Inf Syst Front (2011) 13:579–593
DOI 10.1007/s10796-010-9232-6

Information systems resources and information security

Kuo-chung Chang · Chih-ping Wang

Published online: 27 April 2010

Abstract Recent studies suggest that the number of information security incidents has increased dramatically and has caused significant economic loss worldwide. Awareness of the significance of information security is evidenced by a rapid increase in information security investments. Despite the fact that information security has taken on a new level of importance, academic research on this subject is still in its infancy. A review of literature indicated that past studies largely took a resource based view, suggesting that organizations invest and develop a variety of IS resources so as to ease potential threats caused by information security breaches. However, the resource-based perspective as used in previous studies was somewhat limited. Based on and extending from previous work, this study employed the resource-based view as a theoretical lens to examine the role that IS resources play in determining the level of information security. A field study was conducted to test the hypotheses. The results of the model testing show that IT human, relational, and infrastructure resources have significant impacts on information security.

Keywords IS resources · Information security · Information confidentiality · Information integrity · Information availability

K.-c. Chang (✉) · C.-p. Wang
Department of Information Management, Yuan Ze University, Taiwan, Republic of China
e-mail: changkc@saturn.yzu.edu.tw

C.-p. Wang
e-mail: wang.cp@gmail.com

1 Introduction

Organizations are more dependent than ever on information systems (IS) to enhance business efficiency and effectiveness. However, the proliferation of information technology spawns opportunities to breach corporate systems. Recent surveys reported that increasingly number of information security incidents has caused significant economic loss (Bagchi and Udo 2003; Campbell et al. 2004; Cavusoglu et al. 2004; Gordon and Loeb 2002; Hinde 2002; Power 2002).. Dramatic increases in the number of IT security breaches and resulting monetary losses in recent years have made IT security a top issue in the management of corporate information systems, which is also reflected in the increasing security budgets of firms (Hulme 2002).

Obviously, how to enhance IS security or, alternatively, how to prevent system from being breached are essential questions for organizations to consider. The purpose of this research is to examine critical factors influencing a firm's level of information security. One theoretical perspective that can help inform our understanding of the enhancement of information security is the resource-based view (RBV). This perspective is chose on the ground that it is essential for organizations to invest in and develop a variety of IS resources to thwart the potential threats caused by system breaches. Synthesizing previous RBV research on IS security, this paper presents an integrated model enumerating three sets of IS resources (information technology resources, relationship resources, and IS infrastructure resources) that have profound impacts on information security.

Understanding what IS-related resources influence information security is important for theoretical as well as practical reasons. Theoretically, RBV employed in this study can facilitate the specification of IS resources that are relevant to the subject of information security. Specifically, it requires

competent IT, managerial, and infrastructure resources that can effectively plan, design, implement, and operate security-related technologies and infrastructure to prevent, detect, and respond to security breaches. Secondly, focusing on RBV can advance our understanding of the structure for IS security resources construct by providing detailed exposition of their dimensions. Lastly, this research provides a guideline for organizations regarding how and where IS resources should be deployed to generate superior information security.

The rest of the paper proceeds as follows. In the second section, we review the extant literature related to the subjects of information security and IS resources. Subsequent sections consecutively present the research model and hypotheses derived, outline the research methodology, report the results of the model testing, and discuss the findings and their theoretical and managerial implications. This paper concludes with a discussion about the limitations and directions for future research.

2 Literature review

2.1 Information security

Information security refers the extent to which corporate information is free from disclosure, modification, or destruction due to intentional or unauthorized access (Finne 2000). A literature review shows that information security is composed of three dimensions: confidentiality, integrity, and availability. Table 1 presents a summary of the review (Anderson 2003; Finne 2000; Dhillon and Backhouse 2000; Hong et al. 2003; Joshi et al. 2001; Laudon and Laudon 2000; Schultz et al. 2001; Shih and Wen 2003).

Information confidentiality refers to the extent to which corporate information is kept from being disclosed, exposed, or appropriated. The essence of confidentiality resides in the fact that information remains safe from any unauthorized access (Schultz et al. 2001), either from within the organization or from without (Lee et al. 2004; Wang et al. 1996). Information integrity refers to the extent that information remains consistent and compatible with its original state after being stored and/or transmitted (Lee et al. 2004). In essence, high integrity suggests that information has not been subjected to modification or forgery (Shih and Wen 2003) and that it is error-free (Bovee et al. 2001; Wang et al. 1995, 1996). Information availability refers to the extent to which information is readily accessible, whenever and wherever access is required. The degree of availability is closely related to IS reliability. The longer IS operate properly, the more likely they can be readily accessed and information be appropriately delivered as requested (Dhillon and Backhouse 2000; Joshi et al. 2001). Insufficient protection leaves information systems

