International Business Management 9 (4): 524-531, 2015
ISSN: 1993-5250

Applying Need Pull and Technology Push Theory to Organizational Information Security Management

Geuna Kim and Sanghyun Kim
School of Business Administration, Kyungpook National University,
702-701 Daehak-Ro 80 Buk-Gu, South Korea

Abstract: This study examined the impact of Need Pull (NP) and Technology Push (TP) on the relationships among three Information Security Management (ISM) variables: awareness, development and performance. Data were randomly collected from firms listed with the Korea Foreign Company Association to test the proposed research model. The study's hypotheses were tested using covariance-based structural equation modeling. The results showed that NP and TP had a significant impact on ISM awareness accounting for 36.8% of the variance and that ISM awareness significantly influenced ISM development accounting for 23.6% of the variance which similarly influenced performance, accounting for 14.4% of the variance.

Key words: Need pull, technology push, information security management, performance, relationships

INTRODUCTION

Information Security Management (ISM) issues are becoming crucial for efficient and effective operations as organizations increasingly depend on their information systems to conduct business. The security management of information systems is principally intended to minimize or eliminate potential harm to organizations by controlling unauthorized intrusions and access through the deployment of security mechanisms (Kankanhalli *et al*., 2003). Organizations can establish successful security processes by changing their security management, structure or strategy (Cavusoglu *et al*., 2004). Many firms invest or allocate a large portion of their budgets to building technological solutions for security management.

However, technological tools are not enough to eliminate or prevent external information security risks (Hsu *et al*., 2012). Few studies on the technical aspects of ISM have examined ISM in the organizational context. More research is needed on effective performance measurement, detailed evaluation criteria or construction and ISM implementation in terms of members behavior (Whitman, 2004). Estimating the success of firms ISM applied through fragmented security solutions or related policies and guidelines is a complex task (Zhang *et al*., 2009). An organization's security system may be limited to formal activities and its success cannot be determined unless employee behaviors concerning ISM are understood.

This study addresses two research questions to clarify our understanding of ISM related organizational behavior: what factors influence organizational members recognition of ISM and what routes facilitate ISM implementation and outcomes? To answer these questions, this study investigates the effects of two important variables (need pull and technology push) on organizational ISM, specifically on ISM awareness, development and performance. Globalfirms currently implementing ISM are used as the unit of analysis.

Literature review

Need pull/technology push: Schon (1967) introduced Need Pull (NP) and Technology Push (TP) as two key technological innovation concepts with which to describe technology adoptionand development. Studies in many fields including engineering, marketing and information systems have studied NP and TP as influencing factors in organizational innovation (Chau and Tam, 2000). Studies have emphasized the need for harmony between NP and TP in the development of organizational technological innovation processes (Chidamer and Kon, 1994; Munro and Noori, 1988). Thus, NP and TP should be considered together in discussions of organizational innovation.

The concept of "NP" refers to the key drivers that increase organizational members demands which in turn stimulate innovation (Lee and Shim, 2007). In NP, members needs comprise the key driver which calls attention to the benefit of innovation diffusion within the organization. This study considers NP because it embodies members

Corresponding Author: Sanghyun Kim, School of Business Administration, Kyungpook National University,
702-701 Daehak-Ro 80 Buk-Gu, South Korea

need to call attention to their organization's need for ISM innovation. Studies have claimed that NP is a non-technical expression of internal member needs as well as a key determinant of organizational innovation. For example, Chau and Tam (2000) and Lee and Shim (2007) have argued that NP is a positive determinant of organizations or members decisions concerning new technologies or processes. Shih (2006) adopted the "push-pull" concept to explain the effects of technology adoption, classifying determinants such as task interdependence, task predictability, perceived information-sharing norms, perceived ease of use and perceived usefulness as either a push or pull element, both of which significantly impact member behavior.

TP relies on mechanical competence and external pressure, facilitating the development and application of new technologies. Due to the need to enhance organizational performance, new technologies and processes can be discovered and circulated among members within an organization. This study considers TP in the context of the discovery and diffusion of ISM technologies and examines its effects on ISM awareness. Studies have claimed that seller-invisible pressure and cooperation levels are a part of TP and play critical roles in explaining innovation-related decision processes in organizations (Lee and Shim, 2007).

