Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2013 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2013

Impact of External Pressures on Information Security Policy Compliance in the Banking Industry

Hwee-Joo Kam
Ferris State University, kamh@ferris.edu

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

Gerald E merick
Ferris State University, ismjerry@ferris.edu

Impact of External Pressures on Information Security Policy Compliance in the Banking Industry

Hwee-Joo Kam
Ferris State University
kamh@ferris.edu

Pairin Katerattanakul
Western Michigan University
p.katerattanakul@wmich.edu

Gerald Emerick
Ferris State University
ismjerry@ferris.edu

Abstract
There has been virtually no previous study discussing how external pressures impel banks to stay compliant. These external pressures could be a compelling force driving banks to comply. Hinged on the Neo-Institutional Theory (NIT), this study examines how the external pressures, namely, regulative, normative, and cognitive expectations, drive banks to comply. The research findings reveal that information security policy compliance in banking organizations is directly driven by normative expectation. Normative expectation encompasses the pressures of fulfilling social/moral obligation and conforming to the industry norms defined by the standardized information security mechanisms. Since the findings uncover that normative expectation is a significant force in the institution of banking, this study suggests drafting internal organizational policies to (1) meet normative expectation and (2) provide a new avenue for risk assessment based on the normative elements.

Keywords
Information Security Policy Compliance, Banking Industry, Neo-Institution Theory

1. Introduction
Presently, banking industry is confronting high threats for information security breaches (Symantec, 2010). Information security breaches in a bank will have serious ramifications for the organization. The negative publicity regarding information security breaches will taint the bank's reputation. Since bank is a business entity that relies on profitability, bad reputation will negatively affect its business, causing a loss in profit (Goodhue and Straub, 1991).
Additionally, highly regulated industries, such as the banking industry, are under pressure to comply with federal regulations and are subject to IT auditing. Following the financial scandal involving Enron and WorldCom, the banking industry has been under immense pressure to comply with federal regulations, such as, Sarbanes-Oxley Act (SOX), which mandates standard accounting and financial reporting. Banks are also required to comply with Gramm Leach Bliley

Act (GLBA), a comprehensive federal law that requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information. The pressure to comply has propelled banks to adopt IT governance and integrate information security into their daily practices.

Many extant literatures examine user's perspectives and internal organizational efforts on information security policy compliance (Boss et al., 2009; Bulgurcu, Cavusoglu, and Benbasat, 2010; Chan, Woon, and Kankanhalli, 2005; Herath and Rao, 2009). However, there has been virtually no study discussing how external pressures drive banks to attain compliance. These external pressures may serve as a compelling force to drive banks to comply, as suggested by the Neo-Institutional Theory (NIT) in that organizational survival relies on securing legitimacy from stakeholders through conformity to stakeholders' expectations (DiMaggio and Powell, 1983). Thus, to fill in the gaps, this study draws on NIT to examine how external pressures drive information security policy compliance in the banking industry. The research findings would serve to (1) shed light on the critical external driving forces of information security policy compliance in the banking industry of the United States and (2) provide suggestions to improve the implementation of information security practices across the banking industry.

The rest of this paper is organized as follows. Next section presents relevant literature review and the proposed research model. This is ensued by research methodology and analysis results in the third section. Then, discussion is presented in the fourth section. Finally, this paper uncovers the conclusion, practical implication, limitation along with future research in the fifth section.

2. Literature Review

2.1 Stakeholders and Information Security Policy Compliance

Organizations conform to regulations not only for complying with the regulations but also for meeting their social/moral obligations with respect to the stakeholder's expectations. Generally, stakeholder's expectations of legal and social obligation draw parallel with the internal organizational efforts of staying compliant. This suggests that organizational-stakeholder interaction determines compliance (Interligi, 2010). That is, the existing organizational-stakeholder interaction provides stakeholders the opportunities to influence organizational internal control for information security safeguards (Interligi, 2010). Stakeholders could inflict pressures on organizations, driving organizations to comply. As a result, organizations try to live up to stakeholder's expectations of information security policy compliance.

