A Cross Industry Study: Differences in Information Security Policy Compliance between the Banking Industry and Higher Education

Completed Research Paper

Hwee-Joo Kam
Ferris State University
Big Rapids, MI
ismhweejoo@gmail.com

Pairin Katerattanakul
Western Michigan University
Kalamazoo, MI
p.katerattanakul@wmich.edu

Greg Gogolin
Ferris State University
Big Rapids, MI
ismgreg@yahoo.com

Abstract

This study adopts the Neo-Institutional Theory (NIT) to address the underlying differences in information security policy compliance between the banking industry and higher education. Drawing on the NIT, this study examines how regulative, normative, and cognitive expectations influence the internal organizational efforts of staying compliant across both industries. Using the Partial Least Square (PLS) method, the analysis results suggest that both industries rely on the normative expectation to propel their organizational efforts of attaining compliance. However, the main difference lies within cognitive expectation. In the institution of higher education, cognitive expectation has an indirect effect on information security policies compliance through regulative expectation. On the other hand, cognitive expectation reflects the severity of regulatory pressure in the banking industry. Given these findings, this study presents theoretical implication and provides suggestions to policy makers on the basis of managerial implication.

Keywords: Neo-Institutional Theory (NIT), cross industry study, information security policy compliance

Introduction

In the aftermath of the financial scandals involving Enron and WorldCom, banks had to undergo IT auditing and meet stringent compliance regulations, including the Sarbanes-Oxley Act of 2002 (SOX) and the Gramm-Leach-Bliley Act (GLBA). As of today, information security breaches are high threats for banks (Symantec Global Internet Security Threat Report 2010). Security breaches in any banks will precipitate serious consequences for the organizations because security breaches will draw negative publicity that taints the banks' reputations, causing losses in profits (Goodhue and Straub 1991).

In the same token, universities and colleges face the threat of legal liability for irresponsible handling of sensitive information (Elliot et al. 1991). Universities and colleges are required to comply with the Family Educational Rights and Privacy Act (FERPA) to safeguard student's information. It is important to protect student's information as the exposure of sensitive student data, such as social security numbers, could easily turn students into identity theft victims.

However, unlike the banking industry, higher education is characterized by informality, subjectivity, infrequent and implicit promotions, and tenure that promise stable employment (Dill 1982). Higher education also has loosely coupled systems where the functionality, rewards, sanctions, and departments have low interdependency, thus perpetuating the unique characteristics of subsystem or subculture (Weick 1976).

For organizational survival, organizations have to integrate externally legitimated formal structures to augment the promise of internal participants and external constituents (Meyer and Rowen 1977). For example, to attain information security policy compliance, organizations must respond to the external expectations of information security. Then, organizations establish internal expectations for information security protection. These external expectations constitute regulative, normative, and cognitive expectations (Interligi 2010).

This study suggests that different industries encounter different external expectations with respect to information security safeguards, leading to the differences in the organizational expectations regarding information security policy compliance. Specifically, the differences in external expectations between the banking industry and higher education may precipitate differences in organizational expectations relative to information security protection, thus creating differences in information security policy compliance.

Therefore, the main objectives of this study are to (1) investigate which external factors motivate the information security policies compliance in banking industry and in higher education, and (2) provide suggestions to policy makers on how to enhance information security policy compliance in higher education and in banking industry.

Literature Review

Institution and Neo-Institution Theory

Institutional theorist, Scott (1995), argues that institutions rest on three pillars – regulative, normative, and cognitive – to give meaning and stability to social life. Each pillar represents external expectation that organizations are expected to live up to. In details, these three pillars are:

Regulative pillar stresses activities of sanctioning and monitoring both formal and informal rules. For example, regulative pillar highlights the compliance to SOX and GLBA in banking industry and FERPA in higher education.

Normative pillar focuses on social norm or appropriate behavior based on the prescriptive, evaluative, and obligatory dimension in social life (Scott 2008). Overall, normative pillar highlights the shared values and norms, interpersonal expectations, and valued identities (Javernick-Will and Levitt 2010). In short, it refers to the "right thing to do". For instance, safeguarding student's social security numbers to prevent the incidents of identity theft represents social obligation (i.e., the right thing to do) of the universities and colleges. Also, in the context of information security, professional organizations build normative expectation by defining the industry norms (Hu, Hart, and Cooke, 2007). For example, Information

Systems Audit and Control Association (ISACA) is a professional organization that helps to define the normative framework for outlining the industry norms related to standardized security mechanism.

Cognitive pillar signifies the taken for granted value and shared understanding (Scott 2008, pg. 51). Specifically, culture, as a part of the cognitive pillar, is a socially constructed symbolic representation that shapes the shared belief system (Javernick-Will and Levitt 2010). As a result, this pillar forms the perceptions about an event given the shared belief system built on culture. For instance, with the incidents of data breaches, the stakeholders will interpret and identify these incidents based upon their perceptions built on cultural frame with shared understanding.

Institution constitutes regulative, normative, and cognitive expectations that serve as a template for guiding organizational actions and perspectives (Scott 1995). Hinged on this template, organizations conform to their institutional environment to survive. In the context of organizational survival, organizations undergo institutionalization to adopt practices that foster legitimacy (Meyer and Rowen 1977; DiMaggio and Powell 1983). Legitimacy pertains to the appropriate actions consistent with social norms, values, and beliefs (Suchman 1995).

In particular, organizational survival relies on securing legitimacy from stakeholders through conformity to regulative, normative, and cognitive pressure (DiMaggio and Powell 1983). Reacting to external pressure, organizations undergo coercive, mimetic, and normative isomorphism to espouse certain programs and policies and procedures (DiMaggio and Powell 1983; Kostova and Roth 2002). Under coercive isomorphism, a more powerful authoritative (e.g.: federal government) imposes organizational patterns (e.g., organizational practices and belief systems) whereas through mimetic isomorphism, organizations embrace the patterns of successful organizations to respond to uncertainty (DiMaggio and Powell, 1983; Kostova and Roth, 2002). With normative isomorphism, organizations employ patterns considered appropriate in the environment (DiMaggio and Powell, 1983; Kostova and Roth, 2002). As a result, organizations achieve legitimacy and increase their chances to survive. Accordingly, Neo-Institutional Theory (NIT) suggests that organizations respond to external pressure by complying with federal regulations, by learning from other organizations' successful responses to uncertainty, and by adopting practices that are deemed appropriate in the institution environment.

Differences between Higher Education and Banking Industry

In higher education, the governance and decision making are very distinctive as compared to the rest of the society because the "bottom up" approach in decision making hands some decision making authorities to faculty members (Reis 1997). The institution of tenure clearly separates academia from other institutions, since tenure offers, within limits, lifetime employment (Dill 1982). Along the same line, higher education promotes professional autonomy (Dill 2003), thus enabling scholars the freedom of teaching and carrying out research.

