THE ORGANIZATIONAL CONTEXTS, CONTROLS AND IMPLEMENTATION OF E-BUSINESS

SANGJAE LEE
Sejong University
Seoul, Korea 143-747

HYUNCHUL AHN*
Kookmin University
Seoul, Korea 136-702

ABSTRACT

A control framework for successful business-to-consumer information systems (B2CIS) implementation was developed based on IS controls and implementation studies. Our research model suggests that top management support, system compatibility, IS infrastructure, IS expertise, and perceived importance of IS security affect four control modes: controls for system continuity, access controls, communication controls and informal controls. Furthermore, it posits that B2CIS controls affect B2CIS implementation, which has three dimensions: volume, sophistication, and information contents. Empirical tests indicated that IS infrastructure and perceived importance of IS security affect the usage of four modes of B2CIS controls, while system compatibility affects the usage of all these control modes except communication controls. The controls for system continuity are the most important controls for B2CIS implementation. This study provides insights into the adequacy of security measures undertaken under specific organizational circumstances for systems implementation.

Keywords: business-to-consumer information systems (B2CIS), organizational contexts, controls, implementation of B2CIS.

1. INTRODUCTION

The commercial use of the Internet has provided boundless opportunities for e-business between businesses and consumers or business-to-consumer information systems (hereafter B2CIS) to conduct transactions between a firm and the consumers of its products or services.

Security concerns have increased in all organizations worldwide with the attention of senior information security managers centered on incidents either published in the newsmedia or internally identified (Ezingeard et al., 2005). The 2008 Computer Security Institute/U.S. Federal Bureau of Investigation (CSI/FBI) found that respondents' estimates of the lośses caused by various types of computer security incidents was $288,618. The vast majority of the 522 respondents said their organizations either had (68 percent) or were developing (18 percent) a formal information security policy. Viruses, worms, hackers and employee abuse and misuse have increased the need for awareness of quality security measures (Whitman, 2004).

Using the recent development of mobile and wireless technologies, B2CIS can still be considered in the "contagion" stage in Nolan's stage-growth model of IS (Nolan, 1979), and sales through B2CIS have seen increasing growth in the B2C industry. The appropriate type of control strategies should be exercised at this stage. Thus, the sample can be considered appropriate for the study of security controls.

Previous studies proposed relationships among organizational factors, IS security measures, and IS security effectiveness (Kankanhalli et al., 2003), and the effect of various factors on security adoption such as firm size, industry type, top management support, moral compatibility, peer influence, and computing capacity (Lee and Kozar, 2005). Industry type and organizational use of IT were regarded as the two factors that influence security adoption (Yeh and Chang, 2007).

Despite the great demand for security in electronic commerce (EC), empirical academic studies to enhance the understanding of B2CIS security and controls in an organizational context remain lacking. Furthermore, despite a wealth of public evidence that organizational systems are far less secure than they should be and that systems risk is high, empirical studies on the effect of security and controls also remain lacking. There fore, a gap persists between current development in empirical research on IS security development and the observed requirements for security in Internet-based systems. This study intends to fill this gap and focuses on the effect of organizational contexts on formal and informal controls, as well as the effect of B2CIS controls on B2CIS implementation.

2. B2CIS CONTROLS

Control in general has been viewed primarily in a behavioral sense and has been applied in IS security (Lee et al., 2004; Lee et al., 1998; Suh and Han, 2003). IS controls, a subset of organizational controls, can be thought of as the processes through which an organization achieves its goals, i.e., asset safeguarding, data integrity, systems effectiveness, and system efficiency, through the implementation of IS. In this study, B2CIS controls are specifically defined as controls for security objectives (not general IS objectives) which encompass confidentiality, integrity and availability of systems.

Two broad classes of controls, formal and informal controls, have been identified in this study, which may broaden the scope of available portfolios of controls and overcome the problems (e.g., lack of understanding of controls in organizations) in the traditional cybernetic view of organizational control (Kirsch, 2004). Formal controls are written, management-initiated mechanisms that affect the probability that organizational members will behave in ways that support the purported organizational objectives (which is the cybernetic view of controls).

Formal IS controls are generally classified into management and application controls (Weber, 1999). Management controls

* *Hyunchul Ahn is the corresponding author.*

Received: August 14, 2009 Revised: October 23, 2009 Accepted: November 18, 2009

are fundamental controls in that they encompass general IS management, security management, IS development and maintenance, and operations management. The most important management controls among the B2CIS controls are controls for system continuity. This study suggests that controls for system continuity act as management controls.

In this study, access controls and communication controls are suggested as internal application controls and external application controls, respectively. Internal application controls deal with internal components of B2CIS systems such as the application system interface, while external controls are involved with external B2CIS systems networks, and the communication interface with customers and the network service provider.

Informal B2CIS controls in this study include risk awareness, a sense of responsibility, experience, and collaboration with colleagues for IS staff members in the operation of B2CIS. In the context of IS development or security, informal controls are represented as self controls such as user recognition of responsibility, and clan or social controls such as attachment, commitment, involvement and norms (Lee et al., 2004). The motivation of users to comply with security solutions is also important for the relevance of the security solutions provided (Siponen, 2001).

3. RESEARCH MODEL

Security effectiveness depends on various organizational factors such as size, top management support, industry type, managerial attitudes toward security risks, IT resource posture, and executive management support (Lee and Han, 2000; Kankanhalli et al., 2003; Kotulic and Clark, 2004). A B2CIS controls model ties together five factors representing organizational and IS-related factors. Other variables that have a second- or lower-order effect on B2CIS controls are not included.

The effects of an independent factor on controls for system continuity, access controls, and communication controls are based on similar reasons, as these controls are formal and management-initiated procedures, and technology-based controls. The effect on informal controls can be explained as five independent factors that provide a favorable environment to influence directly or indirectly risk awareness, sense of responsibility, experience, and collaboration. The research model is depicted in Figure 1.

