

Winter 12-13-2014

The Three Musketeers: Impacts of National Culture, Organizational Norms and Institutional Environment on Information Security Policy Compliance

Hwee-Joo Kam
Ferris State University

Pairin Katerattanakul
Western Michigan University

Soon-Goo Hong

Follow this and additional works at: <http://aisel.aisnet.org/wisp2014>

Recommended Citation

Kam, Hwee-Joo; Katerattanakul, Pairin; and Hong, Soon-Goo, "The Three Musketeers: Impacts of National Culture, Organizational Norms and Institutional Environment on Information Security Policy Compliance" (2014). *WISP 2014 Proceedings*. 1.
<http://aisel.aisnet.org/wisp2014/1>

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2014 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Three Musketeers: Impacts of National Culture, Organizational Norms and Institutional Environment on Information Security Policy Compliance

Hwee-Joo Kam
Ferris State University

Pairin Katerattanakul
Western Michigan University

Soon-Goo Hong
Doug-A University

Abstract

This study examines the interplay of national culture, organizational norms, and institutional environment on user compliance with information security policy (ISP). Building on the Neo-Institutional Theory (NIT) and Cross-Cultural Framework, this study intends to (1) investigate the relationship among national culture, organizational norms, and institutional environment for ISP compliance at the individual level; and (2) present the similarities and differences of ISP compliance in a cross-national, cross-industry context. Particularly, this study intends to identify the differences on user's compliance between the higher education and the banking industry in countries including the United States and South Korea. We believe that the stark contrast between both industries in relation to policy compliance coupled with the distinctive differences in national culture between both nations will draw significant findings to explain the interactive effects of national culture, industry's institutional environment and organizational norms on user's compliance.

Keywords: Policy compliance, national culture, organizational norms

INTRODUCTION

Culture profoundly influences organizations (Hofstede 1983). Mainly, culture drives user's compliance with information security policy (ISP) in organizational settings (Da Veiga and Eloff 2010). As there is no "one-size-fits-all" management and technology solution in multiple cultural settings (Ho, Raman and Watson 1989; Straub 1994), mechanism that works in one culture may not work in a different culture (Smith, Winchester and Bunker 2010).

Despite the criticality of cultural influence, there are not many cross-nations studies in term of ISP compliance. There is also a lack of studies for industry-level compliance since industry studies are not popular in information systems research and theory albeit the important impact of industries on information systems (IS) activities (Chiasson and Davidson 2005). Although there are some studies related to industry and national culture for ISP compliance (Hovav and D'Arcy 2012; Kim, Ryu and Kwark 2013), there are virtually no studies focusing on ISP compliance driven by national, organizational, and industry levels.

Therefore, the purpose of this study is twofold. First, this study draws on the Cross-Cultural Framework (Hofstede 1983) and Neo-Institutional Theory (NIT) (Meyer and Rowan 1977; DiMaggio and Powell 1983) to examine how the interplay of national culture, organizational norms, and industry environment drive user's compliance. This will then allow us to yield a theoretical framework that will derive the micro-level of individual's ISP compliance from the macro-level of nation, organization, and industry. Second, this study will compare the higher education and banking industries between the United States and South Korea. The stark contrast between banking and higher education (Kam and Katerattanakul 2013) coupled with the distinctive differences of national culture between the United States and South Korea (Hotstede 1980) will enable us to examine the impact of national culture and industry influences on organizational norms, which ultimately drive user's ISP compliance (Herath and Rao 2009). Next, we can investigate the relations of national culture, organizational norms and

industry's institutional environment to provide suggestions on how to enhance organizational practices for ISP compliance in the context of cultural differences.

HYPOTHESIS STATEMENT

Cross-National Framework

Defined as “the collective mental programming of the people in an environment” (Hofstede 1980), culture is a way of thinking, feeling, and acting. National culture discerns one group of people from another through a unique set of values, beliefs, and assumptions learned in early childhood (Hofstede 1991). Also, national culture is profoundly integrated into everyday life, making it hard to change (Newman and Nollen 1996).