Regarding the banking industry, the banking culture is significantly different from other industry cultures as commercial banks are mostly perceived as hierarchical, bureaucratic, and slow to change (Davis 2004). Banking industry today encounters pressure from competitors, investors, and internal resistance to change (Davis 2004). Banks are also under the pressure of globalization (Bullock 2003) in addition to merger and acquisition, and pressure to perform. This has been followed by a decline in a bank's "family culture" that values executives and employees irrespective of their contributions (Davis 2004). Furthermore, formal policies and procedures define banking industry (Argyris 1958).

Higher education functions in a cultural-cognitive system (Meyer et. al. 2007) that shapes expectations for knowledge creation, dissemination, and research innovation (Reis 1997). On the other hand, banks operate in a relational system (Scott 2008) wherein the external constituents such as Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC) etc. impose immense pressure on banks to comply and hold banks accountable for their actions.

After the financial scandal involving Enron and WorldCom, the banking industry has been confronting immense pressure to comply with regulations such as SOX and GLBA. The pressure to comply has compelled banks to incorporate information security into their daily operations. Similar to the banking industry, higher education is required to stay compliant with regulations like FERPA. Parallel to the violation of federal banking regulation, violating FERPA may result in a lawsuit that adversely affects the institution's public image.

Additionally, universities and colleges are required to comply with GLBA since they are managing student financial aids. Some universities with medical programs have to stay compliant with Health Insurance Portability and Accountability Act (HIPAA) to protect patient's confidential information. However, unlike the banking industry, only a fraction of universities and colleges provide information awareness training, making it more difficult to support IT security implementation (Kvavik 2004) and to draft appropriate policies and procedures (Rezgui and Marks 2008).

Cybercrimes target at banking industry and most banks realize the threats and risks in their environment (Yeh and Chang 2007). Based on the Symantec Global Internet Security Threat Report of 2010, the increase in online banking has triggered a corresponding jump, from 83% in 2008 to 98% in 2009, in the threats to confidential information related to remote access capabilities.

Finally, organization-stakeholder interaction unfolds opportunities to stakeholder's influences and preferred methods for internal control (Interligi 2010). This enables stakeholders to impose pressures on organizations (e.g. banks, universities), urging organizations to meet stakeholder's expectations. Stakeholders of the banking organizations mainly consist of shareholders, the board of directors, customers, financial markets, and government (Behery and Eldomiaty 2010) whereas the main stakeholders of the higher education are government, students, faculty, administrators, alumni, parents and the community where the higher institution resides (Gross and Godwin 2005).

The following Table 1 and Table 1-1 summarize the major differences between banking industry and higher education. We argue that, although both industries face the pressure to comply with regulations, this stake is higher in the banking industry. Additionally, the threats and risks related to information security are also higher in banking industry than they are in higher education.

Table 1. Comparison between Banking Industry and Higher Education

	Banking Industry	Higher Education
Governance, Decision making, and Culture	• Hierarchical and Bureaucratic – slow to change • Formal policies and procedures define banking industry • Relational system	• Bottom up management – give some decision making authorities to faculty members • Tenure system • Academic freedom • Decentralization – lack of system integration and understanding across different departments • Cultural-cognitive system
Pressure to comply / Regulations	High	Medium
Threats and Risks	High	Medium to Low
Training	High	Low

Table 1-1. Differences between Banking Industry and Higher Education

	Banking Industry	Higher Education
Regulative Expectation	The federal government expects the banking industry to comply with regulations, such as SOX and GLBA.	The federal government expects the higher education to comply with FERPA, GLBA, and HIPAA.

Normative Expectation	The stakeholders are shareholders, the board of directors, customers, financial markets, and government (Behery and Eldomiaty 2010). They expect banks to prevent: unsolicited advertisements, accidental release of personal information, misrouting of funds and data errors (Earp and Payton 2006).	The stakeholders are students, faculty, administrators, alumni, and the community (Gross and Godwin 2005). They expect higher education to educate, produce innovative research, and create and share knowledge (Reis 1997).
Cognitive Expectation	The banking stakeholders realize the threats to banking information security (Yeh and Chang 2007) and understand that a bad image caused by data breaches will bring devastating effects to the bank.	There is no high information security awareness among the stakeholders, causing a lack of perception in information security (Rezgui and Marks 2008).

Hypothesis Statement

Extant literatures uncover the industry differences in perception of risk and risk management. Some previous findings revealed that different industries perceive environmental uncertainty, intra-organizational influence, and degree of structural decentralization differently (Hrebiniak and Snow 1980). Environment uncertainty varies across the industries and the structural responses to uncertainty differ across industries, as well (Hrebiniak and Snow 1980). Given that each type of industry encounters uncertainty in a different form (Hrebiniak and Snow 1980), and that risk is associated with uncertainty (Rousseau et al., 1998), each industry shapes the unique perception of risk (Yeh and Chang 2007). Since organizations within the same industry face risks of a similar nature, organizations under the same industry share a similar level of intensity for risk management processes (Zwikael and Ahn 2011). On the other hand, the different nature of risk across industries generates different levels of intensity for risk management. Risk management corresponds to information security policies (Harris 2006). Given the high level of intensity for risk management, the organizations within the same industry can overtly indicate the importance of information security policies to foster security policy compliance (Boss et. al. 2009).

Additionally, hinged on the Neo-Institutional Theory (NIT), homogeneity among organizations ascribes to isomorphism (DiMaggio and Powell 1983). Mainly, isomorphism refers to the constraining process wherein one unit coerces another unit to reach resemblance under the same environmental conditions (Hawley 1968). Highly regulated industries in highly structured environments tend to have homogeneous structure, culture, and output (DiMaggio and Powell 1983). This suggests that "*organizations within the same industry sector may exhibit similar compliance cultures*" (Interligi 2010, pg. 240). Along the same line, security compliance culture shared among organizations in the same industry reflects upon the homogeneous, industry-level perception of security policy compliance. Alternatively, a different industry may encounter different external expectations, leading to different structures, culture, and output. Thus, a different industry may display different organizational expectations toward security policy compliance.

This study compares the banking industry and the higher education due to their similarities and differences. Although both industries must comply with regulations, both industries form different values in perceived pressure to comply, perceived threats, and perceived risks. Because of (1) the different environmental uncertainties related to information security between the banking industry and the higher education and (2) isomorphism that begets distinctive industry-level perception of security policy compliance for each industry, we hypothesize that the banking industry and the higher education would interact with their external uncertainties differently and form different perceptions for information security policy compliance; this would then lead to the differences in information security policy compliance across industries. The stark contrast between higher education and banking industry may draw insights on the external drivers that propel these industries to comply and shed light on the mechanism of implementing security practices in different organizational settings.

