International Journal of Information Management 40 (2018) 54–66

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations

Yun Ji Moon[a,1], Myeonggil Choi[b,1], Deborah J. Armstrong[c,*]

[a] Department of Management Information Systems, Catholic University of Pusan, #57 Oryundae-ro, Geumjeong-gu, Busan, South Korea
[b] Department of Business Administration, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul 06974, South Korea
[c] Department of Business Analytics, Information Systems & Supply Chain, Florida State University, Tallahassee, FL 32306, USA

ARTICLE INFO

Keywords:
Chief security officer
Information security system (ISS) effectiveness
Relational leadership
Social alignment
Organizational performance

ABSTRACT

While information technology has increasingly created various innovation opportunities in organizations, these opportunities have caused serious risks associated with information. Due to these potential risks, information security has become a major concern in organizations, and the role of the chief security officer has begun to attract research attention. Using a social capital theory perspective, this study aims to explore how the level of relational leadership of the chief security officer drives the social alignment between business and IT executives. Specifically, we study how social alignment influences integrated knowledge, information security system (ISS) effectiveness, and organizational performance. Empirical data from one hundred and two government organizations in the Republic of Korea confirms the impact of relational leadership, social alignment, and ISS effectiveness on organizational performance.

1. Introduction

Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, or destruction (Sen & Samanta, 2014). The dependence on information and communication technologies (ICTs) within organizations has caused issues related to ICTs to become a core organizational concern (Knapp, Marshall, Rainer, & Morrow, 2006). The potentially large-scale financial and/or reputational loss from information security breaches drives organizations to vigorously protect their information assets. For example, a survey conducted by PricewaterhouseCoopers (PwC, 2015) shows that there has been an increase in the number of both large and small organizations experiencing security breaches, with 90% of large organizations having suffered a security breach. The Identity Theft Resource Center (ITRC, 2015) found that the number of data breaches in the United States (U.S.) increased by 8.1% from 2014 to 2015, and the cost of cybercrime in the U.S. alone is approximately $100 billion a year (Forbes, 2016a,b).

While security breaches are a concern for organizations, they are especially critical for governmental organizations, where the breach of information and assets may cause widespread societal problems. For example, North Korea launched a cyber-attack against South Korea in 2016, and a massive data breach exposed data belonging to an Internet shopping mall (CNN tech, 2017). According to the BBC (2014), the identification numbers and personal details of an estimated 80% of the 50 million South Korean people have been stolen from banks and other targets. Therefore, the government is considering issuing new identification numbers to every citizen over 17, costing billions of dollars. Thus, information security has become a strategic focus and challenge for governmental organizations. However, the question remains as to what is the most effective approach for information security management, particularly within a government organization.

The prominent information security management countermeasures explored in the literature have been primarily technical in nature (e.g., Goodhue & Straub, 1991; Nance & Straub, 1988; Straub, 1990; Straub & Welke, 1998), and place a premium on sophisticated technologies. Since security is perceived to be a technical issue, the information security staff tends to be positioned in low-level technical functions that focus on implementing the technologies (Kayworth & Whitten, 2010).

However, a more recent view suggests a socio-technical strategy, which emphasizes the importance of integrating security into mainstream aspects of the business and incorporating the human element in designing effective security programs (Goles, White, & Dietrich, 2005; Kayworth & Whitten, 2010). A socio-technical security strategy incorporates technical competence, as well as social, and organizational elements. Information security is understood as a concept that

* Corresponding author at: 821 Academic Way, Tallahassee, FL 32312, USA.
E-mail addresses: yjmoon@cup.ac.kr (Y.J. Moon), mgchoi@cau.ac.kr (M. Choi), djarmstrong@business.fsu.edu (D.J. Armstrong).
[1] Co-first authors.

https://doi.org/10.1016/j.ijinfomgt.2018.01.001
Received 25 August 2017; Received in revised form 19 December 2017; Accepted 4 January 2018
Available online 03 February 2018
0268-4012/ © 2018 Elsevier Ltd. All rights reserved.

encompasses factors such as security technologies, social relationships between organization members, strategy, and security policies. Therefore, this study identifies an *Information Security System (ISS)* as a group of interdependent factors that interact regularly to secure information within an organization.

A major challenge faced by security executives is the need to balance the information needs of the business with the need to secure information assets. An effective ISS should be business driven but also secure, thus alignment between the business and IT functions is key (Kayworth & Whitten, 2010). Kayworth and Whitten (2010) suggest that the lack of alignment between business-oriented tasks and the available technologies to accomplish them often results in ineffective information security. The literature discusses the idea of business-IT alignment[2] for the optimization of ISS (e.g., Bergeron, Raymond, & Rivard, 2004; Chan, Huff, Barclay, & Copeland, 1997; Reich & Benbasat, 1996) and the idea that top-level management plays a major role in achieving ISS effectiveness. Therefore, this paper discusses the business-IT alignment among executives in both units.

According to Wagner, Beimborn, and Weitzel (2014), there are three major views on business-IT alignment: structural alignment, strategic alignment, and social alignment. *Structural alignment* stresses the importance of formal coordination mechanisms in achieving outcomes such as codifying the decision-making rights of the IT unit (e.g., Chan & Reich, 2007). *Strategic alignment* means that the strategic IT plan is aligned with the organizational strategic plan and this alignment can be found in the organizational/departmental artifacts such as the mission statement (e.g., Bergeron et al., 2004; Chan et al., 1997; Reich & Benbasat, 1996). *Social alignment* has traditionally emphasized the cross-domain interconnectedness between business and IT executives that enables the creation of integrated knowledge (e.g., Chan, 2002; Wagner et al., 2014). Recently, the focus of business-IT alignment research has shifted to study the social aspects of alignment, highlighting the importance of informal, relationship-based structures (Chan, 2002).

Wagner et al. (2014) view social alignment as the social capital that exists between business and IT units in which the outcome is integrated business and IT knowledge. Social capital is "the goodwill available to individuals or groups. Its source lies in the structure and content of the actor's social relations. Its effects flow from the information, influence, and solidarity it makes available to the actor" (Adler & Kwon, 2002, p. 23). Consistent with this view is the concept of relational leadership, which is grounded in interpersonal relationships, and is traditionally viewed as the pattern of reciprocal interactions between leaders and followers (Gittell & Douglass, 2012). The concept of relational leadership has more recently been expanded to include relationships that occur in a broader organization-based social network, and is regarded as an important enabler for improving social capital as well as integrated knowledge in an organization (Uhl-Bien, 2006). Integrated knowledge is defined as "a firm's ability to perform repeatedly a productive task which relates either directly or indirectly to a firm's capacity for creating value through effecting the transformation of inputs into outputs" (Grant, 1996, p. 377). Integrated knowledge is developed in stages (Clark & Fujimoto, 1991), starting with a focus on capabilities that address specialized tasks, and then moving the focus to integrating the task specific capabilities into broader cross-functional capabilities.

In this study, we view social alignment as the social capital that exists between business and IT *executives* in which the outcome is integrated knowledge. Within the IT unit, the chief security officer (CSO) is a senior level executive who is accountable for the development and oversite of all security-related policies and programs. The CSO is increasingly being asked to collaborate with business executives and proactively seek to create opportunities for IT to serve business needs. This study uses social capital theory to consider alignment from a social perspective, and views it as the social linkages between executives in the business units and the CSO in the IT unit.

Although prior research argues that business-IT alignment facilitates organizational performance Kearns and Sabherwal (2006–2007); Sabherwal and Chan (2001) point out that there has not been enough theoretical and empirical research conducted on the relationships between the enablers and the outcomes of business-IT alignment. While research has established the influence of business-IT alignment on organizational performance (Reich & Benbasat, 2000; Sabherwal & Chan, 2001), what has been absent is an exploration of the likely driving and intervening factors. The current study attempts to fill this gap by identifying how business-IT alignment affects organizational performance via informal social relationships. Specifically, this paper suggests an integrated research model grounded in social capital theory that includes the enablers of social alignment, the mechanisms of social alignment, and the outcomes of alignment. In summary, the current paper pursues the following three research questions: (1) How does the relational leadership of CSOs in Korean governmental organizations affect business-IT social alignment?; (2) How does the integrated knowledge of business and IT mediate the relationship between social alignment, and ISS effectiveness?; and (3) How does integrated knowledge influence organizational performance?

2. Theoretical background and literature review

This paper proposes a model of the influence of relational leadership of CSOs on the social alignment between business and IT executives, and the outcomes of social alignment. This model utilizes relational leadership (Tsai, Dionne, Wang, & Spain, 2017; Uhl-Bien, 2006) and social alignment (Chan, 2002; Kayworth & Whitten, 2010; Karahanna & Preston, 2013; Wagner et al., 2014) to predict ISS effectiveness and organizational performance. We review the key constructs of our conceptual model and describe the theoretical grounds supporting the relationships contained therein.