Information security management: Information security is behavior directed at maintaining and managing an organization's information assets (Dhillon and Backhouse, 2000). Information security can be also defined as a set of tools for protecting information assets; these tools include not only technical and not-technical mechanisms but also the psychological understanding of organizational members. Yeh and Chang (2007) claimed that information security can prevent security breaches, guarantee business continuity and minimize potential damage. Spears and Barki (2010) defined ISM as the process of maintaining an appropriate level of information security using the human factors and materials provided by a system following the general management cycle.

Organizational members awareness is generally viewed in business terms as the extent to which they have knowledge of fundamental information and its relevance to problem areas within the organization (Templeton *et al*., 2002). In the context of ISM, members must be aware of their organization's security goals (Siponen, 2001). Though, organizations consider security an important issue many lack a full understanding of what they should be doing or how to achieve their security objectives (Furnell *et al*., 2002). An organization unaware of the security measures, it should be implementing will not be able to educate its employees about how its information assets can be protected. An insufficient level of ISM awareness can make even the best security mechanisms inadequate (Siponen, 2001).

Some empirical studies have reported that ISM and decision making can vary depending on variables dormant in the organization. The identification and minimization of security threats require continuous verification, evaluation and empirical scrutiny. Siponen (2001) have proposed diagnostic tools for helping firms ISM by developing management models for extending their information management responsibilities and duties. Those studies found that firms internal and external needs have positive effects on ISM adoption and assimilation.

Moreover, Babatunde and Selamat (2012) studied various factors, classified as either NP or TP that influence ISM development and performance; they proposed a theoretical model to support the establishment and operation of optimized security management systems by evaluating ISM. They provided a direction for future improvements based on their findings by arguing that a realistic explanation of ISM can be derived from employees active participation and awareness.

Studies of ISM and related factors have focused on frameworks and have thus done little to propose advanced models or explain the structural relationships among the relevant factors, particularly concerning ISM. Nor have prior studies offered stable solutions that can be effectively designed and practiced by firms. If firms are to benefit from their security management efforts, they must have appropriate insights into imminent problems and security management measurements within a scope they can accommodate. This study contributes to the literature by empirically examining three key internal (NP) and external (TP) characteristics intrinsic to the ISM process awareness, development and performance.

Variables in the ISM decision process: Previous studies have identified various numbers of innovation steps or stages. For example, Grover and Goslar (1993) proposed that there are three steps users intention, actual use or development and implementation or positive outcomes in the process of implementing new technologies or systems in organizations. However, innovation processes vary depending on the type of technology being implemented, the type and size of the innovating organization and the processes scope and content (Cooper and Zmud, 1990). Following the literature and given its purpose, this study posits that there are three steps in the innovation decision process: ISM awareness, development and performance.

First, ISM awareness is the step in which managers become aware of collect and evaluate information on the

importance of ISM (Grover and Goslar, 1993). At this stage, managers try to identify the internal needs (NP) and external pressure (TP) rationalizing the organizational intention to engage in ISM; organizations there by become more aware of the importance of ISM. Thus, ISM awareness is an organization's intention to adopt ISM after becoming aware of the internal needs and external pressure motivating it.

Second, ISM development is the stage at which organizations adopt and implement ISM gradually throughout the organization; at this stage, ISM becomes more routine and less foreign to members. Finally, ISM performance is the stageat which ISM becomes part of the organization's security management strategy. Organizations integrate ISM for innovation and realize both financial and non-financial improvements such as reduced work errors, protected organizational assets and increased profitability (Spears and Barki, 2010). At this stage, organizational members no longer regard ISM as unique because it has become fully integrated into the organization's daily routine.

Research model and hypotheses: Figure 1 shows the proposed research model with the hypotheses to be tested. The research model incorporates NP-TP theory into the ISM innovation process. In addition, a short survey investigating ISM innovation from the perspective of organizational members was conducted in order to validate the proposed research model. This study, thus considers NP and TP as the key factors influencing an organization's ISM awareness, development and performance. In addition to the interviews, the extant research was reviewed to develop the research model. Its new approach is one of this study's contributions to the ISM literature.