Research Methodology

Proposed Research Model

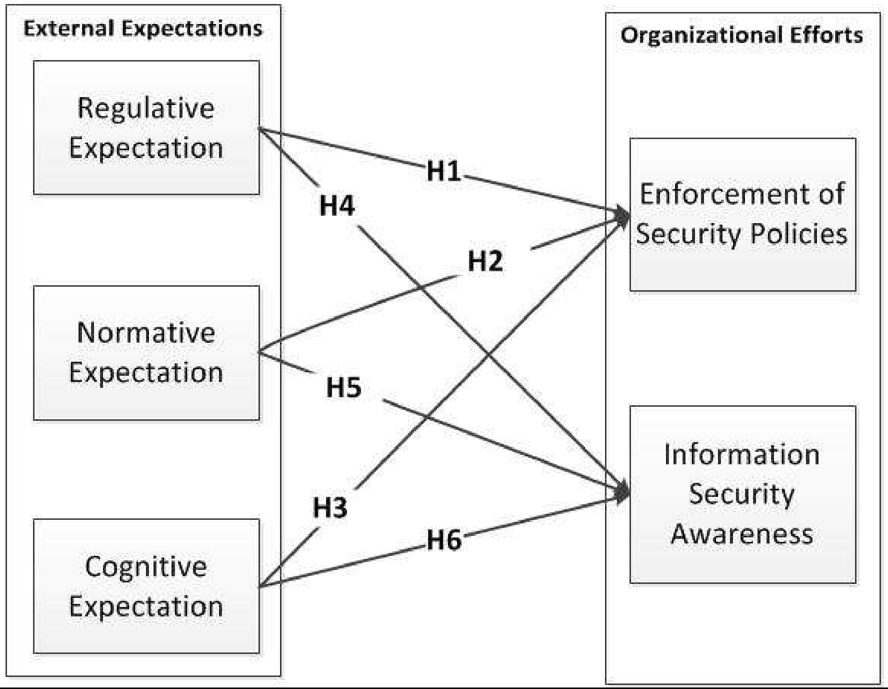

Figure 1: Proposed Research Model

Building on the literature review in the preceding section, we constructed the proposed research model (see Figure 1) based on two notions. First, there are differences across industries that would lead to the differences in information security policy compliance across industries. This notion relies on the concept of isomorphism (DiMaggio and Powell 1983) and the findings of prior studies stressing that different characteristics across industries produce different ways of interacting with external environment across industries (Hrebiniak and Snow 1980; Yeh and Chang 2007; Zwikael and Ahn 2011). Using the same research model (see Figure 1), we ran the higher education and banking data independently and then compared the results to check whether there were any differences in information security policy compliance across both industries.

The second notion draws on the Neo-Institutional Theory (NIT) postulating that organizations will initialize internal efforts to meet external expectations so as to secure legitimacy for organizational survival (Meyer and Rowen 1977; DiMaggio and Powell 1983). Referring to Table 1-1, both banking industry and higher education encounter three external expectations. Thus, hinged on the NIT, the proposed research model suggests that three external expectations – Regulative (REG), Normative (NORM), and Cognitive (COG) expectations – drive universities and banks to stay compliant through the internal efforts of (1) Enforcement of Policies and Procedures (POL) and (2) Information Security Awareness (AWA). Numerous prior studies posited that POL and AWA represented internal efforts of staying compliant within organizations (Boss et al. 2009; Bulgurcu, Cavusoglu, and Benbasat 2010; Chan, Woon, and Kankanhalli 2005; Herath and Rao 2009).

Enforcement of Policies and Procedures emphasizes the policies and procedures within an organization. The efforts of specifying policies and procedures enhance the perceived mandatoriness of security policies among the employees (Boss et al. 2009). As a result, this fosters information security policies compliance.

Information Security Awareness affects employee's beliefs with respects to the benefit of compliance and the cost of non-compliance (Bulgurcu et al. 2010). Organizations want employees to grasp the requirements and the objectives of information security (Bulgurcu et al. 2010).

Referring to the proposed research model (see Figure 1), the six hypotheses are:

H1: Regulative expectation drives organizations to enforce information security policies and procedures

H2: Normative expectation drives organizations to enforce information security policies and procedures

H3: Cognitive expectation drives organizations to enforce information security policies and procedures

H4: Regulative expectation drives organizations to raise information security awareness

H5: Normative expectation drives organizations to raise information security awareness

H6: Cognitive expectation drives organizations to raise information security awareness

Questionnaires

During the questionnaire development, we employed some measurement items used in some of the previous studies about information security (i.e., Boss et al., 2009; Bulgurcu et al. 2010; Chan et al. 2005; Herath and Rao 2009). Our original questionnaire had 20 items measuring the five constructs (i.e., REG, NORM, COG, POL, and AWA). Each of these 20 measurement items applied 7-point Likert scale with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree.

A pilot study was conducted to improve the original questionnaire. We invited five college administrators (e.g., Dean, Associate Dean, Department Chair, Information Security Officer) of an university and five banking professionals (e.g. president of a commercial bank, branch manager, loan officer, officer) to review and answer our questionnaires. Based on their responses, we computed the Cronbach's Alpha and the item-to-total score to evaluate the reliability for each construct. Next, using this reliability assessment and the feedbacks collected from the pilot study, we refined the measurement items in the original questionnaire. The final version of the questionnaire (see Table 2) adopted by this study incorporated 14 measurement items representing the five constructs. This study used the same measurement instrument (see Table 2) for both the higher education and the banking industry samples.

Table 2: Measurement Items

Construct	Item	Description	References
REG	REG1	Legal action from regulator as a result of data breaches	Self-developed through referencing Hu et al. (2007)
	REG2	Realize the legal damages suffered by another organization in the same industry due to data breaches	
	REG3	Inspection by an authorized third-party regulator	
NORM	NORM1	Adopt standardized security practices in the industry	Self-developed through referencing Hu et al. (2007)
	NORM2	Serve the clients through security compliance	
COG	COG1	Negative publicity due to data breaches	Self-developed through referencing Herath and Rao (2009)
	COG2	Loss of prestige due to data breaches	
	COG3	Monetary loss due to data breaches	
	COG4	Loss of stakeholder's trust due to data breaches	
POL	POL1	Formal security policies in the organization setting	Adapted from Boss et al. (2009)
	POL2	Formal security policies to protect computer system	
AWA	AWA1	Employees realize the potential threats to security	Adapted from Bulgurcu et al (2010)
	AWA2	Educating employees about the cost of security problem	
	AWA3	Inform employees of the new threats to security	

Data Collection

To collect data from the banking organizations, we spent about six months to repeatedly post our online survey in the professional forums such as the BankingInfoSecurity forum in the LinkedIn site. We also sent emails to invite the banking employees to participate in our study. These emails were sent to nearly 100 banking information security professionals via social networking sites (e.g. LinkedIn). For the next two months, we distributed email reminders to follow up with the previous email messages we sent out. After approximately eight months, we obtained 31 responses.