The four dimensions of national culture are power distance, uncertainty avoidance, individualism-collectivism, and masculinity-femininity (Hofstede 1983). High power distance indicates a strong dependent relationship wherein subordinates defer to their superiors in decision-making but low power distance signifies interdependence relationship wherein both superiors and subordinates collaborate in decision making (Hofstede 1983). Accordingly, nations that espouse high power distance may allow supervisors to become the sole decision makers in ISP compliance; whereas nations that value low power distance may facilitate partnership between supervisors and subordinates in decision making for ISP compliance.

H1a: The power distance dimension influences user's compliance with ISP

Nations with high uncertainty avoidance face uncertainty with higher level of anxiety than that of the nations with low uncertainty avoidance (Hofstede 1983). In nations of high uncertainty avoidance, people tend to follow rules; but people from nations of low uncertainty avoidance are comfortable with taking risks and handling the unknown (Hofstede 1983). Accordingly, individuals from nations with high uncertainty avoidance may get accustomed to clear, explicit

rules that support user's compliance. Nevertheless, individuals from nations with low uncertainty avoidance may prefer some flexibilities and discretions in regulatory compliance.

H1b: The uncertainty avoidance dimension influences user's compliance with ISP

Whereas individualistic nations view individuals as active agents of the organizations wherein individual well-beings are more important than fringe benefits, use of skills, and working conditions, collectivist nations embrace high group consciousness in that collective group welfares supersede individuals' (Hofstede 1983). Hence, individuals from individualistic nations may comply with ISP if they perceive that ISP compliance will benefit their individual well-beings. Conversely, individuals from collectivist nations may comply with ISP if their compliances will bring benefit to their groups.

H1c: The individualism-collectivism dimension influences user's compliance with ISP

For "masculine" nations, income, career advancement, and recognition have higher priorities than cooperation, desired living areas and job security (Hofstede 1983). This is in contrast to "feminine" nations wherein quality of life and environment has higher priorities than career achievement and recognition (Hofstede 1983). Accordingly, we contend that individuals from masculine nations will comply with ISP if they perceive that ISP compliance will bring rewards to their careers. On the other hand, individuals from feminine nations will comply with ISP if they perceive that ISP compliance will improve the environment and lives of the people.

H1d: The masculinity-femininity dimension influences user's compliance with ISP

Organizational Norms

Organizational norms embody informal rules that monitor member's conduct, creating powerful and consistent effects on member's behaviour (Feldman 1984). We argue that organizational norms are shaped by national culture. Different national culture leads to different managerial practices (Hofstede 1983; Schneider and DeMeyer 1991) as national culture exerts its impacts on decision-making, leadership style, and operations (Newman and

Nollen 1996). Along the same line, through a distinctive set of values (Hofstede 1991), national culture defines social norms that later shape organizational norms (Meyer and Rowan 1977). That is, social norms (i.e. the right thing to do for the community) defined by national culture build perceived norms in organizations. As a consequence, organizations integrate the rules of social norms into their perceived norms to survive (Feldman 1984). Hence, national culture affects organizational norms.

Particularly, high power distance enables top management to employ top-down approach to enforce ISP compliance. Subsequently, management practices cultivate organizational norms (Schein 1983) for user compliance. On the other hand, low power distance may encourage employee's participation in decision making for ISP compliance. In this respect, the Buy-in Theory postulates that users are more willing to accept a system that was developed with their inputs because users' psychological involvement in system development makes them think that the system is personally important (Markus and Mao 2004). Drawing on the Buy-in Theory (Markus and Mao 2004), we posit that low power distance encourages employee's participation in decision-making for ISP, thus increasing employee's acceptance of ISP. This will then nurture the subjective norms that emphasize the importance of ISP.

H2a: The power distance dimension shapes organizational norms to stay compliant

Nations with high uncertainty avoidance may prefer highly structured working environment with well-defined rules (Hofstede 1983). These nations support hierarchical structure that enables organizations to clearly outline rules (Quinn and Rohrbaugh 1983) and eventually establishes organizational norms (Feldman 1984) for ISP compliance. In contrast, nations with low uncertainty avoidance may not be risk averse and may even facilitate growth and entrepreneurial spirit in organizations. Accordingly, organizations that support entrepreneurial activities may permit flexibilities and creativities (Quinn and Rohrbaugh 1983) that will affect organizational norms for ISP compliance.