3.1 Organizational Contexts and B2CIS Controls

(1) Top management support

Top management support is a key requirement for successful implementation of any system. Given the substantial amount of resources needed for B2CIS, top management should be expected to perform a crucial role, leveraging these resources to effectively implement controls and assimilate the controls procedures throughout the organization (Weber, 1999). Kankanhalli et al. (2003) posit that more financial and technical resources will be made available for IS security with top management support. The market/sales function may consider B2CIS controls as a strategic necessity for their business survival and seek top management support for the B2CIS controls. Top management may support training and education for IS and security and this helps promote risk awareness, a sense of responsibility, and the experience of IS staff members.

> Hypotheses 1-1, 1-2, 1-3, 1-4: The greater the extent of top management support, the more likely B2CIS controls (controls for system continuity, access controls, communication controls and informal controls) will be used.

(2) System compatibility

Compatibility with existing attitudes, beliefs, value systems and IS infrastructure ensures less resistance to the adoption, greater security and lesser risk to the adopter (Teo et al., 1997). The alignment in system control with a reengineered work process is critical to sustain reengineering effectiveness (Sia and Neo, 1997). Most organizations would choose to use B2CIS controls if these controls fit easily with their organizational practices, culture, values, and IS infrastructure, requiring minimal adjustments and changes. Further, compatibility promotes risk awareness, a sense of responsibility, and collaboration of users because it fosters interoperable system environments that facilitate error propagation as well as cooperative work environments.

> Hypotheses 2-1, 2-2, 2-3, 2-4: The greater the compatibility of B2CIS, the more likely B2CIS controls (controls for system continuity, access controls, communication controls and informal controls) will be used.

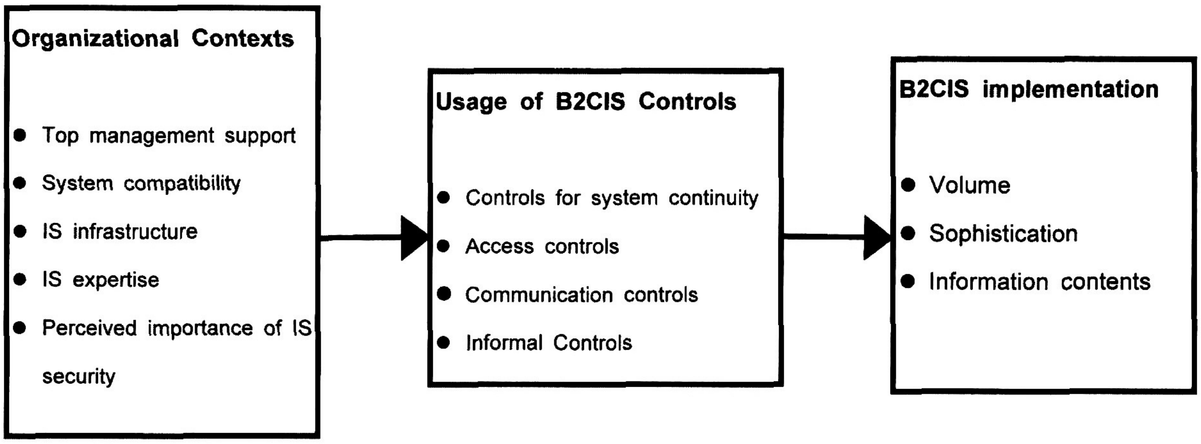

FIGURE 1: Research Model

(3) IS infrastructure

Range-enabling complex transactions and boundary-crossing services across multiple business units are possible through a rich set of infrastructure capabilities (Broadbent et al., 1999). Kotulic and Clark (2004) suggest that IT resource posture, including all of the technologies, capabilities, data and information, affects security program effectiveness. Organizations with an appropriate level of cross-functional and cross-business applications and telecommunications infrastructure, firm-wide consistency in architecture and standards for system development and operation, and experience with integrated database applications are better prepared for B2CIS controls. Such controls are likely to be better implemented in a sophisticated IS infrastructure composed of multiple platforms with different operating systems, applications, and connectivity arrangements. Further, IS infrastructure is related to risk awareness, a sense of responsibility, experience and collaboration of users due to the need for highly sophisticated system resources and integrated systems.

> Hypotheses 3-1, 3-2, 3-3, 3-4: The greater the IS infrastructure, the more likely B2CIS controls (controls for system continuity, access controls, communication controls and informal controls) will be used.

(4) IS expertise

One of the reasons for the failure of small business to utilize IS is lack of IS knowledge (Thong, 1999). The pool of diverse expertise available in organizations is a key element in reducing knowledge barriers during IS implementation. IS expertise is described as knowledge and know-how in advanced technology and methodology in IS (e.g., Internet, telecommunications, enterprise resource planning, knowledge management). However, organizations with less IS expertise have lower technical knowledge and technical potential for B2CIS controls. Organizations with IS expertise can provide a reservoir of assistance for problems or difficulties in the implementation of controls as they occur. A high-degree of in-house expertise in information technologies, especially in Internet and Web-based information systems, is expected to enhance the propensity of an IS department to acquire or implement B2CIS controls. Further, IS expertise affects risk awareness, sense of responsibility, experience and collaboration of users due to a high level of system knowledge owned by users.

> Hypotheses 4-1, 4-2, 4-3, 4-4: Organizations with greater IS expertise will be more likely to implement B2CIS controls (controls for system continuity, access controls, communication controls and informal controls).

(5) Perceived importance of IS Security

Kotulic and Clark (2004) suggest that managerial attitudes toward risk influence management choices relative to the appropriate security measures required. With the growing dependence on IS to increase organizational effectiveness and productivity, the demand for reliability and integrity of information becomes greater (Zviran and Haga, 1999), which increases the necessity of B2CIS controls. The Internet might not always provide the cheaper alternative medium for transactions due to security concerns. Customers do not feel comfortable when they send sensitive information over the Internet if the confidentiality and integrity of the communications and transactions are not ensured. Hence, the higher the security concerns of an organization, the higher the likelihood that B2CIS controls will increase. Further, perceived importance of IS security is positively related to risk awareness, sense of responsibility, experience and collaboration of users, as they may recognize the importance of security and controls for B2CIS and are prepared to take action.

