Winter 12-13-2015

Organizational Security Norms in the Banking Industry: The United States vs. South Korea

Hwee-Joo Kam
Ferris State University

Sanjay Goel
University at Albany, State University of New York

Pairin Katertannakul
Western Michigan University

Soo-Goo Hong
Dong-A University

Organizational Security Norms in the Banking Industry: The United States vs. South Korea

Hwee-Joo Kam, D.Sc.
Ferris State University
Big Rapids, MI. USA

Sanjay Goel, Ph.D.
University at Albany, State University of New York
Albany, NY. USA

Pairin Katertannakul, Ph.D.
Western Michigan University
Kalamazoo, MI.

Soo-Goo Hong, Ph.D.
Dong-A University
Busan, South Korea

ABSTRACT

This study-in-progress examines the similarities and differences in organizational security norms between the banking industry in the United States and South Korea. Organizational security norms refers to appropriate actions related to information security safeguard. Drawing on the Competing Value Framework (CVF), Neo-Institutional Theory (NIT), and Hofstede's Cultural Framework, this study proposes an integrated theoretical framework to assess the impact of national culture, organizational culture, and industry on organizational security norms among the banking employees. In general, this study intends to contribute (1) a theoretical framework encompassing national, organizational and industry cultures, and (2) practical implications to improve information security safeguard in multiple cultural settings.

Keywords: *Organizational culture, norms, security norms, banking industry, national culture*

INTRODUCTION

Cyberattacks are of great concern in the banking industry. In 2015, it was reported that a cybercrime group named "Anunak hackers group" or "Carbanak" stole 1 billion dollars from more than 100 banks worldwide through malware attack (Lennon 2015). The South Korean banking network was also under attack by a malware called "DarkSeoul," paralyzing the entire banking network and rendering ATM machines unusable (Sang-Hun 2013). Banks are mandated to protect customer data. However, as cyberattacks can steal confidential financial data, they can also evoke identity theft, endangering many

individuals' financial wellbeing. Presently, banks in the U.S. face immense pressure to comply with such information security regulations as Gramm Leach Bliley Act (GLBA), a comprehensive federal law that requires financial institutions to develop, implement, and maintain administrative, technical, and physical controls for protecting the security, integrity, and confidentiality of customer data. The Korean government has enacted The Act on Real Name Financial Transactions and Guarantee of Secrecy to protect the privacy of financial transactions, and The Act on the Use and Protection of Credit Information to prohibit misuse of credit information (Cho, Kim and Lee 2015)

In light of security threats, several studies have examined cultural factors at the individual levels in the Information Systems Security (ISS) literature (Dinev, Goo, Hu and Nam 2009; Interligi 2010; Da Veiga and Eloff 2010; Hu, Dinev, Hart and Cooke 2012; Hovav and D'Arcy 2012; Kim, Ryu and Kwark 2013; Rocha Flores, Antonsen and Ekstedt 2014; Dincelli and Goel, 2015). However, there is a lack of research examining the national-, organizational-, and industry-levels to shed light on the organizational security norms. Sociologists define norms as an individuals understanding what others do and think what society expects them to do (Sherif, 1936). We consider security norms as perception that an individual has about adhering the security practices in organization. There are several unanswered questions regarding influence of culture on security norms. For instance, does national culture have a heavier influence on organizational security norms in a highly regulated industry, such as banking? Or does an industry's stringent regulatory requirement supersede a national culture? Does organizational culture have an upper hand on shaping organizational security norms? Above all, how do organizational culture, national culture, and industry environment relate to each other in the context of organizational security norms?

This study develops an integrated model to examine the effects of national culture, industry environment, and organizational culture on organizational security norms in the banking industry of the United States and South Korea. The purpose is twofold: to contribute a theoretical framework of cultural and industry effects on organizational security norms; and to propose practical suggestions for effectively implementing security practices in multiple cultural settings.

This study draws on Competing Values Framework (CVF) (Quinn and Rohrbaugh 1983), Neo-Institutional Theory (NIT) (Meyer and Rowan 1977; DiMaggio and Powell 1983), and Hofstede's cultural framework (Hofstede 1983). There are two reasons for the study's specific focus on the banking industry. First, as most banks are saddled with regulatory pressures to comply with information security policies (ISP), compliance is highly applicable to the banking industry, and therefore, it is appropriate to measure organizational security norms in relation to ISP compliance in the banking industry. Second, there is homogeneity in compliance culture in a highly regulated industry (Interligi 2010) due to isomorphism, in that one industry member coerces another to conform to reach resemblance (DiMaggio and Powell 1983). That is, banking industries around the world may share some similarities despite differences in national culture, so it is feasible to do a comparison of organizational security norms across nations. This study focuses on the United States and South Korea because their distinctive differences in national culture (Hofstede 1983) will highlight the influence of national culture, enabling this study to provide meaningful implications.