H2b: The uncertainty avoidance dimension shapes organizational norms to stay compliant

Individualistic nations may share higher collective efficacy (Hofstede 1994; Hofstede 2001). In general, collective efficacy pertains to shared belief among groups about their ability to complete tasks; and it is an extension of self-efficacy (i.e. beliefs in one's capability to obtain desirable outcomes) to group levels (Bandura 1997; Kim, Ryu and Kwark 2013). Prior studies suggested that individualistic nations display high collective efficacy (Hofstede 1994; Hofstede 2001), thereby shaping the "can do" attitude. That is, high collective efficacy in individualistic nations enables organizations to share a belief that they are capable of carrying out tasks to stay compliant. Gradually, such belief will bring a set of expectations that build organization norms (Feldman 1984). However, collectivistic nations are reported to show relatively low collective efficacy (Hofstede 1994; Hofstede 2001), bringing about a different set of belief systems that may affect organizational norms for ISP compliance.

H2c: The individualism-collectivism dimension shapes organizational norms to stay compliant

Masculine nations may enable managers to build security strategies based on market competition and perceived needs of control on subordinates (Rocha Flores, Antonsen and Ekstedt 2014). In other words, masculine nations enable management to draft strategies for winning the market competition (e.g. protect customer's data to provide the best service than their competitors) and controlling employees (e.g. pressing employees to comply through management forces and punishing those who fail to comply). In contrast, feminine nations may encourage managers to examine how their decisions of ISP compliance would affect the lives of their subordinates (Rocha Flores et. al. 2014). Eventually, management approach to ISP shapes organizational norms.

*H2d: The masculinity-femininity dimension shapes organizational norms to stay compliant***Institutional Environment**

Industry is defined by its institutional environment (Scott 1995). Institutional environment constitutes the notion of legitimacy formed by generalized perceptions that expect organizations to exercise proper behaviour based on social norms, values and beliefs (Suchman 1995). For example, banks are expected to comply with federal regulations, such as, Gramm Leach Bliley Act (GLBA), for safeguarding customer's data. To gain legitimacy for survival (Suchman 1995), banks must abide by strict regulations. That is, occupied with strict regulations, the institutional environment of banking compels banks to fulfil their social obligations through information security safeguard. This shows that industry represents an institution in which its environment is based on the taken for granted, formal or informal rules that restrict, monitor and/or support social behaviour (Scott 1995).

There are uncertainties in institutional environment (Hrebiniak and Snow 1980). Essentially, the environment uncertainty and structural responses to uncertainty differ across industries (Hrebiniak and Snow 1980). This is evident in the comparison of higher education and banking. Most banks recognize the uncertainties caused by threats and risks in their environment (Yeh and Chang 2007). Hence, banks have to devise security measures (e.g. risk management) to manage risk for staying compliant. This is in stark contrast with higher education (Kam et al. 2013). Unlike the banking industry, higher education is not under great pressure to comply. This explains that, although higher education has to comply with Family Education Rights and Privacy Act (FERPA) for protecting student's information (United States Department of Education 2010), not many universities implement security mechanism (Kvavik 2004). In essence, due to the different environmental uncertainties for information security between banking and higher education, both industries react to their external uncertainties differently, leading to different intensity level in enforcing ISP (Kam et al. 2013). Institutional environment is saddled with external pressures (Meyer and Rowan 1977). Neo-Institutional Theory (NIT) posits that, when facing external pressures, organizations adopt

certain policies and procedures by undertaking coercive, mimetic, and normative isomorphism (DiMaggio and Powell 1983). Coercive isomorphism manifests when an authoritative entity coerces organizations to comply with regulations (DiMaggio and Powell 1983). For instance, the federal government required banks to comply with Sarbanes-Oxley (SOX) regulation through standardized financial reporting. As for mimetic isomorphism, organizations imitate the patterns of successful organizations to cope with uncertainty (DiMaggio and Powell 1983). For instance, many organizations employed the well-recognized IT governance framework (e.g. COBIT) that has already been established successfully in other organizations. Normative isomorphism manifests as organizations embrace patterns construed as appropriate in the environment (DiMaggio and Powell 1983). For instance, organizations safeguard client's data as their clients demand information security protection.

