and their associated institutional structures might affect the relationships in the core theories used by behavioral information security researchers.

We chose to investigate general ISA and organizational effort for two primary reasons. First, informing non-malicious employees about the current threat landscape is an important first step in protecting an organization's digital assets (Bulgurcu et al. 2010). Without sound general ISA, non-malicious employees may unknowingly engage in insecure behaviors (Siponen and Vance 2014). Second, keeping an organization's employees aware of the current threat landscape is an ongoing challenge that requires significant organizational effort (Burns et al. 2017; Dhillon et al. 2016). That is, an organization's employees do not arbitrarily (effortlessly) become informed about the relevant threats and their mitigating controls. It takes significant thought, on-going effort, and diligence on the part of an organization's management team to make this happen.

2 Literature Review

2.1 Industry & Behavioural Information Security

Many of the influential behavioural information security papers that have been published in our top journals (e.g., Chen and Zahedi (2016), D'Arcy et al. (2009), and Boss et al. (2015)), have not reported their empirical results comparing their proposed effects across employees in different industry segments (or they used students who are currently not in the work force). Table 1 displays a list of relevant and selected literature related to industry and behavioural information security. Based on our literature review, we see that the behavioural information security literature has largely not integrated cross-industry effects into our theoretical or empirical models. Occasionally, researchers will perform a post-hoc analysis of potential industry effects but these studies often do not explain how or why industry might impact an individual's or an organization's security-related actions. This omission is significant because prior literature in other domains have found that behaviours do vary across industries (Desai et al. 1998; Xu et al. 2003) and the prior information systems (IS) literature has theorized that individuals working in different industries will

[1] For the purposes of our paper, we define industry as a collection of organizations that sell a similar product, provide similar services, operate in similar institutional and/or technical environments, and take actions that are influenced by shared regulative, normative, and cultural-cognitive institutional structures (Chiasson and Davidson 2005; Scott 2008).

Table 1 Literature comparing industry effects

IS research	Sample	Findings	Cross-industry comparison
Yeh and Chang (2007)	Participants (N = 109) were from the major enterprises in Taiwan. They were mainly working in the financial/banking, retail/service, manufacturing, high-tech industries, and others.	Industry type and IT application influenced organizational adoption of security countermeasure. Interestingly, the implementation of security countermeasure had no effect on the perceived threat among the managers.	This study conducted a comparison across four industries, namely, financial/banking, retail/service, manufacturing, and high-tech.
D'Arcy et al. (2009)	Participants (N = 269) were from eight companies located in the United States. They worked in the advertising/marketing, aerospace, financial services, information technology, manufacturing, and others.	User awareness of ISP, security education, training, and awareness (SETA) programs, and computer monitoring deter computer misuse.	This study had a cross-industry sample but did not compare each of their model's based on the specific industry in their sample.
Bulgurcu et al. (2010)	Participants (N = 464) were from different industries, including education, financial services, government, food & beverage, healthcare, manufacturing, nonprofit, medical, bio-technology, pharmacology, real estate, services, information technology, telecommunications, travel, wholesale/retail, and others.	Attitude, normative beliefs, and self-efficacy to comply positively affect employees' intention to comply with the ISP. Additionally, ISA influences employees' attitudes toward compliance.	This study used industry as a control variable. The results revealed that industry has no effect on employees' intention to comply with ISP.
Siponen and Vance (2010)	Participants (N = 1449) were office staff from universities (N = 220), electrical companies (N = 99), and supermarket chain (N = 1130).	Because neutralization techniques (i.e., denial) increase employees' intentions to violate ISP, organizations need to consider neutralization when designing and implementing ISP.	This study did not run a cross-industry comparison. The industry sector, used as a control variable, demonstrated no significant effect on the intention of violating ISP.
Posey et al. (2015)	Participants (N = 380) were professionals from financial, insurance, legal, military, telecommunications, aviation, and medical industries.	Organizational commitment is important to connect security threats to the insiders at a personal level. Moreover, organization's efforts of SETA augment the threat and coping appraisals.	While this study collected data from a broad range of industries, it did not run a cross-industry comparison.

have different patterns of IS-related behaviors (Chiasson and Davidson 2005; King et al. 1994).

2.2 Theoretical Framework

Neo-institutional theory (NIT) is a sociological view of institutions that moves beyond traditional economic explanations of how organizations structure and act (DiMaggio and Powell 1983). NIT conceptualizes institutions as abstract, yet durable, social structures consisting of regulative (formal rules), normative (informal rules), and cultural-cognitive (shared beliefs) dimensions (pillars) that provide meaning as well as structure to a collection of actors who interact in a common market space (Durand and Thornton 2018; Scott 2008). In this sense, actors may be individuals, organizations, associations, or a combination of all of these. From an NIT perspective, a market space consists of organizations in a common industry whereby the regulative, normative, and cultural-cognitive pillars play an important role in determining what constitutes legitimate actions in a given industry environment (Wang 2010; Zucker 1987). Similar institutional structures govern the collection of organizations operating in a specific industry, but the institutional structures may vary (sometimes quite significantly) across industries (Chiasson and Davidson 2005; Kohli and Kettinger 2004; Wang 2010).

The underlying institutional logics in an industry define the industry's institutional structures (Durand and Thornton 2018; Scott 2008). Institutional logics are the set of legitimate actions, values, and beliefs comprising an institution (Friedland and Alford 1991; Thornton and Ocasio 1999). A single institution may have one institutional logic or multiple institutional logics that may complement or compete with each other in order to define the appropriate regulative, normative, and cultural-cognitive pillars (Dunn and Jones 2010; Thornton and Ocasio 2008). To exemplify the idea of an institutional logic, let us consider a healthcare example. In the healthcare industry, there are two competing institutional logics governing health insurance companies in the United States. The first is a market-based or a for-profit-based institutional logic. This logic is rooted in capitalistic principles that suggests the market will determine how health insurance organizations should function in the United States. The second is a government-based or a not for-profit based institutional logic. This logic is rooted in more socialistic principles that suggests the government or state agencies should determine how health insurance organizations should function. Both of these logics are competing to determine the regulative, normative, and cultural-cognitive pillars that define legitimate actions in this particular industry.

Institutions and their associated institutional logics form via a process of institutionalization. Zucker (1977, p. 728) posited that institutionalization is both a process and a property. It is a process by which "*social processes, obligations, or actualities come to take on a rule-like status in social thought and action*" (Meyer and Rowan 1977, p. 343). It is a property such that at any point in the institutionalization process "*the meaning of an act can be defined as more or less a taken-for-granted part of social reality*" (Zucker 1977, p. 728). These taken-for-granted actions define externally legitimated actions such as positions, policies, or programs for organizations to adopt (Meyer and Rowan 1977). Once institutionalized, institutions provide stability, meaning, and structure by outlining the moral, normative, legal, and cultural boundaries that define legitimate activities in a given context (Scott 2008; Suchman 1995). These institutionalized institutions define the guidelines for organizational actions by legitimating those actions in a given market space, which are industry environments in the context of our study.

NIT posits that organizations seek to obtain legitimacy from stakeholders by conforming to their institution's regulative, normative, and cultural-cognitive pillars in order to maximize their chances of success (DiMaggio and Powell 1983).[2] To do so, organizations undergo coercive, mimetic, and normative isomorphism to adopt legitimated programs, policies, and actions (DiMaggio and Powell 1983). Coercive isomorphism occurs when a powerful authoritative entity such as a government agency or a powerful dependent organization forces (coerces) an organization and its employees to act in a specific manner. For instance, Apple may coerce a supply chain partner to use a specific type of encryption algorithm to protect digital data, which Apple has defined as legitimate for the industry. If the partners fail to conform, then Apple may delegitimize or exclude that partner from Apple's digital ecosystem. Mimetic isomorphism occurs when organizations copy the patterns of successful organizations in the same industry (DiMaggio and Powell 1983). For instance, a bank may split its information security employees from its software development employees (i.e., split a single technology department into two separate departments) because other successful competitors have legitimized this organizational structure. Normative isomorphism occurs when organizations espouse typical patterns, which the underlying institutions define as appropriate or legitimate for the particular environment (DiMaggio and Powell 1983). For online retailers, for example, the Payment Card Industry Data Security Standard (PCI) is the norm surrounding online payments and data protection that retailers feel obligated to follow in order to legitimate their status as valid online retailers.

3 Research Hypotheses

NIT proposes that organizations react to external pressures in order to legitimate themselves as viable industry participants by complying with regulations, by copying other organizations' successful responses to uncertainties, and by employing appropriate practices based on their institutional environments (Scott 2008; Wang 2010). However, organizations across industries operate in different institutional and technical environments with unique institutional pressures (Chiasson and Davidson 2005; DiMaggio and Powell 1983; Meyer and Rowan 1977; Scott 2008). Therefore, we propose that the pressures (or perceptions thereof) of the three pillars of institutions will vary across industry segments. We argue that the normative, cultural-cognitive, and regulative institutional pillars will affect how much effort an organization exerts to raise their employees' ISA because of the isomorphic effects of institutions in specific industries. Legitimate participation in an institutional environment generally requires an organization and its employees to behave similar to its institutional or industry competitors (DiMaggio and Powell 1983). In the context of information security, we assert that the institutional and technical pressures across industries promote different security practices because work practices differ across industry, institutional, and technical environments (Angst et al. 2017). Thus, we propose that organizations across industries may exert varying levels of effort to raise their employees' general ISA.

3.1 Regulative Pillar

The regulative pillar of institutions pertains to the official rule setting, sanctioning, and monitoring processes used to constrain (regulate) behaviors in an institutional environment (Scott 2008). The regulative pillar of institutions are the formal rules of the game that feature both rule systems and

[2] The idea that organizations structure and act in pursuit of legitimacy instead of in pursuit of economic rationality (or bounded rationality) is a fundamental aspect of neo (new)-institutional that is different from traditional institutional theory. Traditional institutional theories suggest that organizations form based on transaction cost economics or a series of economically rational or bounded rational choices (North 1990; Scott 2008).

enforcement mechanisms (North 1990). For example, the Federal Deposit Insurance Corporation (FDIC) has enacted a series of guidelines pertaining to the administrative, technical, and physical safeguards that banks in the United States must follow to protect customer data. The FDIC monitors and fines banks in the United States when they fail to follow their rules. Similarly, in the Federal Government contracting market space in the United States, the Federal Information Security Management Act (FISMA) outlines the specific information security procedures that federal contractors must follow in order to be eligible for federal contracts. Contractors who fail to follow these formal rules are subject to having their contracts terminated or their proposals denied. Following these formal rules legitimizes an organization in the institutional environment of that industry.