Table 1 Sample demographics and non-response bias analysis

Characteristics	Category	Frequency	Percentage
Title	CEO	17	13 .49%
	CFO	9	7.14%
	COO	13	10.32%
	CIO	64	50.79%
	IT managers	23	18.25%
Industry	Service	8	6.4%
	Manufacturing	74	58.7%
	Finance	2	1.6%
	Retailing	2	1.6%
	IT	35	27.7%
	Other	5	4.0%
Number of Employees	<100	31	24.6
	101–1,000	64	50.8%
	1,001–10,000	24	19.1%
	>10,000	7	5.6%
Sales (in $1million)	<10	22	17.5%
	10–100	25	19.8%
	100–1,000	46	36.5%
	1,000–10,000	18	14.3%
	>10,000	15	11.9%
Non-response bias analysis	*F*-value		*P*-value
Sales	1.477028		0.230039
Employee number	1.85127		0.136559

vulnerable to attacks, which in turn affects the availability of information (Finne 2000; Flowerday and von Solms 2005; Schultz et al. 2001; Shih and Wen 2003).

2.2 Information system resources

Past research has identified a variety of information systems resources. They can be generally organized into three subsets: information technology resources (ITR), relationship resources (RR) and IS infrastructure resources (IIS). ITR refer to the IS expertise and skills that the focal firm possesses. It can be further divided into two distinct sets of capabilities: IT technical capabilities (ITTC) and IT-business alignment capabilities (IBAC). RR refer to the extent that an information department has established a sense of collaboration and partnership with other functional units (i.e. finance or production) and business partners (i.e. suppliers or customers) of an organization. It consists of two dimensions: internal relationship resources (INR) and external relationship resources (EXR). IIS represent a collection of IT-based assets on which other business applications and services are developed. In this study, it is specifically referred to as information security infrastructure (ISI), which is defined as the technical and management architectures that the focal organization develops to ensure information security. ISI was chosen for this study because it provides functions and services that act as a foundation for systems security (Broadbent and Weill 1997; Byrd et al. 2004; Weill et al. 2002). Each of the resources is described more fully below. Table 2 presents a summary of our literature review and the categorization scheme used in this study.

2.2.1 Information technology resources

Information technology resources (ITR) refer to the IT-related knowledge and skills an enterprise possesses for IT-based initiatives. ITR is composed of IT technical capabilities (ITTC) and IT-business alignment capabilities (IBAC). ITTC refer to the set of technical skills and knowledge that the focal firm possesses. Research has shown that computer programming is a vital technical skill (Bharadwaj 2000; Byrd and Turner 2000; Piccoli and Ives 2005; Lee et al. 1995; Mata et al. 1995; McKenney et al. 1995; Ross et al. 1996; Ray et al. 2005). The IT department of a firm needs to be acquainted with various computer languages and apply them so as to develop information systems that best meet the demands of the enterprise. In addition, scholars have pointed out that the capability to correctly operate information systems is another critical technical skill (Henderson and Venkatraman 1993; Mata et al. 1995; Ravichandran and Lertwongsatien 2005; Ray et al. 2005; Ross et al. 1996). Systems operation knowledge and skills are even more vital in today's competitive marketplace since enterprise systems are increasingly massive and complicated, which requires more delicate handling of systems operations. Organizations need to possess the relevant knowledge and skills to accurately operate their information systems so that enterprise systems can achieve their designated promises. Furthermore, research also indicates that the capability of an enterprise to maintain the operation of its information systems is one of the important technical skills that can help to reduce the chance of systems breakdowns, hence increasing their availability (Lee et al. 1995; Ross et al. 1996). Finally, the capability to diagnose systems problems is another important skill. Such technical know-how allows IS personnel to analyze the scope and depth of system problems and provide solutions in the face of system breakdowns (Ravichandran and Lertwongsatien 2005).

IBAC in this study refer to the knowledge and skills to effectively align IT strategy with business strategy (Lee et al. 1995). This capability can be demonstrated in two ways.

Table 2 Construct structures, scale types, and scale sources

2nd order constructs	Scale types	1st order constructs	Scale types	Item number	Sources
Information technology resources	Formative	IT technical capability	Formative	5	Adapted from Byrd and Turner (2000)
		IT-business alignment capabilities	Formative	6	Adapted from Byrd and Turner (2000) Ravichandran and Lertwongsatien (2005)
Relationship resources	Formative	Internal relationship	Reflective	6	Adapted from Ravichandran and Lertwongsatien (2005)
		External relationship	Reflective	5	
Information security infrastructure	Formative	Information security technology architecture	Formative	7	Based on literature (see Appendix 2)
		Information security management architecture	Formative	11	Based on ISO/IEC27000 (see Appendix 2)
Information security	Formative	Information confidentiality	Reflective	7	Adapted from Lee et al. (2004)
		Information integrity	Reflective	5	
		Information availability	Reflective	4	