Need pull: Some studies have found that NP which is based on an organization's internal needs is an important tool for change in organizations and is more effective in driving innovation than is TP. Myers and Marquis (1969) claimed that understanding NP is animportant part of explaining the innovative aspect of an organization. Utterback (1974) found that between 60 and 80% of cases are derived by NP through meta-analysis. However, the impact of NP in the context of ISM has not been extensively examined. The following hypothesis is proposed in order to fill this research gap:

- H_1: Need Pull (NP) positively influences organizational ISM awareness

Technology push: TP is another factor driving the recognition of the need for new processes in an organization. Research on TP has claimed that technical changes or external pressuresare the basic adjustment tools of innovation. For example, Chau and Tam (2000) found that TP is one of the determinants of the speed and direction of organizational innovation and has a significant influence on organizations innovation processes. Munro and Noori (1988) claimed that the integrated perspective of TP reveals a stronger commitment to change and improvement in anorganization's environment than does the NP approach. Thus, the following hypothesis is proposed:

- H_2: Technology Push (TP) positively influences organizational ISM awareness

ISM process: Security management occurs through the processes ofuse intention, actual use and implementation (Grover and Goslar, 1993) which may vary depending on the organization under study and the research scope being used (Cooper and Zmud, 1990). Empirical research on ISM is insufficient. Most studies addressed the influences of external elements rather than specific management processes, thus focusing on the implementation of management through exogenous variables. However, innovation processes must be determined according to the organization's overall aims at all stages (Zhu *et al*., 2006); doing so can minimize the problems caused by fragmentary innovation adoption (Zmud, 1982).

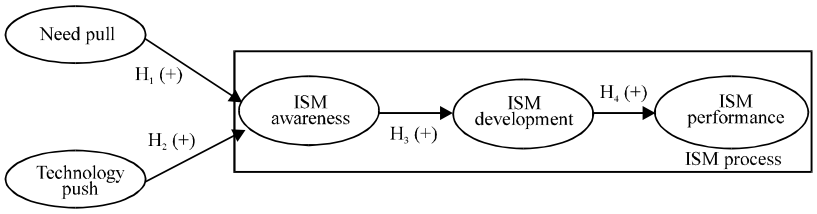

Fig. 1: Research model and hypotheses

Moreover, the phased approach needs to be emphasized because achieving an organizational improvement does not occur all at once but over time (Rogers, 2003). Studies on IT/IS discuss segmented processes such as user initiation, adoption and expansion (Markus and Mao, 2004) but this approach is not appropriate for an examination of ISM.

Spears and Barki (2010) claimed that ISM comprises participation, awareness, development and performance. Rogers (2003) claimed that innovation variables have positive interrelationships. Based on this claim, this study suggests that ISM occurs in three stages: awareness, development and performance and examines their interrelationships. Awareness is the intention and willingness to pursue ISM; development is the degree to which information security is being managed and performance is measured by the financial and non-financial profits produced by members' practice of ISM. Thus, the following two hypotheses are proposed:

- H_3: the process of ISM awareness will positively affect ISM development
- H_4: the process of ISM development will positively affect ISM performance

MATERIALS AND METHODS

Measures: Our measurement model was adapted to the ISM context using previously validated data. Proper measures were taken to ensure the reliability and validity of the measurement instrument. All measures were developed based on a five-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (5). After the measurement variables were developed, the face validity of the measurement items was assessed. Three IS scholars and one management scholar reviewed the measurement items and provided feedback on the length and clarity of each item. Based on the results, several items were modified to fit the purpose of this study. Finally, a pilot study was conducted to validate the measurement model; the results indicate sufficient validity and reliability.