LITERATURE REVIEW

Institutional Environment

Institutional theory (Scott 1995) suggests that industry is an institution that serves as a template to guide appropriate organizational actions and behaviors. Institutional environment represents industry's environment shaped by regulatory pressures and stakeholder's demands (Scott 1995). Since industry's institutional environment differs across industries (Chatmand and Jehn 1994), each industry encounters distinctive environmental complexity that increasingly builds unique industry characteristics (Gordon 1991). As a result, industry characteristics reflect upon its institutional environment. For instance, as the banking industry confronts strict regulatory pressure, banks must outline policies to comply with stringent regulations; this gradually turns banking into a highly regulated industry, and this particular trait comes to exemplify the banking's institutional environment.

Drawing on Neo-Institutional Theory (NIT), institutional environment constitutes regulatory, normative, and cognitive pressures (Meyer and Rowan 1977; DiMaggio and Powell 1983). Whereas

regulatory pressure refers to pressures of sanctioning and monitoring both formal and informal rules, normative pressure refers to expectations of meeting societal norms (the right thing to do) (DiMaggio and Powell 1983; Scott 1995). Cognitive pressure refers to a perception about an occurrence, entity or object, given the shared belief systems (DiMaggio and Powell 1983; Scott 1995). That is, how stakeholders perceive the criticality of information security and data breaches is based on their shared cultural framework. In short, an organization's institutional environment, consisting of regulatory, normative, and cognitive pressures, compels organizations to conform (Meyer and Rowan 1977; DiMaggio and Powell 1983).

Finally, as cultural and legal factors vary across nations, the institutional environment shaped by those factors may show some distinctiveness across nations (Rosenzweig and Singh 1991). Specifically, the institutional environment of banking for one nation may differ from the institutional environment of banking in other nations. Hence, this study examines the institutional environment of banking in the U.S. and South Korea.

Banking Industry

Overall, the distinctive traits of banking culture are hierarchical and competitive (Claessens 2012). Banks operate in relational systems constituting a governance unit that monitors banking regulative and normative controls (Scott 2008). Governance units refer to regularized controls organized by authorities (Scott 2008). For example, banks in the United States are related to Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC). Similarly, banks in South Korea must be insured by Korean Deposit Insurance Fund (KDIC), under the Depositor Protection Law. Also in South Korea, under the PCA (Prompt Corrective Action) system introduced in 1998, an authorized financial supervisory can mandate an order to any financial institutions that perform poorly (Kim, Kim and Ryoo 2006). These relational systems create a regulatory environment (Park and Weber 2006), causing banks to outline formal policies and procedures.

Accordingly, banks in the United States and South Korea are facing tremendous pressure to comply with regulations. In the United States, after the financial scandal involving Enron and WorldCom, the

banking industry has been confronting immense pressure to comply with regulations such as Sarbanes-Oxley Act (SOX) of 2002, which dictates standard accounting and financial reporting. In addition, banks in the United States are mandated to abide by Gramm Leach Bliley Act (GLBA), a comprehensive federal law that requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards for defending the security, integrity, and confidentiality of customer information.

In South Korea, after the financial crisis in 1997-1998, the government re-regulated the banking industry (Park and Weber 2006) to restore public confidence in the banking system by making the system more liable, transparent, and effective (Banker, Chang, and Lee 2010). The Korean government has also enacted the Personal Information Protection Act of 1995 to protect the privacy of citizens from unauthorized data collection and leakage (Greenleaf 2011). Furthermore, the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001 mandates entities which use computers and networks to process personal data for profit, to safeguard personal data for preventing data breaches (Greenleaf 2011).

Finally, U.S. banks suffered from a sophisticated attack launched by the "Carbanak" hacking group (Lennon 2015), and Korean banks were attacked by a malware called "DarkSeoul" (Sang-Hun 2013). Both incidents received wide news coverage, inferring that there is a growing awareness among stakeholders in relation to banking security. This may generate increased pressure on banks to protect their customers' financial data.

Banking Industry: USA vs. South Korea

		USA	**South Korea**
Regulatory Pressure	**Governance Structure**	Regulated by Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC)	Regulated by Korean Deposit Insurance Fund (KDIC) and monitored under the law of PCA (prompt corrective action)
	Regulatory compliance	Banks are mandated to comply with SOX and GLBA	Comply with (1) Personal Info. Protection Act; (2) Act on Promotion of Info. & Comm. Network Utilization and Info. Protection 2001
Normative Pressures	**Reform of Banking Systems**	Following the Enron financial scandals, the U.S. government enacted SOX to mandate standardized financial reporting.	Following the Asian economic crisis, the Korean government re-regulated the banking systems to restore public confidence.