2.1. Relational leadership

Relational leadership is enacted in interpersonal relationships (Hiller, Day, & Vance, 2006), and is defined as a pattern of reciprocal interactions between leaders and followers in which individuals make sense of situations, determine what is to be done, and how to do it (Gittell & Douglass, 2012). Relational leadership refers to leadership that is supportive and focused on developing high quality, trusting, work relationships within the organization (Brower, Schoorman, & Tan, 2000; Uhl-Bien, Graen, & Scandura, 2000). The relationship dyad (leader and follower) creates interpersonal knowledge that can be used to process social information and demonstrate social behaviors (Baldwin, 1997).

Recently, research has expanded the conceptualization of leader from an individual in a formalized position of influence within the organization (e.g., supervisor) to individuals who have developed social influence within the organization (e.g., lead user). Uhl-Bien (2006, p. 655) refers to relational leadership as "a social influence process through which emergent coordination (i.e., evolving social order) and change (e.g., new values, attitudes, approaches, behaviors, and ideologies) are constructed and produced." Thus, relational leadership can involve individuals across traditional organizational boundaries.

2.2. Social alignment and integrated knowledge

In the knowledge-based era, the importance of intangible assets and resources such as social relationships and collective knowledge in organizations is becoming increasingly important (Nahapiet & Ghoshal, 1998). Social capital theory proposes that an organization is understood as "a social community specializing in the speed and efficiency in the creation and transfer of knowledge" (Kogut & Zander, 1996, p. 503).

[2] By 'the business' we are referring to functional areas within an organization outside the IT function such as finance, or manufacturing.

Social relationships between organizational members are viewed as social capital, which can be defined as the sum of the resources embedded in, available through, and derived from an individual's network of relationships (Nahapiet & Ghoshal, 1998), and are considered a resource for action and knowledge transfer (Burt, 1997). Nahapiet and Ghoshal (1998) argue that social capital is a multi-dimensional concept comprised of structural, cognitive, and relational dimensions. According to Nahapiet and Ghoshal (1998), the *structural* dimension refers to the overall pattern of connections between individuals – in other words, who you reach and how you reach them. If there are colleagues (i.e., network ties) that provide access to resources in an organization, these colleagues may provide social exchange channels for knowledge transmission. The *cognitive* dimension refers to those resources that provide shared representations, interpretations, and systems of meaning among individuals. An essential part of a social exchange is that at least some level of shared context should be developed (Boisot, 1995). The *relational* dimension focuses on the facets of the particular relationships people have, such as trust, trustworthiness, and norms. If individuals are not willing to trust others to participate in a social exchange, integrated knowledge cannot be readily accumulated.

Consistent with social capital theory, social alignment emphasizes the cross-domain interconnectedness between business and IT executives that facilitates the creation of integrated knowledge (e.g., Chan, 2002; Kayworth & Whitten, 2010; Wagner et al., 2014). Social alignment can also be thought of as consisting of three relationship-focused dimensions – structural, cognitive, and relational (Karahanna & Preston, 2013; Wagner et al., 2014), which are referred to as linkages. The *structural linkage* between business and IT executives indicates the network structure found in meetings and project conferencing, which benefits from frequent direct contact and cross-functional project teams (Chan, 2002; Chan & Reich, 2007) to develop mutual understanding (Lind & Zmud, 1991). The *cognitive linkage* refers to the extent to which business and IT executives know each other's codes, language, and perspectives (Nahapiet & Ghoshal, 1998). Through shared language and vocabulary, and through developing collective narratives, business and IT executives may understand each other at a deeper level (Reich & Benbasat, 2000). The *relational linkage* indicates the particular facets of the relationships, such as trust and trustworthiness (Nahapiet & Ghoshal, 1998). Trust between individuals in business and IT units enhances cooperation, and cooperation breeds more trust (Chong, Ooi, Chan, & Darmawan, 2011; Jones & George, 1998). Successful knowledge integration requires individuals to be motivated to participate in the integration process (Nahapiet & Ghoshal, 1998). Consequently, trust and cooperation foster collective trust over time, which may engender participation and ultimately produce integrated knowledge.

2.3. Information security system (ISS) effectiveness

In business terms, effectiveness in organizations could be viewed within the context of accomplishing objectives or achieving results. In the same vein, ISS effectiveness refers to the extent to which the goals of the ISS program are achieved, and organizational information is sufficiently protected (Hwang & Choi, 2017). ISS effectiveness is the degree to which the organization establishes controls preventing harm from external and internal threats. Three types of factors have been used to measure ISS effectiveness: *organizational factors* such as user training and security policy enforcement (Chen, Ramamurthy, & Wen, 2012; Son, 2011; Straub, 1990; Warkentin & Willison, 2009), *technology-based factors* such as hardware and software tools (D'arcy & Herath, 2011; Herath & Rao 2009; Kankanhalli, Teo, Tan, & Wei, 2003; Straub, 1990), and *hybrid factors* such as the number of hours per week devoted to ISS threat prevention and deterrence and top management dedication to data security (Kankanhalli et al., 2003; Straub, 1990). Previous research on ISS effectiveness has tended to focus on one aspect of an approach. The present study uses the perspective that ISS effectiveness is achieved via the combined effects of technology-based factors, organization-based factors, and other factors designed to reduce threats from internal and external sources (Hwang & Choi, 2017).

3. Research model and hypotheses

3.1. Relational leadership and social alignment

As stated previously, relational leadership is focused on developing high quality, trusting, work relationships (Brower et al., 2000; Uhl-Bien et al., 2000) via frequent interactions to model the behavior and thus empower employees to work as partners. Though the specific tasks of the CSO may differ across organizations, a CSO is not simply a technical expert who introduces, develops and implements technology, but is also responsible for the operation and control of the ISS at an enterprise-level. A CSO is in charge of safeguarding the intellectual assets of an organization, and plays the role of a technical expert as well as a managerial strategist. Additionally, CSOs are often required to manage human resources in organizations (Soomro, Shah, & Ahmed, 2016). As most of the data breaches and ISS vulnerabilities occur due to employees (Sarkar, 2010; Vance, Lowry, & Eggett, 2013), humans become one of the most critical elements in ISS effectiveness.

To improve ISS and business-IT alignment, CSOs communicate the importance of ISS management and view security issues from a business perspective as well as a technology one. CSOs engaging in relational leadership have been found to have better alignment between business and IT executives and higher organizational success (Kayworth & Whitten, 2010; Soomro et al., 2016). Through the process of sharing knowledge in one-on-one interactions, meetings, or project conferences, the CSO and business executives are able to talk about business issues as well as technology-related issues. Having social capital available in a group can improve the group's effectiveness when based on strong trusting relationships that develop within and beyond the group boundaries (Oh, Labianca, & Chung, 2006). Relational leadership has been found to positively influence social capital (Uhl-Bien, 2006), and social alignment occurs when social capital is developed within the context of a work environment (Wagner et al., 2014). Thus, we hypothesize these mechanisms will occur within the CSO-business executive context as follows:

Hypothesis 1. The level of relational leadership engaged in by the CSO will positively influence the level of social alignment between the CSO and business executives.

H1a. The level of relational leadership engaged in by the CSO will positively influence the level of structural linkage between the CSO and business executives.

H1b. The level of relational leadership engaged in by the CSO will positively influence the level of cognitive linkage between the CSO and business executives.

H1c. The level of relational leadership engaged in by the CSO will positively influence the level of relational linkage between the CSO and business executives.

3.2. Social alignment and integrated knowledge

Social alignment between business and IT executives is a continuous process and includes sharing business and IT domain knowledge and knowledge integration (Kearns & Sabherwal, 2006; Wagner et al., 2014). Shared domain knowledge allows "IT and business executives to be able to participate in the others' key processes and to respect each other's unique contribution and challenges" (Reich & Benbasat, 2000, p. 86); and integrated knowledge results when people interact and combine their information to create new knowledge (Grant, 1996; Okhuysen & Eisenhardt, 2002; Wagner et al., 2014). Social alignment should help to establish a common language, improving

communication and potentially act as a driver of integrated knowledge. Business strategies change with market situations and environmental uncertainties and ISS strategies reflect the business' needs. If a functional unit changes, but the IT unit does not adjust to the change, a lack of alignment may occur. A lack of alignment potentially leads to a shortage of integrated knowledge between business and IT executives, which can hinder organizational success (Chen, Sun, Helms, & Jih, 2008). Thus, this research proposes the following hypotheses related to integrated knowledge:

Hypothesis 2. The level of social alignment between the CSO and business executives will positively influence the level of integrated knowledge.

H2a. The level of structural linkage between the CSO and business executives will positively influence the level of integrated knowledge.