> Hypotheses 5-1, 5-2, 5-3, 5-4: The greater the perceived importance of IS security, the more likely B2CIS controls (controls for system continuity, access controls, communication controls and informal controls) will be used.

3.2 B2CIS Controls and Implementation

IS implementation indicates a major component of an organization's expenditures on new IT and have implementation outcomes such as increased systems use, user satisfaction, systems quality, and budget and schedule performance (Wybo, 2007). The implementation of B2CIS is defined by the extent of B2CIS implementation, as represented by volume, sophistication, and information contents.

The effect of controls on B2CIS implementation can be based on the following considerations. First, before an organization decides to implement B2CIS, the controls for B2CIS need to be planned in order to establish the belief that the system is safe and accurate to users and to increase the capability for implementation and adjustment. Many consumers are discouraged from carrying out transactions via the Internet due to concerns about theft of credit card numbers and other confidential personal information (Yeh and Chang, 2007). Stakeholders such as customers, internal users, trading partners, and industrial associations demand "control assurance" before further implementation of a system. Although IS security is not the only factor slowing down the proliferation of e-commerce, the perceived lack of security is still one of the most likely reasons for the low utilization of online selling and electronic payment systems (Suh and Han, 2003). In the case of EC, customers still demand an "adequate" level of controls that are specified in agreements with the company before sending confidential information (Keller et al., 2005).

Second, the positive influence of controls on implementation can be discussed in light of the IS stage model. The stage model for IS suggests that IS controls are increasingly important as IS installation passes through a lower inflexion point where the IS implementation begins to proceed rapidly with a steep ascent (Nolan, 1979). Security and integrity controls still need to be regarded as basic subsystems in the growth of IS systems. Thus, three modes of formal controls affect B2CIS implementation:

> Hypotheses 6-1, 6-2, 6-3: The usage level of controls for system continuity directly affects B2CIS implementation (volume, sophistication, information contents).

> Hypotheses 7-1, 7-2, 7-3: The usage level of access controls directly affects B2CIS implementation (volume, sophistication, information contents).

> Hypotheses 8-1, 8-2, 8-3: The usage level of communication controls directly affects B2CIS implementation (volume, sophistication, information contents).

Previous organizational studies on accounting controls have suggested the need for the balanced use of various types of organizational control systems (Merchant, 1985). In the context of IS, the formal system lies within a larger informal environment where social beliefs and understanding are established, and commitments and responsibilities are created (Dhillon and Backhouse, 1996). This indicates that management should use a multifaceted approach that stresses informal controls derived from a sense of responsibility and moral commitment as well as formal codes of ethics to ensure computer security.

Informal controls may increase the effectiveness of formal rules, as they represent the extent of the perception of certainty and severity of "sanctions" against committing a deviant act. When potential offenders perceive a high risk of legal punishment or penalties for violation of procedures, they are dissuaded from illicit behavior (Brungs and Jamieson, 2005). Although formal procedures themselves are still essential to protect and safeguard a system, it is equally important for security administrators to make the presence of formal controls felt through attachment, commitment, involvement, and norms (Lee et al., 2004). The severity of punishment must be clearly recognized by system users through education and training in order to prevent antisocial acts by employees. Prior experience is also a key molder of security expectations. Users will demand more controls if they have experienced control failures or security incidents. Thus, from these arguments, there exist the effects of informal controls on B2CIS implementation.

> Hypotheses 9-1, 9-2, 9-3: The usage level of informal controls directly affects B2CIS implementation (volume, sophistication, information contents).

4. RESEARCH METHOD

4.1 Research Design

The data used in validating the research model was gathered as part of a research project on B2CIS implementation (Lee and Ahn, 2007; Lee and Kim, 2007). A structured interview based on a questionnaire was the main method of data collection. One of the researchers visited each of the companies in the sample and the structured interview was conducted with IS staff members. The mail survey method through e-mail or postal delivery was avoided because of the difficulty in obtaining reliable responses from the questionnaire, which addressed such sensitive and confidential issues as IS security and controls. In contrast, interviews stimulate trust and cooperation, which are often required to obtain sensitive information about control systems. Personal contact tends to elicit full, frank responses. In addition, it was important to make sure that these items could be answered by practitioners. Interviews provided the opportunity to aid the respondents in their interpretation of the questions and to allow flexibility in determining the sequence and wording of the questions.

4.2 Participants

The survey instruments were first tested by interviewing B2CIS practitioners. In this pilot testing, wording was corrected to give the right interpretation. The extent to which practitioners felt they possessed the knowledge necessary to provide appropriate responses was evaluated and some items were modified to indicate a more straightforward meaning.

The unit of analysis in this study was the individual B2CIS adopter. Among Korean companies that have adopted B2CIS, companies which seem to have too low a level of B2CIS implementation were excluded, as questions about controls can be answered reliably only by companies which have implemented B2CIS to some extent. 130 were randomly sampled from diverse industries and their B2CIS adoption states confirmed. Ten companies refused to participate in the interview. Some of these companies were afraid of exposing system vulnerabilities. Hence, a total of 120 companies provided analyzable responses.

