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

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.