H2b. The level of cognitive linkage between the CSO and business executives will positively influence the level of integrated knowledge.

H2c. The level of relational linkage between the CSO and business executives will positively influence the level of integrated knowledge.

3.3. Integrated knowledge and information security system (ISS) effectiveness

Recall that ISS effectiveness refers to the ability of ISS to protect against an unauthorized use or deliberate misuse of information assets by people (Straub, 1990). An effective ISS strategy needs to emphasize the importance of considering both the technological and the socio-organizational context (Kayworth & Whitten, 2010; Soomro et al., 2016; Wagner et al., 2014). For example, using formal organizational structures (i.e., hierarchical arrangement of relationships between job functions within an organization; Meyer & Rowan, 1977) to define decision-making rights and responsibilities may help achieve ISS effectiveness. This formal relationship network between business and IT executives in an organization can encourage interaction across network members and facilitate knowledge exchange as individuals know who to see to 'get things done' (Karahanna & Preston, 2013). The coordination processes achieved through communication and knowledge exchange can facilitate effective ISS management (Kayworth & Whitten, 2010). Thus, the more integrated knowledge is within the organization, the more opportunities to explore mechanisms to prevent security breaches. Thus, this research proposes the following hypothesis:

Hypothesis 3. The level of integrated knowledge between the CSO and business executives will positively influence ISS effectiveness.

3.4. ISS effectiveness and organizational performance

As mentioned above, effective ISS using technological and organizational approaches has been found to positively influence the overall performance of organizations (Gupta, 2011; Moffat & Nzulwa, 2016); and ineffective ISS has caused organizations to suffer financial and reputational damage, which in turn, has severely affected organizational performance and market valuation (Gupta, 2011; Kraemer, Carayon, & Clem, 2009). Building on previous findings, we hypothesize that there is a positive relationship between ISS effectiveness and organizational performance within the context of government organizations in the Republic of Korea.

Hypothesis 4. ISS effectiveness will positively influence organizational performance.

3.5. The moderating effect of technical knowledge

The CSO often manages a multitude of functions from administrative security, policies, systems, personnel, to physical security such as facilities and access control (Soomro et al., 2016). Therefore, CSOs should have not only a broad understanding of the technical aspects of IT (e.g., infrastructure and applications), but also a wide range of business domain, legal, and managerial knowledge to prepare for discussions, issues, problems, and conflicts with various stakeholders.

However, in many governmental organizations in the Republic of Korea, the security department is organized around highly technical IT staff whose function is to install an ISS tool. In contrast, a general manager, usually with no or limited technical knowledge, is often appointed as the CSO. There are several documented cases in which a manager who is unfamiliar with various aspects of IT becomes the CSO, and as a result limits the establishment of an effective ISS strategy (Hankook Newpaper, 2015; Yonhap Newspaper, 2015). CSOs with a higher level of technical expertise will be better able to close the gap between the functionality of security technologies and business issues (Whitten, 2008). A CSO with strong technical knowledge is in a better position to understand how ISS strategies can be integrated into the business strategies, and how they can be accomplished or enhanced with technology. CSOs should be able to understand the various aspects of the value proposition of security initiatives and effectively communicate those to other executives. Thus, this research proposes the following hypothesis:

Hypothesis 5. The technical knowledge of the CSO will moderate the integrated knowledge and ISS effectiveness relationship, such that the level of technical knowledge of the CSO will increase the strength of the relationship between integrated knowledge and ISS effectiveness.

Fig. 1 summarizes relationships explored in this study.

4. Research methodology

In this study, we used a quantitative approach to test the proposed model. We begin by providing details about the measures, data collection, and analysis procedures. This is followed by the findings from the study.

4.1. Measurement of constructs

We measured each construct using previously validated scales and adapted some of the items for this study context. The Appendix A provides the constructs, definitions, items, and sources of the measures used in this study. All of the measures are reflective, and used a five-point Likert scale. Several factors that are not included in the research model but have been suggested in the literature to have an influence on ISS effectiveness are included as control variables. These variables include gender, education level, number of certifications, and tenure as a CSO. Previous studies have indicated that the number of years working as a chief information security officer as well as training and education could influence ISS effectiveness (Choi, 2016); thus, we include those in our study. Rather than focusing on just financial performance, we measured organizational performance as consisting of financial performance and business process performance (e.g., information utilization in conducting tasks).

4.2. Data collection

Paper questionnaires were distributed by mid-level information security officers in the South Korean central government and were completed by the CSOs for each department. The CSO position is required within government organizations and is appointed from within the central government and public officers in South Korea (Kim, 2012). The questionnaires were sent to 43 departments and councils of the South Korean central government, and 78 public institutions (e.g., Korea Worker's Compensation & Welfare Service) in South Korea. Of the 121

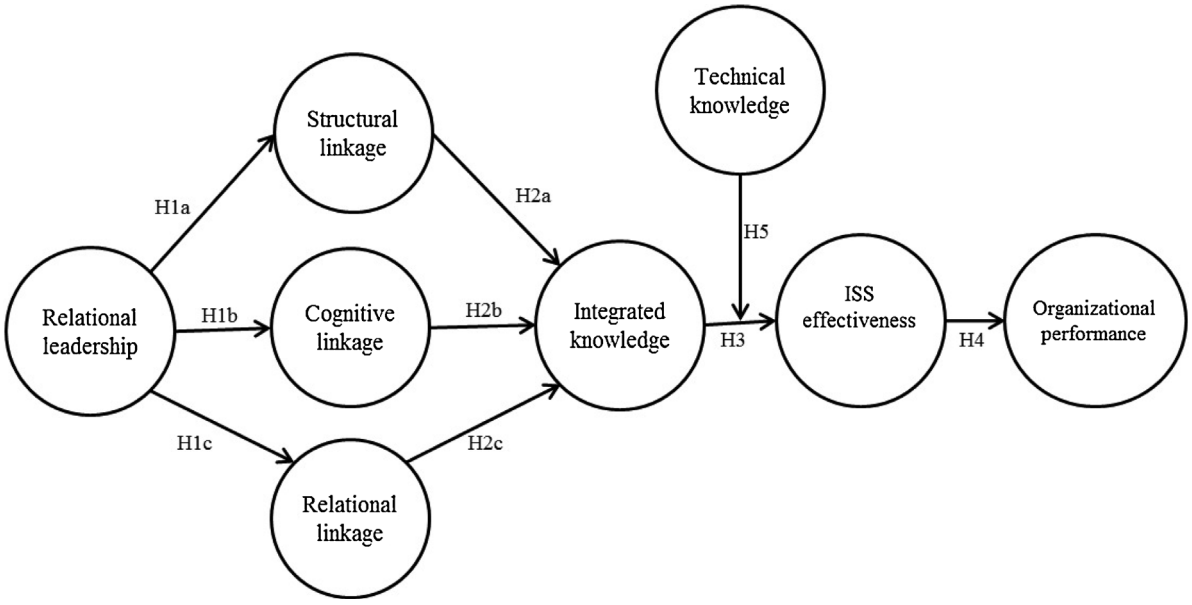


Fig. 1. Conceptual model.

Table 1
Profiles of respondents.

Item	Variable	Frequency	Percentage(%)
Gender	Male	99	97.1
	Female	3	2.9
Age	Under 45 years	2	2.0
	46–50 years	13	12.7
	51–55 years	34	33.4
	56–60 years	46	45.1
	Above 61 years	7	6.8
Work Experience	Less than 10 years	30	29.4
	11–20 years	13	12.7
	21–30 years	42	41.2
	31–40 years	16	15.7
	More than 40 years	1	1.0
CSO Tenure	Less than 1 years	22	21.6
	1–3 years	66	64.7
	3–5 years	7	6.9
	5–10 years	1	1.0
	More than 10 years	6	5.9
IT Tenure	Less than 1 years	28	27.4
	1–10 years	59	57.7
	10–20 years	2	2
	20–30 years	10	9.9
	More than 30 years	3	3.0
Education	High School Diploma	1	1.0
	Junior College	2	2.0
	Bachelor's	22	21.6
	Master's or above	77	75.5
Number of Certifications	0	73	71.6
	1	12	11.8
	2	7	6.9
	3	5	4.9
	4	4	3.9
	More than 5	1	1.0

paper questionnaires sent, 108 were returned, and the questionnaires were collected from May 2015 to November 2015. After removing six questionnaires with incomplete or unreliable responses, 102 valid questionnaires remained, for an effective response rate of 84.3%. Table 1 displays the characteristics of the respondents. As shown in Table 1, most of the respondents were male (97.1%) and were between 51 and 60 years old (78.6%). About half (41.2%) of the respondents had worked for 21–30 years, and 64.7% had worked as a CSO for 1–3 years. Most of respondents (71.6%) did not have any IT-related certifications, but were well educated (75.5% had obtained a master's degree or above).