	Normative Beliefs	This reflects upon the normative belief that the financial systems cannot "cook the book" and must be ethical to the stakeholders.	This reflects upon the normative belief that the financial systems must be responsible to the social welfare as well as the nation's wellbeing.
Cognitive Pressure	**Incidents of Data Breaches**	Some of the U.S. banks suffered from suffered from a sophisticated attack by "Carbanak" hacking group.	The Korean banks were attacked by a malware called "DarkSeoul", rendering the ATM machines unusable.
		The exposure of this incident to the public infers that there is a growing awareness among people, and increasing security concerns among the stakeholders.	Customers failed to withdraw money from the ATM machines due to hacking. This infers that there will be a growing concern about banking security.

Table 2. The Banking System: USA vs. South Korea

Competing Values Framework (CVF)

Organizational culture also refers to taken-for-granted values and assumptions in organizations, representing a collective set of expectations, definition and memories in the organizational setting (Quinn and Rohrbaugh 1983; Schein 1984). That is, organizational culture represents an implicit, internal social system that exudes its influences on organizational practices, strategic planning, and employee behavior. As a result, organizational behavior, decision making, and employees' daily operations align with organizational culture.

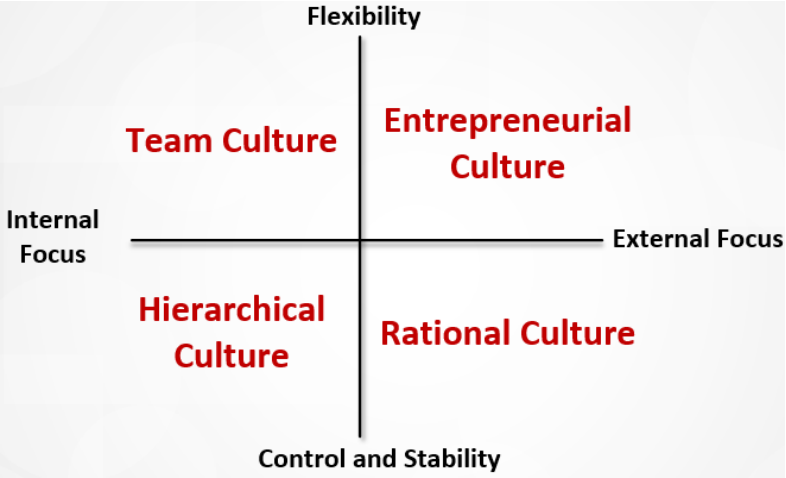

Figure 1. Competing Values Framework (CVF) (Denison and Spreitzer 1991)

This study adopts Competing Values Framework (CVF). Health care research has widely adopted CVF to measure organizational effectiveness for job performance, quality services, etc. (Helfrich et al. 2007)

through organizational culture. CVF is a well-validated framework tailored to examine a global view of organizational culture (Scott, Mannion, Davies and Marshall 2003) for this quantitative study. Some may argue that a quantitative approach will inhibit an in-depth study of organizational culture. However, using a quantitative approach to examine organizational culture *"may be more practical for purposes of analyzing data-based change in organization"*, especially for studies that use cross-sectional comparison (Cooke and Rousseau 1988). As this study conducts a cross-national assessment of organizational culture, CVF is an appropriate framework for data interpretation.

CVF assumes that organizational culture is shaped by human systems that are inherently fraught with competing tensions (Quinn and Rohrbaugh 1983). CVF investigates organizational culture by suggesting that conflicting tensions can be used to uncover *"the basic assumptions that are made about such things as the means to compliance, motive, leadership, decision making, effectiveness, values, and organizational forms"* (Quinn and Kimberly 1984). Mainly, the concept of competing tensions is represented by two dimensions: (1) flexibility vs. stability and control, in which organizations will tilt toward either flexibility for changes, or stability to retain control; and (2) internal focus vs. external focus, in which organizations will prefer either improving the existing organization, or adapting with the external environment (Quinn and Rohrbaugh 1983). The intersections of these two dimensions shape four archetypes in organizational settings: hierarchical, rational, entrepreneurial, and team cultures (Denison and Spreitzer 1991) (Figure 1). An organization may espouse one or more cultures, as depicted below. A combination of different cultural types defines an organization, shaping values, conflict, and tensions.