Stakeholders are individuals or groups with a vested interest in the organizations (Friedman and Miles, 2002). In the banking industry, stakeholders mainly consist of shareholders, board of directors, employees, customers, financial markets, and government (Behery and Eldomiaty, 2010). According to the Banking Industry Technology Secretariat (BITS), stakeholders are concerned with four categories of privacy: (1) unsolicited advertisements, (2) accidental release of personal information, (3) misrouting of funds and (4) data errors (Earp and Payton, 2006). Therefore, in the context of information security, these stakeholders, especially customers, expect their banks to strictly safeguard their information and ensure information security policy compliance.

2.2 Neo-Institutional Theory (NIT)

According to the Neo-Institutional Theory (NIT), to survive, organizations must secure legitimacy from stakeholders by conforming to external expectations (DiMaggio and Powell, 1983). That is, for organizational survival, organizations must secure legitimacy by initiating internal organizational efforts to meet external expectations. Organizations are shaped by phenomena in their institutional environment and increasingly conform to their environment to survive. Concerning organizational survival, organizations undergo institutionalization to embrace practices that engender legitimacy (DiMaggio and Powell, 1983; Meyer and Rowan, 1977). Legitimacy refers to the assumptions of actions that are construed as appropriate based upon the social norms, values, and beliefs (Suchman, 1995). Meanwhile, institutionalization embodies the process *"by which social processes, obligations, or actualities come to take on a rule-like status in social thought and action*" (Meyer and Rowan, 1977, pg. 343). In other words, institutionalization involves social process that shapes social reality. Since institutionalization reflects upon social process, organizations espouse positions, policies, procedures, or programs enforced by public opinions, laws, views of important constituents, or social prestige (Meyer and Rowan, 1977).

2.3 External Expectations

Institution serves as a template that guides organizational action and behavior (Scott, 1995). Specifically, institution consists of regulative, normative, and cognitive pillars (Scott, 2008). Each pillar embodies one aspect of external expectations that impose pressures on organizations. The external expectations constitute:

- Regulative Expectation stresses activities of sanctioning and monitoring both formal and informal rules. For instance, the federal government mandates banks to comply with SOX and GLBA.
- Normative Expectation focuses on social norm or appropriate behaviors based on the prescriptive, evaluative, and obligatory dimension in social life (Scott, 2008). For instance, safeguarding customers' social security numbers to prevent the incidents of identity theft represents social obligation of banks. In the context of information security, normative expectations are also shaped by an affiliation of professional organizations (Hu, Hart, and Cooke, 2007); for example, Information Systems Audit and Control Association (ISACA). Professional organizations define the normative framework that outlines the industry norms related to standardized security mechanism.
- Cognitive Expectation refers to stakeholder's perceptions of an event given the shared belief system built on culture (Scott, 2008). For instance, with the incidents of data breaches, stakeholders will interpret and identify these incidents based upon their perceptions built on culture with shared understanding and meaning.

2.4 Organizational Efforts

Given external expectations, organizations attempt to cope with these external demands. That is, organizational internal structure entails internal organizational efforts and practices that respond to the external expectations for securing legitimacy in favor of organizational survival (Meyer and Rowan, 1977). For information security, the internal organizational efforts of staying compliant involve (1) Enforcement of Policies and Procedures and (2) Information Security Awareness. Numerous previous studies suggested that these two factors lead to information

security policy compliance (Boss et al., 2009; Bulgurcu et al., 2010; Chan et al., 2005; Herath and Rao, 2009).

- *Enforcement of Policies and Procedures* emphasizes the policies and procedures within an organization. The efforts of highlighting policies and procedures enhance the perceived mandatoriness of security policies among the employees (Boss et al., 2009). As a result, this encourages information security policy compliance.
- *Information Security Awareness* highly affects employee's beliefs about the benefit of compliance and the cost of non-compliance (Bulgurcu et al., 2010). Within an organization, employees are expected to be aware of the requirements and the objectives of information security (Bulgurcu et al., 2010).