TABLE 1: Positions of respondents

Position	Number of respondents	Percentage of respondents
Executives	14	11.7
Executive Manager	9	7.5
Manager	27	22.5
Assistant Manager	38	31.7
Employees of Lower Level	32	26.7

TABLE 2: Profile of Sample

Types of the company	Number of Companies	Percentage (%)
Retail industry		
— book store	5	4.2
— sellers of computer related equipments	14	11.7
— shopping malls	5	4.2
— other retailers	11	9.2
Bank	9	7.5
Stock trading	23	19.2
Travel/Tourism/Hotel	8	6.7
Printing/Publishing	2	1.7
Electronic business	22	18.3
Electronic auction	2	1.7
Game business	4	3.3
Education business	3	2.5
Communication service	5	4.2
Media	2	1.7
Manufacturing	5	4.2
Total	120	100

TABLE 3: Elapsed time of B2CIS implementation

Firm size	No. of firms	% of firms
Elapsed time < 1 year	5	5
1 year ≤ elapsed time < 2 year	35	29.2
2 year ≤ elapsed time < 3 year	32	26.7
3 year ≤ elapsed time < 4 year	20	16.7
4 year ≤ elapsed time < 5 year	14	11.7
5 ≤ elapsed time	12	10
Missing	1	0.8

Respondents were B2CIS staff or managers. If they did not know exactly how to respond to some of the questions, they called upon more knowledgeable staff members to help complete the responses and consulted with colleagues who had sufficient knowledge of the subject area. Differences in the organizational levels of respondents did not significantly influence their responses. The characteristics of respondents and sample firms are suggested in Tables 1, 2, and 3. About 53.4% of the responding organizations had more than 50 employees.

4.3 Measures

Tables 4, 5, 6 describe the operationalization of each variable in organizational contexts, controls, and implementation along with corresponding references. Most of the variables in the model are measured by items written in the form of a statement with which the respondent is to agree or disagree on a 7-point Likert-type scale. Items for the independent variables were refined based on earlier empirical work on innovation.

Items for B2CIS controls were refined based on various studies concerning IS controls such as Weber (1999), and ISACA (2009) that explain the concepts, objectives, characteristics, and techniques of IS controls and auditing. The items for the constructs indicate the usage level of B2CIS controls.

The measures for B2CIS implementation are based on the adoption and implementation literature on EC, especially EDI and the Internet, (Massetti and Zmud, 1996; Premkumar and Ramamurthy, 1995) (Table 6). The measures for B2CIS volume indicate the proportion that a company uses B2CIS rather than other complementary means such as e-mail or fax. B2CIS sophistication represents the level of sophistication in the use of different types of business functions that are handled through B2CIS. B2CIS sophistication also includes the extent to which an organization's business processes are integrated with B2CIS. Information contents of B2CIS indicate the extent to which various types of information related to products and services is provided effectively to customers. The items of information contents include the provision of searching products/services information, and provision of related information.

5. RESULTS

5.1 Measurement Properties

Validity and reliability tests were conducted for each variable. Construct validity was assessed using convergent and discriminant validity. Convergent and discriminant validity can be tested using principal component factor analysis (with varimax rotation). Separate domain factor analyses were performed with items belonging to factors in organizational contexts factors affecting controls, items belonging to controls, and items belonging to implementation. The three commonly employed decision rules for identification of factors – minimum eigenvalue of 1, simplicity of structure, minimum factor loading of 0.5 – were followed (Hair et al., 1979). Tables 7, 8, and 9 show the results of the final factor analysis; the internal reliability coefficient (Cronbach's alpha), the items associated with each factor, each item's factor loading, and each factor's eigenvalue.

The principal component factor solution with varimax rotation explained 69.4 percent of the systematic covariance among the

TABLE 4: Items for organizational contexts affecting B2CIS controls

Variables	Description of items	Sources
Top management support	The investment of adequate financial and other resources for the development and operation of B2CIS (TOP1) The interest of top management in using B2CIS (TOP2) The awareness of top management of the benefits of new technologies (TOP3) The vision of top management to project respondent's firm as a leader in the use of B2CIS (TOP4)	Grover (1993) Premkumar and Ramamurthy (1995)
System compatibility	Implementing the changes caused by the adoption of B2CIS is compatible with existing operating practices. Implementing the changes to work procedures initiated by the adoption of B2CIS is compatible with the beliefs and values existing in our firm. The adoption of B2CIS is compatible with firm's IT infrastructure. There exist favorable attitudes toward B2CIS adoption within our firm.	Premkumar and Ramamurthy (1995) Reich and Benbasat (1900) Rogers (1995)
IS infrastructure	The existence of a good telecommunications infrastructure (INF1) The existence of shared databases for various applications (INF2) The existence of integrated IS applications encompassing different functional areas (INF3) The existence of firm-wide communication network services (INF4) The existence of large-scale data processing facilities (INF5) The existence of firm-wide messaging services (INF6)	Broadbent et al. (1999) Grover (1993) Premkumar and Ramamurthy (1995)
IS expertise	The IS employees' awareness of the functions of advanced technology and methodology in IS (e.g., Internet, telecommunications, enterprise resource planning, knowledge management) (EXP1) The existence of many experts on advanced technology and methodology in IS (EXP2) The IS employees' understanding of advanced technology and methodology in IS (EXP3) The IS employees' knowledge of advanced technology and methodology (two items) (EXP4, EXP5)	Thong (1999)
Perceived importance of IS security	The importance of the responsibility related to IS security (CON1) The loyalty of customers to security functions (CON2) The importance of security control procedures for overall system performance (CON3) The sensitiveness of system performance to errors and system failures (CON4)	ISACA (2009)

27 scale items for B2CIS controls. The results revealed that all the variables, except controls for system continuity and access controls, were separately loaded on the same factor as originally suggested. The five items measuring controls for system continuity and the three items measuring access controls loaded on a single factor. To determine if they are separate constructs, both the theoretical conceptualization and empirical validation were examined. Past literature on IS security and controls (ISACA, 2009; Weber, 1999) has clearly differentiated between these two constructs and the theoretical conceptualization of