Then, upon receiving the permission from some bank presidents, we invited the banking employees to participate in our online survey by sending out email attached with a link to the online survey site. Particularly, we sent emails to the banking employees from one community bank and two commercial banks in the Midwest region of the United States. We received 60 responses from these three banks. Also, we spent four semesters to collect data from some of our MBA students enrolling in two universities in the Midwest region of the United States. These students were part-time MBA students who were working full-time in the banking industry. We received 17 responses from this data collection method.

Overall, we collected 108 responses. These participants were 13 bank tellers (12%), 8 branch managers (7%), 8 compliance officers (7%), 6 credit analysts (6%), 5 directors of IT (4.5%), 9 information security specialists (8%), 4 IT workers (4%), 4 loan assistants (4%), 5 loan managers (4.5%), 4 mortgage officers (4%), 3 trust officers (3%), 9 vice presidents (8%), 3 bank presidents (3%), 27 other (18%) and undisclosed (7%). Most of our participants were working in a large bank with more than 400 employees and many of them had less than 10 years of working experience (88%). The average age was 33 years old.

On the other hand, we spent 5 months to collect data for higher education. We sent out emails to faculty members, administrators (e.g., Presidents, Provosts, Associate Provosts, Deans, Associate Deans, Department Chairs), and staff members (e.g., Information Security Officers, IT personnel) of three state-funded universities in the Midwest region of the United States. Two of these universities are research-focused universities and each has more than 20,000 students whereas the other university is a student-centered university with only 5000 students. The emails invited the recipients to participate by presenting the study objectives along with a hyperlink to the online questionnaires. We sent emails to approximately 250 people. After two months, we sent email reminder to follow up with the previous email messages we sent. We also made phone calls and engaged in face-to-face conversation to remind the email recipients to participate in this study. Then, after two months, we obtained 100 responses. The participants included 51 faculty members (51%), 38 administrators (38%), and 11 staff members (11%). About one-third of the respondents came from each of the three universities. Almost 70% of the respondents spent less than 10 years with their universities and their average age was 38 years old.

Measurement Assessment

This section uncovers various tests performed to check construct reliability and validity of the measuring instrument. The hypothesized model (see Figure 1) consisted of five latent, reflective constructs -- REG, NORM, COG, POL, and AWA. We separated the banking sample from that of the higher education so that the hypothesis testing for one sample was independent of the other.

This study employed Partial Least Square (PLS) method and used SmartPLS software for hypotheses testing. SmartPLS software functions as a component-based path modeling application hinged on the PLS method (Vance, Elie-Dit-Cosaque, and Straub 2008). We selected PLS method as the PLS path modeling is appropriate even with a very small sample size (Chin 1998; Haenlein and Kaplan 2004; Henseler, Ringle, and Sinkovics 2009). Unlike the covariance-based Structural Equation Modeling that demands a sample size of more than 100 observations (Nasser and Wisenbaker 2003), PLS path modeling works with a sample size as low as 50 observations (Chin and Newsted 1999).

Higher Education Sample

First, we tested the construct reliability of the measurement instruments for the higher education sample. Construct reliability was assessed by examining the Composite Reliability (CR) score (Fornell and Larcker 1981) and the Cronbach's alpha of each construct. Results in the following Table 3 show CR values ranging from 0.733 to 0.924 and Cronbach's alpha ranging from 0.771 to 0.878. These values exceed 0.70, thus proving construct reliability (Chin 1998).

Table 3. CR, AVE, and Cronbach's Alpha for the Higher Education Sample

Construct	Composite Reliability	AVE	Cronbach's Alpha
REG	0.8657	0.6824	0.7713
NORM	0.9020	0.8216	0.7836
COG	0.9342	0.7803	0.9077
POL	0.9308	0.8706	0.8515
AWA	0.9074	0.7658	0.8463

To assess convergent validity, the average variance extracted (AVE), referring to a measure of variance explained by a latent construct for the variance observed in its measurement items, should be at least 0.5 or higher (Fornell and Larcker 1981). The AVE values, ranging from 0.68 – 0.87 (see Table 3), prove convergent validity of the measurement instruments for higher education sample.

Furthermore, this study adopted bootstrapping with 500 random re-samples followed by examining the t-values of the outer model loadings. Convergent validity is demonstrated if all the measurement items load significantly on their respective latent construct. Overall, for each factor loading, the t-value should be larger than 1.96 and its corresponding p-value will be significant at least at 0.05 level (Gefen and Straub 2005). Table 4 shows that every measurement item significantly loaded on its respective latent construct with loading > 0.7, t-value > 2.5, and p-value < 0.001. This thus proves convergence validity.

Table 4: Factor Loading and t-value for the Higher Education Sample

Construct	Item	Factor Loading (t-value)
REG	REG1	0.7221***(8.6949)
	REG2	0.7850***(10.2510)
	REG3	0.8167***(14.9624)
NORM	NORM1	0.9214***(26.7761)
	NORM2	0.9023***(21.8076)
COG	COG1	0.8455***(4.9488)
	COG2	0.8260***(4.5505)
	COG3	0.7576***(4.2429)
	COG4	0.7163***(4.8646)
POL	POL1	0.9425***(62.2833)
	POL2	0.9174***(33.6074)
AWA	AWA1	0.8299***(16.7628)
	AWA2	0.9394***(64.0373)
	AWA3	0.8905***(30.1609)

***p-value < 0.001

To assess discriminant validity, two tests were conducted. First, in the AVE analysis, the square root of the AVE of each construct must be larger than the correlations of this construct to all the other constructs (Chin 1998). The results depicted in Table 5 reveal strong discriminant validity.

Table 5. Construct Correlations and Square Root of AVE (in shaded cells) for Higher Education Sample

	REG	NORM	COG	POL	AWA
REG	0.8261				
NORM	0.4983	0.9064			
COG	0.4209	0.3694	0.8833		
POL	0.5723	0.5280	0.2923	0.9931	
AWA	0.5807	0.5184	0.3162	0.5458	0.8751

The second test assessed the cross-loadings of measurement items on the latent constructs. Table 6 shows excellent discriminant validity since each measurement item loads higher on its intended construct than on any other constructs and the difference in loadings is at least 0.10 (Gefen and Straub 2005).