2.5 Proposed Research Model

For information security in the banking industry, the externally legitimated formal structures included three external expectations: Regulative Expectation (REG), Normative Expectation (NORM), and Cognitive Expectation (COG). Additionally, internal organizational efforts included Enforcement of Information Security Policies and Procedures (POL) and Information Security Awareness (AWA). According to the NIT, in order to survive, organizations must initiate internal organizational efforts to conform to the external expectations for securing legitimacy (DiMaggio and Powell, 1983). That is, all external expectations would have direct effects on internal organizational efforts of attaining policy compliance. Thus, this study proposed the research model shown in Figure 1 and the following six hypotheses for this model.

H1: Regulative expectation drives banking organizations to enforce information security policies and procedures
H2: Normative expectation drives banking organizations to enforce information security policies and procedures
H3: Cognitive expectation drives banking organizations to enforce information security policies and procedures
H4: Regulative expectation drives banking organizations to raise information security awareness
H5: Normative expectation drives banking organizations to raise information security awareness
H6: Cognitive expectation drives banking organizations to raise information security awareness

3. Research Methodology and Analysis Results

3.1 Questionnaire

To develop the questionnaire used in this study, we adopted some measurement items used in some 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 consisted of 20 items measuring the five constructs (i.e., REG, NORM, COG, POL, and AWA). Each of these 20 measurement items used 7-point Likert scale with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree.

A pilot study was conducted to refine the original questionnaire. Overall, seven banking professionals participated in this pilot study. These banking professionals responded to and provided their feedbacks on each measurement item in the original questionnaire. From their responses, we calculated the Cronbach's alpha and the item-to-total score to assess the reliability for each construct. Then, based on this reliability assessment and the feedbacks collected from

the pilot study, we modified the measurement items in the original questionnaire. The final version of the questionnaire used in this study included 12 measurement items representing the five constructs.

3.2 Data Collection

Given the difficulty in data collection, we spent almost two years to collect data. First, we spent approximately six months to repeatedly post our online survey in the professional forums such as the BankingInfoSecurity forum in LinkedIn site. Additionally, we sent email to invite bank's employees to participate in our study. The email was sent to approximately 100 banking information security professionals via social networking sites (e.g. LinkedIn). For the next two months, we sent email reminder to follow up the previous email messages we sent. After approximately eight months, we received 31 responses.

Then, upon obtaining permission from the bank presidents, we distributed the invitations for survey participation to the employees in one community bank and two commercial banks in the Midwest region. These invitations provided a link to the online survey of this study. We received 60 responses from these three banks. Additionally, we spent four semesters to collect data from some MBA students in two universities in the Midwest region. These students were part-time MBA students who were working full-time in banking industry. We received 17 responses from this data collection method.

Totally, we collected 108 responses. These participants included 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%) or undisclosed (7%) positions. Most of our participants were working in a large bank with more than 400 employees and a large portion of the participants had less than 10 years of working experience (88%).

3.3 Measurement Assessment

Among the five latent constructs in the proposed research model in Figure 1, three of them were exogenous variables –REG, NORM, and COG. The other two latent constructs were endogenous variables –POL and AWA.

This study employed Structural Equation Modeling (SEM) and used AMOS software with Maximum Likelihood (ML) estimation. We assessed reliability and validity of the measuring instrument used in this study by conducting Confirmation Factor Analysis (CFA). In this study, CFA estimated the measurement model of the five latent constructs with 12 measuring items from the questionnaire.

CFA of the measurement model provided the following results (see Table 1). The ratio between Chi-square (χ^2 = 53.2) and degrees of freedom (df = 44) was 1.21, which was below the recommended maximum cut-off value of 3.0 (Krause, Scannell, and Calntone, 2000). The root mean square error of approximation (RMSEA) was 0.044, which was below the suggested maximum cut-off value of 0.06 (Hu and Bentler 1999). The goodness-of-fit index (GFI) and the adjusted goodness-of-fit index (AGFI) were 0.928 and 0.873 respectively, thus indicating good fit (Hu and Bentler 1999). The comparative fit index (CFI) and the normed fit index (NFI) were 0.985 and 0.922 respectively, suggesting an adequate fit (Hu and Bentler 1999). These results suggested that the measurement model of the five latent constructs with 12 measurement items fit the sample data fairly well.