Not all industries, however, are subject to the same regulatory pressures. For instance, the recruiting (head hunting) and the home hospice care industries have minimal formal oversight whereas the banking and healthcare industries are heavily regulated (in the United States). Banks must comply with a series of regulations such as Sarbanes-Oxley Act (SOX), the Gramm Leach Bliley Act (GLBA), and Dodd-Frank restrictions. From an information security perspective, these regulations require financial institutions to maintain administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of customer information (Bauer and Bernroider 2017; Hu et al. 2007). As a result, banks in the banking industry have exerted significant effort developing their general ISA and training programs (Baskerville et al. 2014; Rockness and Rockness 2005). The healthcare industry has similar regulative pressures in place, which has affected how much effort healthcare organizations devote toward general ISA in that industry. For instance, the Health Insurance Portability and Accountability Act (HIPAA) regulates how healthcare facilities must protect patient's privacy. This legislation has significantly increased general ISA in the healthcare industry (Angst et al. 2017; Davidson and Heslinga 2006). Therefore, we hypothesize the following main effect of perceived regulatory pressures on organizational effort to inform their employees about general ISA:

> *H1a: Organizations in industries with greater perceived regulative pressures will exert greater effort (or perceptions thereof) to raise their employees' general ISA.*

This effect, however, may vary significantly from industry-to-industry because regulations affect certain industries more than other's (even though most industries have at least some degree of regulatory pressure). Different industries have different enforcement mechanisms and sanctions when an organization violates an element of the regulative pillar. In the higher education industry (in the United States), for instance, the Family Education and Privacy Act (FERPA) provides a set of regulatory guidelines that all institutions in higher education must follow to protect students' digital data. In theory, colleges and universities in the United States risk losing federal funding for FERPA violations. However, we are not aware of any college or university that has lost federal funding due to a FERPA violation. We speculate that it would probably take multiple FERPA violations without ever implementing any corrective actions before a college or university would realistically lose any federal funding. Contrarily, failure to adhere to the institutionalized regulations in the health care industry results in actual monetary fines (i.e., Anthem paid $16 million in fines for their data breach in 2015). Therefore, although both industries (higher education and healthcare) have strong regulative pressures, organizations in both of these industries may have much different security awareness and education programs because the actual enforcement of the specific regulatory requirements differs substantially across the industry segments.

In the context of information security, this argument suggests that organizations operating in industries with different real or perceived sanctions related to violating the formal information security rules and regulations will treat information security matters differently due to the varying enforcement mechanisms and sanctions across industry environments (Hrebiniak and Snow 1980; Chatman and Jehn 1994). That is, to secure regulative-based legitimacy, an organization operating in an institutional environment with higher perceived (or real) sanctions for failing to follow the formal information security rules of the game will be more vigilant to implement and administer stronger information security awareness and education programs. For example, to avoid security breaches that may lead to sanctions and reduced regulative-based legitimacy in its institutional environment, we assert that organizations in industries with high degrees of perceived (or real) sanctions such as those in the banking, health care, or social media industries will exert more effort to raise their employees' general ISA. Hence, we propose the following qualifying hypothesis of the regulatory pillar:

> *H1b: An industry with greater perceived sanctions will amplify the effect of perceived regulative pressure on perceived organizational effort to raise their employees' general ISA.*

3.2 Normative Pillar

The normative pillar of institutions refers to the informal rules of the game, which are the typical (usual) behaviors that determine how market space participants should act (March and Olsen 1989; Scott 2008). We argue that organizations may be coerced (coercive isomorphism) to employ security practices acknowledged by the legitimate third parties (not necessarily regulators) so that organizations could secure normative-based legitimacy in their industries (Deephouse 1996). In the banking industry, for instance, bankers may be coerced to follow a set of informal guidelines pertaining to ransomware attacks. Failure to follow those informal rules of the game may be just as detrimental as not following the formal rules of the game because the organization may lose normative-based legitimacy in a given market space, which may result in losing reputation, pricing power, and customers (Scott 2008; Wang 2010). We propose that the perceived pressures from the normative pillar of institutions will affect organizational effort to raise general ISA because following industry ISA norms is a sign of legitimacy, which can influence the long-term viability of an organization and its employees (Scott 2008; Suchman 1995).

Not all industries, however, have strong institutionalized norms related to information security. In the higher education industry, for instance, there are not a uniform set of institutional norms related to FERPA best practices. We posit that less pressure from the normative pillar of institutions will result in less organizational effort to make their employees aware of general ISA, because fewer institutionalized norms means that legitimate actions are ill-defined in that industry environment. These ill-defined institutionalized norms may make it difficult to construct general ISA training programs. Therefore, we hypothesize the following main effect of perceived normative pressures:

> *H2a: Organizations in industries with greater perceived normative pressures will exert greater effort (or perceptions thereof) to raise their employees' general ISA.*

However, we propose that the strength of this main effect may also vary significantly from industry-to-industry due to the varying indirect costs (resulting from sanctions) associated with not following the institutionalized industry norms. For instance, the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework is an institutionalized norm in the healthcare industry due to its applicability to HIPPA (Appari and Johnson 2010). However, healthcare providers who choose not to follow the OCTAVE norm do not typically risk losing patients or having insurance companies drop them for not following this norm. Contrarily, retailers who do not follow the PCI norms for handling online credit card transactions may lose customers or damage their reputation because customers have become accustomed to conducting business with legitimate PCI compliant retailers (especially online retailers). Therefore, even though there may be strong perceived normative pressures in both industries, we assert that the effect may vary across different industries because the informal sanctions vary across industries. These informal sanctions resulting from not following the normative pillar institutions may make organizations more cautious and deliberate, which will result in greater organizational effort in developing their training and awareness programs. Hence, we propose the following qualifying hypothesis of the normative pillar:

> *H2b: An industry with greater perceived sanctions will amplify the effect of perceived normative pressure on perceived organizational effort to raise their employees' general ISA.*

3.3 Cultural-Cognitive Pillar

The cultural-cognitive pillar of institutions represents the shared (taken-for-granted) beliefs that constitute the nature of social reality, which may vary considerably from culture-to-culture, industry-to-industry, and society-to-society (Douglas 1986; Scott 2008). For this institutional pillar, culture does not simply refer to national cultures. It may refer to occupational or industry specific cultures (among others) whereby the members of a collective share a common belief system (Scott 2008; Trice 1993). Culture influences human behaviors by shaping the ends (goals) and the means (strategies) of action (Swidler 1986). That is, culture provides the values towards which action is oriented and a tool kit that contains the habits and styles that shape behaviors (Aurigemma and Mattson 2018; Douglas 1986; Menard et al. 2018; Swidler 1986). These values and toolkits vary from industry-to-industry because different industries and their respective institutions have different histories and rituals (Meyer and Rowan 1977), which define the cultural-cognitive institutional pillar.

In an information security context, certain industries have stronger shared (taken-for-granted) cultural-cognitive beliefs concerning information security than other industries due to the nature of the work performed in different industries. For instance, it would be surprising if the oil and gas industry had equally strong-shared beliefs concerning the definition of secure computing as the social media industry. The social media industry is highly digitized and data driven whereas the oil and gas industry is much less digitized. Therefore, we would expect the cultural-cognitive institutional pressures to be weaker in the oil and gas industry relative to the social media industry. Striving for cultural-cognitive legitimacy in terms of information security actions and awareness programs will vary across industries because the shared-belief systems vary within and across industries (Gordon 1991). Therefore, we propose the following main effect of the cultural-cognitive pillar:

> *H3a: Organizations in industries with greater perceived cultural-cognitive pressures will exert greater effort (or perceptions thereof) to raise their employees' general ISA.*

However, we also suggest that this effect will not be consistent across industries. Two industries may both have high institutional cultural-cognitive pressures but experience different effects because these two industries may have different tolerances for risk and ambiguity, which are a component of the cultural-cognitive pillar of institutions (Aldrich and Fiol 1994). All industries encounter varying degrees of uncertainty, but different industries have varying perceptions of risk in the face of that uncertainty (Hrebiniak and Snow 1980; Rousseau et al. 1998; Yeh and Chang 2007), which can mitigate our proposed main effect of cultural-cognitive institutional pressures. Organizations that operate in the same industry often share similar risk management activities because their perceptions of risk are similar (Zwikael and Ahn 2011). Different industries, however, may exhibit different risk management practices due to industry specific risk factors and varying perceptions of risk.

For instance, let us assume that the retail and higher education industries both have weak-shared cultural-cognitive beliefs concerning the definition of secure computing. If the higher education industry is more risk averse than the retail industry, then we are suggesting that this will amplify the effect of the weak cultural-cognitive institutional pressures. We may also see a similar effect with two industries having strong-shared cultural cognitive beliefs concerning information security because the risk profiles in the two industries may vary. These differences should logically influence how much effort an organization exerts to inform their employees about culture-specific threats and controls because risk aversion and information security actions are highly correlated activities.

We assert that the real or perceived threat of sanctions in an institutional environment for not conforming to the cultural-cognitive pillar of institutions should influence the risk management practices of an organization. If, for instance, two industries both have high-perceived cultural-cognitive pressures to conform to a specific set of security practices but one industry has higher real or perceived sanctions for failing to follow those cultural-cognitive pressures, then we propose that this will affect how much effort an organization exerts to inform their employees about general security issues. Higher perceived sanctions are threats to an organization that attempts to establish cultural-cognitive legitimacy, which should (we posit) increase the amount of effort they exert towards information security related initiatives. Lower perceived sanctions, on the other hand, may mitigate the effect of culturally defined security related practices in an institutional environment. As such, we propose the following qualifying hypothesis of the cultural-cognitive pillar:

> *H3b: An industry with greater perceived sanctions will amplify the effect of perceived cultural-cognitive pressure on perceived organizational effort to raise their employees' general ISA.*

3.4 Moderating Effect of Perceived Normative Pressures

Institutions operate in complex environments with interrelationships among the legal (regulative), social (normative), and cultural (cultural-cognitive) pillars (Scott 2008). Depending on the research context, each institutional structure may mediate or moderate the effects of the other institutional structures. In the context of information security, institutional norms (or perceptions thereof) are of paramount importance in determining organizations' information security actions. New information security threats emerge continuously, which makes it challenging for the regulatory pillar of institutions to keep up with the changing threat landscape. Often, by the time regulations pass through the formal legislative process, there are a different set of threats affecting organizations, which may mitigate the impact of regulations in determining how much effort an organization exerts towards specific information security actions. However, institutional norms related to information security threats formed by associations such as the ISACA (Information Systems Audit and Control Association), PCI, and ISO (International Organization for Standardization) may be institutionalized at a much faster rate due to having fewer bureaucratic hurdles. Furthermore, regulations often pass after norms have become institutionalized in certain market spaces. In these instances, the norms might amplify the impact of regulations on how much effort an organization exerts towards its information security practices because the institutionalized regulations are reinforcing existing institutionalized security related norms. Therefore, we propose the following moderating hypothesis:

> *H4: Perceived normative pressures will moderate the effect perceived regulative pressure on organizational effort (or perceptions thereof) to raise their employees' general ISA.*

The combination of institutional norms and cultural-cognitive belief systems may have a powerful impact on a variety of organizational actions (Cooter 2000; Scott 2008). For instance, the European Union has different cultural values pertaining to digital privacy than the United States, which has resulted in different security practices pertaining to the social media and online search industries. However, certain institutional norms may qualify the impact of the cultural-cognitive institutional pressures on a variety of information security actions. For example, institutional norms pertaining to spam filters or filtering out potentially harmful email messages might mitigate the impact of an industry culture's strong belief system related to personal privacy on an organization's security policies related to the confidentiality of digital data. Therefore, institutional norms (or perceptions thereof) might qualify the impact of cultural-cognitive pressures in the context of information security because certain norms articulate global security standards that are expected to be followed irrespective of the cultural-cognitive belief systems in a particular market space. Therefore, we propose the following moderating hypothesis:

> *H5: Perceived normative pressures will moderate the effect perceived cultural-cognitive pressure on organizational effort (or perceptions thereof) to raise their employees' general ISA.*

3.5 Summary of Research Hypotheses

Figure 1 displays our research hypotheses. Our research hypotheses are generally organized into "a" and "b" hypotheses. The "a" hypotheses propose general main effects related to an employee's institutional environment. These hypotheses are built on the idea that industries operate in different institutional and technical environments with unique institutional pressures (Chiasson and Davidson 2005; DiMaggio and Powell 1983; Meyer and Rowan 1977; Scott 2008). Therefore, employees who perceive greater institutional pressures from these pillars in their industry environments will be positively associated with greater perceived organizational effort to raise general ISA. The "b" hypotheses propose that the magnitude of the effects (path coefficients) of the "a" hypotheses will vary by industry because different industries have institutionalized security practices in unique ways. In other words, the effect of the "a" hypotheses will not be consistent across employees working in all industries even when industries share common perceptions of the three institutional pillars. We specifically argue that the threat of sanctions (real or perceived) in different industries may amplify the effects of the institutional pressures from any of the three pillars of institutions because formal and informal sanctions may de-legitimize an organization in its institutional environment. Finally, the non "a" and "b" hypotheses (H4 and H5) in Fig. 1 propose that perceived normative pressures will amplify the effects of both perceived regulatory and perceived cultural-cognitive pressures. We suggest that this is the case because institutional norms are particularly powerful in the context of information security due to the continuously changing threat landscape.

4 Research Design and Methods

To investigate these industry differences empirically, we surveyed employees across four different industries – banking, healthcare, retail, and higher education. These industries operate in different institutional environments with ample real and perceived variability along the three institutional pillars. Our study investigates employees' perceptions of their organization's institutional environment and their perceptions of how much effort their organizations exert to raise their general ISA. We compare the perceptions of employees who work in the banking, healthcare, retail, and higher education industries. This approach is similar to the approach of several other papers that have investigated industry effects using employees' cognitions and perceptions. For instance, Hu et al. (2007) interviewed banking managers to investigate the internal and external pressures that banks undergo in relation to SOX and Yeh and Chang (2007) used employees' perceptions to investigate industry differences related to security countermeasures.

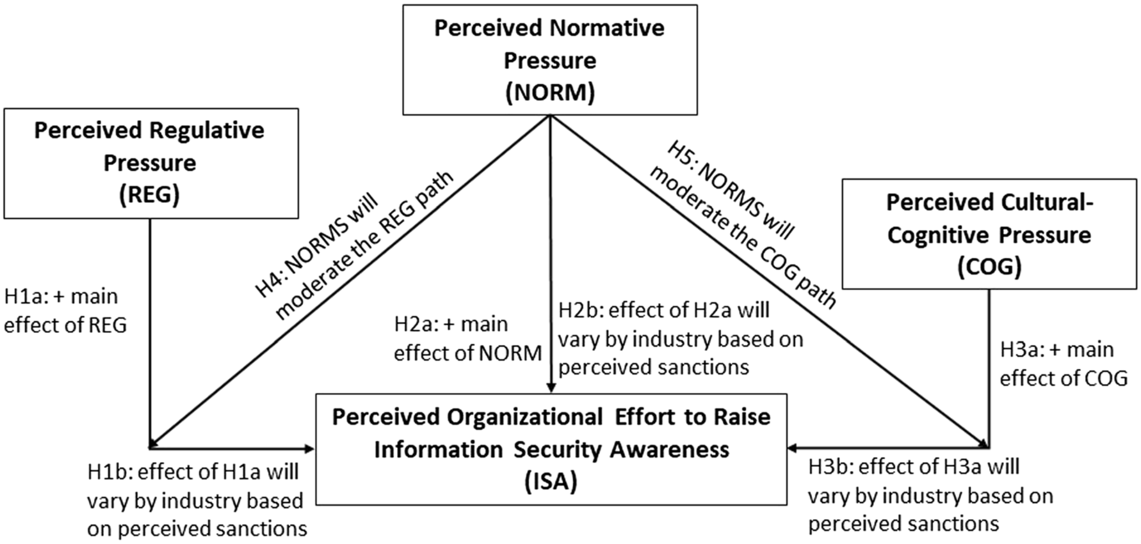

Perceived Normative Pressure (NORM)
Perceived Regulative Pressure (REG)
Perceived Cultural-Cognitive Pressure (COG)
H4: NORMS will moderate the REG path
H5: NORMS will moderate the COG path
H1a: + main effect of REG
H2a: + main effect of NORM
H2b: effect of H2a will vary by industry based on perceived sanctions
H3a: + main effect of COG
Perceived Organizational Effort to Raise Information Security Awareness (ISA)
H1b: effect of H1a will vary by industry based on perceived sanctions
H3b: effect of H3a will vary by industry based on perceived sanctions

Fig. 1 Research model

4.1 Measurement Items & Instrument Validation

We used existing measurement items from pre-validated multi-item scales as our starting point for the measures for some of our latent constructs. For other latent constructs that did not contain previously published pre-validated multi-item scales, we self-developed them by referencing Hu et al. (2007) and Yeh and Chang (2007) as our starting points. To do this scale development, we used a panel of expert information security researchers and scale developers to provide an initial content (face) validity of our adapted measurement items and our new measurement items (prior to any of our pilot studies). After our measurement items were developed and/or adapted to fit our research context, we designed our survey instrument using best practices related to instruction wording and question order as advocated by Dillman et al. (2014, pp. 65-105 & 157-165). Finally, in order to remedy potential common method bias procedurally via our instrument, we used best practices by Podsakoff et al. (2012) particularly related to the proximal separation between the measures of the independent and dependent variables.

After we developed our initial survey instrument, we ran two pilot studies. The first pilot study consisted of 50 college administrators in a university in the Midwest region of the United States. The second pilot study consisted of a panel of three information security professionals. After these pilot studies, we refined our survey instrument to remove identified ambiguities in the measurement items and in the instruction wording. Appendix 1 (Table 11) displays the final measurement items. We measured all items reflectively using 7-point Likert scales with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree.

4.2 Participants and Procedures

We sent out online surveys to participants holding managerial and professional-level positions in organizations across these four industry segments (banking, healthcare, retail, and higher education). We did not include entry-level employees in our study because entry-level employees may not be knowledgeable about their institutional environments or the security awareness programs at their organizations. This lack of knowledge would make comparing responses across participants problematic so we did not include these entry-level employees in our study. We identified organizations in these industries based on personal contacts, alumni networks, and part-time MBA students from two public Midwestern universities. In each of the four industry groups, the participants came from between 8 and 10 different organizations, which were all mostly large (i.e., more than 600 employees). All of our survey participants held full-time managerial or professional level positions in their organizations and had more than 5-years of work experience in their organizations and/or in their respective industries. The average age of our survey participants was 33 for our banking employees, 45 for our retail employees, 47 for our healthcare employees, and 36 for our higher education employees. Table 2 shows the demographic data of our survey participants.

5 Data Analysis & Results

To analyze our survey data, we used Partial Least Squares (PLS) with SmartPLS 3.2 software. PLS is a rigorous and acceptable technique for evaluating path coefficients in structural models (MacKenzie et al. 2011). Before running our PLS models, however, we first successfully screened our data for potential issues that may jeopardized our results such as outliers, multi-collinearity, and non-normality (Fornell and Bookstein 1982). We then evaluated our PLS models in two steps. We first evaluated the validity and the reliability of our measures with a measurement model. We then tested our research model (Fig. 1) using a series of structural models to evaluate our hypothesized relationships.

5.1 Measurement Model

We evaluated our measurement models in terms of convergent and discriminant validity of our constructs. In our paper, we assessed 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 and composite reliability values greater than 0.7 are considered acceptable thresholds for convergent validity (Chin 1998; Fornell and Larcker 1981). In our data, all of our values met the recommended thresholds for validity and construct reliability (see Table 3). Therefore, we had strong evidence for convergent validity in our data.

To determine discriminant validity in our data, we analyzed the square root of the AVE for each construct. 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 or exceeded the criteria for discriminant validity (see Table 4).

To evaluate our measurement model further, we analyzed the factor loadings of each measurement item on its intended construct. Appendix 2 (Tables 12, 13, 14, and 15) contains these factor loadings. All of our items loaded greater than the expected threshold of 0.7 for all industries (except one

Table 2 Demographic data

	Banking		Retail		Healthcare		Higher education	
Age								
18–29	5	4.6%	2	2.0%	2	1.8%	0	0%
30–44	27	25.0%	28	28.6%	12	10.5%	46	46%
45–60	75	69.4%	45	46.0%	56	49.1%	49	49%
> 60	1	1.0%	23	23.4%	44	38.6%	5	5%
Total	108	100%	98	100%	114	100%	100	100%
Gender								
Male	55	50.9%	68	69.4%	56	49.1%	76	76%
Female	53	49.1%	30	30.6%	58	50.9%	24	24%
Total	108	100%	98	100%	114	100%	100	100%
Positions								
Faculty	0	0%	0	0%	0	0%	37	37%
Middle mgmt.	78	72.2%	78	79.6%	60	52.6%	50	50%
Upper mgmt.	8	7.4%	7	7.1%	2	1.8%	5	5%
IT professional	22	20.4%	13	13.3%	52	45.6%	8	8%
Total	108	100%	98	100%	114	100%	100	100%

perceived normative measurement item for the retail industry group). Although 0.7 is the recommended threshold, individual item loadings between .40 and .70 are acceptable for inclusion so long as composite reliabilities are above .70 (Chin 1998), which they were for all of our measurement items. The factor loadings in Appendix 2 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 (Gefen and Straub 2005).