5. Data analysis and results

We used a multi-step process to evaluate the research model. SPSS version 21 and SmartPLS version 2.0 (Ringle, Wende, & Will, 2005) were used in the multi-stage approach. In the first stage, we examined the measurement model for proper psychometric properties (i.e., measurement model), while in the second stage we focused on testing the research model and hypotheses (i.e., structural model). Table 2 shows the descriptive statistics.

Before analyzing the data, exploratory factor analysis was conducted using principle component analysis. Orthogonal factor rotation-varimax was conducted. Table 3 shows the results of the exploratory factor analysis.

Partial least squares (PLS) was used to empirically evaluate the theoretical model (Gefen & Straub, 2005; Thatcher & Perrewe, 2002). Smart PLS 2.0 (Ringle et al., 2005) was used for data analysis, and 1500 bootstrap samples were used to empirically calculate standard errors and evaluate statistical significance (Gefen, Rigdon, & Straub, 2011).

5.1. Measurement model

PLS consists of two main sections. In the first section the measurement model and its validity (convergent and discriminant) are evaluated (Gefen & Straub, 2005). We used the procedure outlined by Chin

Table 2
Descriptive Statistics.

	Mean	STD	MIN	MAX
Structural linkage	3.163	1.254	1	5
Relational linkage	4.754	0.403	3	5
Cognitive Linkage	4.277	0.457	3	5
Integrated knowledge	4.585	0.543	3	5
Organizational performance	4.111	0.716	2	5
ISS effectiveness	4.557	0.453	3	5
Relational leadership	4.608	0.404	3	5
Technical Knowledge	4.585	0.054	2	5

Table 3
Factor Loadings.

		Factor						
		1	2	3	4	5	6	7
Organizational Performance	ORG_PRM4	.940	.115	.112	.033	.026	.104	.037
	ORG_PRM2	.870	.238	.100	-.137	.032	.056	.114
	ORG_PRM3	.868	.290	.131	.008	.065	.022	.114
	ORG_PRM1	.845	-.018	.086	.189	.095	.093	.049
	ORG_PRM7	.701	.186	.184	.381	.217	.151	.013
	ORG_PRM5	.614	.260	.184	.375	.182	.153	.117
Relational leadership	REL_LED6	.157	.833	.276	.119	.066	.210	.088
	REL_LED7	.260	.713	.257	.157	.126	.206	.176
	REL_LED4	.332	.629	.013	-.180	.121	.339	.141
	REL_LED1	.171	.600	.208	.429	.025	.034	.065
	REL_LED5	.266	.588	.292	.262	.037	.382	.012
	REL_LED9	.187	.540	.207	.349	-.022	.362	.203
ISS Effectiveness	EFFCT4	.182	.105	.829	.208	.144	.060	.083
	EFFCT5	.313	.135	.742	.037	-.020	.346	.231
	EFFCT3	.141	.433	.720	.221	.193	.010	-.027
	EFFCT6	.271	.206	.707	.047	-.006	.386	.252
	EFFCT2	-.009	.147	.703	.041	.068	.078	.030
Relational linkage	LIN_REL2	.100	.088	.167	.801	.044	.207	.237
	LIN_REL3	.104	.099	.067	.728	.000	.269	.176
	LIN_REL1	.073	.485	.116	.599	-.032	.105	.175
Structural linkage	LIN_STR3	.099	.061	.115	.017	.940	-.010	.021
	LIN_STR1	.036	.103	.093	.047	.932	.123	-.051
	LIN_STR2	.180	.018	.053	-.010	.888	.016	.114
Integrated knowledge	INT_KNO1	.064	.256	.124	.365	.007	.716	.008
	INT_KNO3	.254	.324	.255	.256	.117	.700	.160
	INT_KNO2	.128	.352	.318	.230	.118	.640	.220
Cognitive linkage	LIN_COG2	.107	.188	.237	.231	.029	.047	.801
	LIN_COG1	.169	.134	.065	.302	.059	.210	.790

Table 4
Validity and reliability of the reflective constructs.

	AVE	Composite reliability	R square	Cronbach's alpha
Relational leadership	0.650	0.917		0.891
Cognitive linkage	0.817	0.899	0.234	0.776
Relational linkage	0.703	0.876	0.378	0.789
Structural linkage	0.875	0.955	0.041	0.929
Integrated knowledge	0.789	0.912	0.419	0.866
ISS effectiveness	0.694	0.918	0.368	0.887
Organizational performance	0.749	0.947	0.237	0.933

(1998) for reflective measures to evaluate construct reliabilities and the convergent and discriminant validity of the model. The value of the indicator reliability, composite reliability, and average variance extracted (AVE) assesses convergent validity (Fornell & Larcker, 1981). Table 4 shows the AVEs were above the 0.5 threshold, (Chin 1998; Fornell & Larcker 1981; Thatcher & Perrewe, 2002), the composite reliabilities (CR) were all greater than 0.7 (Thatcher & Perrewe, 2002), and the Cronbach's alpha values were greater than 0.7, indicating that the data were reliable (Bagozzi & Yi, 1988).

To evaluate the discriminant validity of the constructs, we used the procedure recommended by Fornell & Larcker (1981). The Fornell–Larcker criterion suggests that discriminant validity is shown when the square root of each AVE is larger than the constructs' correlation with any other latent construct (Fornell & Larcker, 1981). Table 5 shows the square root of the average variance extracted (AVE) and the correlations among reflective constructs. All of the constructs correlated more strongly with their own measures than with any of the other constructs. This indicates convergent and discriminant validity. Finally, cross-loadings were calculated, and all indicators showed higher loadings with their respective construct than with any other reflective construct (Chin, 1998).

Additionally, we analyzed the data for indications of common method bias. We used the method based on Podsakoff, MacKenzie, Lee, and Podsakoff (2003) and PLS analysis by Liang, Saraf, Hu, and Xue (2007). The indicators of all of the constructs were associated reflectively with the method factor. Each indicator variance explained by the principle constructs and by the method factor was computed (Chin, Thatcher, & Wright, 2012). Table 6 shows that most of method loadings were not significant. Moreover, whereas the average substantive explained variance for an indicator was 0.709, the common method-based variance was only 0.038. Based on the results of this test, we believe common method bias was not a significant threat in this study.

Taken together, the results of the tests demonstrate that the measurement model meets the rigorous standards expected (Straub, Boudreau, & Gefen, 2004), and we present the structural model evaluation next.

Table 5
Correlation of the latent variable scores.

	Integrated knowledge	ISS effectiveness	Cognitive linkage	Relational linkage	Structural linkage	Organizational Performance	Relational leadership
Integrated knowledge	**0.888**						
ISS effectiveness	0.606**	**0.833**					
Cognitive linkage	0.495**	0.432**	**0.903**				
Relational linkage	0.599**	0.430**	0.543**	**0.838**			
Structural linkage	0.209*	0.224*	0.119	0.092	**0.935**		
Organizational performance	0.463**	0.486**	0.366**	0.374**	0.259**	**0.865**	
Relational leadership	0.742**	0.640**	0.483**	0.615**	0.203**	0.571**	**0.806**

Square root of the average variance extracted (AVE) is on the diagonal in bold.
*** $p < 0.001$.
** $p < 0.01$.
* $p < 0.05$.

5.2. Structural model assessment

The second section of PLS presents the results from the structural model and the relative importance of each independent variable (Gefen & Straub, 2005; Gefen et al., 2011). The structural model was tested using the loadings, significance of the path coefficients, and t values. The model explained 36.8% of the total variance in ISS effectiveness. Fig. 2 shows the results of the structural model assessment.

The first hypothesis (H1) looked at the positive influence of relational leadership on three types of social alignment, and was supported ($\beta = 0.204$, $p < .05$; $\beta = 0.483$, $p < .001$; $\beta = 0.615$, $p < .001$). The second hypothesis (H2) looked at the relationship between social alignment and integrated knowledge, and was supported ($\beta = 0.139$, $p < .05$; $\beta = 0.228$, $p < .01$; $\beta = 0.462$, $p < .001$), indicating that the linkages established between CSOs and business executives positively influenced the level of integrated knowledge. The third hypothesis (H3) looked at the positive influence of integrated knowledge on ISS effectiveness, and was supported ($\beta = 0.607$, $p < .001$). The fourth hypothesis (H4), looked at the positive influence of ISS effectiveness on organizational performance, and was supported ($\beta = 0.487$, $p < .001$).

Additionally, the control variables did not influence ISS effectiveness in this study. Unlike previous studies that found that work experience and education and training could influence ISS effectiveness in organizations (Choi, 2016), work experience and the education level of a CSO did not influence ISS effectiveness. One explanation for this result may be the homogeneous nature of the CSOs in the South Korean government context.