Focusing on human relations, *team culture* highlights flexibility and change in organizations (Denison and Spreitzer 1991). The core values constituting trust, belonging, participation, and teamwork propel leaders to act supportively and considerately for developing human potential and memberships (Denison and Spreitzer 1991). Like team culture, *entrepreneurial culture* values flexibility and change, but its external focus promotes growth, resource acquisition, and adaptation to the external environment (Denison and Spreitzer 1991). Leaders are entrepreneurial, risk takers and visionary, striving to achieve visibility, legitimacy, and external support (Denison and Spreitzer 1991).

At the other end of the spectrum, *rational culture* emphasizes achieving well-defined objectives by directing organizational members to become more competitive and successful (Denison and Spreitzer 1991). Leaders are very goal-oriented, directive, and effective to facilitate high productivity and efficiency for winning market competition (Denison and Spreitzer 1991). On the other hand, *hierarchical culture* emphasizes internal efficiency, homogeneity and coordination to maintain internal security, control, and stability (Denison and Spreitzer 1991). Leaders are methodical, conservative, and rule enforcers who exert control to bring order through attention to technical matters (Denison and Spreitzer 1991).

HYPOTHESES DEVELOPMENT

Prior studies suggested that organizational culture is partly shaped by industry (Chat and Jehn 1994; Dastmalchian, Lee, and Ng 2000; Gordon 1991). Particularly, an industry's institutional environment compels organizations under the same industry to adopt appropriate organizational culture for survival (DiMaggio and Powell 1983). As noted, institutional environment is built on cultural values and norms (Scott 1995; Scott 2008; Zucker 1977), and therefore, banking's institutional environment in one nation may demonstrate some differences from the other nations due to cultural differences (Rosenzweig and Singh 1991). Surveying different industries across Canada and South Korea, a prior study revealed that differences in the same industry across nations can be attributed to the differences in national culture (Dastmalchian, Lee, and Ng 2000). In this respect, our goal is to study the impact of national culture and organizational culture on perceived security norms in an organization. We define four hypotheses each based on one of the four quadrants of Competing Value Framework and evaluate its impact on security norms in an organization.

National culture interacts with organizational culture (Dastmalchian, Lee, and Ng 2000; Trompenaars and Hampden-Turner 1998) in that national culture produces moderating effects (Dinev, Goo, Hu, and Nam 2009) on employees' perception of security (Hovav and J. D'Arcy 2012). Prior studies have proven the moderating effects of national culture (Dinev, Goo, Hu, and Nam 2009). In particular, this study argues national culture moderates the relationship between organizational culture and perceived security norms because both national culture (Hofstede 1983) and organizational culture (Schein 1984) produce values and

norms; and two different sets of values and norms may either synchronize or collide with each other. That is, national culture may enervate organization culture whose values are in contrary to those of the national culture. Therefore, national culture moderates the aforementioned relationship to either weaken or strengthen the relationship in the context of perceived security norms.

As organizational culture affects how an employee thinks, feels, and perceives (Schein 1984), this study proposes that organizational culture drives employee's perceived security norms with national culture as a moderator. Perceived security norms (subjective norms) refer to informal rules that monitor an employee's conduct (Feldman 1984), creating powerful effects on his/her behaviors. As perceived security norms dictate "the right thing" (Herath and Rao 2009), perceived security norms encourage an employee's compliance behavior (Herath and Rao 2009; Johnston and Warkentin 2010).

Particularly in a nation with high uncertainty avoidance (i.e. South Korea), people tend to prefer a well-defined working structure, and to follow rigid instructions (Hofstede 1983). This represents a stark contrast to entrepreneurial cultures that promote flexibility. In particular, an entrepreneurial culture cultivates flexibility, thereby minimizing the rigid and clear rules required by employees living in a culture of high uncertainty avoidance (Newman and Nollen 1996). Particularly, employees from a nation of high uncertainty avoidance require a set of well-defined rules to comply with ISP; but entrepreneurial culture does not facilitate these rules to enforce security practices.

On the other hand, people living in a nation of low certainty avoidance (i.e. the United States) would prefer to work in a more flexible environment, thereby aligning with the values of the entrepreneurial culture that encompasses flexibility, innovation, and risk-taking (Denison and Spreitzer 1991). As an entrepreneurial culture interacts with a national culture of low uncertainty avoidance, organizations appreciate flexibility rather than strict monitoring, thus making it more difficult to monitor employees' behavior for ISP enforcement. Without being able to enforce ISP, it becomes hard to cultivate employees' perceived security norms. Accordingly, entrepreneurial culture will produce no significant impact on perceived security norms in U.S. banks.

H1: In the banking industry, the impact of entrepreneurial culture on perceived security norms is more negative in a nation of high uncertainty avoidance than in a nation of low uncertainty avoidance.