Part of our empirical test of the "b" hypotheses was to perform a multi-group analysis. However, for a multi-group analysis to be meaningful, we first had to assess measurement invariance (i.e., the same construct is being measured across different groups) between the measurement items among the different industry groups. To do this, we followed the three-

Table 3 Construct reliability & validity

Construct	ISA	COG	NORM	REG
Industry: Banking (*N* = 108)				
AVE	0.841	0.713	0.870	0.753
Cronbach's alpha	0.937	0.800	0.850	0.839
Composite reliability	0.955	0.882	0.930	0.901
Industry: Retail (*N* = 98)				
AVE	0.857	0.718	0.930	0.793
Cronbach's alpha	0.944	0.811	0.893	0.870
Composite reliability	0.960	0.884	0.949	0.920
Industry: Healthcare (*N* = 114)				
AVE	0.808	0.730	0.870	0.779
Cronbach's alpha	0.921	0.823	0.852	0.859
Composite reliability	0.944	0.889	0.931	0.914
Industry: Higher education (*N* = 100)				
AVE	0.809	0.821	0.813	0.686
Cronbach's alpha	0.921	0.890	0.770	0.773
Composite reliability	0.944	0.932	0.897	0.868
Entire sample (all industries): (*N* = 426)				
AVE	0.888	0.767	0.768	0.803
Cronbach's alpha	0.958	0.849	0.852	0.877
Composite reliability	0.969	0.908	0.908	0.924

Table 4 Discriminant validity & inter-construct correlations

	Banking				Retail			
	ISA	COG	NORM	REG	ISA	COG	NORM	REG
ISA	*0.917*				*0.926*			
COG	0.705	*0.845*			0.314	*0.847*		
NORM	0.747	0.686	*0.933*		0.295	0.355	*0.950*	
REG	0.684	0.657	0.651	*0.868*	0.498	0.456	0.358	*0.890*
	Healthcare				Higher Education			
	ISA	COG	NORM	REG	ISA	COG	NORM	REG
ISA	*0.899*				*0.899*			
COG	0.556	*0.854*			0.426	*0.906*		
NORM	0.670	0.538	*0.933*		0.477	0.468	*0.902*	
REG	0.587	0.479	0.654	*0.883*	0.598	0.429	0.600	*0.828*
	Entire Sample (All Industries)							
	ISA	COG	NORM	REG				
ISA	*0.942*							
COG	0.486	*0.876*						
NORM	0.440	0.451	*0.876*					
REG	0.634	0.513	0.511	*0.896*				

Italic cells represent the square of AVE step process outlined by Henseler et al. (2014) 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 and configural invariance and partial invariance for the equality of mean values and variances, which enabled us to run the multi-group analyses. Appendix 3 contains the statistical details concerning these invariance tests.

Our survey instrument measured the independent and dependent variables on the same questionnaire. Therefore, we had to ensure that our measurement method instead of our constructs of interest were not affecting our results. To test for common method variance with our measurement model, we used the unmeasured latent method factor approach discussed by Podsakoff et al. (2012). 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.

5.2 Structural Models for Hypotheses Testing

We tested our hypotheses using a series of structural PLS models. Consistent with Wilkinson's (1999) recommendation, we report the effect size (F^2) along with null-hypothesis significance testing (NHST) for all of our models because the NHST is sensitive to sample size. The effect size (F^2), however, is not sensitive to sample size so it produces a more accurate measure of the magnitude of the effect between two variables (Cohen 1992; Ferguson 2009). An effect size (F^2) larger than 0.02, 0.15, and 0.35 signifies small, medium, and large effect size, respectively (Cohen 1977).

We first evaluated the "a" hypotheses with all of the data analyzed together (i.e., all subjects in a single model). We then evaluated the "b" hypotheses by splitting the sample by industry group. With the split sample, we ran a series of multi-group comparisons between the research subjects in the different industry segments.[3] To test whether the multi-group differences were due to perceived sanction differences, we ran ANOVAs between each of the industry groups based on their perceptions of sanctions.[4] Finally, we evaluated H4 and H5 with the entire sample and with the sample split by industry segment because perceived norms might moderate within and/or between industry segments similarly or differently.

5.2.1 Empirical Tests for the Main Effects ("a" Hypotheses)

Table 5 displays the path coefficients and effect sizes used to test each of the "a" hypotheses. This model containing our entire sample explained roughly 44.6% of the variance in perceived organizational effort to raise general ISA in our data. We found that perceived regulatory pressure (H1a) positively affected employees' perceptions of organizational effort to raise general ISA across employees in our entire sample ($\beta = 0.481$, $p < 0.001$). When employees perceived high regulatory institutional pressures, they perceived that their organizations exerted high levels of effort to raise their general ISA. The effect size of perceived regulatory institutional pressures was the highest among the three institutional pressures in our data. We also found empirical evidence supporting the hypothesized effect of perceived normative pressures on perceived organizational effort to raise general ISA (H2a) ($\beta = 0.108$, $p < 0.05$). Greater perceived normative pressures resulted in greater perceptions of how much effort their organizations exerted to increase their employee's general ISA. The effect size of perceived normative pressures was the lowest of the three institutional pressures in our data (but still statistically significant). We found a similar statistically significant effect for perceived cultural-cognitive pressures (H3a). In our data, greater perceived cultural-cognitive pressures resulted in greater perceptions of organizational effort to raise general ISA ($\beta = 0.191$, $p < 0.001$). Therefore, we have strong support for all three main effects in our data.

5.2.2 Empirical Tests of the Industry Differences ("b" Hypotheses)

We tested the "b" hypotheses by running a series of multi-group analyses and ANOVAs comparing the four industry segments. For the multi-group analyses in PLS, we used the Welch-Satterthwaite test, which assumes unequal variances between groups (Hair et al. 2016), to test for significance differences in the path coefficients across each industry segment. Table 6 displays the results from these multi-group

Table 5 Path coefficient (t-Value) and effect size (F^2)

Entire sample (all industries)	$N = 420$ $R^2 = 0.446$
REG ➔ ISA	0.481 (8.418)*** $F^2 = 0.266$
NORM ➔ ISA	0.108 (1.972)* $F^2 = 0.015$
COG ➔ ISA	0.191 (4.080)*** $F^2 = 0.045$

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

[3] For the multi-group analyses, we ran PLS multi-group analyses (PLS-MGA) with bootstrapping (using 500 random re-samples) to calculate the path coefficients (β) for each path in the proposed research model.

[4] We asked each survey participant a single question concerning their perceptions about the perceived sanctions for violating one of the institutional pillars. The ANOVAs tested differences using this single item measure.

Table 6 Multi-group analyses

REG ➔ ISA	Differences in Path Coefficients (β)			
(H1b)		Banking	Healthcare	Higher Education
	Healthcare	0.076		
	Higher Education	0.086	0.162	
	Retail	0.136	0.213	0.050
NORM ➔ ISA	Differences in Path Coefficients (β)			
(H2b)		Banking	Healthcare	Higher Education
	Healthcare	0.086		
	Higher Education	0.261*	0.347**	
	Retail	0.261*	0.347**	0.000
COG ➔ ISA	Differences in Path Coefficients (β)			
(H3b)		Banking	Healthcare	Higher Education
	Healthcare	0.088		
	Higher Education	0.087	0.001	
	Retail	0.211	0.123	0.124

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

analyses. In these multi-group analyses, we find no support for inconsistent effects based on perceived regulatory institutional pressures (H1b) and perceived cultural-cognitive pressures (H3b). That is, all industry segments have no statistically significant differences in the effects of perceived regulatory and cultural-cognitive pressures on perceptions of organizational effort to raise general ISA. These two effects were consistent across employees in all industries irrespective of specific industry characteristics. However, we find support for differences in perceived normative institutional pressures (H2b) in these multi-group comparisons. Particularly, we found significant differences in the path coefficients between the banking and retail industries (β difference = 0.261, $p < 0.05$), between the banking and higher education industries (β difference = 0.261, $p < 0.05$), between the healthcare and retail industries (β difference = 0.347, $p < 0.01$) and between the healthcare and higher education industries (β difference = 0.347, $p < 0.01$).

In order to determine if the significant differences in the perceived normative pressures path across the different industry segments varied based on perceived sanctions (as we predicted in our "b" hypotheses), we ran a series of ANOVAs to test for differences in perceived sanctions. Table 7 displays the ANOVA differences. From these ANOVAs, we see that the industry segments where the subjects had the lowest perceived sanctions (retail and higher education) had no statistical difference. We also see that the industry segments where the subjects had the highest perceived sanctions (banking and healthcare) had no statistical difference. However, we see significant differences between perceived sanctions between the retail industry segment (low perceived sanctions) and both the banking and healthcare industry segments (high-perceived sanctions). We see the same statistically significant differences between higher education (low perceived sanctions) and both banking and healthcare (high-perceived sanctions). The statistically significant multi-group differences (Table 6) are between the industry segments with low perceived sanctions and those with high-perceived sanctions. The perceived normative paths are statistically greater for the banking and healthcare industry segments relative to the higher education and retail industry segments, which is consistent with the Scheffe ANOVA differences that we found. Therefore, we have support for H2b in the hypothesized direction based on perceived institutional sanctions.

Table 7 ANOVAs between industry segments comparing perceived sanctions (Scheffe test)

(I) Industry		(J) Industry	Mean difference (I-J)	std. error
Banking		Higher Ed.	1.375***	0.190
Mean	*5.69*	Health Care	−0.288	0.184
SDEV	*1.205*	Retail	0.828***	0.191
Higher Ed		Banking	−1.375***	0.190
Mean	*4.31*	Health Care	−1.664***	0.188
SDEV	*1.376*	Retail	−0.547	0.195
Health Care		Banking	0.288	0.184
Mean	*5.97*	Higher Ed.	1.664***	0.188
SDEV	*0.964*	Retail	1.117***	0.189
Retail		Banking	−1.828***	0.191
Mean	*4.86*	Higher Ed.	0.547	0.195
SDEV	*1.861*	Health Care	−1.117***	0.189

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

5.2.3 Empirical Test for the Moderating Effect of NORMS (H4 & H5)

We tested these moderating effects with the entire sample together and for each industry segment separately. Table 8 displays the R^2 values for each model and Table 9 displays the effect sizes along with the path coefficients for each path.