5.3. The moderating effect of technical knowledge

The fifth hypothesis (H5) asserted that the technical knowledge of the CSO would positively moderate the relationship between integrated knowledge and ISS effectiveness. This influence was significant, but in the opposite direction to the hypothesis. The level of technical knowledge of the CSO negatively influenced the relationship between integrated knowledge and ISS effectiveness ($\beta = -2.203$, $p < .001$). As shown in Table 7, we analyzed the impact of the individual variables on the endogenous variable in the model to determine the effect size. The effect size of the moderation is moderate (Cohen, 1988). A summary of the results of the hypotheses tests is provided in Table 8.

6. Discussion and implications

The results of the study show that the relational leadership of the CSO positively affects social alignment, which influences the integrated knowledge developed between the CSO and business executives. This integrated knowledge resulted in a higher level of ISS effectiveness, and higher organizational performance. These results suggest several implications for research and practice. We being by detailing the implications for research, then address implications that may be helpful for practitioners. First, this study is significant in that it considers the alignment between IT and business from a new point of view – that of social alignment. In order to facilitate social alignment between CSOs and business executives, CSOs should endeavor to exploit opportunities for building strong relationships (i.e., network ties) in an organization. In South Korean government organizations, there exist informal network ties such as one's alma matter (i.e., school ties) and regionalism. Informal network ties (e.g., regionalism) may have a greater influence than formal authority in a governmental organization. Although

Table 6
Effect analysis of moderation on dependent variable.

	Direct effect (path)		Indirect effect (path)		Total effect	R^2	Effect size ($f^{2)}$)
Basic Model	LED → PER	0.579	LED → STR → INT → ISS → PER LED → COG → INT → ISS → PER LED → REL → INT → ISS → PER	0.132	0.711	0.238	
	LED → ISS	0.684	LED → STR → INT → ISS LED → COG → INT → ISS LED → REL → INT → ISS	0.256	0.940	0.368	
Moderation Model (technical knowledge)	LED → PER	0.579	LED → STR → INT → KNO → ISS → PER LED → COG → INT → KNO → ISS → PER LED → REL → INT → KNO → ISS → PER	−0.454	0.124	0.238 (△0)	
	LED → ISS	0.684	LED → STR → INT → KNO → ISS LED → COG → INT → KNO → ISS LED → REL → INT → KNO → ISS	−0.931	−0.247	0.476 (△.108)	0.206

a. LED (relational leadership), PER (performance), STR (structural linkage), COG(cognitive linkage), REL (relational linkage), INT (integrated knowledge), ISS (ISS effectiveness), KNO (technical knowledge).

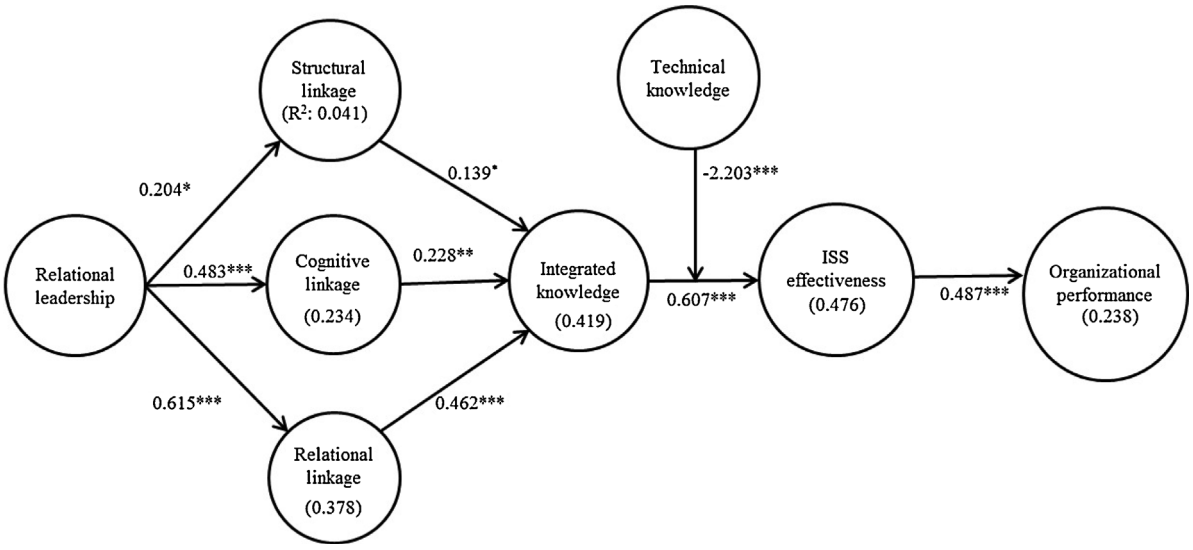


Fig. 2. The results of the structural assessment model.

Table 7
Analysis of common method bias.

Construct	Indicator	Substantive Factor Loading	Variance Explained	Method Factor Loading	Variance Explained
Relational leadership	REL_LED1	0.741***	0.5487	−0.014	0.000
	REL_LED4	0.690***	0.476	0.015	0.000
	REL_LED5	0.744***	0.554	0.106	0.011
	REL_LED6	1.080***	1.167	−0.202*	0.0406
	REL_LED7	0.771***	0.595	0.110	0.012
	REL_LED9	0.340	0.115	0.428*	0.183
Relation linkage	LIN_REL1	0.717***	0.514	0.120	0.014
	LIN_REL2	0.892***	0.795	−0.031	0.000
	LIN_REL3	0.908***	0.824	−0.088	0.008
Structural linkage	LIN_STR1	0.945***	0.894	0.009	0.000
	LIN_STR2	0.896***	0.802	0.016	0.000
	LIN_STR3	0.967***	0.936	−0.025	0.001
Cognition linkage	LIN_COG1	0.904***	0.817	0.002	0.000
	LIN_COG2	0.904***	0.817	−0.002	0.000
Integrated knowledge	INI1	1.036***	1.073	−0.253**	0.063
	INT2	0.891***	0.794	0.037	0.001
	INT3	0.760***	0.578	0.186**	0.035
ISS effective-ness	EFFECT2	0.844***	0.719	−0.231*	0.053
	EFFECT3	0.708***	0.501	0.148	0.022
	EFFECT4	0.980***	0.959	−0.135	0.018
	EFFECT5	0.853***	0.727	0.049	0.002
	EFFECT6	0.811***	0.657	0.108	0.012
Organizational perfor-mance	ORG_PRM1	0.832***	0.692	0.028	0.000
	ORG_PRM2	0.983***	0.965	−0.071	0.005
	ORG_PRM3	0.903***	0.816	0.064	0.004
	ORG_PRM4	0.974***	0.948	−0.021	0.000
	ORG_PRM5	0.225*	0.051	0.613***	0.376
	ORG_PRM7	0.364***	0.132	0.507***	0.257
Technical knowledge	TEC_KNO1	0.910***	0.829	0.047	0.002
	TEC_KNO2	0.7952***	0.631	0.161*	0.026
	TEC_KNO3	1.028***	1.057	−0.235*	0.055
		Average	0.709	Average	0.038

* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

members are situated within a formal network, their relationships may facilitate little communication. Formal authority-based relationships do not always mirror the informal social structure within organizations. When the informal social structure does not coincide with the formal authority structure, organizational performance often suffers (Gulati & Puranam, 2009). Therefore, the relational leadership of a CSO may benefit organizational performance because it reinforces the information, behaviors, and normative directions for the organization members (Soda & Zaheer, 2012), resulting in more effective business-IT alignment. This suggests that relationships, rather than hierarchical authority structures may be a key to new forms of effective leadership (Drath, 2001) that should be explored.

Second, the direct predictors of ISS effectiveness in this study were the level of cognitive, structural, and relational linkages between the CSO and business executives. Chan and Reich (2007) stated that more focused investigations of alignment are needed to go beyond 'alignment is good' statements, and to explore subtleties concerning how, when, and where alignment really matters. Consistent with Wagner et al.'s (2014) conceptual propositions, this study found that social alignment (consisting of structural, cognitive, and relational linkages) enables knowledge sharing and the development of integrated knowledge. Future research should incorporate aspects of social capital into business-IT alignment models so as to engage in a more comprehensive exploration of alignment within organizations.

Third, this study is significant in that it empirically tested the relationships between social alignment, ISS effectiveness and organizational performance. Previous research in the IT field has commonly viewed information security problems through the lens of deterrence theory (e.g., D'arcy & Herath, 2011; Siponen & Vance, 2010). This theory proposes that people make rational decisions toward committing or abstaining from illicit activities based on benefit maximization and cost minimization. If formal (i.e., legal) sanctions for an illicit act are perceived as certain and severe, individuals are usually deterred from engaging in that act (Gibbs, 1975). Similarly, much of the behavioral IS security research posits that the more employees perceive the risks and costs of formal sanctions, the more likely they are to comply with IS security policies (D'arcy & Herath, 2011).