Eventually, organizations achieve legitimacy and improve their chances to survive (Suchman 1995). In this respect, NIT posits that organizations handle external pressure by complying with regulations, by copying other organizations' successful handling of uncertainty, and by adopting organizational practices deemed appropriate in the environment. Thus, coercive, mimetic, and normative isomorphism that reflects upon an industry's institutional environment drive organizational norms to comply.

H3: Institutional environment drives organizational norms to stay compliant

Information Security Policy (ISP) Compliance

Organizational norms entail perceived norms that dictate the right thing to do (Herath and Rao 2009). Perceived norms enforce ISP compliance (Johnston and Warkentin 2010), encouraging user to comply. That is, as users perceive that complying with ISP is construed as the right thing to do, they will be more willing to comply.

H4: Organizational norms drive user' to comply with ISP

FUTURE RESEARCH

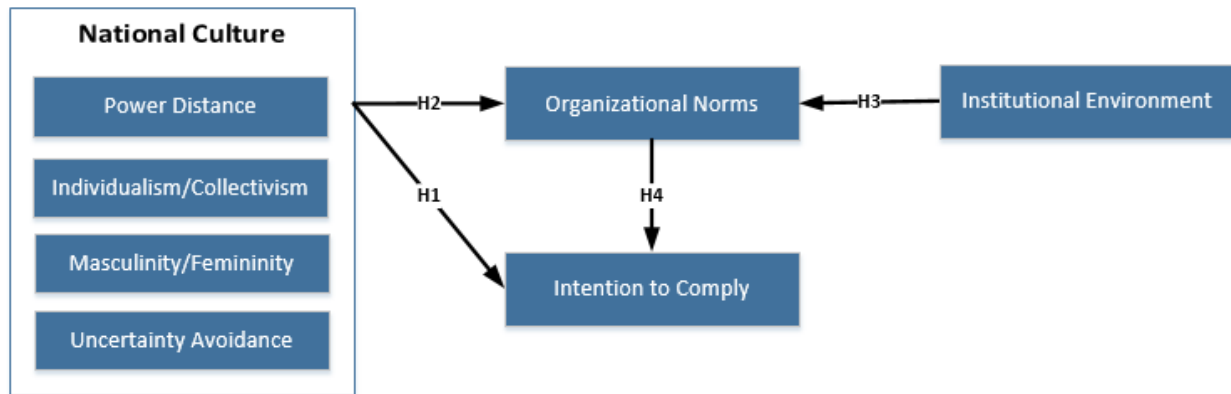


Figure 1. Proposed Research Model

Based on the proposed model (figure 1), we ran a pilot study after forming an online survey using 7-points Likert scales with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree. Due to page limitations, we cannot share the results of our pilot study. Up until this point, we modified our measurement instrument based on the participant's feedback collected from our pilot study. Next, we collected banking data from the banks in the United States (N=134) and South Korea (N=121). In the near future, we will continue collecting data from the higher education in the United States and South Korea for data analysis.

REFERENCES

- Bandura, A. 1997, *Self-Efficacy: The Exercise of Control*, New York, NY: W.H. Freeman
- 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), September, pp 523-548.
- Chiasson, M. W. and Davidson, E. 2005. "Taking Industry Seriously in Information Systems Research", *MIS Quarterly* (29:4), pp. 591-605.
- Chin, W.W. 1998. *The Partial Least Squares Approach to Structural Equation Modelling*. Lawrence Erlbaum Associates, NJ: Mahwah.
- Chin, W.W. and Newsted, P.R. 1999, *SEM Analysis with Small Samples using Partial Least Squares*, In R. Hoyle (Ed.), *Statistical Strategies for Small Sample Research*, Sage Publication, CA: Thousand Oaks.
- Da Veiga, A. and Eloff, J.H.P. 2010, "A Framework and Assessment Instrument for Information Security Culture," *Computers and Security*, (29:2), pp.196-207