TABLE 5: Items for controls

Variables	Description of items	Sources
Controls for system continuity	Contingency planning procedures to ensure system and network continuity in a timely fashion (CN1-1) Procedures for error logging, incident reporting and correction of errors (CN1-2) Review procedure to ensure that the unauthorized processing is followed up (CN1-3) Procedures for recording messages for the correction of errors and reprocessing of corrected messages (CN1-4) Backups of the critical data and program files (CN1-5)	ISACF (1992) Weber (1999)
Access controls	Access control procedures such as passwords to control system login (CN2-1) Usage of access controls software to control access to sensitive files and programs (CN2-2) Automated authentication procedures embedded in system to ascertain the identity of system users (CN2-3)	
Communication controls	Authentication of the content of user activities while they are using system (CN3-1) Suspension of system access (e.g., the disability of terminal, microcomputer, or data entry device activity) in case of the security violations of users (CN3-2) Checking of transaction messages for duplication, omission or inaccuracies before the messages are processed in the application (CN3-3) Checking of transaction messages for duplication, omission or inaccuracies after they are generated and before being transmitted (CN3-4) Authentication of the receiver or sender of transaction messages after the messages are generated or received (CN3-5) Usage of embedded software to check correctness of data fields before received messages are processed in internal applications (CN3-6) Retransmission of messages if the messages are omitted, duplicated, or inaccurate (CN3-7) Usage of network software that helps promptly correct corrupt and improper transaction messages (CN3-8) Usage of message identification codes or digital signatures to effectively authenticate the messages (CN3-9) Encryption of high risk data (e.g., customer credit card number, password) using the encryption tools during their transmission (CN3-10)	
Informal controls	Recognition of the risks of the possible propagation of errors from one system to another (CN4-1) Recognition of the importance of their responsibility for the performance of B2CIS (CN4-2) Recognition of the possibility that their work can significantly affect organizational performance (CN4-3) Usage of experience to cope with system errors (CN4-4) Usage of experience to identify which security procedures should be applied strictly (CN4-5) Communication of information with colleagues to process tasks (CN4-6) Cooperation with colleagues to assist in correcting errors (CN4-7) Trust of the security related works of colleagues (CN4-8) Appraisals of security related works of colleagues to see whether they are incorrect (CN4-9)	

TABLE 6: Items for implementation

Variables	Description of items	Sources
Volume (%)	The extent (%) to which an organization's transactions with consumers are handled through B2CIS (VOL)	Hart and Saunders (1998) Massetti and Zmud (1996)
Sophistication	Provision of authentication service (SOP1) Easiness in ordering products / services (SOP2) Sophistication in the usage of video image, and in interface display (SOP3) The integration with electronic payment system (SOP4) The integration with customer database system (SOP5) The integration with accounting system (SOP6) The integration with inventory and logistics system (SOP7)	Huizingh (2000) McGowan and Madey (1998) Ramamurthy and Pemkumar (1995)
Information contents	Provision of product browse function (CONT1) Provision of functions that search products / services using various conditions (CONT2) Provision of company information (CONT3) Provision of information concerning maintenance and use of products/ service (CONT4)	Huizingh (2000) Spiller and Lohse (1997-1998)

TABLE 7: Measurement properties for the scale items of organizational contexts affecting B2CIS controls

Variables	Items	Loadings	Alpha Value	Eigen Value
Top Management Support	TOP1 TOP2 TOP3 TOP4	0.708 0.867 0.820 0.875	0.842	2.75 (34.4)
System Compatibility	COMPA1 COMPA2 COMPA3 COMPA4	0.593 0.794 0.639 0.549	0.657	2.70 (33.8)
IS infrastructure	INF1 INF2 INF3 INF4 INF5 INF6	0.606 0.629 0.809 0.568 0.600 0.525	0.847	3.31(22.0)
IS expertise	EXP1 EXP2 EXP3 EXP4 EXP5	0.728 0.753 0.690 0.751 0.731	0.892	3.84 (25.6)
Perceived importance of IS security	CON1 CON2 CON3 CON4	0.758 0.848 0.867 0.772	0.835	2.70 (33.8)

the study has followed those definitions. On the empirical side, a separate factor analysis of the items measuring just those two variables was performed. The results revealed that they loaded on two separate factors, confirming that they are two independent constructs. These results give us confidence in controls for system continuity and access controls as two separate variables. All the items exhibited adequate discriminant validity since no significant cross-loading of items among factors was noticed.

The principal component factor solution with varimax rotation produced a two-factor solution that explained 66.7 percent of the systematic covariance among the 11 scale items for B2CIS implementation. All two empirically derived factors had eigenvalues greater than one. Seven items were dropped from the original scale items for B2CIS implementation due to their failure to address the decision rules in factor analysis.

The coefficient alphas of the research variables are indicated in Tables 7, 8, 9. All scales exhibited sufficient reliability as they exceeded Nunnally's (1978) reliability guidelines of 0.7. The factor analysis and reliability analysis show moderate or strong evidence for the validity and reliability of the research variables.

5.2 Test of Hypotheses

Given the exploratory nature of the study, the multiple regression method was used to test the research model. Multiple regression analyses were performed for each of the four controls variables as dependent variables (Table 10). The standardized beta and t-values are suggested for each independent variable. Multiple regression analyses were performed for each of the three dependent variables of B2CIS implementation (Table 11).

TABLE 8: Measurement properties for the scale items of B2CIS controls

Variables	Items	Loadings	Alpha Value	Eigen Value
Controls for system Continuity	CN1-1 CN1-2 CN1-3 CN1-4 CN1-5	0.784 0.846 0.764 0.779 0.546	0.903	3.31 (41.3)
Access Controls	CN2-1 CN2-2 CN2-3	0.843 0.804 0.877	0.926	2.95 (36.9)
Communication Controls	CN3-1 CN3-2 CN3-3 CN3-4 CN3-5 CN3-6 CN3-7 CN3-8 CN3-9 CN3-10	0.688 0.674 0.818 0.820 0.778 0.811 0.743 0.791 0.691 0.589	0.944	6.49 (34.2)
Informal Controls	CN4-1 CN4-2 CN4-3 CN4-4 CN4-5 CN4-6 CN4-7 CN4-8 CN4-9	0.718 0.820 0.777 0.803 0.756 0.732 0.571 0.737 0.724	0.934	6.22 (32.8)

TABLE 9: Measurement properties for the scale items of B2CIS implementation

Variables	Items	Loadings	Alpha Value	Eigen Value
Volume (%)	VOL	NA	NA	NA
Sophistication	SOP1 SOP2 SOP3 SOP4 SOP5 SOP6 SOP7	0.771 0.581 0.535 0.789 0.751 0.800 0.817	0.892	3.99 (36.2)
Information Contents	CONT1 CONT2 CONT3 CONT4	0.875 0.816 0.770 0.758	0.867	3.36 (30.5)

NA: Because the variable is composed of a single item, no reliability and validity analysis is conducted.