However, the current study shows that ISS effectiveness can be obtained through informal social alignment and knowledge integration. The role of the CSO includes the management of people and processes as well as information security, as the CSO is responsible for developing, overseeing and coordinating all facets of the security efforts across the organization. This broad range of job functions often leads decision makers to seek out individuals with more management-related backgrounds. Looking at the background of CSOs, generally about 26% currently hold MBA degrees and that number is increasing (CSO Online, 2009). In many organizations, the CSO is one of the senior functional

Table 8
Summary of Hypothesis.

Hypothesis	Std Regression Weight	Sig Level	Supported
H1 CSO Relational leadership positively influences social alignment.			
H1-a CSO relational leadership positively influences structural linkage.	0.204	0.05	Yes
H1-b CSO relational leadership positively influences cognitive linkage.	0.483	0.001	Yes
H1-c CSO relational leadership positively influences relational linkage.	0.615	0.001	Yes
H2 Social alignment positively influences integrated knowledge.			
H2-a Structural linkage positively influences integrated knowledge.	0.139	0.05	Yes
H2-b Cognitive linkage positively influences integrated knowledge.	0.228	0.01	Yes
H2-c Relational linkage positively influences integrated knowledge.	0.462	0.001	Yes
H3 Integrated knowledge positively influences information security system effectiveness.	0.607	0.001	Yes
H4 Information security system effectiveness positively influences organizational performance.	0.487	0.001	Yes
H5 Technical knowledge positively moderates integrated knowledge – information security system effectiveness	−2.203	0.01	No*

* Opposite direction to hypothesis.

executives similar in status to a CFO or CIO, and Forbes reported that by 2018, 75% of CSOs will report directly to the CEO (Forbes, 2016a,b). Accordingly, this research highlights the CSO's role in terms of relational leadership and the ability to manage business-IT social alignment as a mechanism for ISS effectiveness.

Fourth, while our research model was successful in predicting many relationships, one of the hypotheses was not supported (H5). Contrary to our expectation, the level of technical knowledge of the CSO *negatively* moderated the relationship between integrated knowledge and ISS effectiveness. In the U.S., IS practitioners with significant technology-related experience are promoted to the senior executive position of CSO. But in Korean governmental organizations, most central and local governmental organizations appoint the CSO as a top-level officer who is a civil servant. After executives with a lengthy management career acquire some technical knowledge, they are likely to be appointed as a CSO. In addition, the Korean government's information security department is part of the general management division in charge of human resource and budget management, and the top officer of the general management division is often appointed to the CSO position. Therefore, a CSO in a Korean governmental organization may not be a technical professional with significant experience in the information security department, but a general manager.

The respondents in this study reflect this characteristic as about 58% of the CSOs had more than 30 years of experience in governmental organizations, and 86.3% of them had been in IT and CSOs less than three years. In addition, 71.6% of the respondents did not have any IT certifications. We speculate that the rejected hypothesis may reflect the cultural distinctiveness of Korean governmental organizations in that the overall relatively low level of IT experience of the CSOs in our study affected the moderation of the relationship between integrated knowledge and ISS effectiveness. Specifically, the more technical knowledge the CSO possessed, the weaker the relationship between integrated knowledge and ISS effectiveness. So rather than increasing the influence of shared understanding on ISS effectiveness, the CSOs with more technical knowledge were perhaps not able to effectively communicate the various aspects of the value proposition of security initiatives to other executives thus destabilized the influence of integrated knowledge on ISS effectiveness. Future research should test the validity of the moderation within a Korean governmental organization context as well as other contexts such as private organizations within South Korea, and public/private organizations outside South Korea.

From a practitioner standpoint, the first implication is regarding the more technical CSOs. The CSOs with a more technical career background in Korean governmental organizations may experience some difficulties in developing social alignment between business and IT because they may have weaker social networks within their organization. The enforcement of the CISO (Chief Information Security Officer) ordinance by the Korean Ministry of Science and Information Communication Technology in 2014 forced organizations to designate CSOs. This enforcement ordinance contributed to an increase in the number of CSOs but there is large variation in the tasks and activities of a CSO in each organization. While CSOs should excel in leadership skills and strategic thinking, they are still practitioners and technical supervisors in government organizations. In the event of a security incident an immediate and systematic response by a CSO may be difficult because ISS requires both general management skills and technical knowledge. A lack of informal network may prevent the more technical participants from demonstrating relational leadership aimed at promoting social alignment and accumulating integrated knowledge. On the other side, a lack of technical knowledge may prevent less technical participants from understanding the extent of the security incident and may jeopardize ISS effectiveness. If ISS is an important asset, Korean governmental organizations need to have a proper understanding of the full extent of the CSO's strategic role within the organization. By more clearly articulating and standardizing the qualifications required for a CSO, Korean government organizations could significantly increase ISS effectiveness.

Related to this issue, at the time of the CSO's appointment, decision makers need to consider the technical experience of the individual within ICT department as well as the individual's educational and career background. Decision makers would be advised to examine the individual's relevant knowledge, experience and background against the needed qualifications of a CSO, and then appoint only fully qualified personnel. The government should also consider hiring 'outsiders' to a CSO position within Korean government organizations. The public officer personnel system is a closed personnel system, and thus it is not easy to recruit a CSO. Therefore, it may be necessary to recruit outside specialists with appropriate qualifications from the private sector to CSO positions, and then socialize them into the government organizational culture after hiring. Even after appointment, whether an insider or an outsider, the CSO should continuously engage in short-term and long-term training courses on the latest technical and managerial knowledge needed to remain effective as a CSO.

7. Limitations and future research

In addition to implications, this study has a few limitations. First, the moderating effect of the CSO's technical knowledge hypothesized in this study was counter to expectations. We proposed a positive moderation because of the unique role of CSOs as an executive-position and supervisor/technical practitioner-position. Due to the nature of our sample, it appears that the technical knowledge of CSOs may be an obstacle to business – IT alignment. Therefore, future research, should further segment the sample based on the career background of the CSOs, and explore the impact of business-IT alignment.

Second, when looking at the relationship between relational leadership and social alignment (H1), it is important to note that a CSO's leadership style may also be affected by his/her skills, behaviors and

traits as effective leadership is a combination of traits, skills, and behaviors (Strang, 2007). The current study focused on relational leadership, but future studies might consider other leadership traits, behaviors, and skills, such as personal effectiveness, influencing social alignment, and cognitive ability to integrate knowledge (Katz & Kahn, 1978; Schermerhorn, Hunt, & Osborn, 2003; Strang, 2007).

Third, previous research has found that structural linkages (formal and informal interactions) between CIOs and top management teams did not influence knowledge integration in the private sector (Karahanna & Preston, 2013; Smaltz, Sambamurthy, & Agarwal, 2006). The current study represented structural linkage as only informal interaction between CSOs and business executives and utilized only the public sector context within South Korea. Future research might explore the relationships emerging from formal and informal linkages and knowledge integration in both the public and private sectors.

Fourth, with respect to the relationship between integrated knowledge and ISS effectiveness (H3), this study investigated knowledge integration only at the executive level. Research has found that to develop a high level of ISS effectiveness, employee compliance is necessary (Siponen & Vance, 2010). Future research could examine the relationship between knowledge integration and compliance among security officers and employees at the different levels within organizational hierarchy as well as expand the model to corporate CSOs within the Republic of Korea and beyond.

Fifth, as seen in Table 5, there are a few highly correlated variables (e.g., relational leadership and integrated knowledge). CSOs within Korean governmental organizations have a tendency to highly evaluate their level of leadership skill and knowledge, as well as the level of performance of their organization. This result is consistent with, and can be interpreted through, previous research that has found the concept of "saving face" to influence behavior within organizations based in Asia (Kim & Nam, 1998; Park, Dai Hwang, & Harrison, 1996). While the correlations are elevated, all of the constructs correlated more strongly with their own measures than with any of the other constructs indicating sufficient discriminate validity. Future research should test these results in other contexts to confirm or refute the findings.

Finally, this study indicates a significant effect of social alignment on ISS effectiveness and organizational performance. Integrated knowledge could act as an antecedent for organizational performance and ISS effectiveness, and future research could explore how social alignment between CSOs and business executives could be developed. We assert that future study of this issue would be best served by longitudinal observation. Future research could compare the development and/or effect of strategic and social alignment over time to tease out a more complete picture of the phenomenon.

8. Conclusion

This study explored, from a social capital perspective, how the level of relational leadership of the CSO drives the social alignment between the CSO and business executive, which in turn influences integrated knowledge, ISS effectiveness and organizational performance. Interestingly, and in contrast to prediction, the level of technical knowledge of the CSO dampened the relationship between integrated knowledge and ISS effectiveness, perhaps indicating a substitution effect. Finally, the results showed that the level of ISS effectiveness positively influenced organizational performance including financial and business process focused performance.