Table 6. Cross-loadings of Measurement Items on Latent constructs for Higher Education Sample

	AWA	COG	NORM	POL	REG
AWA1	**0.9193**	0.2982	0.4643	0.5236	0.5598
AWA2	**0.8331**	0.2609	0.3832	0.4512	0.5023
AWA3	**0.8709**	0.2695	0.5105	0.4549	0.4594
COG1	0.2089	**0.8392**	0.2728	0.1835	0.3409
COG2	0.2347	**0.9247**	0.3621	0.2170	0.3902
COG3	0.357	**0.8721**	0.2601	0.2832	0.3843
COG4	0.2762	**0.8951**	0.4076	0.3131	0.3654
NORM1	0.4967	0.3507	**0.9186**	0.5079	0.4939
NORM2	0.4402	0.3174	**0.8940**	0.4460	0.4046
POL1	0.4925	0.2775	0.5122	**0.9288**	0.4899
POL2	0.5251	0.2683	0.4743	**0.9373**	0.5756
REG1	0.5509	0.234	0.4577	0.5637	**0.8484**
REG2	0.4272	0.4667	0.3933	0.3211	**0.8057**
REG3	0.4406	0.3913	0.3753	0.4904	**0.8236**

Banking Industry Sample

Table 7 shows construct reliability since the values of CR and Cronbach's Alpha for all the constructs exceed or close to 0.70 (Chin 1998).

Table 7. CR, AVE, and Cronbach's Alpha for the Banking Sample

	Composite Reliability	**AVE**	**Cronbach's Alpha**
REG	0.8188	0.6015	0.6753
NORM	0.9081	0.8316	0.7981
COG	0.8671	0.6210	0.8007
POL	0.9276	0.865	0.8451
AWA	0.9175	0.7881	0.8650

After bootstrapping with 500 random re-samples, we assessed the t-values of the outer model loadings. Table 8 shows that every measurement item significantly loads on its respective latent construct with loading > 0.7, t-value > 2.5, and p-value < 0.001. This demonstrates convergence validity.

Table 8. Factor Loading and t-value for the Banking Sample

Construct	**Item**	**Factor Loading (t-value)**
REG	REG1	0.7221***(8.0504)
	REG2	0.7850***(10.0813)
	REG3	0.8167***(13.164)
NORM	NORM1	0.9214***(33.2043)
	NORM2	0.9023***(21.721)
COG	COG1	0.8455***(4.1079)
	COG2	0.8260***(3.5989)
	COG3	0.7576***(3.3725)
	COG4	0.7163***(4.4021)
POL	POL1	0.9425***(63.3418)
	POL2	0.9174***(35.4613)
AWA	AWA1	0.8299***(17.0929)
	AWA2	0.9394***(63.175)
	AWA3	0.8905***(33.0846)

***p-value < 0.001

In Table 9, the square root of the AVE of each construct is larger than the correlations of this construct to all the other constructs, thereby exhibiting discriminant validity (Chin 1998).

Table 9. Construct Correlations and Square Root of AVE (in shaded cells) for the Banking Sample

	REG	**NORM**	**COG**	**POL**	**AWA**
REG	0.7756				
NORM	0.5084	0.9119			
COG	0.4098	0.2915	0.7880		
POL	0.4196	0.5855	0.2221	0.9301	
AWA	0.3803	0.5631	0.1592	0.6537	0.8877

Next, we also examined the cross-loadings of measurement items on the latent constructs to test discriminant validity. Table 10 below shows excellent discriminant validity as each measurement item loads higher on its intended construct than on any other constructs and the difference in loadings is at least 0.10 (Gefen and Straub 2005).

Table 10. Cross-loadings of Measurement Items on Latent constructs

	AWA	COG	NORM	POL	REG
AWA1	**0.8299**	0.1433	0.4260	0.5405	0.3561
AWA2	**0.9394**	0.1266	0.5930	0.6404	0.3547
AWA3	**0.8905**	0.1605	0.4591	0.5503	0.3028
COG1	0.1673	**0.8455**	0.3033	0.2373	0.4182
COG2	0.0744	**0.8260**	0.2173	0.0912	0.2687
COG3	0.1203	**0.7576**	0.1522	0.1605	0.3153
COG4	0.0987	**0.7163**	0.2090	0.1479	0.2170
NORM1	0.5288	0.2641	**0.9214**	0.5702	0.5068
NORM2	0.4971	0.2681	**0.9023**	0.4943	0.4163
POL1	0.6545	0.2253	0.5902	**0.9425**	0.4154
POL2	0.5541	0.1848	0.4916	**0.9174**	0.3612
REG1	0.2871	0.2122	0.3939	0.2478	**0.7221**
REG2	0.1897	0.3202	0.3436	0.3385	**0.7850**
REG3	0.3791	0.3949	0.4357	0.3752	**0.8167**

Hypothesis Testing

After evaluating measurement properties of the instrument, we tested all the six hypotheses of the hypothesized model based on the PLS structural model (see Figure 1) for the higher education and the banking samples. We estimated the path coefficients (β) of the structure model using the bootstrapping technique with 500 random re-samples (Mathieson, Peacock, and Chin 2001; White, Varadarajan, and Dacin 2003).

For higher education, to evaluate the significance of the path coefficients, we inspected the significant level of each t-value. Results in Table 11 demonstrate that H3 and H6 are not supported, indicating that cognitive expectation had no direct effect on the higher education's efforts of staying compliant.

Table 11. Hypotheses Testing

	Higher Education			**Banking Industry**		
Hypothesis	**β**	**t-value**	**Supported**	**β**	**t-value**	**Supported**
H1: REG → POL	0.4114	4.4398**	Yes	0.1608	1.3532	No
H2: NORM → POL	0.3231	3.1365*	Yes	0.5008	4.0530**	Yes
H3: COG → POL	-0.0002	0.0017	No	0.0102	0.0889	No
H4: REG → AWA	0.4193	4.5481**	Yes	0.1432	1.4412	No
H5: NORM → AWA	0.2986	3.2286*	Yes	0.5038	4.1787**	Yes
H6: COG → AWA	0.0294	0.3579	No	-0.0464	0.4347	No

**p-value < 0.001 *p-value < 0.01

On the other hand, as we ran hypotheses testing for the banking industry sample, the hypotheses testing results exhibit that only H2 and H5 are supported (see Table 11). That is, only normative expectation has direct effect on the banking organizational efforts of staying compliant.

Discussion

Our analysis results reveal that cognitive expectation has no direct impact on information security policy compliance in higher education. Historically, universities were established in the medieval period where the institution of higher education operated under the cultural-cognitive model in support of social progress and justice (Meyer et. al. 2007). To date, modern universities and colleges follow this cultural-cognitive model to promulgate social progress through knowledge creation and dissemination, teaching, and research (Reis 1997), but not through information security safeguard. Due to a lack of perception in information security in higher education (Rezgui and Marks 2008), cognitive expectation does not emphasize the criticality of information security in higher education. For example, in the University of Texas, Austin, nearly 200,000 electronic records consisting of students' social security numbers had been illegally accessed (Marks 2007) and, on March 11, 2005, a stolen laptop from the University of California, Berkeley exposed names and social security numbers of 98,000 students (Marks 2007). Nevertheless, drawing on the perception of universities' stakeholders, the academic rankings of these universities were not affected at all.