We computed the Composite Reliability (CR) and the Average Variance Extracted (AVE) values for the five latent constructs. All CR values (see Table A1 in the Appendix), except that for the REG construct (i.e., 0.664), were above the recommended threshold of 0.70 (Fornell and Larcker 1981; Hair et al. 1998; Segars 1997). Similarly, all AVE values (see Table A1 in the Appendix) were above the suggested threshold of 0.50 (Hair et al. 1998; Segars 1997), confirming that the five latent constructs had captured a relatively high level of variance. All the results of these reliability tests indicated a reasonably high level of instrument reliability.

Then, convergent validity of the instrument was assessed by examining all loadings from CFA results. All loadings were high (ranging from 0.559 to 0.965, see Table A2 in the Appendix) with t-values (ranging from 4.254 to 11.768, see Table A2 in the Appendix) well above the 2.54 threshold, thus supporting the statistical significance of the loadings (p-value < 0.01). Additionally, all Squared Multiple Correlations (R^2) values were high (ranging from 0.311 to 0.677, see Table A2 in the Appendix). These results indicated convergent validity, asserting that the measuring items in this study were "good" measures of the constructs (Gefen, Straub, and Boudreau, 2000).

Finally, discriminant validity of the instrument was evaluated by examining the square root of the AVE of each construct (see Table A3 in the Appendix). The square root of the AVE of each construct was greater than any of the construct's correlations with other constructs. This provided evidence for discriminant validity of the constructs in the model (Fornell and Larcker 1981; Segars 1997).

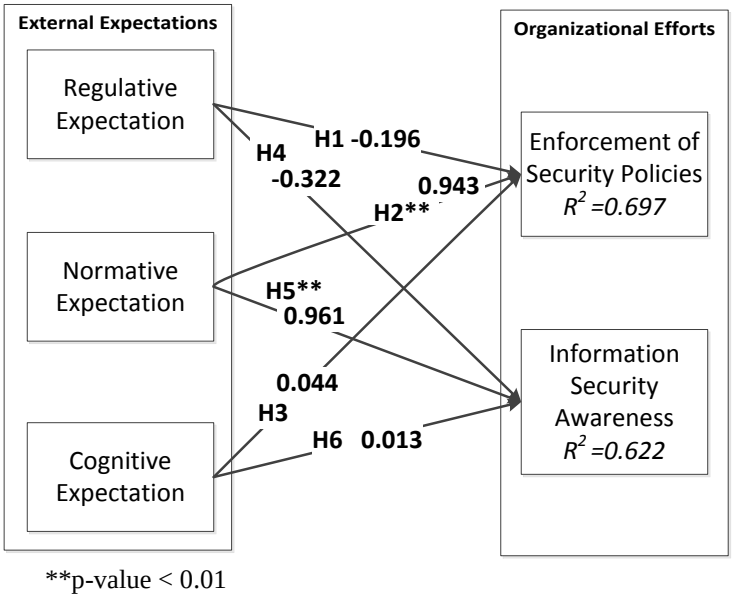
3.4 Hypothesis Testing

Model-fit test of the proposed research model yielded the following results (see Table 1). The ratio between Chi-square (χ^2 = 69.5) and degrees of freedom (df = 45) was 1.54, which was below the recommended maximum cut-off value of 3.0 (Krause et al., 2000). The RMSEA value (0.071) was slightly above the suggested maximum cut-off value of 0.06 (Hu and Bentler 1999). The GFI and the AGFI were 0.910 and 0.844, respectively. In addition, the CFI and the NFI were 0.960 and 0.898 respectively. In sum, these results suggested that the proposed research model fairly fit the sample data.