Data collection and sample: The unit of analysis in this study is the organization. Data were collected from organizations currently implementing ISM. The participating organizations were randomly selected from the Korea Foreign Company Association (FORCA) with which >12,160 foreign firms are registered. Using FORCA enhanced generalizability as it allowed the consideration of firms that were diverse in terms of factors such as size, sales and location. A total of 191 responses were collected; 8 incomplete ones were excluded for a final sample of 183 respondents. Table 1 breaks down the data on the 183 respondents in terms of their industry, respondent position, frequency and ISM practices. Thelogistics/transportation industry (27.9%) accounted for the largest portion of respondents, followed by IT (26.8%) and manufacturing (16.4%). Respondents occupied diverse positions: CEOs (6.6%), CFOs (17.8%), CIOs (10.9%), CTOs (33.3%), senior IT managers (32.2%) and others (2.2%). IT-related positions (CTO and IT managers) accounted for more than half of respondents. About 39% of respondents practiced ISM quarterly while about 27% practiced monthly. Regarding specific ISM actions, 86.89% of respondents controlled accessibility to internal systems, 79.8% presented strong security policies and 67.2% checked for security vulnerabilities on a continuous basis.

Table 1: Breakdown of the study participants

Demographic categories	Frequencies	Percentage
Primary industry		
IT	49	26.8
Manufacturing	30	16.4
Education/service	24	13.1
Logistics/transportation	51	27.9
Finance/banking	26	14.2
Other	3	1.6
Current position		
CEO	12	6.6
CFO	27	14.8
CIO	20	10.9
CTO	61	33.3
Senior IT manager	59	32.2
Other	4	2.2
Frequency of ISM practice		
Once a year	15	8.2
Quarterly	71	38.8
Bimonthly	43	23.5
Monthly	49	26.8
Other	5	2.7
ISM practicesand actions (multiple responses)		
Presenting strong security policies (penalty/compensation)	146	79.8
Controlling accessibility to internal systems	159	86.9
Maintaining a system of precaution/monitoring	82	44.8
Checking security vulnerabilities on a continuous basis	123	67.2
Using up-to-date HW/SW (e.g., anti-virus SW, firewall)	91	49.7
Providing continuous education and training on ISM	101	55.2
Investing in ISM along with placing personnel	57	31.2
Other	12	6.6
Total	183	100.0

RESULTS AND DISCUSSION

Analysis of the measurement model: Before testing the structural model, the measurement model was tested to determine the overall fitness of the data and validation using Confirmatory Factor Analysis (CFA) with AMOS 19.0. Several fit indices the Normed Fit Index (NFI), the Goodness-of-Fit Index (GFI), the Adjusted Goodness-of-Fit Index (AGFI), the Comparative Fit Index (CFI) and the Root Mean Square of Approximation (RMSEA) were used

to test the overall fitness of the measurement. A very good fit was demonstrated with NFI, GFI and CFI>0.90, AGFI>0.80 and RMSEA<0.05 (Bentler, 1990; Browne and Cudeck, 1993).

The results for the measurement model (Model 1), with 20 items measuring the 5 variables, indicate that NFI (0.84), CFI (0.85) and RMSEA (0.09) were below the acceptable level. The Modification Indices (MI) indicated that two items measuring ISM awareness (ISMa 3) and ISM development (ISMd 4) had a cross-loading issue, implying that those items loaded on other variables in the research model. Thus, a reevaluation of the measurement model without these two items was required to improve the overall fitness. The revised measurement model (Model 2) was examined after the items were deleted; its indices demonstrated a good fit. The revised measurement model was based on 18 items. Table 2 shows the results of the fit indices for the measurement model. Model 2 had a better fit for the data than did Model 1.

Psychometric properties of measures: After demonstrating the overall fit of the measurement model, internal consistency, item reliability and discriminant validity were examined to demonstrate construct validity. First, internal consistency was tested for each variable using Cronbach's alpha, the most commonly used tool in the social sciences. According to Teo *et al.* (1999), the minimum threshold for Cronbach's alpha is 0.7. As shown in Table 3, Cronbach's alpha ranged from 0.82-0.92, exceeding the threshold.