First, IT departments, acting on the enterprise's business strategy, can outline IT strategies, plans, and technical investments as well as implement IT technical architecture (Henderson and Venkatraman 1993; Lee et al. 1995). Also, IBAC signifies that firms are able to identify and employ emerging information technologies to transform the enterprise so as to gain competitive advantages and perhaps even change the structure of the industry in which the focal firm is situated (Cash and Konsynski 1985; Henderson and Venkatraman 1993; Swanson 1994). Second, an IT department with high IBAC involves a deep understanding of the business processes and the organizational goals. With this business knowledge, the IT department is able to develop effective IS strategies and provide information services that fit organizational needs (Feeny and Willcocks 1998; Mata et al. 1995)

2.2.2 Relationship resources

Relationship resources (RR) refer the spirit of partnership that the IT department of the focal firm has cultivated with its clients within and outside of the organization. It is comprised of two dimensions: internal relationship resources (INR) and external relationship resources (EXR) (Mata et al. 1995; Ross et al. 1996; Byrd and Turner 2000). While INR reflect the working and collaborating ties that the IT department has forged with other departments within the organization, EXR suggest similar working relationships that the IT department has established with business partners from outside the company. This working relationship allows social exchanges between the IT department and its clients from within or outside of the organization, leading to the development of closer ties, as well as the establishment of mutual trust and respect. The reciprocal relationship cultivates a sense of bonding from which the working parties share a common view (Piccoli and Ives 2005). Moreover, the spirit of partnership also entices the participating parties to put greater emphasis on sharing responsibilities and contributing resources to accomplish their common goals (Bharadwaj 2000; Ross et al. 1996). In addition, good relationships lead to greater mutual coordination, as well as adjustments that take the needs of counterparts into account. As a result, disputes rarely arise, and those that do occur are often effectively resolved using mechanisms developed for this purpose (Lee et al. 1995; Ross et al. 1996; Ravichandran and Lertwongsatien 2005; Weill et al. 2002).

2.2.3 IS security infrastructure resources

Substantial studies addressing the issue of information security have paid great attention to the development of an IS technical architecture (Broadbent and Weill 1997; Byrd et al. 2004; Weill et al. 2002). However, IS researchers have also recognized that information security is not merely a technical issue, but also a management one (Chang and Ho 2006; Dhillon and Backhouse 2000; Dutta and McCrohan 2002; Vermeulen and Von Solms 2002; von Solms and von Solms 2004). Hence, IS infrastructure in this study involves both security-related technical and management architectures. IS technical architecture (ISTA) refers to a set of IT-based assets (i.e. software and hardware) that protect information systems from threats associated with security breaches. Based on literature review, this framework consists of seven components: information transmissions; access rights authentication; access control; encryption and decryption; storage and backup; malicious protection; log analysis. The information transmission component encompasses both Internet security control software and hardware and is aimed at maintaining the stability of enterprise-wide network communications and guarding against information damage caused by malicious access (Tickle 2002; Twitchell 2004; Velissarios and Santarossa 1999). The identification and authority component includes verification and authentication techniques associated with verifying users' identities and access rights (Budiarto and Masahiko 2002; Joshi et al. 2001; Priem and Butler 2001). The data access control component consists of access control tools and equipment to control information access (Cheng 1999; Ferraiolo et al. 2001; Gunter 2000; Zhang and Yang 2003), while the data encryption and decryption component consists of technology that functions to protect sensitive information from unauthorized access (Joshi et al. 2001; Twitchell 2004; Velissarios and Santarossa 1999). The data storage and backup component includes backup devices that keep information accessible during system failures or data impairment (Twitchell 2004; Schultz et al. 2001; Weill et al. 2002). The malicious program protection component consists of anti-virus, anti-spyware and webpage filtering software and hardware that work to reduce the risk that information might be compromised due to malicious code (Flowerday and von Solms 2005; Tickle 2002). Finally, the log analysis component includes log server and analysis technology to diagnose and detect systems anomalies by examining log data.

IS management architecture (ISMA) refers the rules and regulations promulgated by an organization to manage and control the security of information systems. These management mechanisms provide a set of precepts that govern individual behaviors in alignment with organizational information security requirements. They specify the roles and responsibilities that employees should follow in keeping information from becoming unprotected. ISMA developed in this study is primarily

derived from the ISO/IEC27000 framework—currently the most comprehensive and recognized of its kind in information security management. The framework is comprised of ten components: information security policy; asset management; human resources security; physical and environmental security; communications and operation management; access control; information systems acquisition, development and maintenance; information security incident management; and business continuity management. A brief description of each follows.

Information security policy serves as the foundation for and defines the overall objectives related to information security within an organization. Asset management refers to the rules and standards that aim to assist an organization to perform risk assessments and classify its information properties. The human resources management component defines the training programs that outline the roles and responsibilities that employees should follow in keeping information secure. The physical and environmental security component provides user imperative security guidelines within the surroundings that information systems are located in. The communications and operations management component contains system operation regulations and procedures aimed at ensuring the proper use and transmission of information, in an effort to reduce damage to information systems and lower the risk of system failures. The access control component consists of rules specifying access rights. Information systems acquisition, development and maintenance management involves practices that implant information security management rules within the process of acquiring, developing, and maintaining information systems to shelter the data contained within information systems. The information security incident management component entails a set of rules specifying the procedure and practices to be followed in the event of information breaches. Last of all, the business continuity management component refers to the rules that define how organizations maintain their business operations following information breach incidents.