We found partial support for the proposed moderating effect of perceived normative pressures and perceived regulatory pressures (H4) for employees in the banking ($\beta = -0.144$, $p < 0.05$) and healthcare ($\beta = -0.104$, $p < 0.05$) industries but no support for employees in the retail ($\beta = -0.02$, $p > 0.05$) and higher education ($\beta = 0.175$, $p > 0.05$) industries. This means that we found a differential effect of the perceived regulatory pressure path for the employees in the two industries with the highest perceived sanctions in our sample so this moderating effect also might be associated with perceived sanctions. Figure 2 graphically displays this moderating effect for the banking and healthcare industries. We can see from this figure that the effect of having low perceived regulatory pressures is mitigated by having strong perceived normative pressures in both the banking and healthcare industries.

We also found partial support for the proposed moderating effect of perceived normative pressures and perceived cultural-cognitive pressures (H5) for the entire sample ($\beta = 0.07$, $p < 0.05$) and for the employees in the banking industry ($\beta = -0.121$, $p < 0.05$). Figure 3 graphically displays this moderating effect. This effect is interesting because the sign of the coefficient for the interaction effect is different for the sub sample of banking employees versus all employees aggregated together. Greater perceived normative institutional pressures does amplify the effect of both high and low perceived cultural-cognitive pressures but the differential effect varies across the banking sample and the entire sample.

6 Discussion & Conclusion

Table 10 displays a summary of our conclusions. The main effects of three pillars of institutions were supported in our data and perceived regulatory pressures had the greatest effect size. Greater perceived institutional pressures were associated with greater perceived organizational effort to increase their employee's general ISA, which is our core set of hypotheses. We found support for the qualifying effects by industry for only the normative path. For this path, the industries with greater perceived sanctions had an amplified effect. We found partial support for the moderating hypotheses for certain industry segments but not for others. When significant, greater perceived norms amplified both main effects (but the interaction effect was not significant in all of our models).

Interestingly, we found that perceived regulatory institutional pressures did not have a differential effect on perceived organizational effort to raise employees' general ISA in highly regulated industries relative to less regulated industries. This finding may be because the regulatory institutional pressures rely heavily on the normative institutional pillar to take effect (Scott 2008). That is, an industry's institutional norms enhance the regulatory pressures, but the regulatory institutional pillar by itself may not prevail without the shared institutional norms that express its importance (March and Olsen 1989; Scott 2008). For example, the COBIT framework is an institutionalized norm primarily used in the banking industry, which enhances the effect of SOX regulations during the planning and implementation of IT governance. Without the COBIT framework, SOX regulations may become 'just another' regulatory institutional pressure that banks in the banking industry are required to follow, which may mitigate the regulatory pressure's effectiveness in encouraging information security related behaviors.

In our data, perceived institutional norms in an industry also had an interesting mitigating effect on weak cultural-cognitive institutional pressures. In the presence of strong perceived institutional norms, we found weak cultural-cognitive institutional pressures concerning information security did not have a negative effect on perceived organizational effort to raise their employees' general ISA. In this case, the strong normative institutional pressures washed out the potential negative main effect of weak cultural-cognitive institutional pressures. We found this effect most prevalent in the employees in the banking industry. Relative to the other three industries in our study, the banking industry is unique because of the global security related institutional norms that govern the banking industry. These global institutionalized norms had a powerful mitigating effect on the perceived cultural-cognitive institutional pressures.

Table 8 R-Squared values of ISA

Models	Banking	Retail	Healthcare	Higher education	Entire sample (all industries)
Main effects only	0.650	0.263	0.557	0.313	0.446
Interaction of NORM*REG	0.667	0.264	0.570	0.346	0.466
Interaction of NORM*COG	0.659	0.281	0.558	0.319	0.450

Table 9 Path coefficient (t-Value) and effect size (F^2)

	Banking	Retail	Healthcare	Higher education	Entire sample (all industries)
REG ➔ ISA with NORM as a moderator	−0.144 (2.300)* $F^2 = 0.052$	−0.022 (0.022) $F^2 = 0.001$	−0.104 (1.970)* $F^2 = 0.028$	0.175 (1.918) $F^2 = 0.052$	0.006 (0.268) $F^2 = 0.000$
COG ➔ ISA with NORM as a moderator	−0.121 (1.970)* $F^2 = 0.025$	0.074 (1.432) $F^2 = 0.025$	−0.015 (0.408) $F^2 = 0.001$	0.155 (1.324) $F^2 = 0.010$	0.070 (2.140)* $F^2 = 0.007$

We tested each interaction effect separately in different models

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$

6.1 Research Limitations

Like all research, our paper has several limitations. First, we can only draw conclusions about employees working in specific industries and not industry-level effects per se. We did not attempt to aggregate the perceptions within or between industries to make any type of industry-level conclusions. Our paper is an individual-level study whereby we compare employees' perceptions based on each employees' industry. Furthermore, the perceptions of the employees working in each of our sampled industries may not accurately reflect the institutional environment of all organizations in an industry's institutional environment. However, Ashforth et al. (2010) suggested that higher-level conclusions (i.e., industry-level effects in our case) can be derived from individual-level data because organizations are the collection of the beliefs of its individual employees.

Second, we only compared four industries in our study. These four industries provided ample perceived and real variance along the three institutional pillars to test our research model but we make no claims that these four industry environments represent all industries. However, future research could test our model using different industry environments. For example, highly labor-intensive industries such as the agriculture and construction industries or digital only industries such as the social media and online search industries might amplify or mitigate the magnitude and direction of the industry differences that we reported in our paper. Therefore, future research could investigate a different sample of industries to refine our understanding of industry differences.

Third, although our sample sizes across each of our industries were large enough to test our hypothesized differences, increasing the sample size in each industry would allow for additional analyses. For example, having a larger sample size in each industry would allow us to compare occupational differences (professional versus managerial) within and between industries. It might be reasonable to surmise that professional staff would have different perceptions about their organization's management relative to staff who are already working in the managerial ranks. Unfortunately, we did not have the necessary sample size to run this type of analysis in our study. However, this would make for an interesting future study that would further refine our understanding of how industry and an employee's occupation within that industry impacts perceptions of general ISA or a different security-related dependent variable.

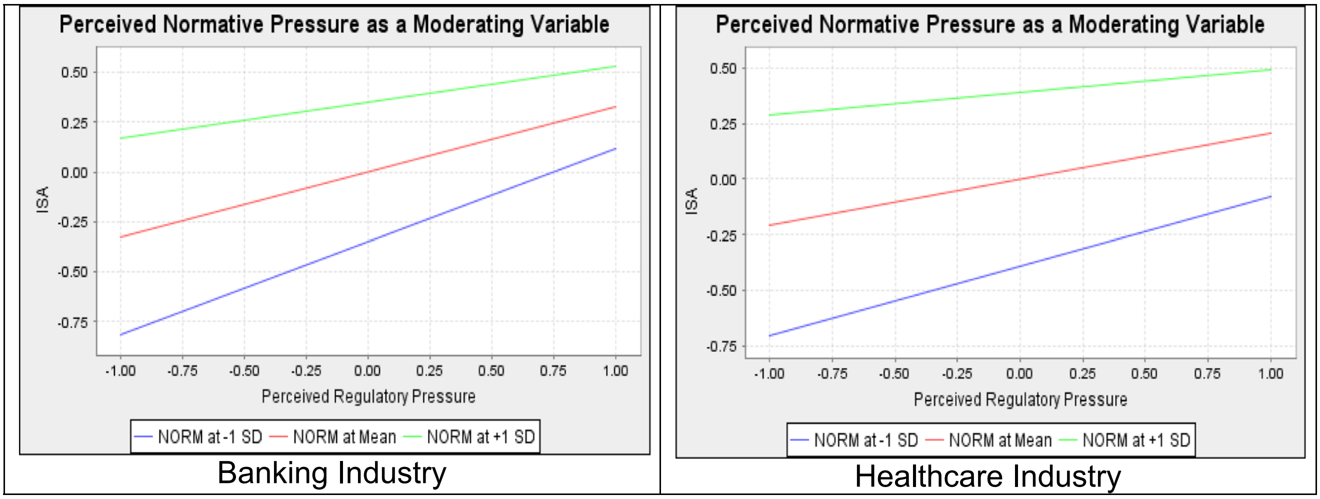
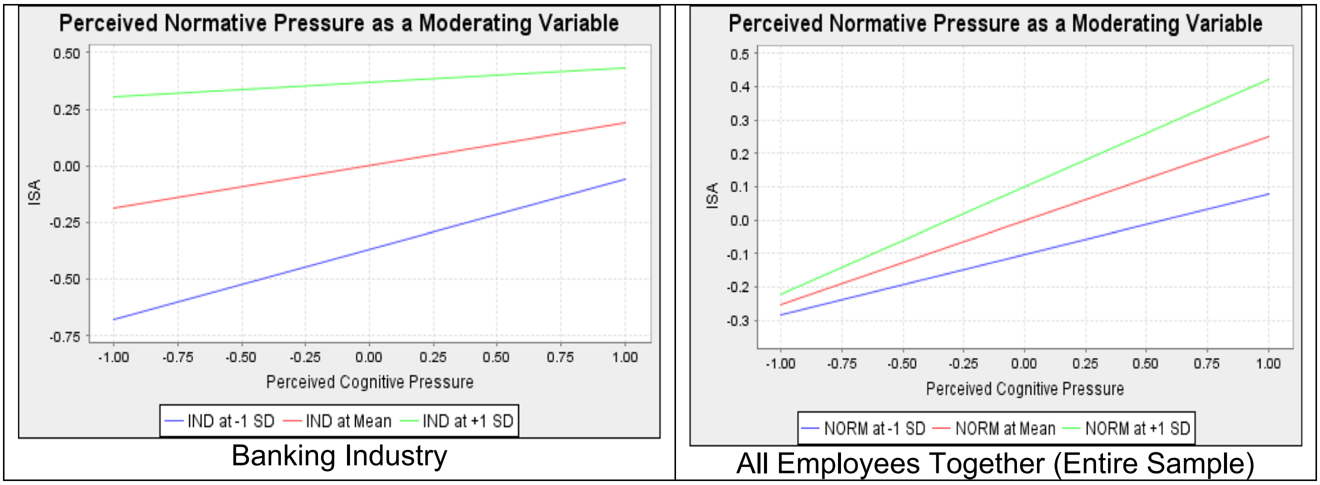


Fig. 2 Moderating effect of perceived normative pressure on perceived regulatory pressure



Banking Industry

All Employees Together (Entire Sample)

Fig. 3 Moderating effect of perceived normative pressure on perceived cultural-cognitive pressure

6.2 Practical Contributions

Individual organizations are players who play by the rules of the game that are defined by the normative, regulative, and cultural-cognitive pillars of institutions (Scott 2008; Wang 2010). It is difficult for organizations to change the rules of the game because the social structures governing those organizations are relatively stable (Meyer and Rowan 1977; Scott 2008; Suchman 1995), which makes it challenging for organizations to manage institutional structures actively. Having said this, we see three important practical contributions to our study. First, our paper focused on individual-level perceptions of those institutional structures. Therefore, managers may actively manage the perceptions of their employees. Based on our results, increasing the perceived threat of sanctions at the institutional level can have a powerful effect on how much effort an organization exerts to increase their employees' general ISA, which can promote an environment inside of the organization that focuses on information security.