Furthermore, we examined the regression coefficients to test each hypothesis. These regression coefficients were ranging from -0.322 to 0.961 (see Figure 1). Only the t-values of the regression coefficients for H2 and H5 were significant at p-value < 0.01; thus, only H2 and H5 were supported. That is, only normative expectation (excluding regulative and cognitive expectations) had significant effects on bank's internal organizational efforts for information security policy compliance.

	χ^2 , (df)	χ^2/df	GFI	AGFI	CFI	NFI	RMSEA
Measurement Model	53.2 (44)	1.21	0.928	0.873	0.985	0.922	0.044
Proposed Research Model (hypothesis testing)	69.5 (45)	1.54	0.910	0.844	0.960	0.898	0.071

Table 1: Model-Fit Test Results



**p-value < 0.01

Figure 1: Proposed Research Model – Hypothesis Testing

4. Discussion

The analysis result showed that most of the hypotheses in the proposed research model were not supported. In general, the hypothesis testing result showed that only normative expectation significantly affected bank's internal efforts for information security policy compliance.

The institution structure of banking embodies the high correlation (i.e., 0.563) between regulative and normative expectations, which could possibly be explained by the incidents of Enron and WorldCom financial scandals. Following the Enron and WorldCom scandals, SOX was enacted to mandate banks and financial services adopting the internal controls and procedures for financial reporting. The enactment of SOX exerts regulatory pressure to make sure that the banking organizations practice ethical conduct for fulfilling social obligation (i.e., normative expectation). In short, federal regulations push for meeting the social norm, suggesting that regulative expectation links to normative expectation.

Result of this study also uncovered that cognitive expectation has no direct impact on information security policy compliance in banking organizations. Rather, it mirrors how regulatory pressure shapes stakeholder's perception towards information security policy compliance. This study contended that the enactment of information security laws and regulations in the banking industry represents a rational choice to prevent another financial scandal in the near future. Institution theorist posited that the process of rational choices causes institutionalization (Scott, 2008) that shapes new conception. That is, cognitive elements emerge after the process of rational choices (Scott, 2008).

The rational choice of imposing regulative pressure impels organizations to undergo institutionalization, resulting in the formation of new meanings and values (Zucker, 1977). Such regulatory power serves as an impetus, driving changes in banking organizations (Hu et al., 2007). For instance, the recent changes in the banking organizations are represented by the reality wherein every bank has a compliance officer to oversee the information security policy compliance. Due to these changes, stakeholders gradually shape new perceived value of

information security based upon the new meanings and understanding related to the criticality of information security. Overall, the process of rational choice could also explain the high correlation (i.e., 0.42) between regulative and cognitive expectations.

In response to the new information security regulations as well as stakeholder's perception, the banking industry would establish well-developed information security mechanisms that serve as an information security guideline for the banking organizations. These mechanisms would evolve to become the banking industry's information security standard and eventually transform to social obligations (i.e., normative expectation) that the banking organizations are expected to live up to.

Thus, there are two main components of normative expectation – the pressure to fulfill the social/moral obligation and the pressure to conform to industry norms regarding standardized information security mechanisms. The pressure of satisfying social/moral obligation urges banks to engage in ethical organizational practice so as to benefit the overall community. Additionally, banks have to conform to the industry's standardized information security mechanisms for meeting the strict regulatory demand.

Banking organizations try to attain normative expectation not only by satisfying social obligation but also by adopting industry norms related to standardized information security mechanisms. Banking organizations initiate their internal organizational efforts to follow the industry's standardized information security mechanisms and conform to the social obligations. Thus, the normative expectation (neither regulative expectation nor cognitive expectation) directly affects bank's internal organizational efforts for information security policy compliance.

5. Conclusion

This study examined how external expectations affect information security policy compliance in the banking industry. The study was based on NIT postulating that, to survive, organizations must secure legitimacy from stakeholders by conforming to external expectations (DiMaggio and Powell, 1983). The three external expectations include regulative, cognitive, and normative expectations.