Table 2: Fit indices for the measurement model

Models	NFI	GFI	AGFI	CFI	RMSEA
Measurement model (model 1)	0.84	0.91	0.82	0.85	0.09
Revised measurement model (model 2)	0.95	0.96	0.89	0.92	0.04
Recommended threshold	≥0.90	≥0.90	≥0.80	≥0.90	≥0.05

Table 3: Results for reliability and construct validity

Variables	Items	Mean	SD	Factor loading	Cronbach's alpha
Need pull	Np 1	5.12	0.08	0.76	0.82
	Np 2	4.55	0.55	0.84	
	Np 3	5.20	0.71	0.82	
	Np 4	4.95	0.28	0.79	
Technology push	Tp 1	5.18	0.30	0.81	0.84
	Tp 2	4.72	0.59	0.89	
	Tp 3	5.36	0.91	0.85	
	Tp 4	5.16	0.21	0.76	
ISM awareness	ISMa 1	3.24	0.57	0.80	0.88
	ISMa 2	4.76	0.20	0.76	
	ISMa 4	5.29	0.97	0.83	
ISM development	ISMd 1	4.38	0.79	0.84	0.92
	ISMd 2	5.22	0.41	0.89	
	ISMd 4	5.01	0.08	0.87	
ISM performance	ISMp 1	4.37	0.70	0.90	0.90
	ISMp 2	5.24	0.75	0.81	
	ISMp 3	4.90	0.13	0.86	
	ISMp 4	5.81	0.58	0.88	

Item reliability was assessed by testing individual item loadings. Chin (1998) claimed that item reliabilityis demonstrated if an item loading exceeds 0.7 for the proposed factor and is <0.4 for other factors. The results for item reliability indicate that all items exceeded 0.7, implying that all items were sufficient for assessing each variable in the proposed research model individually.

Finally, discriminant validity was assessed by using the Average Variance Extracted (AVE) and Pearson's correlation. To demonstrate discriminant validity, the square root of AVE for each latent variable should exceed the vertical and horizontal correlations between the latent variables (Fornell and Larcker, 1981). The results indicated that the AVE of all the latent variables exceeded the correlations of each one. Table 4 shows the result for discriminant validity.

Hypotheses test: Structural Equation Modeling (SEM) was formulated with AMOS 19.0 to find the best fitting model and to test the proposed hypotheses. SEM provides important information such as the overall fitness of the structural model, the standardized path coefficient (β) and the squared multiple correlation (R^2) which indicate how well the structural model predicts the hypothesized relationships. In particular, the standardized path coefficient indicates the strength of the causal relationships between two variables.

First, the results of the fit indices test showed that the structural model fit very well with the data (n = 183). The NFI (0.96), GFI (0.97) and CFI (0.98) all exceeded the required threshold (0.90) and the AGFT (0.91) exceeded the minimum threshold (0.80). The RMSEA (0.03) was <0.05 and the χ^2/df value (1.84) was <3. Thus, each hypothesis could be tested by examining the standardized path coefficient. The test results provided support for all hypotheses (Fig. 2).

First, NP and TP were hypothesized to have a positive effect on ISM awareness. The results showed that NP had a positive effect on ISM awareness (β = 0.416, t = 6.546), supporting H_1. In addition, TP had a positive effect on ISM awareness (β = 0.270, t = 3.850), supporting H_2. These results imply that TP has a higher impact on ISM awareness than does NP. Thus, managers consider ISM important because of their internal needs, a result similarto the findings of studies on the effects of NP and TP on technological innovation (Chau and Tam, 2000; Lee and Shim, 2007).

Table 4: Results for discriminant validity

Latent variables	1	2	3	4	5
Need pull	**0.80**				
Technology push	0.44	**0.83**			
ISM awareness	0.48	0.41	**0.80**		
ISM development	0.36	0.25	0.47	**0.87**	
ISM performance	0.27	0.40	0.38	0.40	**0.86**

The square root of the AVE is indicated along the diagonal (in bold type)

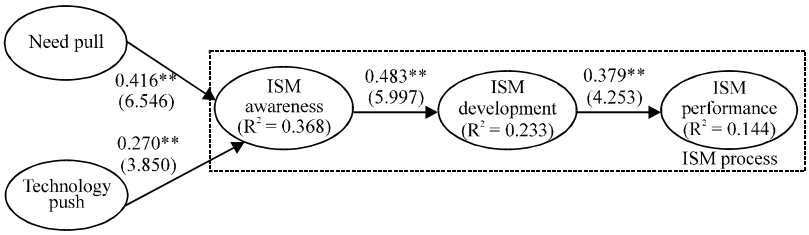

Fig. 2: The structural model ($p<0.05, 0.01$)

The hypotheses on the ISM variables were tested. The results showed thatISM awareness had a significantly positive influence on ISM development ($\beta = 0.483$, $t = 5.997$), supporting H_3; ISM development had a significantly positive effect on ISM performance ($\beta = 0.379$, $t = 4.253$), supporting H_4. These results imply that the positive relationships between variables in technological innovation processes are valid for ISM.