3 Research model and hypothesis

Figure 1 depicts the research model developed in this study. The model asserts that a firm's IS resources are related to the level of information security. Specifically, this study contends that organizational information technology resources, relationship resources and information security infrastructure have a profound impact on information security. There are three hypotheses associated with the model, which are described next.

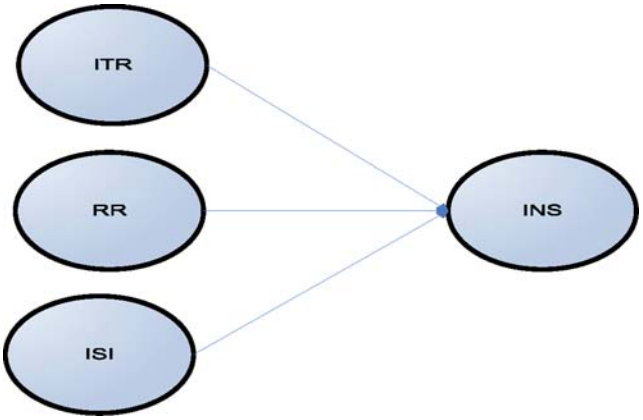

Fig. 1 Research model

3.1 Information technology resources and information security

IT technical capabilities (ITTC) involve technical skills and know-how associated with designing and operating information systems. ITTC may include such skills as programming, system operation, problem diagnose. These capabilities have profound impacts on the level of information security that a firm can achieve. For example, when designing information systems, programming capability allow IT recruits to inscribe covert access codes to shield IS from unauthorized entry and information disclosures, and thus risks related to information confidentiality subside (Benantar and Guski 1996; Twitchell 2004). Moreover, programming capabilities can also effectively reduce bugs generated during the system development, lowering the probability of systems breakdown and thus enhancing systems availability. In addition, IT workforce who knows how the systems are functioned is able to reduce the probability of system damage due to inappropriate systems operation, which in turn increasing the rate of system availability. Diagnosing ability is critical to information availability due to the fact that when systems undergo malfunctions or ruptures it allows IS staff to quickly pinpoint the source of problems and thus reduce the time to restore failed systems, making information more readily accessible when required.

IT-business alignment capabilities (IBAC) reflect IT department's understanding of the business environments and goals set by an enterprise. With this knowledge, IT departments can align IT strategy with corporate strategy and thus provide technical solutions to help their firm solve business problems. Additionally, understanding a firm's business environments and goals enable IT workforce to develop an information assets classification scheme in terms of their importance to the business needs and conduct information assets risk assessments. A clear asset classification scheme and robust risk assessments allow the firm to

protect information properties with proper management and technical solutions. In this way, the authority to access information of great importance is highly restricted; only personnel with proper clearance can access such information. Moreover, classified information can be encrypted before being transmitted, which enhances information integrity. Further, high IBAC allows the firm to effectively allocate limited resources to allow un-interrupted operation of information systems, and thus enhance the systems availability rate. Based on the aforementioned statements, we hypothesized:

H1 The extent of information technology resources that a firm possesses is positively associated with the extent of information security.

3.2 Relationship resources and information security

Past studies have recognized the importance of building relationships internally within the firm between the IS function and other areas or departments (Armstrong and Sambamurthy 1999; Bharadwaj 2000; Jarvenpaa and Leidner 1998; Ross et al. 1996). Such relationships help the support for collaboration (i.e. information exchange) within and across the firm. Information departments that share good relationships with other departments in the organization encourage the circulation of intelligence related to information security. Speedy exchange of information on information security effectively prevents information security incidents and facilitates organizational ability to tackle security events more effectively if they do occur. Moreover, when IT departments launch information security initiatives, reciprocal relationships create a sense of partnership that renders counterparts willing to share the risks and responsibilities, which prompts other departments to follow security related regulations and practices, as well as actively report security events such as information theft or compromise. Additionally, strong internal relationships encourage other departments within an organization to share information regarding potential information systems security issues. As a result, systems availability is enhanced.

As IT turns the supply chain into a interconnected network, good external relationships lead to better communication and more reciprocal respect between the focal firm and its business partners, which breeds a sense of bonding and inspires cooperation. In such an atmosphere, business partners become more willing to collaborate with the focal firm and respond more promptly when security events take place. In addition, good external relationships generate a sense of partnership in which business partners are more likely to share their information on potential security problems in such a way that allows the focal organization to take preemptive initiatives and thereby fend off intentional intrusions, information thefts, and systems downfalls. Consequently, these preventative efforts result in improved information security. When data errors or systems failures occur during data transmission, strong support from business partners enables the focal organization to quickly identify the cause of the problems and provide solutions, and the speedy reaction also enhances information integrity and availability. Considering to the aforementioned statements, we hypothesized:

H2 The extent of relationship resources that a firm possesses is positively associated with the extent of information security.