On the other hand, regulative and normative expectations directly influence the universities' and colleges' efforts of staying compliant. There is a high correlation between the regulative and the normative expectations (0.4983), inferring that the interaction between these two expectations would eventually drive information security policy compliance. Market-based model in higher education could explain this high correlation. With dwindling resources (e.g., a decline in state support), higher education gradually adopts market-based model (Dill 2003; Pusser 2002) to provide services (e.g., continuing education) for securing financial health. Essentially, market-based model involves competition in term of tuition fees, proximity (i.e., geographical location) and enrollment space (Leslie and Johnson 1974). A shift to market-based model indicates that higher education become consumer driven (Ruch 2001).

Under the market-based model, higher education will comply with information security regulations (i.e., regulative expectation) to gain competitive advantage if the market demands that universities and colleges should safeguard information security as a mean of exercising Corporate Social Responsibility (CSR). Generally, CSR underscores the organizational activities in favor of social well-being (Campbell 2007), thus representing normative expectation. That is, as the consumers expect higher education to meet social normative expectation through information security safeguard, universities and colleges will comply with information security policy to gain a competitive edge in the consumer driven market. For instance, to exercise CSR through information security safeguard, universities will protect students' social security number (SSN) by using User Access Control (UAC) that allows only a handful of authorized users accessing students' SSN. This enables universities and colleges to abide by information security regulations such as FERPA (i.e., regulative expectation).

Additionally, we assert that, in higher education, the impact of regulative expectation relies on cognitive expectation given the high correlation between cognitive and regulative expectations (0.4209). In the institution of higher education, the cultural-cognitive model represents cognitive expectation with a deeply ingrained sense of obligations toward social progress (Meyer et. al. 2007). Presently, universities and colleges follow this cultural-cognitive model to foster social progress through knowledge creation and dissemination, teaching, and research (Meyer et. al. 2007). Under the prevalence of cognitive influence, regulatory pressure will prevail only when the regulations are consistent with the academic cultural-cognitive model (Dill 1982). That is, although cognitive expectation has no direct impact on information security policy compliance in higher education, the regulative-based legitimacy (i.e., regulative expectation) will take effect only if it is built on the cultural-cognitive model (i.e., cognitive expectation) of higher education. For example, any information security policies that hinder knowledge creation and dissemination, teaching, and research in the institution of higher education will encounter serious resistance that will lead to organizational inefficiency.

On the other hand, despite the severity of regulatory pressure in the banking industry, only normative expectation, but not either regulative expectation or cognitive expectation, directly influences information security policy compliance. Similar to the findings of higher education, the institution of banking relies on the interrelation between regulation and normative expectations to attain information security policy compliance. Although the hypothesis testing results indicate that only the normative expectation directly impacts the internal organizational efforts of staying compliant, the high correlation between the regulation and normative expectations (0.5084) suggests the linkage between both expectations influences information security policy compliance in the banking industry. Enron and WorldCom financial scandals can corroborate this high correlation. After the Enron and the WorldCom scandals, SOX was enacted to mandate banks and financial services to employ the internal controls and procedures for financial reporting. The enactment of SOX imposes regulatory pressure to ensure that the banking organizations exercise ethical conduct for fulfilling social obligation (i.e., normative expectation). That is, federal regulations drive banking organizations to meet the social norm, suggesting the connection between regulative and normative expectations.

Reacting to the present regulatory pressure, the banking industry would build well-defined information security mechanisms that function as a guideline of information security safeguard for the banking organizations. These mechanisms (e.g., IT Governance, COBIT) would develop into the industry security standard and eventually transform to social obligations (i.e., normative expectation) that the banking organizations are expected to live up to (Hu, Hart, and Cooke 2007). In summary, instead of generating direct effect on information security policy compliance in the banking industry, regulative expectation drives normative expectation to attain information security policy compliance.

Additionally, this study reveals that cognitive expectation has no direct impact on information security policy compliance in the banking organizations. Rather, it reflects on how regulatory pressure shapes stakeholder's perception toward information security policy compliance. We maintain that the enactment of information security laws and regulations in the banking industry indicates a rational choice to avoid another financial scandal in the near future. Institution theorist suggested that the process of rational choices propels institutionalization (Scott 2008), leading to new cognitive conception. That is, cognitive elements arise after the process of rational choices (Scott 2008).

The rational choice of forcing regulatory pressure drives organizations to undertake institutionalization, causing the construction of new meanings and values (Zucker 1977). Such regulatory power becomes an impetus that stimulates changes in banking organizations (Hu et al. 2007). For instance, the recent changes in the banking organizations are reflected upon the reality wherein every bank has a compliance officer to supervise the information security policy compliance. Because of these changes, stakeholders gradually form new perceived value of information security hinged on the new meanings related to the criticality of information security. Basically, the process of rational choice explains the high correlation (i.e., 0.4098) between regulative and cognitive expectations in the banking industry.

Conclusion

This study reveals how the differences in institutional environment bring about the differences in information security policy compliance between banking industry and higher education. In the institution of banking, the external environment consists of a strong relationship between regulative and normative expectations. However, only normative expectation directly influences information security policy compliance in the banking industry. That is, developed for handling regulatory pressure, the standard of information security safeguard plays the most significant role in information security policy compliance in the banking industry.

Likewise, the institution of higher education embodies a strong relationship between the regulative and normative expectations but the difference is that both regulative and normative expectations directly affect information security policy compliance. Additionally, a stark contrast between higher education and banking industry with regard to cognitive expectation emerges despite that cognitive expectation does not have any significant effect on information security policy compliance in both industries. The institution of higher education is defined by the prevalence of cognitive expectation since its inception in the medieval period (Meyer et. al. 2007). This suggests that, although cognitive expectation does not display direct effect, its dominance in the institution of higher education produces indirect effect on information security policy compliance through regulative expectation. Conversely, the coercive force associated with regulative expectation instigates changes in the banks, leading to the changes in cognitive expectation. Therefore, cognitive expectation plays a passive role in information security policy compliance in the institution of banking.

Research Implication and Limitation

There are various behavioral researches that study antecedents of individual's policy compliance and non-compliance to produce theoretical foundations related to the technology acceptance model, organizational behavior, social influence etc. (Warkentin and Willison 2009). However, only few studies focus on policy compliance at the industry level. Grounded in NIT, this study contributes to information systems research by highlighting information security policy compliance between banking industry and higher education. This contribution is significant since "*industry receives little attention in information systems research and theory*" despite the important influence of industries on IS activities (Chiasson and Davidson 2005, pg. 591).