The second piece of meaningful information drawn from the SEM analysis is the squared multiple correlation (R^2) between exogenous and endogenous variables in the research model. The R^2 value reflects the percentage of the variance explained by each endogenous variable in the model (Wixom and Watson, 2001). The results indicate that NP and TP explained 36.8% of the variance in ISM awareness and that ISM awareness explained 23.3% of the variance in ISM development which in turn explained 14.4% of the variance in ISM performance. Figure 2 shows the results of the structural model analysis, including the standardized path coefficients among variables as well as their respective significance levels and variance.

Many organizations have developed ISM to minimize the potential for damage and prevent unauthorized internal and external access. Studies have focused on the technical aspects of information security but security concerns not only technical issues but also userbehaviors. Thus, this study developed a research model that incorporates NP and TP theory into three ISM processes-awareness, development and performance.Data collected from multinational firms were analyzed to test the proposed hypotheses and the results supported each one.

The findings of this study have important theoretical and practical implications. Theoretically, this study provides important insights to the IS literature, particularly to ISM research. As its data were collected from multinational organizations, this study offers broadly applicable descriptive information about organizational ISM practices. In addition, the proposed model contributes to prior literature by applying both NP and TP in the context of ISM. By demonstrating the ISM process in which information security proceeds from ISM awareness to ISM development and performance, the research model contributes to future ISM studies. Finally, this study developed validated measurement items for NP and TP within the ISM context which can be used in future ISM research using NP and TP as ananalytical framework.

CONCLUSION

These findings also have practical implications that can benefit many organizations. First, the findings help managers understand their employees psychologies and behaviors better, thus guiding them in their ISM development. Firms without ISM experience can obtain a clearer and deeper understanding of the ISM process through this study, allowing them to protect their information assets better. This study also deepens our understanding of organizations internal needs and external pressures, helping security analysts find new technologies that can motivate employees to protect information assets.

The results also inform managers about what their employees need to make information security activities routine, thus ensuring that information assets are protected. To top-level managers, this study highlights the significant influence NP and TP exert on ISM awareness, consequently affecting organizational members security behavior. Finally, these results can help managers developand implement information security-related practices and encourage security-informed behavior in organizational members.

As in any social science research, this study has some limitations. First as do most surveys, ours had a low response rate and some non-response bias. The bias was assessed by comparing early respondents with late ones, the results indicating that it was not a serious concern. However because late respondents may be different from non-respondents, future research should validate this study's results. Second, the generalizability of the results may be limited at the global level. This study randomly sampled data from an association of foreign firms (i.e., FORCA) but future studies should validate these results using data drawn from the global level.

RECOMMENDATIONS

Moreover, future research should extend the proposed research model by considering more variables and categories (e.g., cognitive, environmental, economic factors). As the ISM process may vary according to the size, value, revenue and age of the firm (among other factors), future research should alsoexaminethose variables to provide a better understanding of ISM.

REFERENCES

Babatunde, D.A. andM.H. Selamat, 2012. Investigating information security management and its influencing factors in the nigerian banking industry: A conceptual model. Int. J. Soc. Sci. Econ. Art, 2: 55-59.

Bentler, P.M., 1990. Comparative fit indexes in structural models. Psychol. Bull., 107: 238-246.

Browne, M.W. and R. Cudeck, 1993. Alternative Ways of Assessing Model Fit. In: Testing Structural Equation Models, Bollen, K.A. and J.S. Long (Eds.). SAGE Publication, Newbury Park, USA., ISBN-13: 9780803945074, pp: 136-162.

Cavusoglu, H., B. Mishra and S. Raghunathan, 2004. A model for evaluating IT security investments. Commun. ACM, 47: 87-92.

Chau, P.Y.K. and K.Y. Tam, 2000. Organizational adoption of open systems: A technology-push, need-pull perspective. Inform. Manag., 37: 229-239.