Employees from a collectivist nation perceive teamwork as a permanent and long-term activity, but employees from individualistic nations view teamwork as something transitory and task-specific (Gibson and Zellmer-Bruhn 2001). Team work can have significant impact on the responsibility users feel towards collective security of the organization. Where collectivist cultures are more receptive to teamwork (Kirkman and Shapiro 2001) and enhance team cooperation for team performance (Eby and Dobbins 1997), individualistic cultures allow individuals to resist teamwork through limited pressure to conform (Kirkman and Shapiro 2001).

East Asian countries like South Korea generally embrace team culture as a means to maintain harmony within in-group (Triandis et al. 1988). In collectivist cultures, in-group refers to a social group that is interested in one's welfare (Triandis et al. 1988). As collectivist culture encourages employees to spend private time together (Hofstede 1983), a group of people working together can be considered as an in-group. In a highly regulated industry (i.e. banking) where security compliance is important, team leaders in a collectivist culture will be under pressure to mandate security compliance among the team members; and team members will be obliged to comply, and not challenge the leader's request for maintaining group harmony. That is, team members are expected to practice *Inhwa*, referring to maintaining harmony and showing loyalty to their in-groups (Lee 2012). The *Inhwa* culture promotes clan management, thereby supporting compliance through "clan" leadership (Lee 2012) and fosters perceived security norms leaning toward compliance.

H2: In the banking industry, team culture generates higher impact on perceived security norms in a nation of high collectivism and low individualism, than in a nation of high individualism and low collectivism

This study also proposes that a rational culture in nations embracing long-term orientation (Hofstede and Bond 1988) is more effective in enhancing employee's perceived security norms. As noted, pragmatism espoused by long-term orientation augments the efficiency advocated by a rational culture. There are two alternate processes of human decision making system 1 and system 2. System 1 is fast, automatic, intuitive

approach, while System 2 is slower, analytical mode, where reason dominates. Rational culture would encourage more deliberate long-term thinking that would lead to a culture encouraging more rational security decisions that we believe would be more precise and appropriate.

H3: In the banking industry, a rational culture generates higher impact on perceived security norms in a nation of long-term orientation than in a nation of short-term orientation

The South Korean culture emphasizes vertical relationships (i.e. Father-Son, Supervisor-Subordinate etc.), in that respect to authority is highly emphasized (Lee 1998). In this context, power distance based on respect to authority aligns with hierarchical culture for authoritarian leadership (Denison and Spreitzer 1991). Therefore, in a nation of high power distance (i.e. South Korea), hierarchical culture is strengthened to effectively enforce ISP. As organizations highlight the importance of ISP, employees will perceive that information security safeguard is important (Boss et al. 2009), increasing their perceived security norms. Conversely, low power distance may diminish hierarchical culture, rendering hierarchical culture less effective in enforcing ISP. In a nation of low power distance (i.e. the U.S.), employees may not easily give in to their superiors' demands, thus undermining the power structure in hierarchical culture. As a result, hierarchical culture in a nation of low power distance is not as effective as that in a nation of high power distance in cultivating perceived security norms.

H4: In the banking industry, hierarchical culture generates higher impact on perceived security norms in a nation of high power distance than in a nation of low power distance

Our conceptualized model and the hypotheses can be seen in Figure 2.