Hence, this study differs from many prior behavioral researches of policy compliance in that it (1) highlights the external factors driving information security policy compliance at the industry level and (2) relates the findings of industry compliance to the organizational and individual level of policy compliance. In essence, this study draws a sharp contrast between information security policy compliance in banking industry and in higher education, suggesting theoretical foundation and managerial implication related to policy compliance at both the organizational and individual level.

Theoretical Implication

Drawing on institution theory, banks operate in relational systems with connections between banking organizations and external constituents (Scott 2008, pg. 185). In other words, banks are linked to government agencies, for example, Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and non-profit organizations such as Information Systems Audit and Control Association (ISACA). In the banking relational systems, there is a governance unit that applies regulative and normative controls (Scott 2008, pg. 186) to the banks. Mainly, governance units constitute regularized controls arranged by authorities and legitimate parties (Scott 2008, pg. 186).

This study suggests that, normative expectation, built on regulative expectation, drives information security policy compliance in the banking industry. That is, the governance unit of the banking relational systems exerts normative pressure/expectation hinged on regulatory pressure/expectation to drive banks to comply. Accordingly, normative expectation could form the perceived norms of security policy compliance in the banking organizations. In other words, normative pressure that compels banks to comply with regulations shapes internal organizational norm. This notion aligns with the Fear Appeal Model (FAM) in that social influence, referring to perceived norms within the firm, could promote employees' information security policy compliance (Johnston and Warkentin 2010). Authority could highlight the perceived norms within the firm to cultivate employee's behavior for information security policy compliance.

In this respect, this study proposes a theoretical implication of its findings - in information security policy compliance context, how normative expectation shapes social influence that positively impacts employee's intention to comply (Johnston and Warkentin 2010). In particular, how industry norms shape or relate to organizational norms. For instance, with respect to information security safeguard, a theoretical framework could be established to explain how industry norms (e.g., IT Governance such as COBIT and COSO), defined in the banking relational systems, shape organizational norms/social influence in support of information security policy compliance among employees. This relationship should be investigated across different industries to find a common pattern or the differences.

Additionally, the research findings suggest that cognitive expectation affects regulative expectation in higher education. Unlike the banking industry, higher education functions in cultural-cognitive systems (Meyer et. al. 2007) wherein its cognitive model dictates how universities and colleges should handle regulatory pressure. In particular, cognitive model defines cultural frame that serves to interpret, identify, and perceive events in a way that establishes meanings (Scott 2008, pg. 187). The cultural frame of higher education provides some flexibility for higher education to manage regulatory pressure, thereby allowing higher education to be less strictly accountable for external constituents in term of information security safeguard. Hence, this study proposes that industries operate on a cognitive framework that defines regulatory pressure will less likely be impelled to attain policy compliance. This proposition can serve as a foundation to explore the industry-level and/or organizational compliance from a cognitive perspective.

Managerial Implication

This study makes some suggestions for practical implication as well. Since cognitive expectation is a hidden force in the institution of higher education, promoting information security policy compliance in the university settings would require policy makers to align information security policy with the cognitive model of higher education characterized by academic freedom in favor of knowledge dissemination and creation, innovation research, and teaching. Prior to drafting policies, universities should form collaborative efforts to foster mutual understanding among the policy makers and professors/researchers. With mutual understanding, policy makers can then delineate useful guidelines to safeguard information security while not violating academic freedom. For instance, policy makers can draft a policy that requires academic researchers to encrypt sensitive data and decrypt them using effective mechanism without delaying information sharing.

Additionally, information security policy which aligns with the cognitive model of higher education would promote self-efficacy (Warkentin, Johnston, and Shropshire 2011) that shapes end-user's information security policy compliance (Johnston and Warkentin 2010). This is because information security policy that is relevant to existing cognitive model of higher education would emphasize on situation support (e.g., academic freedom, innovation research) and would also persuade higher education's employees (especially researchers and professors) to participate in information security policy compliance. Situation support and persuasion are major contributors to self-efficacy (Warkentin et al. 2011) that shapes end-user's security policy compliance (Johnston and Warkentin 2010).

On the other hand, normative expectation is a dominant force in the institution of banking. In this respect, policy makers in the banking industry can draft policies to encourage employees to continue their education to learn about the new industry standard for staying complaint. For example, attending conferences held by the Information Systems Audit and Control Association (ISACA) which is a well-respected, non-profit organization in charge of disseminating industry-level knowledge related to information assurance.

In addition, the presence of banking employees in highly recognized conferences and/or workshops will leave an impression that banks are paying attention to the industry-level mechanism of information security safeguard. That is, banks are aware of the industry norms for information security protection. This will make banks appear legitimate, enabling them to fulfil normative-based legitimacy.

Limitation

Finally, this study is not without limitation. This study encountered difficulty in data collection and the sample size was relatively small (N=108 and 100 for banking industry and higher education respectively). Another limitation is the generalizability of the research findings. This study mostly collected data of higher education from only three public colleges and universities. Additionally, this study collected banking data from only three community and commercial banks in the Midwest region of the U.S.. Hence, the researchers may want to exercise their judgment when referencing these research findings.

References

Argyris, C. 1958. "Some Problems in Conceptualizing Organizational-Climate - A Case-Study of a Bank," *Administrative Science Quarterly* (2:4), pp. 501-520.

Behery, M. H. and Eldomiaty, T. I. 2010. "Stakeholders-oriented Banks and Bank Performance. Perspective from International Business Management," *International Journal of Commerce and Management* (20:2), pp. 120 – 150.

Bullock, G. 2003. "Culture and Banking – Banking and Culture," Retrieved from http://www.ubs.com/1/ShowMedia/bank_for_banks/news/archive?contentId=28299andname=N4B%20August%202003.pdf.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., and Boss, R.W. 2009. "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Campbell, J. 2007. "Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility," *Academy of Management Review* (32:3), pp. 946-67.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy and Security* (1:3), pp. 18–41.

Chin, W.W. 1998. *The Partial Least Squares Approach to Structural Equation Modeling*, Lawrence Erlbaum Associates, Mahwah, NJ.

Chin, W.W. and Newsted, P.R. 1999. "Structural Equation Modeling analysis with Small Samples Using Partial Least Squares," in R. Hoyle (Ed.), *Statistical Strategies for Small Sample Research*, Sage.

Davis, S. 2004. "Culture In Banking: The 'Soft Stuff' Drives the Hard Results", Retrieved from www.dibc.co.uk/culture_in_banking.pdf.