Second, although institutional structures are stable, they can still be changed (North 1990; Tolbert and Zucker 1983). Organizations can collaborate with other organizations in their industry environments to establish security related norms or culture-cognitive beliefs surrounding information security. For instance, social media firms may work together to form a set of digital guidelines that organizations in the social media industry are expected to follow. Working to legitimize certain practices that all organizations in an industry are expected follow (as it pertains to information security) may take time, but these institutionalized norms (once developed) can have a strong impact on the security practices of the organizations that are governed by those institutional structures. Third, knowing that employees in different industries have different perceptions and the effects of those perceptions also vary may be important for the development of security training and education programs in organizations. Aligning training programs with the institutional structures in specific industries may be a better approach than having a one-size fits all

Table 10 Summary of results

Findings			Support
REG ➔ ISA	H1a	This path coefficient is significant with the greatest effect size (see Table 5)	*Yes*
	H1b	There are no significant differences in the β values across the four industry segments (see Table 6).	No
NORMS ➔ ISA	H2a	The path coefficient is significant (see Table 5).	*Yes (but small effect size)*
	H2b	The high-perceived sanction industry segments differ from the low perceived sanction industry segments with a stronger effect for the high-perceived sanction industry segments (see Table 6 and Table 7).	*Yes*
COG ➔ ISA	H3a	The path coefficient is significant (see Table 5).	*Yes (but small effect size)*
	H3b	There are no significant differences in the β values across the four industry segments (see Table 6).	No
REG ➔ ISA with NORM as a moderating variable	H4	This moderating hypothesis is supported for the banking and healthcare employees in our sample (see Table 9 and Fig. 2).	*Partial*
COG ➔ ISA with NORM as a moderating variable	H5	This moderating hypothesis is supported for the banking employees in our sample and the aggregated model with all employees (see Table 9 and Fig. 3).	*Partial*

approach. Based on our findings related to industry differences, we speculate that the types of trainings that work well in one institutional environment may not work as well in another institutional environment.

6.3 Theoretical Implications

On the surface, using individual-level perceptions may seem counter to NIT, which is typically used for organizational-level research. However, Subbady (Suddaby 2010, p. 17) suggested the following concerning the use of employee level data in NIT empirical research:

> *Institutional work, of course, is conducted by individuals and it is somewhat surprising to me how individuals often disappear from institutional research. Institutional logics, for example, must have a perceptual component that operates cognitively at the level of individuals. That is, if we take seriously the notion that institutions are powerful instruments of cognition, there must be some opportunity in conducting research on how institutional logics are understood and influence at the individual level of analysis.*

Because employees are organizational actors whose comprehensions, beliefs, and attitudes toward their organizations affect organizational actions (Singh and Lumsden 1990), their collective views represent an organization as an entity in a particular institutional environment (Hannan and Freeman 1977; Suddaby et al. 2009). Although perceptions may vary from individual-to-individual, a collective view of employees' perceptions (Ashforth et al. 2010) can represent the security practices exercised in an organizational context. Therefore, comparing differences in perceptions among employees across industries should shed some light on how external institutional pressures affect security behaviors through organizational efforts of raising ISA.

To the best of our knowledge, very few studies have examined how the external environment affects general ISA. We suggest that understanding how employees perceive their external institutional environment is important for three primary reasons. First, different industries have institutionalized security practices and (formal and informal) enforcement mechanisms to varying degrees. We argue that these unique security practices and enforcement mechanisms across industries may increase or decrease organizational effort to inform their employees about general ISA due to different perceived institutional pressures across industries. Second, we suggest that institutional isomorphism will result in similar security and risk management practices in a specific industry, but these security and risk management practices may differ across industries. Organizations want to be perceived as legitimate participants in their corresponding industries so they tend to behave in a similar manner to other organizations in the same industry (DiMaggio and Powell 1983), which may result in similar effort (or perceptions thereof) regarding their ISA initiatives. Third, certain industries are more digital due to the nature of their work and the pressures from the three pillars of institutions. More digital industries may have stronger normative information security practices relative to less digital industries, which may result in differing levels of effort that organizations across industries devote to inform their employees about the current threat landscape.

Appendix A

There are four reflective constructs in our paper: 1) REG – perceived regulatory institutional pressure, 2) NORM – perceived normative institutional pressure, 3) COG – perceived cultural-cognitive institutional pressure, and 4) ISA – perceived organizational effort to raise general information security awareness.

Table 11 Measurement items

Construct	Measurement items		References
REG	REG1	My organization is aware of the legal damages that have occurred to other organizations within our industry, when those organizations have violated federal laws and regulations on information security.	Self-developed by referencing Hu et al. (2007)
	REG2	If my organization were to violate federal laws and regulations on information security (e.g., SOX, GLBA, FERPA), my organization would be liable for legal claims from the people we serve.	
	REG3	If my organization were to violate federal laws and regulations on information security (e.g., SOX, GLBA, FERPA, HIPAA), an authorized third party regulator would take legal action against us.	
NORM	NORM1	My organization maintains standardized, well-recognized practices in the industry, in	Self-developed by referencing Hu et al. (2007)

Table 11 (continued)

Construct	Measurement items		References
		order to secure sensitive data.	
	NORM2	My organization is aware of what other organizations (in the same industry) are doing to secure sensitive data.	
	NORM3	My organization wants us to be aware of the recent trends and practices of information security practices in the industry.	
COG	COG1	To better serve our clients, my organization must keep their data secure.	Self-developed by referencing Hu et al. (2007) and Yeh and Chang (2007)
	COG2	To remain competitive, my organization must protect our clients' sensitive data.	
	COG3	To earn trust from our clients, my organization must prevent data breaches that will expose our clients' sensitive data.	
ISA	ISA1	My organization makes sure that we are aware of potential threats to information security and the negative consequences that could arise from an information security breach.	Adapted from Herath and Rao (2009) and Chan et al. (2005)
	ISA 2	My organization educates us about the cost of potential information security problems.	
	ISA 3	My organization provides training so that we are aware of management's concerns about information security and the risks that security breaches pose to the company and the people we serve.	
	ISA 4	My organization has provided training to us on the importance of information security.	

Appendix B - Factor Loading

Table 12 Factor loading for each industry

	Banking				Healthcare				Retail				Higher Education			
	COG	NORM	ISA	REG	COG	NORM	ISA	REG	COG	NORM	ISA	REG	COG	NORM	ISA	REG
COG1	0.887	0.605	0.690	0.568	0.938	0.545	0.586	0.482	0.944	0.418	0.358	0.372	0.805	0.239	0.206	0.363
COG2	0.858	0.541	0.575	0.630	0.933	0.633	f0.578	0.562	0.920	0.439	0.365	0.375	0.886	0.375	0.229	0.365
COG3	0.785	0.415	0.499	0.460	0.846	0.400	0.373	0.382	0.852	0.333	0.403	0.459	0.850	0.344	0.331	0.417
NORM1	0.626	0.897	0.673	0.525	0.579	0.926	0.716	0.697	0.503	0.917	0.399	0.454	0.269	0.929	0.276	0.270
NORM2	0.520	0.901	0.626	0.551	0.509	0.907	0.626	0.567	0.379	0.930	0.306	0.480	0.403	0.951	0.285	0.409
NORM3	0.476	0.816	0.513	0.411	0.439	0.746	0.426	0.454	0.101	0.653	0.176	0.378	0.417	0.923	0.204	0.374
ISA1	0.674	0.677	0.914	0.647	0.563	0.655	0.928	0.593	0.392	0.371	0.914	0.481	0.330	0.238	0.925	0.489
ISA2	0.597	0.528	0.875	0.614	0.494	0.614	0.926	0.565	0.364	0.342	0.934	0.440	0.258	0.246	0.887	0.437
ISA3	0.647	0.695	0.945	0.655	0.517	0.651	0.936	0.556	0.384	0.318	0.960	0.474	0.285	0.247	0.940	0.463
ISA4	0.664	0.647	0.933	0.592	0.575	0.676	0.916	0.575	0.411	0.351	0.926	0.518	0.289	0.298	0.950	0.453
REG1	0.497	0.486	0.528	0.855	0.430	0.581	0.573	0.918	0.395	0.500	0.465	0.872	0.460	0.426	0.521	0.909
REG2	0.528	0.411	0.494	0.854	0.525	0.576	0.493	0.885	0.435	0.419	0.464	0.883	0.401	0.327	0.385	0.901
REG3	0.658	0.569	0.715	0.893	0.503	0.674	0.604	0.915	0.313	0.407	0.389	0.820	0.344	0.219	0.401	0.861

Table 13 Factor loading for all industries (entire sample)

	All Industries			
	COG	NORM	ISA	REG
COG1	0.884	0.403	0.390	0.411
COG2	0.898	0.422	0.414	0.451
COG3	0.846	0.362	0.465	0.478
NORM1	0.403	0.903	0.423	0.446
NORM2	0.439	0.936	0.440	0.515
NORM3	0.329	0.783	0.253	0.363
ISA1	0.482	0.414	0.931	0.596
ISA2	0.437	0.390	0.930	0.584
ISA3	0.449	0.418	0.958	0.601
ISA4	0.464	0.435	0.949	0.609
REG1	0.458	0.503	0.609	0.908
REG2	0.467	0.446	0.545	0.905
REG3	0.454	0.420	0.547	0.874

Table 14 Factor loadings, mean, t-values, and standard deviation (STDEV) for banking, healthcare, and higher education industries