- DiMaggio, P. J., Powell, W.W. 1983, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review*, (48:2) April, pp 147-160.
- Feldman, D. C. 1984, "The Development and Enforcement of Group Norms," *Academy of Management Review*, (9:1), pp. 47-53.
- Fornell, C. and Larcker, D. 1981, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, (18:1), February, 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* (16:5), September, pp 91-109.
- Haenlein, M and Kaplan, A.M. 2004. "A Beginner's Guide to Partial Least Squares Analysis," *Understanding Statistics* (3:4), pp 283 – 297.
- 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), pp 277-319.
- Herath T and Rao H. 2009, "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18), April, pp. 106-125.
- 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
- Ho, T.H., Raman, K.S. and Watson, R. T. 1989, "Group Decision Support Systems: The Cultural Factor," *Proceedings of 10th International Conference on Information Systems*, pp. 119-129.
- Hofstede, G. 1980, *Culture's Consequences: International Differences in Work-Related Values*. Sage Publications, CA: Beverly Hills.
- Hofstede, G. 1983, "The Cultural Relativity of Organizational Practices and Theories," *Journal of International Business Studies* (14:2), June, pp. 75–90
- Hofstede, G. 1991. *Cultures and Organization: Software of the Mind*. McGraw-Hill, NJ: New York.
- Hovav, A. and D'Arcy, J., 2012, "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information & Management* (49:2), March, pp 99-110.
- Hu Q, Dinev T, Hart P, Cooke D, 2012, "Managing Employee Compliance with Information Security Policies: The Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), August, pp. 615-660.
- Johnston, A. C. and Warkentin, M. 2010, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:4), September, pp 549–566.
- Kam, H. J., Katerattanakul, P. and Gogolin G. 2013, "A Cross Industry Study: Differences in Information Security Policy Compliance between the Banking Industry and Higher Education," *In: 34th International Conference on Information Systems (ICIS) Proceedings*.
- Kvavik, R.B. 2004. "Information Technology Security: Governance, Strategy and Practice in Higher Education", *EDUCAUSE* (5).

- Kim D., Ryu Y. and Kwark, Y. 2013, "A Cross-Cultural Perspective of Information Security Collective Efficacy," *In: 34th International Conference on Information Systems (ICIS) Proceedings*.
- Leidner, D. E., Carlsson, S., Elam, J. and Corrales, M. 1999, "Mexican and Swedish Managers' Perceptions of the Impact of EIS on Organizational Intelligence, Decision Making, and Structure," *Decision Sciences* (30:3), June, pp 632–658.
- Markus, M.L. and Mao, Y. 2004, "Participation in Development and Implementation – Updating an Old, tired Concept for Today's IS Contexts," *Journal of the Association for Information Systems* (5), pp. 514–544
- Meyer J. W. and Rowan B. 1997, "Institutionalized Organizations - Formal-Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), September, 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), October, pp 729-757.
- Newman, K.L and Nollen, S. D. 1996, "Culture and Congruence: the Fit between Management Practices and National Culture," *Journal of International Business Studies* (27:4), October, pp 753–779.
- Quinn, R. E., J and Rohrbaugh. 1983, "A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Effectiveness," *Management Science* (29:3), pp. 363–377
- Rocha Flores, W., Antonsen, E. and Ekstedt, M. 2014, "Information Security Knowledge Sharing in Organizations: Investigating the effect of Behavioral Information Security Governance and National Culture," *Computers & Security* (43), June, pp 90–110.
- Schneider, S.C. and DeMeyer, A. 1991, "Interpreting and Responding to Strategic Issues: the Impact of National Culture," *Strategic Management Journal* (12:4), May, pp. 307–320.
- Smith S, Winchester D, Bunker D and Jamieson R. 2010, "Circuits of Power: a Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization," *MIS Quarterly* (34:3), pp. 463–486.
- Straub, D. 1994. "The Effect of Culture on IT Diffusion: Email and FAX in Japan & United States," *Information System Research*, (5:1), pp. 24-47.
- Suchman, M.C. 1995. "Managing Legitimacy - Strategic and Institutional Approaches," *Academy of Management Review* (20:3), July, pp 571-610.
- 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.
- 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.