RESEARCH METHODOLOGY

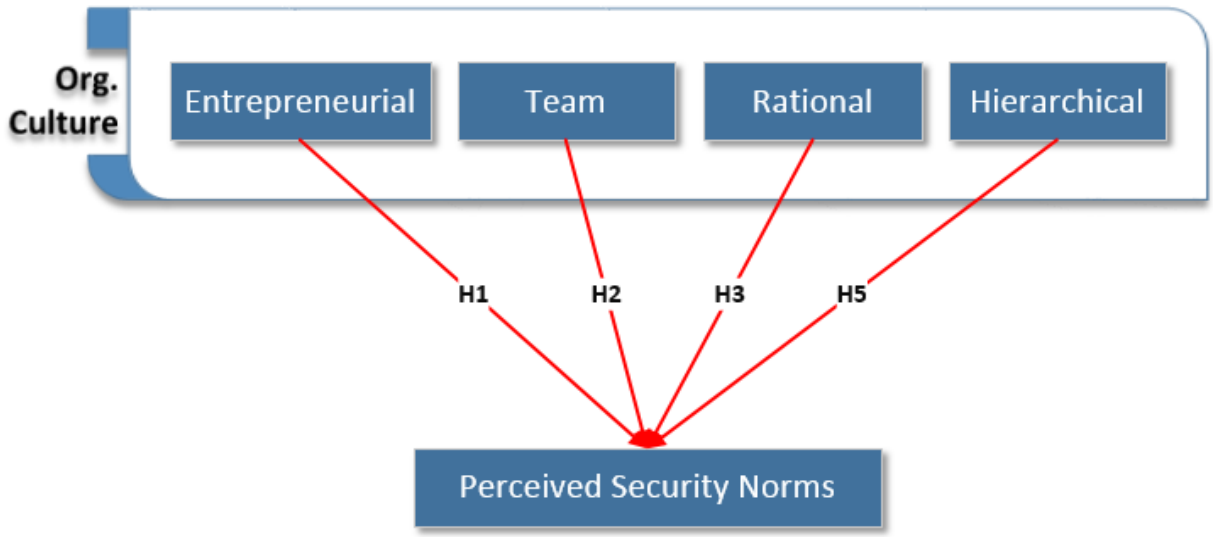

Figure 2. Proposed Research Model

We formed an online survey using 7-points Likert scales, with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree. We adapted measurement items from the prior literature (Helfrich et al. 2007; Herath and Rao 2009). We ran a pilot study by sending out online surveys to banking employees in the U.S., and after two months, received 51 responses (N=51). On reviewing feedback from the banking participants, we modified our measurement items. Finally, our measurement items consist of 8 reflective constructs: team culture (TEAM), entrepreneurial culture (ENT), rational culture (RAT), hierarchical culture (HIE), perceived security norms (NORM).

This study employs SmartPLS 3.0 software that supports component-based path modelling, enabling us to work with small sample size (Chin 1998). In contrast to the covariance-based Structural Equation Modelling (SEM) that requires a sample size over 100 observations, the component-based Partial Least Squares (PLS) path modelling has the ability to operate with a sample size as small as 50 (Chin 1998). Our sample sizes for the U.S. banks are relatively small (N=128 for U.S. and N=121 for South Korea), thus making PLS a viable choice.

CONCLUSION

This study proposes an integrated model to examine differences in organizational security norms in the banking industry between the United States and South Korea. This research contributes to the ISS field with a theoretical framework encompassing national and industry impacts on organizational security norms; and practical implications for adopting IT governance frameworks and security practices in multiple cultural settings. Finally, this study, a research-in-progress, will continue its data analysis to derive further meaningful conclusions.

There are very serious practical implications of this work especially as banks struggle to motivate the users to improve their security behavior understanding the prevalent security norms will help banks put together programs that work towards complementing or shifting the security norms in an organization. This research can also help organizations identify better candidates from a security perspective during recruitment by understanding their basic personalities and understanding of security norms. In other words, the research findings will have practical relevance, thereby contributing to the information systems security (ISS) literature (Siponen and Vance 2014).

References

Abrams, D., Ando, K., & Hinkle, S. (1998). Psychological Attachment to the Group: Cross-Cultural Differences in Organizational Identification and Subjective Norms as Predictors of Workers' Turnover Intentions. *Personality and Social Psychology Bulletin*, *24*(10), 1027-1039.

Allaire, Y., & Firsirotu, M. E. (1984). Theories of Organizational Culture. *Organization Studies*, *5*(3), 193–226.

Banker, R. D., Chang, H., & Lee, S.-Y. (2010). Differential Impact of Korean Banking System Reforms on Bank Productivity. *Journal of Banking & Finance*, *34*(7), 1450–1460.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & 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), 151–164.

Cameron, K. S., & Quinn, R. E. (2005). *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework*. John Wiley & Sons.

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.

Chen, C. C., Chen, X.-P., & Meindl, J. R. (1998). How can Cooperation be Fostered? The Cultural Effects of Individualism-Collectivism. *Academy of Management Review*, *23*(2), 285–304.

Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. *Modern Methods for Business Research*, *295*(2), 295–336.

Cho, C.-H., Ahn, C. S., Kim, S. J., & Lee, H. S. (n.d.). PLC - Doing business in South Korea. Retrieved September 16, 2015, from http://us.practicallaw.com/5-501-0628

Claessens, R. (2012). *Corporate Culture in Banking*. UK: AuthorHouse.

Cohen, J. (2013). *Statistical Power Analysis for the Behavioral Sciences*. Academic Press.

Cooke, R. A., & Rousseau, D. M. (1988). Behavioral Norms and Expectations A Quantitative Approach to the Assessment of Organizational Culture. *Group & Organization Management*, *13*(3), 245–273.

Dastmalchian, A., Lee, S., & Ng, I. (2000). The Interplay between Organizational and National Cultures: A Comparison of Organizational Practices in Canada and South Korea Using the Competing Values Framework. *The International Journal of Human Resource Management*, *11*(2), 388–412.

Da Veiga, A., & Eloff, J. H. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, *29*(2), 196–207.

Davis, S. (2004). Culture In Banking: The "Soft Stuff"Drives the Hard Results. *Accountancy Ireland, October*, 15–17.