Because normative expectation had direct impacts on organizational efforts for information security policy compliance, the practical implication of this study pertains to normative expectation. Banks are business entity associated with risk (Kelly, 2006). Thus, this study suggests meeting normative expectation and assessing risk from the perspective of normative pressure. In this respect, top management can draft internal organizational policies to serve two purposes: (1) attaining normative expectation and (2) providing a new avenue for risk assessment. Particularly, banks can draft internal policies to attain social obligation. For instance, the internal policies could encourage banks to provide free seminars for educating the public about identity theft. Such internal policies promote bank's participation in the community service, enabling banks to fulfill social obligation (Campbell, 2007). The free seminar would also provide banks an opportunity to clearly present a chain of actions for handling identity theft incidents. When presenting a series of steps for identity theft solution in the public setting, banks render their actions traceable in the public's eyes. This engenders high perceived traceable institution's action ascribed to institutional trust (Riegelsberger, Sasse, and McCarthy, 2005).

Institutional trust is embedded with social and organizational context (Williamson, 1993). It is rationally based and signifies the outcome of stakeholder's assessment of institution's

performance (Mishler and Rose, 2001). This thereby infers that institutional trust pertains to stakeholder's belief of environmental security facilitated by guarantees, safety nets, and other performance structures (Shapiro, 1987). Gaining institutional trust enables banks to garner support from stakeholders and build the external network structure to ease the external pressures (Fischer and Pollock, 2004).

Since the aforementioned internal policies foster the achievement of normative expectation in support of institutional trust, banks can assess risk related to institutional trust and calculate the cost of losing institutional trust. Currently, many banks assess risk by examining the criticality of informational assets (e.g. confidential business transaction), functional assets (e.g. network infrastructure), and physical assets (e.g. database server) (McCumber, 2004). In addition to evaluating asset's criticality, the criticality of institutional trust provides a new dimension for risk assessment.

This study also suggests several research implications. As the proposed research model fairly fit the sample data, future research may investigate other alternative models. For example, the model that represents the direct effects of regulative expectation on both normative and cognitive expectations or the model that incorporates legitimacy as another construct. Additionally, to improve the generalizability of the research findings, the future research may include investment banking and other financial services in other regions. Finally, the future research may use external pressures -- regulative, normative, and cognitive -- to address risk and trust in the banking industry.

This study is not without limitation. First of all, this study encountered difficulty in data collection, and therefore, the sample size was relatively small (N=108). However, in general, the small sample size was found in numerous previous studies related to information security in banking industry (e.g., Deane et. al., 1995; Yeh and Chang, 2007).

Additionally, the banking data was skewed and thus may require a larger sample size for more accurate results. Although small sample size and non-normal data may cause difficulty in convergence and create biases against goodness-of-fit indices (Hau and Marsh, 2004), result of this study demonstrated that the goodness-of-fit indices meet the suggested threshold and that the average variance estimate (AVE) was above the suggested minimum threshold of 0.50 for each construct. This thus proves that researchers could safely draw on the result of this study to derive new research findings.

Another limitation is generalizability of research findings as this study mainly collected data from participants in the Midwest region. Hence, the researchers may want to exercise their judgment when referencing these research findings.

References

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

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), p.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), p.523-548.

Byrne, B.M. (2010) *Structural Equation Modeling with AMOS. Basic Concepts, Applications, and Programming, 2nd Edition*, New York, NY: Routledge.

Campbell, J. (2007) "Why Would Corporations Behave In Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility", *Academy of Management Review*, 32 (3), p.946-967.

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), p.18–41.

Deane, F., Barrelle, K., Henderson, R., and Mahar, D. (1995) "Perceived acceptability of biometric security systems", *Computers & Security*, 14 (3), p.225-231.

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), p.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), p.105-122.

Fischer, H.M. and Pollock, T.G. (2004) "Effects of Social Capital and Power on Surviving Transformational Change: The Case of Initial Public Offerings", *Academy of Management Journal*, 47 (4), p.463-481.

Friedman, A. L. and Miles, S. (2002) "Developing Stakeholder Theory", Journal of Management Studies, 39(1), p. 1 - 21

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

Gefen, D., Straub, D., and Boudreau, M. (2000) "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice", *Communications of the Association for Information Systems*, (7) 7, p.1-78.