3.3 Information security infrastructure and information security

The availability of IS technology architecture (ISTA) and IS management architecture (ISMA) is one of the critical preemptive measures for the enhancement of information security. In terms of ISTA, identity authentication techniques (such as AD Server) strengthen the user identification and authorization control by preventing unauthorized access to a firm's critical IS. Cytological tools (i.e. encryption and decryption) fortify the protection of data from unauthorized theft or modification in the process of transmission or storage. Data storage apparatus (i.e. NAS Server/tape device) enable the focal firm to recover data in the event of data errors or systems damage. As enterprises become increasingly dependent on computer networks to distribute and access information, computer network security control gears (i.e. Firewall and IDS) support firms by guarding against malicious attacks (i.e. denial of service) and keeping systems nonstop. Further, malicious program protection techniques provide vulnerability assessment reports that can buttress information system defenses against malicious code intrusions (i.e. viruses, worms, Trojan horses, phishing). Also, log analysis devices assist the firm to detect and fend off illegal access attempts. Studies have found that application of information security-related software and hardware can deter the misuse and abuse of information systems (Nance and Straub 1988). Another study by Kankanhalli et al. (2003) pointed out that better ISTA led to a smaller probability of information damage. Straub and Nance (1990) and Straub and Welke (1998) also found that the employment of information technology can effectively prevent, detect, and deter behaviors that violate information security.

In addition to the technical architecture, ISMA has a profound impact on information security. Research has shown that clear policies and proper information use regulations can serve as guidelines for users, helping them

to understand what proper behaviors are (Kankanhalli et al. 2003). For example, clearly-defined rules for the maintenance of information systems standardize maintenance procedures and prevent damage caused by misuse. Additionally, information transmission security management, or rules that define the procedure on how data should be encrypted before transmitting, can effectively thwart the possibility of classified information being subjected to unauthorized browsing, changes or forgery. Past studies have shown that a strong ISMA makes potential abusers recognize the serious consequences of their actions, and consequently allows a firm to deter behaviors associated with violating information security and reduce potential abuses of hardware, data and information services (Kankanhalli et al. 2003; Straub 1990; Straub and Welke 1998). Following the above statements, we hypothesized the following:

H3 The information security infrastructure resources that a firm possesses are positively associated with the extent of information security.

4 Research method and data analysis

4.1 Sample

A sample was drawn from the Information Management Association of Taiwan (IMA). IMA was chosen because it is the largest and most important IT professional association in Taiwan and represents a cross section of managerial positions extensively involved in information security. Senior executives involved in information security were targeted as the key respondents. The sampling frame yielded a list of 811 senior executives. 511 surveys were effectively delivered among which 190 were returned, yielding a total response rate of 37%. Out of these, 126 were complete and usable. Table 1 presents the titles of the respondents and the profiles of the respondent organizations in the sample. A non-response bias test was performed to compare employee numbers and the annual sales between early and late responding firms (Armstrong and Overto 1977; Keil et al. 2000). As shown in Table 1, results exhibited no significant difference ($p>0.1$).

4.2 Measurement model

A survey instrument was developed by identifying appropriate measurements following a comprehensive literature review. For constructs lacking previous measures, new items were developed. A 7-point Likert scale was used for all measures, with endpoints ranging from strongly disagree (1) to strongly agree (7). All the variables (ITR, RR, ISI, and IS) were modeled as second order constructs. Appendix and Table 2 present the instruments, scale types, and their sources as employed in this study.

While ITR and ISI were formed by two formative first order constructs, the other two (RR and IS) were made up of two reflective ones. Conceptualization of the formative construct was based on two criteria. First, it consisted of multiple dimensions that were not the manifestation but the cause of the construct (Law and Wong 1999; MacCallum and Browne 1993). Second, no correlation was assumed among component variables (Chin 1998; Chin and Gopal 1995; Cohen et al. 1990). For example, the level of ITR is based on the two facets of IT capability: ITTC and IBAC. While high ITTC contribute to a firm's overall ITR, a firm's overall ITR may not serve as the manifestation of ITTC because the same level of ITR can be achieved through different combinations of ITTC and IBAC. Moreover, no theoretical arguments have suggested that ITTC and IBAC are correlated. In other words, increasing ITTC does not necessarily lead to a growth in IBAC. All other variables were closely examined and conceptualized based on the same criteria. Table 2 shows the structure of the constructs in the study.