Denison, D. R., & Spreitzer, G. M. (1991). Organizational Culture and Organizational Development: A Competing Values Approach. *Research in Organizational Change and Development*, *5*(1), 1–21.

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.

Dincelli, E., & Goel, S. (2015, October). Research Design for Study of Cultural and Societal Influence on Online Privacy Behavior. In Proceedings of 2015 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, Newark, Delaware.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User Behaviour towards Protective Information Technologies: The Role of National Cultural Differences. *Information Systems Journal*, *19*(4), 391–412.

Earley, P. C., & Gibson, C. B. (1998). Taking Stock in Our Progress on Individualism-Collectivism: 100 Years of Solidarity and Community. *Journal of Management*, *24*(3), 265–304.

Eby, L. T., & Dobbins, G. H. (1997). Collectivistic Orientation in Teams: An Individual and Group-Level Analysis. *Journal of Organizational Behavior*, *18*, 275–295.

Feldman, D. C. (1984). The Development and Enforcement of Group Norms. *Academy of Management Review*, *9*(1), 47–53.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014a). Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. *Computers & Security*, *43*, 90–110.

Gibson, C. B., & Zellmer-Bruhn, M. E. (2001). Metaphors and Meaning: An Intercultural Analysis of the Concept of Teamwork. *Administrative Science Quarterly*, *46*(2), 274–303.

Gómez, C., Kirkman, B. L., & Shapiro, D. L. (2000). The Impact of Collectivism and In-Group/Out-Group Membership on the Evaluation Generosity Of Team Members. *Academy of Management Journal*, *43*(6), 1097–1106.

Gordon, G. G. (1991). Industry Determinants of Organizational Culture. *Academy of Management Review*, *16*(2), 396–415.

Greenleaf, G. (2011). Asia-Pacific Data Privacy: 2011, Year of Revolution? *Kyung Hee Law Journal, Forthcoming*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?Abstract_id=1914212

Gundlach, M., Zivnuska, S., & Stoner, J. (2006). Understanding the Relationship between Individualism–Collectivism and Team Performance through an Integration of Social Identity Theory and the Social Relations Model. *Human Relations*, *59*(12), 1603–1632.

Helfrich, C. D., Li, Y.-F., Mohr, D. C., Meterko, M., & Sales, A. E. (2007). Assessing an Organizational Culture Instrument based on the Competing Values Framework: Exploratory and Confirmatory Factor Analyses. *Implementation Science*, *2*(13), 1–14.

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.

Hofstede, G. (1983). The Cultural Relativity of Organizational Practices and Theories. *Journal of International Business Studies*, 75–89.

Hofstede, G. (1991). *Cultures and Organizations: Software of the Mind : Intercultural Cooperation and Its Importance for Survival*. London ; New York: McGraw-Hill.

Hofstede, G., & Bond, M. H. (1988). The Confucius Connection: From Cultural Roots to Economic Growth. *Organizational Dynamics*, *16*(4), 5–21.

Hogg, M. A., & Reid, S. A. (2006). Social Identity, Self-Categorization, and the Communication of Group Norms. *Communication Theory*, *16*(1), 7–30.

Hovav, A., & D'Arcy, J. (2012). Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in The US and South Korea. *Information & Management*, *49*(2), 99–110.

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

Interligi, L. (2010). Compliance Culture: A Conceptual Framework. *Journal of Management & Organization*, *16*(2), 235–249.

Jetten, J., Postmes, T., & McAuliffe, B. J. (2002). We're all Individuals': Group Norms of Individualism and Collectivism, Levels of Identification and Identity Threat. *European Journal of Social Psychology*, *32*(2), 189–207. http://doi.org/10.1002/ejsp.65

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

Kim, S.-M., Kim, J.-Y., & Ryoo, H.-T. (2006). Restructuring and Reforms in the Korean Banking Industry. In *Participants in the meeting* (p. 259). Retrieved from http://papers.ssrn.com/sol3/Delivery.cfm?abstractid=1188516#page=266

Kirkman, B. L., & Shapiro, D. L. (2001). The Impact of Cultural Values on Job Satisfaction and Organizational Commitment in Self-Managing Work Teams: The Mediating Role of Employee Resistance. *Academy of Management Journal*, *44*(3), 557–569.

Kong, K. (2012, January 13). Third Apparent Suicide in Korea Savings Bank Scandal. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052970204409004577156293952924250

Lee, C. Y. (2012). Korean Culture and Its Influence On Business Practice in South Korea. *Journal of International Management Studies*, *7*(2), 184–191.

Lee, S. (1998). Organizational Flexibility in Korean Companies: Rules and Procedures on Managerial Discretion and Employee Behaviour. *International Journal of Human Resource Management*, *9*(3), 478–493.