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), p.13-27.

Hair, J.F. Jr., Anderson, R.E., Tatham, R.L., and Black, W.C. (1998) *Multivariate Data Analysis, 5th Edition*, Upper Saddle River, NJ: Prentice Hall.

Hau, K.T. and Marsh, H. W. (2004) "The use of item parcels in structural equation modeling: Non-normal and small sample sizes", *British Journal of Mathematical and Statistical Psychology*, 57 (2), p.327-351.

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), p.106-125.

Hu, L. and Bentler, P.M. (1999) "Cutoff criteria for fit indexes in covariance structure analysis: Coventional criteria versus new alternatives", *Structural Equation Modeling, 6* (1), p.1-55.

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), p.153-172.

Interligi, L. (2010) "Compliance Culture: A Conceptual Framework", *Journal of Management and Organization*, 16 (2), p.235-249.

Kelly, J.M. (2006) "Cultivating a Holistic Compliance Culture", *http://www.aba.com/nr/rdonlyres/cc139b64-7199-4568-bad5-3effe9f7bda3/45238/bcnd2006coverstory.pdf*.

Krause, D.R., Scannell, T.V., and Calantone, R.J. (2000) "A Structural Analysis of the Effectiveness of Buying Firms' Strategies to Improve Supplier Performance", *Decision Sciences*, 31 (1), p.33-55.

McCumber, J. (2004) *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Boca Raton, FL: Auerbach,.

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

Mishler, W. and Rose, R. (2001) "What are the Origins of Political Trust? Testing Institutional and Cultural Theories in Post-Communist Societies", *Comparative Political Studies*, 34 (1), p.30-62.

Riegelsberger, J., Sasse, M.A., and McCarthy, J.D. (2005) "The Mechanics of Trust: A Framework for Research and Design", *International Journal of Human-Computer Studies*, 62 (3), p.381-422.

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

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

Segars, A.H. (1997) "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research", *Omega*, 25 (1), p.107-121.

Shapiro, S.P. (1987) "The Social Control of Impersonal Trust", *American Journal of Sociology*, 93 (3), p.623-658.

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

Symantec (2010) "The Symantec Internet Security, "Threat Report Trends for 2009", *http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf*.

Williamson, O.E. (1993) "Calculativeness, Trust, and Economic Organization", *Journal of Law and Economics*, 36 (2), p.453-486.

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

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

Appendix

Construct	AVE	Composite Reliability
REG	0.501	0.664
NORM	0.739	0.848
COG	0.528	0.765
POL	0.771	0.853
AWA	0.698	0.872

Table A1: AVE and Composite Reliability

Item	Description	Factor Loading	t-value	R^2
REG1	Regular inspection by an authorized third-party regulator	0.607	na	0.369
REG2	Legal action against banks for violating federal laws on information security	0.796	4.254	0.634
NORM1	Adopt standardized security practices in the industry	0.949	na	0.091
NORM2	Serve the clients through security compliance	0.760	8.617	0.577
COG1	Loss of reputation due to the incident of data breaches	0.709	na	0.503
COG2	Monetary loss due to the incident of data breaches	0.874	5.644	0.765
COG3	Loss of client's trust due to the incident of data breaches	0.558	5.112	0.311
POL1	Enforce the written policies on information security	0.956	na	0.914
POL2	Punish employees for violating information security policies	0.762	9.118	0.581
AWA1	Educate employees about the cost of security problems	0.702	8.981	0.493
AWA2	Provide training to raise awareness of management's concerns about security	0.965	na	0.931
AWA3	Provide training to raise information security awareness	0.823	11.768	0.677

Table A2: CFA of Measurement Model

	REG	NORM	COG	POL	AWA
REG	0.708				
NORM	0.563	0.860			
COG	0.420	0.219	0.727		
POL	0.454	0.725	0.194	0.878	
AWA	0.309	0.640	0.115	0.735	0.835

Table A3: Correlations and Square Root of AVE (shaded Cell)