A panel of judges made up of five IS experts were asked to evaluate the preliminary questionnaire to ensure that the items rightly captured the content of the constructs in the research model; following this, another 5 IS managers were asked to examine the appropriateness of the items and constructs. The instrument was modified based on their feedback. To assess the validity of the formative constructs (ITTC, IBAC, ISTA, and ISMA), the weightings in the principal component analysis was examined. While item weightings for three of the five ITTC measures were found to be significant, three out of six measures for IBAC were observed significant. For ISTA, out of 7 measures 4 item weightings were detected significant whereas 6 of 11 ISMA scales were significant. However, to retain content validity (Diamantopoulos and Siguaw 2006; Diamantopoulos and Winklhofer 2001; Petter et al. 2007) all of the indicators were kept in the model. A multicollinearity test was performed to determine whether the formative measures are highly correlated. Variance inflator factor statistics for the formative measures ranged between 1.85 and 9.82, which is below the suggested threshold (Diamantopoulos and Winklhofer 2001; Kleinbaum et al. 1988). Therefore, all formative measures were retained.

Data associated with reflective constructs were subjected to exploratory factor analysis to assess psychometric properties of the measurement in this study. As shown in Table 3, Cronbach's α ranged from 0.88 to 0.95, indicating that the measurements were reliable. The factor analysis yielded a 5-factor solution (See Table 3). Loadings below 0.5 (INR1, EXR1, INA4) were removed from the item list

Table 3 Descriptive statistics, factor loadings, and Cronbach's α

Item code	Means	Standard deviation	Standardized loadings	Alpha
Internal relationship				0.90
INR1	4.95	1.36	0.40[a]	
INR2	4.79	1.26	0.74	
INR3	4.83	1.41	0.81	
INR4	4.58	1.45	0.61	
INR5	5.07	1.42	0.71	
INR6	4.98	1.47	0.66	
External relationship				0.88
EXR1	4.63	1.41	0.47[a]	
EXR2	4.44	1.53	0.77	
EXR3	4.44	1.46	0.74	
EXR4	4.79	1.38	0.64	
EXR5	4.94	1.29	0.59	
Information confidentiality				0.96
INC1	5.02	1.54	0.64	
INC2	5.43	1.39	0.71	
INC3	4.75	1.55	0.69	
INC4	5.04	1.47	0.77	
INC5	4.79	1.64	0.80	
INC6	5.10	1.53	0.78	
INC7	5.10	1.62	0.83	
Information integrity				0.97
INI1	5.32	1.38	0.83	
INI2	5.38	1.31	0.80	
INI3	5.33	1.32	0.81	
INI4	5.42	1.29	0.82	
INI5	5.40	1.42	0.72	
Information availability				0.91
INA1	4.73	1.59	0.91	
INA2	4.83	1.58	0.83	
INA3	4.70	1.57	0.89	
INA4	5.13	1.50	0.39[a]	

[a] indicate removed items

(Hair et al. 1992). The remaining items were subject to an examination of construct validity using output from the partial least square (PLS). As shown in Table 4, internal consistency reliability (ICR) (Agarwal and Karahanna 2000; Barclay et al. 1995), the square root of average variance extracted (AVE) (Chin 1998; Hair et al. 1998; Yi and David 2003), and item loadings (Falk and Miller 1992; Hair et al. 1998) were all above the recommended guidelines. The results suggested strong convergent validity. In addition, the square root of AVE proved greater than all of the inter-construct correlations and the loadings to a latent variable that an item intends to measure should be greater than those to other latent variables. The results suggest adequate discriminant validity (Barclay et al. 1995; Fornell and Larcker 1981).

Organizational size was included as a control variable in the analysis. It was included because the availability of resources may be constrained due to the size of the firm and thus has impact on a firm's capability to enhance information security. The participating firms were divided into three groups in terms of annual sales. Firms with sales less than 100 million were regarded as small firms, while organizations with sales exceeding 1 billion as large ones. Firms with annual sales in between were categorized as medium.

The extent of common method bias was assessed with three tests. First, a partial correlation method was used (Podsakoff et al. 2003). The highest factor from a principle component factor analysis was added into the structure model as another control factor on all dependent variables. This factor did not significantly increase the variance explained in any of the dependent variables, indicating no common method bias. Then we ran Lindell and Whitney's (2001) test that uses reporting level to CEO as a marker

Table 4 Convergent and discriminant validity

INCstruct	ICR	INR	EXR	INC	INI	INA
INIernal Relationships (INR)	0.93	**0.86**				
External Relationships(EXR)	0.91	0.67	**0.83**			
Information INCfidentiality (INC)	0.96	0.61	0.59	**0.89**		
Information INIegrity (INI)	0.98	0.61	0.58	0.74	**0.95**	
Information INAilability (INA)	0.97	0.50	0.46	0.38	0.40	**0.96**
INR02		0.86	0.55	0.53	0.52	0.46
INR03		0.91	0.59	0.60	0.50	0.44
INR04		0.80	0.50	0.39	0.44	0.36
INR05		0.87	0.56	0.48	0.56	0.43
INR06		0.87	0.59	0.55	0.57	0.49
EXR02		0.47	0.85	0.46	0.38	0.32
EXR03		0.48	0.84	0.49	0.37	0.25
EXR04		0.65	0.89	0.50	0.57	0.45
EXR05		0.63	0.87	0.56	0.63	0.45
INC01		0.50	0.52	0.86	0.73	0.34
INC02		0.50	0.48	0.87	0.68	0.27
INC03		0.58	0.63	0.89	0.70	0.30
INC04		0.54	0.53	0.91	0.65	0.39
INC05		0.51	0.51	0.91	0.64	0.39
INC06		0.49	0.42	0.86	0.57	0.27
INC07		0.57	0.53	0.92	0.63	0.39
INI01		0.60	0.54	0.70	0.98	0.41
INI02		0.60	0.56	0.72	0.97	0.37
INI03		0.56	0.52	0.71	0.96	0.40
INI04		0.53	0.52	0.65	0.93	0.32
INI05		0.57	0.58	0.75	0.94	0.42
INA01		0.48	0.43	0.36	0.39	0.97
INA02		0.48	0.42	0.34	0.41	0.94
INA03		0.48	0.38	0.37	0.36	0.96