Appendix A

Construct	Source	Definition	Item[a]
Relational Leadership	Carmeli and Gittel (2009), Gittell (2003)	Relational leadership includes three foci, which are shared goals, shared knowledge, and mutual respect.	In this organization, we share a common vision. In this organization, we act toward common goals.* Employees in this organization act without having a clear direction. * Employees in this organization know what tasks their coworkers deal with. In this organization, we share with one another the subjects we work on. Sharing with one another in the context of work enables us to better understand the needs of each other. Sharing with one another about our work issues enables us to better understand how our actions impact other coworkers. There is a great deal of respect between one another at work. * When someone expresses her/his different opinion, we respect it. Mutual respect is at the basis of our relationships in this organization. *
Structural Linkage[b]	Karahanna and Preston (2013), Smaltz et al. (2006)	Structural linkage was measured as the frequency of informal interaction between of CSO and business executives.	I have informal contact with TMT (top management team) members. I socialize with the TMT members (e.g., social gatherings, golf, tennis, etc.). I have informal exchanges with TMT members.

Cognitive Linkage[b]	Karahanna and Preston (2013)	Cognitive linkage measures the degree to which the CSO and business executives share a common language and terminology in their communication.	The CSO and TMT members share a common language in our conversations. The CSO primarily uses business terminology when interacting with TMT members. The CSO avoids using information security jargon when interacting with TMT member. *
Relational Linkage[b]	Karahanna and Preston (2013)	Relational linkage measures the degree to which the CSO and business executives have developed a relationship of respect and trust.	The TMT members and CSO act in the best interest of the organization. The TMT members and CSO trust and respect each other. The TMT members and CSO are competent in what they do.
Integrated Knowledge	Boynton, Zmud, and Jacobs (1994), Karahanna and Preston (2013)	Integrated knowledge measures the degree to which the CSO and business executives have a shared understanding regarding the role of ISS within the organization.	The CSO and TMT members have a shared understanding of the role of information security in our organization. The CSO and TMT members have a shared view of the role of information security as a competitive weapon for our organization. The CSO and TMT members have a shared understanding of how information security can be used to increase the productivity of our organization's operations.
ISS Effectiveness	Hwang and Choi (2017), Kankanhalli et al. (2003), Knapp, Marshall, Rainer, and Ford (2007), Straub (1990)	ISS measures the degree to which the organization establishes controls preventing harm from external and internal threats.	Our information security policy describes the basic items in detail. * Our organization provides information security education and training for officers. Our organization establishes effective response systems toward information security accidents. Our organization's security controls protects information assets such as hardware and software. Our organization's security controls protect the organization's data. Our organization's security controls protect the organization's information services.
Organizational Performance	Kim, Shin, and Kwon (2012), Powell and Dent-Micallef (1997), Tippins and Sohi (2003)	Organizational performance measures the financial productivity of the organization and the execution of business processes within the organization.	Our organization achieved higher productivity than the goal over the past 3 years. Our organization was more profitable than the goal over the past 3 years. Our organization achieved a higher ROI than the goal over the past 3 years. Our organization achieved higher financial performance than the goal over the past 3 years. Our organization is better than other government organizations in connecting (e.g., communication and information sharing) parties. Our organization is better than other government organizations in reducing costs and human labor. * Our organization is better than other government organizations in bringing complex analytical methods to processing tasks. Our organization is better than other government organizations in bringing detailed information to processing tasks. *

CSO's Technical Knowledge	Byrd and Turner (2000), Lee, Trauth, and Farwell (1995)	Technical knowledge measures the knowledge of CSO in terms of planning, organizing, and leading IT-related projects.	The CSO is very capable in terms of planning, organizing, and leading projects. The CSO is very capable in terms of planning and executing work in a collective environment. The CSO is very capable in terms of teaching others.

*Item dropped.

[a]Items were measured on a five-point Likert scale where 1 denoted "strongly disagree" and 5 denoted "strongly agree."

[b]Items measuring the structural, relational and cognitive linkages were measure on a five-point Likert scale where 1 denoted "every day" and 5 denoted "never".

References

Adler, P. S., & Kwon, S.-W. (2002). Social capital: Prospects for a new concept. *Academy of Management Review, 27*, 17–40.

BBC (2014). *South Korean id system to be rebuilt from scratch.* (October 14, 2014) Retrieved from http://www.bbc.com/news/technology-29617196 (Accessed 01 June 2017).

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94.

Baldwin, M. W. (1997). Relational schemas as a source of if-then self-inference procedures. *Review of General Psychology, 1*(4), 326–335.

Bergeron, F., Raymond, L., & Rivard, S. (2004). Ideal patterns of strategic alignment and business performance. *Information & Management, 41*(8), 1003–1020.

Boisot, M. (1995). *Information space: A framework for learning in organizations, institutions and culture.* London: Routledge.

Boynton, A. C., Zmud, R. W., & Jacobs, J. C. (1994). The influence of IT management practice on IT use in large organizations. *MIS Quarterly, 18*(3), 299–318.

Brower, H. H., Schoorman, F. D., & Tan, H. H. (2000). A model of relational leadership: The integration of trust and leader-member exchange. *The Leadership Quarterly, 11*(2), 227–250.

Burt, R. S. (1997). The contingent value of social capital. *Administrative Science Quarterly, 41*(3), 339–365.

Byrd, T. A., & Turner, D. E. (2000). Measuring the flexibility of information technology infrastructure: Exploratory analysis of a construct. *Journal of Management Information Systems, 17*(1), 167–208.

CNN tech (2017). *Researchers find possible North Korea link to massive cyberattack.* (May 16, 2017), Retrieved from http://money.cnn.com/2017/05/15/technology/wannacry-hack-responsible-hackers/index.html (Accessed 02 July 2017).

CSO Online (2009). *What is a chief security officer?* (April 19, 2009) Retrieved on 12/01/2017 from http://www.CSOonline.com/article/221739/What_is_a_Chief_Security_Officer.

Carmeli, A., & Gittel, J. H. (2009). High-quality relationships, psychological safety, and learning from failures in work organizations. *Journal of Organizational Behavior, 30*(6), 709–729.

Chan, Y. E., & Reich, B. H. (2007). IT alignment: What have we learned? *Journal of Information Technology, 22*(4), 297–315.

Chan, Y. E., Huff, S. L., Barclay, D. W., & Copeland, D. G. (1997). Business strategic orientation, information systems strategic orientation, and strategic alignment. *Information Systems Research, 8*(2), 125–147.

Chan, Y. E. (2002). Why haven't we mastered alignment? The importance of the informal organization structure. *MIS Quarterly Executive, 1*(2), 97–112.

Chen, R., Sun, C., Helms, M. M., & Jih, W. (2008). Aligning information technology and business strategy with a dynamic capabilities perspective: A longitudinal study of a Taiwanese semiconductor company. *International Journal of Information Management, 28*(5), 366–378.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157–188.

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing common method bias: Problems with the ULMC technique. *MIS Quarterly, 36*(3), 1003–1019.

Chin, W. W. (1998). The partial least square approach to structural equation modeling. In G. A. Marcoulides (Ed.). *Modern methods for business research* (pp. 295–336). Mahwah, NJ: Lawrence Erlbaum & Associates.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability, 8*(7), 638.

Chong, A. Y. L., Ooi, K. B., Chan, F. T., & Darmawan, N. (2011). Does employee alignment affect business-IT alignment? An empirical analysis. *Journal of Computer Information Systems, 51*(3), 10–20.

Clark, K. B., & Fujimoto, T. (1991). *Product development performance.* Boston, MA Harvard: Business School Press.

Cohen, J. (1988). *Statistical power analysis.* Hillsdale, NJ: Erlbaum & Associates.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658.

Drath, W. (2001). *The deep blue sea: Rethinking the source of leadership.* San Francisco, CA: Jossey-Bass.

Forbes (2016a). *Cyber-crime costs projected to reach $2 trillion by 2019.* (Jan 17, 2016) Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#535bc38d3a91 (Accessed 02 June 2017).

Forbes (2016b). *Top cyber security salaries in U.S. metros hit $380,000.* (Jan 9, 2016) Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000/#59e3f1a47ef8.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using pls-graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*, 91–109.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii–xiv.

Gibbs, J. P. (1975). Crime, punishment, and deterrence. *Southwestern Social Science Quarterly, 48*, 515–530.

Gittell, J. H., & Douglass, A. (2012). Relational bureaucracy: Structuring reciprocal relationships into roles. *Academy of Management Review, 37*(4), 709–733.

Gittell, J. H. (2003). A theory of relational coordination. In K. Cameron, J. Dutton, & R. Quinn (Eds.). *Positive organizational scholarship: Foundations of a new discipline* (pp. 279–295). San Francisco, CA: Berrett-Koehler Publishers.