Hypothesis 1-3 is accepted as top management support significantly affects communication controls. System compatibility significantly affects controls for systems continuity, access controls, and informal controls, which supports hypotheses 2-1, 2-2, and 2-4. IS infrastructure and perceived importance of IS security are the most important factors for controls, as all the hypotheses,

TABLE 10: Multiple regression results
(Independent variables: organizational contexts, dependent variables: B2CIS controls, *** p < 0.01, ** p < 0.05, * p < 0.1)

Dependents	Controls for systems continuity		Access controls		Communication controls		Informal controls	
Independents	Beta	t value (p value)	Beta	t value (p value)	Beta	t value (p value)	Beta	t value (p value)
Top management support	0.088	0.939 (0.175)	0.025	0.256 (0.399)	-0.148	-1.542 (0.063)*	0.071	0.815 (0.209)
System compatibility	0.157	1.821 (0.035)**	0.167	1.903 (0.030)**	0.089	1.016 (0.156)	0.145	1.826 (0.035)**
IS infrastructure	0.409	3.520 (0.000)***	0.338	2.863 (0.003)***	0.424	3.590 (0.000)***	0.318	2.977 (0.002)***
IS expertise	0.019	0.166 (0.434)	0.101	0.881 (0.190)	0.098	0.857 (0.197)	0.077	0.738 (0.231)
Perceived importance of IS security	0.177	2.332 (0.010)***	0.215	2.772 (0.004)***	0.320	4.146 (0.000)***	0.367	5.235 (0.000)***
R²	0.648		0.632		0.633		0.713	
Adjusted R²	0.394		0.373		0.401		0.487	
F	16.495		15.142		15.272		23.568	
Sig. F	0.000***		0.000***		0.000***		0.000***	

TABLE 11: Multiple regression results
(Independent variables: B2C controls, dependent variables: B2CIS implementation, *** p < 0.01, ** p < 0.05, * p < 0.1)

Dependents	Volume		Sophistication		Information contents	
Independents	Beta	t value (p value)	Beta	t value (p value)	Beta	t value (p value)
Controls for system continuity	0.225	1.504 (0.068)*	0.195	1.571 (0.060)*	0.310	2.441 (0.008)***
Access controls	-0.205	-1.099 (0.137)	-0.116	-0.745 (0.229)	-0.388	-2.449 (0.008)***
Communication controls	-0.236	-1.448 (0.075)*	0.499	3.678 (0.000)***	0.351	2.534 (0.006)***
Informal controls	0.409	2.743 (0.004)***	0.133	1.063 (0.145)	0.340	2.680 (0.004)***
R²	0.105		0.433		0.352	
Adjusted R²	0.074		0.411		0.330	
F	3.379**		19.509***		15.629***	
Sig. F	0.012		0.000		0.000	

hypotheses 3-1, 3-2, 3-3, 3-4, 5-1, 5-2, 5-3 and 5-4,j are supported. IS expertise, however, fails to affect controls, which contradicts hypotheses 4-1, 4-2, 4-3, and 4-4.

Hypotheses 6-1, 6-2, and 6-3 are accepted as controls for system continuity, and they significantly and positively affect volume, sophistication, and information contents. Access controls do not significantly and positively affect all three controls, rejecting hypotheses 7-1, 7-2, and 7-3. Communication controls significantly affect sophistication and information contents. Thus, hypotheses 8-2 and 8-3 are partly accepted. Hypothesis 9-1 and 9-3 are accepted as volume and information contents are affected by informal controls.

6. DISCUSSIONS AND CONCLUSION

6.1 Summary of Findings

Top management support weakly affect B2CIS controls, which indicates that the implementation of controls is less affected by management support than by other system characteristics like system compatibility and IS infrastructure. This indicates that top management does not play an active role in reinforcing security, probably due to their low recognition of security and controls.

System compatibility significantly affects three of four controls, which indicates the precondition of controls involves the compatibility between B2CIS and present application systems. Organizations are faced with an extremely complex IT environment composed of different IT platforms demanding a more cautious process in the planning of security controls. The low system compatibility increases system complexity due to the incompatible interconnection arrangements of individual hardware and software components to integrate the system, thereby not attaining significant benefits from the control systems. Further, compatible systems demand more usage of controls given that security risks can be propagated more easily from one system to another in such environments. Thus system compatibility increases both the ease of implementation of B2CIS controls and the necessity of controls to mitigate threats in highly interconnected system environments, which is possible through system compatibility.

The significant effect of IS infrastructure on B2CIS controls indicates that sophisticated IS infrastructure demands that controls should be promptly operated to identify errors or failures in a timely fashion so that subsequent processing is not delayed or affected, reducing the severity or problems at a later stage; appropriate backup, retention, and contingency plans need to be in place to minimize the domino effect of systems failure or message errors on existing systems. This supports the notion that security needs differ in relation to organizational computerization (Yeh and Chang, 2007). As a part of the IS development plan, security planning should be upgraded according to the development stages of IS determined by IS infrastructure. Business should use IS infrastructure as a starting point for understanding their security requirements and adopt appropriate security countermeasures.

IS expertise fails to affect B2CIS controls, which indicates that controls are provided as routine procedures by vendors during the implementation of B2CIS and the implementation and operation of controls do not require much in-house IS expertise. Vendors provide several options in controls which are standardized according to the state of customers' systems and customers can select one of these options.