variable to adjust the corrections among principal constructs. High correlations among any of the items of the study's principal constructs and the reporting level would indicate common method bias as reporting level is theoretically unrelated to the study's principal constructs. The result shows that the average correlation among them was r=0.034 (average p-value=0.42), indicating minimal evidence of common method bias. Finally, the correlation matrix (Table 5) does not indicate any highly correlated factors (highest correlation is r=.74), whereas evidence of common method bias should have resulted in extremely high correlations (r>.90). The results suggest that common method bias is not major concern in this study.

4.3 Results of the structural model

PLS Graph 3.0 was used to estimate the structural model. PLS is chosen as the analysis technique for this study because of the presence of formative latent variables in the model. A bootstrapping approach was used to generate 200 random samples of observations from the original data set to evaluate the significance of the path coefficients. Since

Table 5 Results of post hoc exploratory analysis

ISS component	IS resources component	Coefficient	*t*-value
INC	IBAC	0.2090	1.84*
	ITTC	0.0440	0.56
	INR	−0.1200	1.23
	EXR	0.1160	1.50
	ISMA	0.3590	3.46***
	ISTA	0.2880	2.69**
INI	IBAC	0.2730	1.94*
	ITTC	0.2620	2.93**
	INR	−0.1340	1.45
	EXR	0.1530	1.93*
	ISMA	0.1750	1.01
	ISTA	0.2080	1.60
INA	IBAC	−0.3160	1.56
	ITTC	0.2340	1.89*
	INR	0.2810	1.97*
	EXR	0.0740	0.59
	ISMA	0.3300	1.65*
	ISTA	0.0970	0.60

INC information confidentiality; *INI* information integrity; *INA* information availability; *ITTC* IT technical capability; *IBAC* IT-business alignment capabilities; *INR* internal relationships; *EXR* external relationships; *ISTA* information security technology architecture; *ISMA* information security management architecture

Significance Key:*<0.05;**<0.01;***<0.001

the research model comprises of higher order latent constructs and PLS Graph 3.0 cannot directly permit the representation of second-order latent constructs, the path model was evaluated using the computed first-order factor scores as indicators of the second-order constructs to estimate the path coefficients (Agarwal and Karahanna 2000; Yi and David 2003). The results of path coefficients for hypothesis testing are presented in Fig. 2.

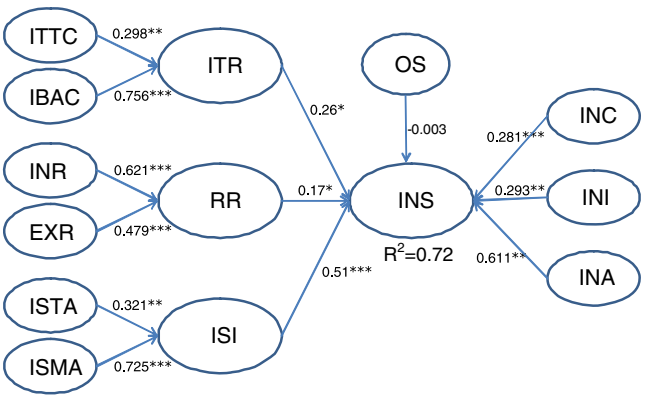

Fig. 2 PLS results of hypotheses tests

As hypothesized, support was found for all posited influence of IS resources on information security. Hypothesis 1 anticipates that the extent to which a firm's information technology resources (ITR) is positively associated with information security. Consistent with the hypothesis, the relationship between ITR and information security is positive and significant at 0.001 (path coefficient=0.36; *t* value=4.62). Hypothesis 2 postulates that the extent to which the relationship resources (RR) that an IT department holds with its customers (i.e. other departments and business partners) is positively associated with information security. The result reveals that the path coefficient (0.19) from RR to information security is positive and significant at the 0.01 level (*t* value=3.37). We found support for hypothesis 3, wherein we expected the extent of information security infrastructure (ISI) to positively affect information security at the significance level of 0.001 (path coefficient=0.41; *t* value=4.81). The results also show that approximate 72% of the variance in information security is accounted for by IS resources. Organization size had no significant impact on information confidentiality (path coefficient=−0.003; *t* value=0.057).