Lennon, M. (n.d.). Hackers Hit 100 Banks in "Unprecedented" $1 Billion Cyber Heist: Kaspersky Lab. *SecurityWeek.com*. Retrieved from http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

Meindl, J. R., Hunt, R. G., & Lee, W. (1989). Individualism-Collectivism and Work Values: Data from the United States, China, Taiwan, Korea, and Hong Kong. *Research in Personnel and Human Resources Management*, *1*(1), 59–77.

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure As Myth and Ceremony. *American Journal of Sociology*, 340–363.

Moorman, R. H., & Blakely, G. L. (1995). Individualism-Collectivism as an Individual Difference Predictor of Organizational Citizenship Behavior. *Journal of Organizational Behavior*, *16*(2), 127–142.

Newman, K. L., & Nollen, S. D. (1996). Culture and congruence: The Fit between Management Practices and National Culture. *Journal of International Business Studies*, 753–779.

Oyserman, D., Coon, H. M., & Kemmelmeier, M. (2002). Rethinking Individualism and Collectivism: Evaluation of Theoretical Assumptions and Meta-Analyses. *Psychological Bulletin*, *128*(1), 3.

Park, K. H., & Weber, W. L. (2006). A Note on Efficiency and Productivity Growth in the Korean Banking Industry, 1992–2002. *Journal of Banking & Finance*, *30*(8), 2371–2386.

Quinn, R. E., & Kimberly, J. R. (1984). Paradox, Planning, and Perseverance: Guidelines for Managerial Practice. In *Managing organizational transitions* (pp. 295–313). Homewood, IL: Dow Jones-Irwin.

Quinn, R. E., & Rohrbaugh, J. (1983). A Spatial Model of Effectiveness Criteria: Towards A Competing Values Approach to Organizational Analysis. *Management Science*, *29*(3), 363–377.

Rosenzweig, P. M., & Singh, J. V. (1991). Organizational Environments and the Multinational Enterprise. *Academy of Management Review*, *16*(2), 340–361.

Sang-hun, C. (2013, March 20). Cyberattack Hits South Korean Banking Networks. *The New York Times*. Retrieved from http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

Schein, E. H. (1984). Coming to a New Awareness of Organizational Culture. *Sloan Management Review*, *25*(2), 3–16.

Schneider, S. C., & De Meyer, A. (1991). Interpreting and responding to strategic issues: The impact of national culture. *Strategic Management Journal*, *12*(4), 307–320.

Schwartz, S. H. (1990). Individualism-Collectivism Critique and Proposed Refinements. *Journal of Cross-Cultural Psychology*, *21*(2), 139–157.

Schwartz, S. H. (1999). A Theory of Cultural Values and Some Implications for Work. *Applied Psychology*, *48*(1), 23–47.

Scott, T., Mannion, R., Davies, H., & Marshall, M. (2003). The Quantitative Measurement of Organizational Culture in Health Care: A Review Of The Available Instruments. *Health Services Research*, *38*(3), 923–945.

Scott, W. R. (1995). *Institutions and organizations*. Thousand Oaks, CA: Sage Publications.

Scott, W. R. (2008). *Institutions and organizations: Ideas, interests, and identities*. Thousand Oaks, CA: Sage Publications.

Sherif, M. (1936). *The psychology of social norms*. NewYork: Harper.

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.

Triandis, H. C. (1989). The Self and Social Behavior in Differing Cultural Contexts. *Psychological Review*, *96*(3), 506.

Triandis, H. C., Bontempo, R., Villareal, M. J., Asai, M., & Lucca, N. (1988). Individualism and Collectivism: Cross-Cultural Perspectives on Self-Ingroup Relationships. *Journal of Personality and Social Psychology*, *54*(2), 323.

Trompenaars, F., & Hampden-Turner, C. (1998). *Riding the Waves 0f Culture: Understanding Diversity in Global Business* (2nd ed.). London: McGraw-Hill.

Wagner, J. A. (1995). Studies of Individualism-Collectivism: Effects on Cooperation In Groups. *Academy of Management Journal*, *38*(1), 152–173.

Warkentin, M., Charles-Pauvers, B., & Chau, P. Y. (2015). Cross-cultural IS Research: Perspectives from Eastern and Western Traditions. *European Journal of Information Systems*, *24*(3), 229–233.

Zammuto, R. F., & O'Connor, E. J. (1992). Gaining Advanced Manufacturing Technologies' Benefits: The Roles of Organization Design and Culture. *Academy of Management Review*, *17*(4), 701–728.

Zucker, L. G. (1977). The Role of Institutionalization in Cultural Persistence. *American Sociological Review*, 726–743.