The significant effect of the perceived importance of IS security on controls indicates that as system users recognize the necessity of system security, more controls will be implemented. When users recognize the impact of errors on organizational performance, they will enforce, for instance, more application level checking before commencing each stage of internal processing. This supports the assertion that managers' perceptions of potential IS threats are critical to security adoption (Yeh and Chang, 2007). An online edit check and reconciliation can be considered to check uniqueness and serial continuity of the sequence number of transactions and make their value acceptable among different applications.

The significant effects of system compatibility, IS infrastructure, and perceived importance of IS security on informal controls indicate that knowledge and experience regarding security, and informal discussions among employees, might become important as system compatibility, IS infrastructure, and perceived importance of IS security increase the necessity of system guidelines and security practices. This supports the importance of human morality in IS security (Siponen, 2001), and the recommendation of Khalfan (2004) that security management must address end-user security awareness and education. Further, as a professional's knowledge about a task increases and his expertise grows, the professional's perceptions of self-control increase. Professional IS staff members are expected to exercise greater levels of self-control when they internalize the core values "Confidentiality, Integrity and Availability of information," as a guideline for system management and improved customer service.

The significant effect of controls for system continuity on B2CIS implementation indicates that appropriate backup, retention, and contingency plans need to be in place to minimize the domino effect of systems failure or message errors on existing systems. The purpose is to identify errors or failures in a timely fashion so that subsequent processing is not delayed or affected, reducing the severity of security problems at a later stage. The impacts of communication controls on sophistication and information contents are significant, indicating that as companies increase the sophistication and information contents of B2CIS, they recognize the need for a high level of formalized procedures and technical controls to manage various types of transactions and connections with customers.

The significant effects of informal controls on implementation indicate that knowledge and experience regarding security, and informal discussions among employees become important as they might extend to B2CIS implementation. As the probability of detection and the severity of penalties are made clear to employees, abusive actions or unintentional breaches of security decrease and customer satisfaction with Internet-based transaction processes increases. The role of informal controls can be greater when the risks from a highly automated and sophisticated system are diverse. B2CIS adopters and their staff members need to rely on their experience, knowledge of role expectations, security-related knowledge and skills, and social beliefs to cope with inadvertent errors and failures.

The effect of access controls on B2CIS implementation is not significant, and this indicates weak intent to install access controls given the high expertise and resources needed to develop and maintain access controls for a sophisticated B2CIS system, and to ensure convenient and easy access.

6.2 Implications

The growing dependence on IS to increase organizational effectiveness and productivity creates demand for studies on the factors affecting B2CIS controls. IS management departments could obtain guidance on the extent and type of controls to be implemented in B2CIS. IS management should review system compatibility and IS infrastructure before implementing IS controls. The potential impact of security breaches and errors, which contributes to increasing security concerns, should be decided to determine the extent of the controls to be implemented. From a security management and planning perspective, future studies should weigh the usage rate of security measures against their effectiveness in enhancing system performance.

IS managers should pay attention to the importance of controls in the Internet environment for successful implementation of B2CIS. One way of increasing the level of concern about security is to perform penetration testing and report IS vulnerabilities as well as business impact to management and users. Another way is explaining to top management how IS security can provide tangible business benefits by raising the level of confidence customers have in their organization. Some form of management and user education may thus be necessary in the context of IS security (Khalfan, 2004).

Managers should focus on controls for system continuity and, further, how to reinforce both controls for system continuity and informal controls. The communication controls and informal controls are also simultaneously enhanced. The first strategy largely emphasizes "automated controls" enabled by IT (e.g., edit checks, user authentication using passwords, file backup), while the next control strategy emphasizes "humanistic controls" (e.g., improved communication, social norms, enhanced personal commitment, work experience). These combined controls will overcome security issues being confronted in the implementation of controls for B2CIS more than when they are established separately. Controls and system continuity and communication controls can be more effective when their users are responsible, faithful, knowledgeable and experienced enough to assess whether the control activities meet their functional goals, and to oversee security efforts for the implementation of B2CIS. In order to expand system implementation, controls for system continuity and communication controls should be accompanied by an appropriate level of risk recognition, sense of responsibility, experience, and interaction of internal system users and IS staff members.

6.3 Limitations

It will be interesting to investigate the differences in security and controls among industries in future studies using a larger sample base. The generalizability of this study's findings could be limited because the sample was composed of Korean companies only. In future studies, it may be necessary to include a diverse set of companies in other countries. Further, this study focuses on the internal organizational view of controls of B2CIS and it is important to assess customers' perceptions of security and controls given the customer-oriented nature of B2CIS. Moreover, the measures of controls which are exploratory in nature and other variables (e.g., system compatibility) used in this study should be more rigorously developed in future studies. In addition, this study used a multiple regression method to test the research model. Future studies could use a structural equations model to rigorously test causal relations among variables using a larger amount of data.

6.4 Conclusion

A major premise of the study was that there exists a direct relationship between contextual factors and the usage of the appropriate security measures required. Furthermore, the research model posits that B2CIS controls affect B2CIS implementation. IS infrastructure and perceived importance of IS security affect the usage of four dimensions of B2CIS controls, while system compatibility affects the usage of three out of four dimensions of B2CIS controls except communication controls. The controls for system continuity are the most important controls for B2CIS implementation.

This study provides insights on the theory and practice of IS controls by examining factors affecting B2CIS controls. Study of the factors that affect B2CIS controls can indicate the direction of the control design. The empirical evidence regarding the effect of controls on implementation in B2CIS provides a basis for logical and prudent decision procedures when managers have to determine the mode and level of controls in the process of B2CIS implementation for overall system success and high efficiency of the control systems.

REFERENCES

[1] Broadbent, M., Weil, P., Clair, D.S. "The implications of information technology infrastructure for business process redesign," *MIS Quarterly* (23:2), 1999, 159-182.

[2] Brungs, A., Jamieson, R. "Identification of legal issues for computer forensics," *Information Systems Management*, 2005, 57-66.