Dill, D.D. 1982. "The Management of Academic Culture: Notes on the Management of Meaning and Social Integration," *Higher Education* (11:3), pp. 303-320.

Dill, D.D. 2003. "Allowing the Market to Rule: The Case of the United States," *Higher Education Quarterly* (57:2), pp. 136-157.

DiMaggio, P.J. and Powell, W.W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", *American Sociological Review* (48:2), pp. 147-160.

Earp, B.E. and Payton, F.C. 2006. "Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professional," *Journal of Organizational Computing and Electronic Commerce* (16:2), pp. 105-122.

Elliott, R., Young M. O., Collins, V. D., Frawley, D. and Temares, M. L. 1991. Information Security in Higher Education. Boulder, CO: The Association Management of Information Technology in Higher Education.

Fornell, C. and Larcker, D. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Gefen, D. and Straub, D.W. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of AIS*, 16 (1), pp. 91-109.

Gross, K. and Godwin, P. 2005. "Education's Many Stakeholders," *Universities Businesses*, Retrieved from http://www.universitybusiness.com/viewarticle.aspx?articleid=174

Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures," *Information and Management* (20:1), pp. 13-27.

Haenlein, M. and Kaplan, A.M. 2004. "A Beginner's Guide to Partial Least Squares Analysis," *Understanding Statistics* (3:4), pp. 283 – 297.

Harris, S. 2006. "How to Write an Information Risk Management Policy," *TechTarget*, Retrieved from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1178845_mem1,00.html.

Hawley, A. 1968. Human Ecology. pp. 328-37 in David L. Sills (Ed.), International Encyclopedia of the Social Sciences. New York, NY: MacMillan

Herath, T. and Rao, H.R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Henseler, J., Ringle, C.M., and Sinkovics, R.R. 2009. “The Use of Partial Least Squares Path Modeling in International Marketing,” *Advances in International Marketing,* 20*,* 277-319.

Hrebiniak, L. G. and Snow C. C. 1980. “Industry Differences in Environmental Uncertainty and Organizational Characteristics Related to Uncertainty”, *The Academy of Management Journal* (23:4), pp. 750-759

Hu, Q., Hart, P., and Cooke, D. 2007. “The Role of External and Internal Influences on Information Systems Security – A Neo-Institutional Perspective,” *Journal of Strategic Information Systems* (16:2), pp. 153-172.

Interligi, L. 2010. “Compliance Culture: a Conceptual Framework,” *Journal of Management and Organization* (16:2), pp. 235-249.

Javernick-Will, A. and Levitt, R. 2010. “Mobilizing Institutional Knowledge for International Projects,” *Journal of Construction Engineering and Management* (136:4), pp. 430-441.

Johnston, A. C. and Warkentin, M. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Quarterly*, (34:3), pp. 549–566.

Kostova, T. and Roth, K. 2002. “Adoption of an Organizational Practice by Subsidiaries of Multinational Corporations: Institutional and Relational Effects,” *Academy of Management Journal* (45:1), pp. 215-233.

Kvavik, R.B. 2004. “Information Technology Security: Governance, Strategy and Practice in Higher Education”, *EDUCAUSE* (5).

Leslie, L. L. and Johnson, G. P. 1974. “The Market Model and Higher Education,” *The Journal of Higher Education* (45:1), pp. 1-20.

Marks, A. 2007. “Exploring Universities’ Information Systems Security Awareness in a Changing Higher Education Environment: A Comparative Case Study Research,” Ph.D. Thesis, University of Salford.

Mathieson, K., Peacock, E., and Chin, W.W. 2001. “Extending the technology acceptance model: the influence of perceived user resources,” *The data base for advances in information systems* (32:3), 86–112.

Meyer, J. W., Ramirez F. O., Frank, D. J. and Schofer, E. 2007. *Higher Education as an Institution, In Sociology of Higher Education: Contributions and Their Contexts*, Johns Hopkins University Press, Baltimore, MD.

Meyer, J.W. and Rowan, B. 1977. “Institutionalized Organizations - Formal-Structure as Myth and Ceremony,” *American Journal of Sociology* (83:2), pp. 340-363.

Nasser, F. and Wisenbaker, J. 2003. “A Monte Carlo Study Investigating the Impact of Item Parceling on Measures of Fit in Confirmatory Factor Analysis,” Educational and Psychological Measurement (63:5), pp. 729-757.

Pusser, B. 2002. “Higher Education, the Emerging Market and the Public Good,” In P.A. Graham & N. Stacey (Eds.), *The Knowledge Economy and Postsecondary Education.* (pp. 105-125). Washington, D.C.: National Academy Press.

Reis, R.M. 1997. *Tomorrow’s Professor: Preparing for Academic Careers in Science and Engineering*, Wiley-IEEE Press, Picataway, NJ.

Rezgui, Y. and Marks, A. 2008. “Information Security Awareness in Higher Education: An Exploratory Study,” *Computers and Security*, 27(7-8), pp. 241-253.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). “Not So Different After All: A Cross-Discipline View of Trust,” Academy of Management Review, 23 (3), pp. 393-404.

Ruch, R. S. 2001. Higher Education Incorporated: The Rise of the for-profit University, Baltimore, MD: The John Hopkins University Press and Baltimore.

Scott, W.R. 1995. *Institutions and Organizations*, Sage, Thousand Oaks, CA.

Scott, W.R. 2008. *Institutions and Organizations, Ideas and Interest 3rd Edition*, Sage, Thousand Oaks, CA.

Suchman, M.C. 1995. “Managing Legitimacy - Strategic and Institutional Approaches,” *Academy of Management Review* (20:3), pp. 571-610.

Symantec Internet Security 2001. Threat Report Trends for 2009. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D. 2008. “Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture,” *Journal of Management Information Systems* (24:4), pp. 73-100.

Warkentin, M., Johnston A. C. and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems*, (20:3), pp. 267 - 284.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105

Weick, K. 1976. Educational organizations as loosely coupled systems. *Administrative Science Quarterly* (21:1), pp. 1–19.

White, J.C., Varadarajan, P.R., Dacin, P.A. 2003. "Market situation interpretation and response: the role of cognitive style, organizational culture, and information use," *Journal of Marketing* (67:3), pp. 63–79.

Yeh, Q. and Chang, A. J. 2007. "Threats and Countermeasures for Information System Security: A Cross-Industry Study," *Information and Management* (44:5), pp. 480-491.

Zucker, L. G. 1977. "The Role of Institutionalization in Cultural Persistence," *American Sociological Review* (42:5), pp. 726-743.

Zwikael, O. and Ahn, M. 2011. "The Effectiveness of Risk Management: an Analysis of Project Risk Planning across Countries and Industries," *Risk Analysis* (31:1), pp. 25-37.