	Banking Industry				Healthcare Industry				Higher Education			
	Loading	Mean	STDEV	t-value	Loading	Mean	STDEV	t-value	Loading	Mean	STDEV	t-value
COG1 ← COG	0.887	0.890	0.025	35.280	0.938	0.929	0.030	31.760	0.944	0.942	0.022	43.696
COG2 ← COG	0.858	0.856	0.070	12.203	0.933	0.923	0.031	30.153	0.920	0.916	0.027	34.240
COG3 ← COG	0.785	0.776	0.102	7.733	0.846	0.791	0.125	6.761	0.852	0.849	0.041	20.793
NORM1 ← NORM	0.897	0.897	0.019	47.105	0.926	0.927	0.015	62.228	0.917	0.919	0.029	32.097
NORM2 ← NORM	0.901	0.901	0.020	45.222	0.907	0.905	0.025	36.722	0.930	0.918	0.040	23.128
NORM3 ← NORM	0.816	0.816	0.033	24.899	0.746	0.731	0.079	9.399	0.653	0.626	0.140	4.671
ISA1 ← ISA	0.914	0.914	0.017	52.356	0.928	0.926	0.019	48.294	0.914	0.913	0.021	44.587
ISA2 ← ISA	0.875	0.873	0.039	22.475	0.926	0.924	0.019	49.387	0.934	0.933	0.018	52.332
ISA3 ← ISA	0.945	0.946	0.014	66.809	0.936	0.934	0.016	57.265	0.960	0.959	0.010	100.352
ISA4 ← ISA	0.933	0.935	0.013	74.365	0.916	0.913	0.024	38.496	0.926	0.925	0.022	41.772
REG1 ← REG	0.855	0.850	0.038	22.248	0.918	0.917	0.019	48.434	0.872	0.869	0.030	29.005
REG2 ← REG	0.854	0.848	0.046	18.660	0.885	0.879	0.031	28.598	0.883	0.882	0.028	31.200
REG3 ← REG	0.893	0.895	0.018	48.579	0.915	0.913	0.017	54.150	0.820	0.819	0.049	16.901

Table 15 Factor loadings, mean, t-values, and standard deviation (STDEV) for retail and all the industries (entire sample)

	Retail Industry				All Industries			
	Loading	Mean	STDEV	t-value	Loading	Mean	STDEV	t-value
COG1 ← COG	0.805	0.793	0.091	8.847	0.884	0.883	0.019	46.779
COG2 ← COG	0.886	0.871	0.065	13.668	0.898	0.898	0.023	38.887
COG3 ← COG	0.850	0.850	0.062	13.763	0.846	0.844	0.029	28.934
NORM1 ← NORM	0.929	0.925	0.038	24.164	0.903	0.903	0.012	73.140
NORM2 ← NORM	0.951	0.947	0.031	30.544	0.936	0.935	0.008	116.583
NORM3 ← NORM	0.923	0.916	0.043	21.574	0.783	0.782	0.033	23.723
ISA1 ← ISA	0.925	0.925	0.018	50.648	0.931	0.932	0.009	105.147
ISA2 ← ISA	0.887	0.885	0.032	27.697	0.930	0.930	0.010	90.344
ISA3 ← ISA	0.940	0.940	0.019	49.750	0.958	0.958	0.006	161.558
ISA4 ← ISA	0.950	0.950	0.011	89.343	0.949	0.949	0.007	132.961
REG1 ← REG	0.909	0.910	0.022	41.170	0.908	0.908	0.011	85.752
REG2 ← REG	0.901	0.894	0.034	26.636	0.905	0.905	0.012	77.655
REG3 ← REG	0.861	0.858	0.038	22.751	0.874	0.874	0.015	56.965

Appendix C: 3-Step Measurement Invariance Testing Using Permutation

We used the MICOM three-step procedure for measurement invariance testing (Ringle et al. 2016). The first step involves configural invariance where we made sure 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 (Ringle et al. 2016). Next, in step 2, if a correlational value is close to 1 and falls within the range of the confident intervals, then it indicates compositional invariance. Finally, step 3 incorporates 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 tables (from Tables 16, 17, 18, 19, 20, and 21) display the results for our invariance tests for each industry pair. The permutation test in SmartPLS 3.2 requires us to make a comparison of two groups at a time. We found that for each pair of group comparison, the criteria for compositional invariance has been 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 (Ringle et al. 2016). Therefore, we conclude that our Multi-Group Analysis (MGA) produces meaningful statistical results.

Table 16 Banking vs. Healthcare

Construct	Step 1	Step 2			Step 3a			Step 3b			M.I.[a]
	Configural invariance	Correlation	Confident intervals	Compositional invariance	Mean difference	Confident intervals	Equal mean	Variance difference	Confident intervals	Equal variance	
COG	Yes	0.999	[0.990, 1.000]	Yes	−0.097	[−0.271, 0.265]	Yes	0.134	[−0.477, 0.481]	Yes	Full
ISA	Yes	1.000	[1.000, 1.000]	Yes	−0.271	[−0.237, 0.260]	No	0.412	[−0.517, 0.487]	Yes	Partial
NORM	Yes	0.999	[0.997, 1.000]	Yes	−0.386	[−0.262, 0.263]	No	0.225	[−0.354, 0.347]	Yes	Partial
REG	Yes	0.999	[0.997, 1.000]	Yes	−0.419	[−0.270, 0.268]	No	0.682	[−0.906, 0.825]	Yes	Partial

[a] M.I. stands for Measurement Invariance

Table 17 Banking vs. Higher education

Construct	Step 1	Step 2			Step 3a			Step 3b			M.I.[a]
	Configural invariance	Correlation	Confident intervals	Compositional invariance	Mean difference	Confident intervals	Equal mean	Variance difference	Confident intervals	Equal variance	
COG	Yes	0.997	[0.996, 1.000]	Yes	0.266	[−0.280, 0.264]	No	−0.230	[−0.556, 0.640]	Yes	Partial
ISA	Yes	1.000	[1.000, 1.000]	Yes	1.139	[−0.244, 0.281]	Yes	−0.790	[−0.381, 0.361]	No	Partial
NORM	Yes	0.995	[0.982, 1.000]	Yes	0.216	[−0.271, 0.273]	Yes	−0.315	[−0.372, 0.394]	Yes	Full
REG	Yes	0.998	[0.995, 1.000]	Yes	0.900	[−0.266, 0.274]	No	−0.322	[−0.365, 0.369]	Yes	Partial

[a] M.I. stands for Measurement Invariance

Table 18 Banking vs. Retail

Construct	Step 1	Step 2			Step 3a			Step 3b			M.I.[a]
	Configural invariance	Correlation	Confident intervals	Compositional invariance	Mean difference	Confident intervals	Equal mean	Variance difference	Confident intervals	Equal variance	
COG	Yes	0.993	[0.986, 1.000]	Yes	−0.074	[−0.248, 0.281]	Yes	0.450	[−0.648, 0.611]	Yes	Full
ISA	Yes	1.000	[1.000, 1.000]	Yes	0.570	[−0.284, 0.272]	No	−0.867	[−0.461, 0.489]	No	Partial
NORM	Yes	1.000	[0.998, 1.000]	Yes	0.489	[−0.274, 0.276]	No	−1.051	[−0.385, 0.370]	Yes	Partial
REG	Yes	0.999	[0.995, 1.000]	Yes	0.535	[−0.263, 0.274]	No	−0.800	[−0.473, 0.463]	No	Partial

[a] M.I. stands for Measurement Invariance

Table 19 Healthcare vs. Higher education

Construct	Step 1	Step 2			Step 3a			Step 3b			M.I.[a]
	Configural invariance	Correlation	Confident intervals	Compositional invariance	Mean difference	Confident intervals	Equal mean	Variance difference	Confident intervals	Equal variance	
COG	Yes	0.999	[0.995, 1.000]	Yes	0.657	[−0.275, 0.272]	No	−0.962	[−0.801, 0.819]	No	Partial
ISA	Yes	1.000	[1.000, 1.000]	Yes	1.202	[−0.283, 0.256]	Yes	−0.923	[−0.390, 0.382]	No	Partial
NORM	Yes	0.999	[0.997, 1.000]	Yes	0.550	[−0.297, 0.262]	No	−0.508	[−0.477, 0.483]	No	Partial
REG	Yes	0.995	[0.994, 1.000]	Yes	1.123	[−0.275, 0.285]	Yes	−0.749	[−0.367, 0.401]	No	Partial

[a] M.I. stands for Measurement Invariance

Table 20 Healthcare vs. Retail

Construct	Step 1	Step 2			Step 3a			Step 3b			M.I.[a]
	Configural invariance	Correlation	Confident intervals	Compositional invariance	Mean difference	Confident intervals	Equal mean	Variance difference	Confident intervals	Equal variance	
COG	Yes	0.988	[0.984, 1.000]	Yes	0.382	[−0.272, 0.271]	No	−0.271	[−0.890, 0.940]	Yes	Partial
ISA	Yes	1.000	[1.000, 1.000]	Yes	0.650	[−0.271, 0.271]	No	−1.000	[−0.490, 0.449]	Yes	Partial
NORM	Yes	0.999	[0.993, 1.000]	Yes	0.736	[−0.284, 0.267]	No	−1.269	[−0.393, 0.470]	Yes	Partial
REG	Yes	0.999	[0.997, 1.000]	Yes	0.753	[−0.271, 0.269]	No	−1.225	[−0.477, 0.537]	Yes	Partial

[a] M.I. stands for Measurement Invariance

Table 21 Higher education vs. Retail

Construct	Step 1	Step 2			Step 3a			Step 3b			M.I.[a]
	Configural invariance	Correlation	Confident intervals	Compositional invariance	Mean difference	Confident intervals	Equal mean	Variance difference	Confident intervals	Equal variance	
COG	Yes	0.996	[0.985, 1.000]	Yes	−0.364	[−0.282, 0.270]	No	0.694	[−0.647, 0.683]	No	Partial
ISA	Yes	0.999	[0.995, 1.000]	Yes	−0.610	[−0.286, 0.281]	No	−0.079	[−0.333, 0.332]	Yes	Partial
NORM	Yes	0.990	[0.970, 1.000]	Yes	0.234	[−0.292, 0.277]	Yes	−0.724	[−0.388, 0.374]	No	Partial
REG	Yes	0.999	[0.995, 1.000]	Yes	−0.286	[−0.278, 0.293]	No	−0.491	[−0.375, 0.362]	No	Partial

[a] M.I. stands for Measurement Invariance

References

Aldrich, H. E., & Fiol, C. M. (1994). Fools rush in? The institutional context of industry creation. *Academy of Management Review, 19*(4), 645–670. https://doi.org/10.5465/amr.1994.9412190214.

Alexander, E. A. (2012). The effects of legal, normative, and cultural-cognitive institutions on innovation in technology alliances. *Management International Review, 52*(6), 791–815. https://doi.org/10.1007/s11575-011-0123-y.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management, 6*, 279–314. https://doi.org/10.1504/IJIEM.2010.035624.