Chidamer, S.R.and H.B. Kon, 1994. A research retrospective of innovation inception and success: The technology-push, demand-pull question. Int. J. Tech. Manag., 9: 94-112.

Chin, W., 1998. The Partial Least Squares Approach for Structural Equation Modeling. In: Modern Methods for Business Research, Marcoulides, G.A. (Ed.). Lawrence Erlbaum Associates, New Jersey, pp: 295-336.

Cooper, R.B. and R.W. Zmud, 1990. Information technology implementation research: A technological diffusion approach. Manage. Sci., 36: 123-139.

Dhillon, G.and J. Backhouse, 2000. Information system security management in the new millennium. Commun. ACM, 43: 125-128.

Fornell, C. and D.F. Larcker, 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Market. Res., 18: 39-50.

Furnell, S.M., M. Gennatou and P.S. Dowland, 2002. A prototype tool for information security awareness and training. Logist. Inform. Manage., 15: 352-357.

Grover, V.and M.D. Goslar, 1993. The initiation, adoption and implementation of telecommunications technologies in U.S. organizations. J. Manage. Inform. Syst., 10: 141-163.

Hsu, C., J.N. Lee and D.W. Straub, 2012. Institutional influences on information systems security innovations. Inform. Syst. Res., 23: 1-22.

Kankanhalli, A., H.H. Teo, B.C.Y. Tan and K.K. Wei, 2003. An integrative study of information systems security effectiveness. Int. J. Inform. Manage., 23: 139-154.

Lee, C.P. and J.P. Shim, 2007. An exploratory study of radio frequency identification (RFID) adoption in the healthcare industry. Eur. J. Inform. Syst., 16: 712-724.

Markus, M.L. and J.Y. Mao, 2004. Participation in development and implementation-updating an old, tired concept for today's IS contexts. J. Assoc. Inform. Syst., 5: 514-544.

Munro, H. and H. Noori, 1988. Measuring commitment to new manufacturing technology: Integrating technological push and marketing pull concepts. IEEE Trans. Eng. Manage., 35: 63-70.

Myers, S. and D.G. Marquis, 1969. Successful Industrial Innovations: A Study of Factors Underlying Innovation in Selected Firms. National Science Foundation, Washington, DC., USA., Pages: 117.

Rogers, E.M., 2003. Diffusion of Innovations. 5th Edn., Free Press, New York, USA., pp: 27-30.

Schon, D.A., 1967. Technology and Change: The New Heraclitus. 1st Edn., Dell Publishing, New York, ISBN-10: 0080124925, pp: 270.

Shih, H.P., 2006. Technology-push and communication-pull forces driving message-based coordination performance. J. Strat. Inform. Syst., 15: 105-123.

Siponen, M.T., 2001. Five dimensions of information security awareness. Comput. Soc., 31: 24-29.

Spears, J.L. and H. Barki, 2010. User participation in information systems security risk management. MIS Q., 34: 503-522.

Templeton, G.F., B.R. Lewis and C.A. Snyder, 2002. Development of a measure for the organizational learning construct. J. Manage. Inform. Syst., 19: 175-218.

Teo, T.S.H., V.K.G. Lim and R.Y.C. Lai, 1999. Intrinsic and extrinsic motivation in internet usage. Omega, 27: 25-37.

Utterback, J.M., 1974. Innovation in industry and the diffusion of technology. Science, 183: 620-626.

Whitman, M.E., 2004. In defense of the realm: Understanding the threats to information security. Int. J. Inform. Manag., 24: 43-57.

Wixom, B.H. and H.J. Watson, 2001. An empirical investigation of the factors affecting data warehousing success. MIS Q., 25: 17-32.

Yeh, Q.J. and A.J.T. Chang, 2007. Threats and countermeasures for information system security: A cross-industry study. Inform. Manag., 44: 480-491.

Zhang, J., B.J. Reithel and H. Li, 2009. Impact of perceived technical protection on security behaviors. Inform. Manage. Comput. Secur., 17: 330-340.

Zhu, K., K.L. Kraemer and S. Xu, 2006. The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. Manage. Sci., 52: 1557-1576.

Zmud, R.W., 1982. Diffusion of modern software practices: Influence of centralization and formalization. Manage. Sci., 28: 1421-1431.