Goles, T., White, G. B., & Dietrich, G. (2005). Dark screen: An exercise in cyber security. *MIS Quarterly Executive, 4*(2), 303–318.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information and Management, 20*(1), 13–27.

Grant, R. M. (1996). Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization Science, 7*(4), 375–387.

Gulati, R., & Puranam, P. (2009). Renewal through reorganization: The value of inconsistencies between formal and informal organization. *Organization Science, 20*(2), 422–440.

Gupta, M. (2011). *Three essays on information technology security management in organizations.* State University of New York at Buffalo.

Hankook Newpaper (September 17, 2015), Retrieved from http://www.hankookilbo.com/v_print.aspx?id=c9870a301fa044df9008bdd64f2ff5dd (Accessed 28 July 2017).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Hiller, N. J., Day, D. V., & Vance, R. J. (2006). Collective enactment of leadership roles and team effectiveness: A field study. *The Leadership Quarterly, 17*(4), 387–397.

Hwang, K., & Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Government Information Quarterly, 34*(2), 183–198. http://dx.doi.org/10.1016/j.giq.2017.02.001.

ITRC (2015). *Data breach report* Retrieved from http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf (Accessed 20 June 2017).

Jones, G. R., & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of Management Review, 23*(3), 531–546.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154.

Karahanna, E., & Preston, D. S. (2013). The effect of social capital of the relationship between the CIO and top management team on firm performance. *Journal of Management Information Systems, 30*(1), 15–55.

Katz, D., & Kahn, R. L. (1978). *The social psychology of organizations.* New York: Wiley.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 9*(3), 2012–2052.

Kearns, G. S., & Sabherwal, R. (2006). Strategic alignment between business and information technology: A knowledge-based view of behaviors, outcome, and consequences. *Journal of Management Information Systems, 23*(3), 129–162 2006-7.

Kim, J. Y., & Nam, S. H. (1998). The concept and dynamics of face: Implications for organizational behavior in Asia. *Organization Science, 9*(4), 522–534.

Kim, G., Shin, B., & Kwon, O. (2012). Investigating the value of sociomaterialism in conceptualizing IT capability of a firm. *Journal of Management Information Systems, 29*(3), 327–362.

Kim, J. (2012). National information security agenda and policies. *Journal of Digital Convergence, 10*(1), 105–111.
Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help. *Information Security and Risk Management, 15*(4), 51–58.
Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. *International Journal of Information Security and Privacy, 1*(2), 37–60.
Kogut, B., & Zander, U. (1996). What firms do? Coordination, identity, and learning. *Organization Science, 7*(5), 502–518.
Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computer & Security, 28*(7), 509–520.
Lee, D. M. S., Trauth, E., & Farwell, D. (1995). Critical skills and knowledge requirements of IS professionals: A joint academic/industry investigation. *MIS Quarterly, 19*(3), 313–340.
Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59–87.
Lind, M. R., & Zmud, R. W. (1991). The Influence of a convergence in understanding between technology providers and users on information technology innovativeness. *Organization Science, 2*(2), 195–217.
Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363.
Moffat, P. M., & Nzulwa, J. (2016). Effect of strategic security management practicies on firm performance: A case of Kenya revenue authority. *The Strategic Journal of Business & Change Management, 3*(4).
Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of Management Review, 23*(2), 242–266.
Nance, W. D., & Straub, D. W. (1988). An investigation into the use and usefulness of security software in detecting computer abuse. *Proceedings of the ninth international conference on information systems* (pp. 283–294).
Oh, H., Labianca, G., & Chung, M. H. (2006). A multilevel model of group social capital. *Academy of Management Review, 31*(3), 569–582.
Okhuysen, G. A., & Eisenhardt, K. M. (2002). Integrating knowledge in groups: How simple formal interventions enable flexibility. *Organization Science, 13*(4), 370–386.
Park, H., Dai Hwang, S., & Harrison, J. K. (1996). Sources and consequences of communication problems in foreign subsidiaries: The case of United States firms in South Korea. *International Business Review, 5*(1), 79–98.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.
Powell, T. C., & Dent-Micallef, A. (1997). Information technology as competitive advantage: The role of human business, and technology resources. *Strategic Management Journal, 18*(5), 375–405.
PricewaterhouseCoopers (2015). *2015 information security Breaches survey, HM government* Retrieved from: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf (Accessed 01 August 2017).
Reich, B. H., & Benbasat, I. (1996). An empirical investigation of customer-oriented strategic systems. *Information Systems Research, 1*(3), 325–347.
Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quarterly, 24*(1), 81–113.
Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS 2.0 (Beta)*. Hamburg, Germany: University of Hamburg. http://www.Smartpls.De.
Sabherwal, R., & Chan, Y. E. (2001). Alignment between business and IS strategies: A configurational approach. *Information Systems Research, 12*(1), 11–33.
Sarkar, K. R. (2010). Assessing insider threats to information security using technical: Behavioural and organizational measures. *Information Security Technical Report, 15*(3), 112–133.
Schermerhorn, J. R., Hunt, J. G., & Osborn, R. N. (2003). *Organizational behavior* (8th ed.). New York, NY: Wiley.
Sen, S., & Samanta, S. (2014). Information security. *International Journal of Innovative Research in Technology, 1*(11), 224–231.
Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.
Smaltz, D. H., Sambamurthy, V., & Agarwal, R. (2006). The antecedents of CIO role effectiveness in organizations: An empirical study in the healthcare sector. *IEEE Transactions on Engineering Management, 53*(2), 207–222.
Soda, G., & Zaheer, A. (2012). A network perspective on organizational architecture: Performance effects of the interplay of formal and informal organization. *Strategic Management Journal, 33*(6), 751–771.
Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296–302.
Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security needs a more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225.
Strang, K. D. (2007). Examining effective technology project leadership traits and behaviors. *Computers in Human Behavior, 23*, 424–462.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.
Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*, 380–427 (Article 24).
Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.
Thatcher, J. B., & Perrewe, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly, 26*(4), 381–396.
Tippins, M. J., & Sohi, R. S. (2003). IT competency and firm performance: Is organizational learning a missing link? *Strategic Management Journal, 24*(8), 745–761.
Tsai, C.-Y., Dionne, S. D., Wang, A.-C., & Spain, S. M. (2017). Effects of relational schema congruence on leader-member exchange. *The Leadership Quarterly, 28*(2), 268–284.
Uhl-Bien, M., Graen, G., & Scandura, T. (2000). Implications of leader-member exchange (LMX) for strategic human resource management systems: Relationships as social capital for competitive advantage. In G. R. Ferris (Ed.). *Research in personnel and human resource management* (pp. 103–133). Greenwich, CT: Information Age Publishing.
Uhl-Bien, M. (2006). Relational leadership theory: Exploring the social processes of leadership and organizing. *The Leadership Quarterly, 17*(6), 654–676.
Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263–290.
Wagner, H.-T., Beimborn, D., & Weitzel, T. (2014). How social capital among information technology and business units drives operational alignment and IT business value. *Journal of Management Information Systems, 31*(1), 241–271.
Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101–105.
Whitten, D. (2008). The chief information security officer: Analysis of the skills required for success. *Journal of Computer Information Systems, 48*(3), 15–19.
Yonhap Newspaper (September 16, 2015), Retrieved from http://www.yonhapnews.co.kr/bulletin/2015/09/16/0200000000AKR20150916221100003.HTML (Accessed 02 January 2017).

Yun Ji Moon has a Ph.D from Ewha Womans University in Management Information Systems. Her research interests include adoption of information technology, mobile business, organizational impact of information technology, knowledge management, and e-service quality model. Her papers have appeared in Information & Management, Canadian Journal of Administrative Sciences, Journal of Computer Information Systems, and International Journal of Hospitality Management. She is currently working as an assistant professor in the department of Management Information Systems, at Catholic University of Pusan, South Korea. She can be reached at yjmoon@cup.ac.kr.

Dr. Myeonggil Choi earned his Ph D at KAIST (Korea Advanced Institute of Science and Technology), and worked as a senior researcher at Electronics and Telecommunication Research Institute (ETRI), and Agency for Defense(ADD), and currently working as an associate professor in the department of Business Administration, at Chung-Ang University, Seoul. He has conducted security research in government. His research interest includes information security systems for e-government, evaluation of information security, and organizational behavior toward information security.

Deborah J. Armstrong is an associate professor of Management Information Systems in the College of Business at The Florida State University. Dr. Armstrong's research interests cover a variety of issues at the intersection of IS personnel and cognition involving the human aspects of technology, change, and learning. Her research has appeared in *Management Information Systems Quarterly*, *Journal of Management Information Systems*, the *European Journal of Information Systems* and *Communications of the ACM*, among others.