Ashforth, B. E., Rogers, K. M., & Corley, K. G. (2010). Identity in organizations: exploring cross-level dynamics. *Organization Science, 22*(5), 1144–1156. https://doi.org/10.1287/orsc.1100.0591.

Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security, 73*, 219–234. https://doi.org/10.1016/j.cose.2017.11.001.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004.

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *SIGMIS Database, 48*(3), 44–68. https://doi.org/10.1145/3130515.3130519.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do Systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690.

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: insights from three agent-based models. *Information*

Systems Frontiers, 19(3), 509–524. https://doi.org/10.1007/s10796-015-9608-8.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(3), 18–41. https://doi.org/10.1080/15536548.2005.10855772.

Chang, K., & Wang, C. (2011). Information systems resources and information security. *Information Systems Frontiers, 13*(4), 579–593. https://doi.org/10.1007/s10796-010-9232-6.

Chatman, J. A., & Jehn, K. A. (1994). Assessing the relationship between industry characteristics and organizational culture: how different can you be? *Academy of Management Journal, 37*(3), 522–553. https://doi.org/10.5465/256699.

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205–222. https://doi.org/10.25300/MISQ/2016/40.1.09.

Chiasson, M. W., & Davidson, E. (2005). Taking industry seriously in information systems research. *MIS Quarterly, 29*(4), 591–605. https://doi.org/10.2307/25148701.

Chin, W. W. (1998). *The partial least squares approach to structural equation modeling*. Mahwah: Lawrence Erlbaum Associates.

Cohen, J. (1977). *Statistical power analysis for the behavioral sciences*. New York: Academic Press.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155.

Cooter, R. D. (2000). Three effects of social norms on law: expression, deterrence, and internalization. *Oregon Law Review, 79*(1), 1–23.

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: an empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1–15. https://doi.org/10.1007/s10796-017-9755-1.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160.

Davidson, D. E., & Heslinga, D. D. (2006). Bridging the IT adoption gap for small physician practices: an action research study on electronic health records. *Information Systems Management, 24*(1), 15–28. https://doi.org/10.1080/10580530601036786.

Deephouse, D. L. (1996). Does isomorphism legitimate? *Academy of Management Journal, 39*(4), 1024–1039. https://doi.org/10.5465/256722.

Desai, C., Wright, G., & Fletcher, K. (1998). Barriers to successful implementation of database marketing: a cross-industry study. *International Journal of Information Management, 18*(4), 265–276. https://doi.org/10.1016/S0268-4012(98)00015-2.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: an organizational transformation case study. *Computers & Security, 56*, 63–69. https://doi.org/10.1016/j.cose.2015.10.001.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys. In *The tailored design method* (4th ed.). Hoboken: Wiley.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101.

Douglas, M. (1986). *How institutions think*. Syracuse: Syracuse University Press.

Dunn, M. B., & Jones, C. (2010). Institutional logics and institutional pluralism: the contestation of care and science logics in medical education, 1967–2005. *Administrative Science Quarterly, 55*(1), 114–149. https://doi.org/10.2189/asqu.2010.55.1.114.

Durand, R., & Thornton, P. H. (2018). Categorizing institutional logics, institutionalizing categories: a review of two literatures. *Academy of Management Annals, 12*(2), 631–658. https://doi.org/10.5465/annals.2016.0089.

Ferguson, C. J. (2009). An effect size primer: A guide for clinicians and researchers. *Professional Psychology: Research and Practice, 40*(5), 532–538. https://doi.org/10.1037/a0015808.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research, 19*(4), 440–452. https://doi.org/10.2307/3151718.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312.

Friedland, R., & Alford, R. (1991). Bringing society back in: Symbols, practices and institutional contradictions. In W. Powell & P. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 232–263). University Of Chicago Press.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: tutorial and annotated example. *Communications of the Association for Information Systems, 16*(1), 16. https://doi.org/10.17705/1CAIS.01605.

Gordon, G. G. (1991). Industry determinants of organizational culture. *Academy of Management Review, 16*(2), 396–415. https://doi.org/10.5465/amr.1991.4278959.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208.

Hair, J. F., Jr., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles: Sage Publications.

Hannan, M. T., & Freeman, J. (1977). The population ecology of organizations. *American Journal of Sociology, 82*(5), 929–964. https://doi.org/10.1086/226424.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M., & Calantone, R. J. (2014). Common beliefs and reality about partial least squares: comments on Rönkkö & Evermann (2013). *Organizational Research Methods, 17*(2), 182–209.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in Organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6.

Hrebiniak, L. G., & Snow, C. C. (1980). Industry differences in environmental uncertainty and organizational characteristics related to uncertainty. *Academy of Management Journal, 23*(4), 750–759. https://doi.org/10.5465/255561.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004.

King, J. L., Gurbaxani, V., Kraemer, K. L., McFarlan, F. W., Raman, K. S., & Yap, C. S. (1994). Institutional factors in information technology innovation. *Information Systems Research, 5*(2), 139–169. https://doi.org/10.1287/isre.5.2.139.

Kohli, R., & Kettinger, W. J. (2004). Informating the clan: controlling physicians' costs and outcomes. *MIS Quarterly, 28*(3), 363.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. *MIS Quarterly, 35*(2), 293–334. https://doi.org/10.2307/23044045.

March, J. G., & Olsen, J. P. (1989). *Rediscovering institutions: the organizational basis of politics* (1st edn.). New York: The Free Press.

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: a cross-cultural examination. *Computers & Security, 75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. https://doi.org/10.1086/226550.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853.

North, D. C. (1990). *Institutions, institutional change and economic performance*. New York: Cambridge University Press.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology, 63*(1), 539–569. https://doi.org/10.1146/annurev-psych-120710-100452.

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

Ringle, C. M., Sarstedt, M., & Henseler, J. (2016). Testing measurement invariance of composites using partial least squares. *International Marketing Review, 33*(3), 405–431. https://doi.org/10.1108/IMR-09-2014-0304.

Rockness, H., & Rockness, J. (2005). Legislated ethics: from Enron to Sarbanes-Oxley, the impact on corporate America. *Journal of Business Ethics, 57*(1), 31–54. https://doi.org/10.1007/s10551-004-3819-0.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: a cross-discipline view of trust. *Academy of Management Review, 23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617.

Scott, W. R. (2008). *Institutions and organizations, ideas and interest* (3rd ed.). Thousand Oaks: Sage.

Singh, J. V., & Lumsden, C. J. (1990). Theory and research in organizational ecology. *Annual Review of Sociology, 16*(1), 161–195. https://doi.org/10.1146/annurev.so.16.080190.001113.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502. https://doi.org/10.2307/25750688.

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*(3), 289–305. https://doi.org/10.1057/ejis.2012.59.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal, 22*(1), 77–94. https://doi.org/10.1111/j.1365-2575.2011.00378.x.

Suchman, M. C. (1995). Managing legitimacy: strategic and institutional approaches. *Academy of Management Review, 20*(3), 571–610. https://doi.org/10.5465/amr.1995.9508080331.

Suddaby, R. (2010). Challenges for institutional theory. *Journal of Management Inquiry, 19*(1), 14–20.

Suddaby, R., Gendron, Y., & Lam, H. (2009). The organizational context of professionalism in accounting. *Accounting, Organizations and Society, 34*(3), 409–427. https://doi.org/10.1016/j.aos.2009.01.007.

Swidler, A. (1986). Culture in action: symbols and strategies. *American Sociological Review, 51*(2), 273–286. https://doi.org/10.2307/2095521.

Thornton, P. H., & Ocasio, W. (1999). Institutional logics and the historical contingency of power in organizations: executive succession in the higher education publishing industry, 1958–1990. *American Journal of Sociology, 105*(3), 801–843. https://doi.org/10.1086/210361.

Thornton, P. H., & Ocasio, W. (2008). Institutional logics. In R. Greenwood, C. Oliver, R. Suddaby, & K. Sahlin-Andersson (Eds.), *The Sage handbook of organizational institutionalism* (Vol. 840, pp. 99–128). Thousand Oaks: SAGE Publications Ltd.

Tolbert, P. S., & Zucker, L. G. (1983). Institutional sources of change in the formal structure of organizations: the diffusion of civil service reform, 1880–1935. *Administrative Science Quarterly, 28*(1), 22–39. https://doi.org/10.2307/2392383.

Trice, H. M. (1993). *Occupational subcultures in the workplace*. Ithaca: Cornell University Press.

Wang, P. (2010). Chasing the hottest IT: effects of information technology fashion on organizations. *MIS Quarterly, 34*(1), 63–85.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101–105. https://doi.org/10.1057/ejis.2009.12.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: a longitudinal study. *Decision Support Systems, 92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013.

Wilkinson, L. (1999). Statistical methods in psychology journals: guidelines and explanations. *American Psychologist, 54*(8), 594–604. https://doi.org/10.1037/0003-066X.54.8.594.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005.

Xu, X. M., Kaye, G. R., & Duan, Y. (2003). UK executives' vision on business environment for information scanning: a cross industry study. *Information & Management, 40*(5), 381–389. https://doi.org/10.1016/S0378-7206(02)00045-9.

Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: a cross-industry study. *Information & Management, 44*(5), 480–491. https://doi.org/10.1016/j.im.2007.05.003.

Zucker, L. G. (1977). The role of institutionalization in cultural persistence. *American Sociological Review, 42*(5), 726–743. https://doi.org/10.2307/2094862.

Zucker, L. G. (1987). Institutional theories of organization. *Annual Review of Sociology, 13*(1), 443–464. https://doi.org/10.1146/annurev.so.13.080187.002303.

Zwikael, O., & Ahn, M. (2011). The effectiveness of risk management: an analysis of project risk planning across industries and countries. *Risk Analysis, 31*(1), 25–37. https://doi.org/10.1111/j.1539-6924.2010.01470.x.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. Hwee-Joo Kam is an Assistant Professor at the University of Tampa. She teaches courses related to information security (e.g., penetration testing, secure coding, information assurance, and database security). She primarily researches behavioral information security and has published in a variety of refereed journals (e.g., Computers & Education and JIT). Dr. Kam is also CISSP certified.

Dr. Thomas Mattson is an Assistant Professor at the University of Richmond. He has published in a variety of peer-reviewed journals, including JAIS, MISQ, CAIS, and Computers & Security. Dr. Mattson researches a variety of information systems topics including behavioral information security and online networks of practice.

Dr. Sanjay Goel is a Full Professor and Chair of the Information Technology Management Department in the School of Business, at the University at Albany. He has published over 75 articles in refereed journals including top journals such as IEEE Journal of Selected Areas in Communication, DSS, CAIS, CACM and the Information & Management Journal.