[3] Computer Security Institute (CSI), CSI/FBI computer crime and security survey, http://www.gocsi.com/forms/csi_survey.jhtml, 2008.

[4] Dhillon, G., Backhouse, J. "Risks in the use of information technology within organizations," *International Journal of Information Management* (16:1), 1996, 65-74.

[5] Ezingeard, J.N., McFadzean, E., Birchall, D. "A model of information assurance benefits," *Information Systems Management*, Spring, 2005, 20-29.

[6] Hair, J.F., Anderson, R.E., Tatham, R.L., Grablowsky, B.J. *Multivariate Data Analysis,* Tulsa, OK; PPC Books, 1979.

[7] Hart, P.J., Saunders, C.S. "Emerging electronic partnerships: Antecedents and dimensions of EDI use from the supplier's perspective," *Journal of Management Information Systems* (14:4), Spring 1998, 87-111.

[8] Huizingh, E.K.R.E. "The content and design of Web sites: An empirical study," *Information & Management* 37, 2000, 123-134.

[9] ISACA (Information Systems Audit and Control Association), COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd edition, 2009.

[10] Kankanhalli, A., Teo, H.H., Tan, B.C.Y., Wei, K.K. "An integrative study of information systems security effectiveness," *International Journal of Information Management* (23), 2003, 139-154.

[11] Keller, S., Powell, A., Horstmann, B., Predmore, C., Crawford, M. "Information security threats and practices in small business," *Information Systems Management*, 2005, 7-19.

[12] Khalfan, A.M. "Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors," *International Journal of Information Management* (24), 2004, 29-42.

[13] Kirsch, L.J. "Deploying common systems globally: The dynamics of control," *Information Systems Research* (15:4), 2004, 374-395.

[14] Kotulic, A.G., Clark, J.G. "Why there aren't more information security research studies," *Information & Management* (41), 2004, 597-607.

[15] Lederer, A.L., Mirchandani, D.A., Sims, K. "The link between information strategy and electronic commerce," *Journal of Organizational Computing and Electronic Commerce* (7:1), 1997, 17-34.

[16] Lee, S., Ahn, H. "Fuzzy cognitive map based on structural equation modeling for the design of controls in business-to-consumer e-commerce web-based systems," *Expert Systems With Applications* (36:7), 2009, 10447-10460.

[17] Lee, S., Han, I. "The impact of organizational contexts on EDI controls," *International Journal of Accounting Information Systems* 1, 2000, 153-177.

[18] Lee, S., Han, I., Kym, H. "The impact of EDI controls on EDI implementation," *International Journal of Electronic Commerce* (2:4), Summer 1998, 71-98.

[19] Lee, S., Kim, K. "Factors affecting the Implementation Success of Internet based Information Systems," *Computers in Human Behavior* (23:4), July 2007, 1853-1880.

[20] Lee, Y., Kozar, K.A. "Investigating factors affecting the adoption of anti-spyware systems," *Communication of the ACM* (48:8), 2005, 72-78.

[21] Lee, S.M., Lee, S.G., Yoo, S. "An integrative model of computer abuse based on social control and general deterrence theories," *Information & Management* (41), 2004, 707-718.

[22] Massetti, B., Zmud, R.W. "Measuring the extent of EDI usage in complex organizations: Strategies and illustrative examples," *MIS Quarterly* (20:3), September 1996, 331-345.

[23] McGowan, M.K., Madey, G.R. "The influence of organization structure and organizational learning factors on the extent of EDI implementation in U.S. firms," *Information Resources Management Journal* (11:2), Summer 1998, 17-27.

[24] Merchant, K.A. *Control in Business Organizations*, Boston: Pitman Publishing, 1985.

[25] Nolan, R.L. Managing the crises in data processing, *Harvard Business Review*, March-April 1979, 115-126.

[26] Nunnally, J.C. *Psychometric Theory*, New York:McGraw-Hill, 1978.

[27] Premkumar, G., Ramamurthy, K. "The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems," *Decision Sciences* (26:3), 1995, 303-336.

[28] Ramamurthy, K., Premkumar, G. "Determinants and outcomes of electronic data interchange diffusion," *IEEE Transactions on Engineering Management* (42:4), November 1995, 332-351.

[29] Sia, S.K., Neo, B.S. Reengineering effectiveness and the redesign of organization control: A case study of the Inland Revenue Authority of Singapore, *Journal of Management Information Systems* (14:1), Summer 1997, 69-92.

[30] Siponen, T. M. "On the role of human mortality in information system security: From the problems of descriptivism to non-descriptive foundations," *Information Resources Management Journal* (14:4), 2001, 15-23.

[31] Spiller, P., Lohse, G.L. "A classification of Internet retail stores," *International Journal of Electronic Commerce* (2:2), Winter 1997-1998, 29-56.

[32] Suh, B., Han, I. "The impact of customer trust and perception of security control on the acceptance of electronic commerce," *International Journal of Electronic Commerce* (7:3), 2003, 135-161.

[33] Teo, T.S.H., Tan, M., Buk, W.K. "A contingency model of Internet adoption in Singapore," *International Journal of Electronic Commerce* (2:2), 1997, 95-118.

[34] Thong, J.Y.L. "An integrated model of information systems adoption in small businesses," *Journal of Management Information Systems* (15:4), 1999, 187-214.

[35] Weber, R. *Information Systems Control and Audit*, Prentice Hall Inc., Upper Saddle River, New Jersey, 1999.

[36] Whitman, M.E. In defense of the realm: Understanding the threats to information security, *International Journal of Information Management* (24), 2004, 43-57.

[37] Wybo, M. "The IT sales cycle as a source of context in IS implementation theory," *Information & Management* (44:4), June 2007, 397-407

[38] Yeh, Q-J., Chang, A.J-T. "Threats and countermeasures for information system security: A cross-industry study," *Information & Management* (44:5), 2007, 480-491.

[39] Zviran, M., Haga, W.J. "Password security: An empirical study," *Journal of Management Information Systems* (15:4), 1999, 161-185.