In order to provide a detailed understanding of how these resources have impact across different components of information security, a post hoc analysis was conducted in an attempt to make explicit the relationships between specific IS resources and information security dimensions that were covert. As shown in Table 5, IBAC, ISMA, and ISTA are significantly effective in strengthening information confidentiality. To enhance information integrity, IBAC, ITTC and EXR are important predictors. Finally, ITTC, INR, and ISMA are critical to information availability.

5 Discussions

5.1 Implications

This study has several academic implications. First, unlike the extant research that was largely anecdotal and a-theoretical, this study provides a parsimonious but cogent framework to examine the impact of IS resources on information security through the application of RBV as a theoretical lens. RBV facilitates the specification of IS resources that are relevant to the subject under question. The results of this study suggest that in order to effectively enhance information security, three distinct resources are critical: technological, relational, and information security-related infrastructure assets. Additionally, this study through an ad hoc analysis also identified varying relationship patterns between IS resources and each of the information security dimensions. The results of the ad-hoc analysis provide guidelines for organizations regarding how and where IS

resources should be deployed to generate superior information security.

Generally speaking, this study suggests that firms need to develop and accumulate their human, relational, and security-related infrastructure resources and direct such resources towards enhancing the level of information security. However, when closely examining the impact of IS resources on each of the individual information security dimension, the findings suggest that the impact of IS resources on information security is not monolithic but multiform. Specifically, to successfully enhance information confidentiality, IT personnel with high management knowledge (IBAC) and thorough information security architecture are critical. IBAC is critical to information confidentiality because not all information is of equal value, nor is it technically possible to protect all information assets from illegally accessed. IT workforce with high IBAC allows the firm to outline a clear asset classification scheme that provides guideline for determining what information assets must be protected and the degree of protection required for them. Building up an information security infrastructure is essential for superior information confidentiality. Technological aspect of the infrastructure entails the availability and deployment of a myriad of information security technologies and equipments that deter unauthorized users from accessing the systems and thus protected information from being compromising. Evidence also shows that a robust management architecture is also important for information confidentiality since the issue of employee compliance is a major concern even the technological architecture is in place. Proper management architecture ensures all information users act in alignment with organizational information assess regulations (Vermeulen and Von Solms 2002).

The results also provide indication that competent IT human resources (IBAC and ITTC) and good external relationship (EXR) are closely related to information integrity. Competent IT workforce allows a firm to outline clear asset scheme and then effectively plan, design, implement security-related technologies to prevent and detect events affecting data integrity. A resilient ISTA can provide secure computer networks and equipments (i.e. cytological tools and NAS Server/tape device) that protect data from modification or errors. EXR is essential for information integrity because data tranactions across organizations are subject to fabrication or counterfeit due to the lack of security mechnisms to ensure the data integrity as in organization. When data errors occur during data transmission, good external relationships with business partners enable the focal organization to quickly identify the cause of the problems and provide solutions, and thus enhance information integrity.

Lastly, this study finds that in the realm of information availability, competent technical capability (ITTC), good internal relationship (INR), and a robust IS management architecture (ISMA) are important. This is because information availability is closely associated with system reliability within the firm. The more reliable the systems are, the more readily available the information whenever it is needed. Technically proficient IT workforce can effectively develop reliable information systems, detect potential system glitches, and restore failed systems, resulting in information availability improvement. IS-business reciprocal relationships create a sense of partnership that strengthens business partners' willingness to report system problems so that IT department can tackle them more readily if they do occur. This result signals that the task to enhance information availability cannot be viewed as merely an IT project but an organizational initiative that requires the coordination of other departments in the firm in information exchange and swift reaction to system-compromising incidents.

Moreover, the findings of this study provide guidelines for organization to effectively enhance information security. Firms need to reconceptualize the nature of information security. It should not be viewed merely as a technical project directed by the IT department alone but an enterprise mission requiring concerted endeavors from the organization as a whole. Secondly, overall information security effectiveness calls for a careful analysis of the current situation of each of the component of information security. Organizational goals for information security thus can be mapped and specific IS resource be developed and allocated to fit security objectives. For example, firms that intend improve information confidentiality should focus managerially competent IT personnel and information security architecture. High investment on developing relationship resources may be less effective. Similarly, firms endeavoring to enhance information integrity need to level their efforts in developing technically and managerially competent IT workforce, installing necessary technical equipments that protect data from being compromised, and developing good relationships with business partners. Lastly, if firms aim to ensure that information can be assessed whenever and wherever is needed, substantial attention should be paid to recruiting and/or cultivating technically competent IT workforce, putting management measures in place that harness employee behaviors, and a close coordination between IT department and external business partners. Internal relationships and management architecture are less effective for information availability effectiveness.

5.2 Limitations and future research directions

Several limitations of this study should be noted when interpreting the findings. First, the relative small sample size was a limitation. Given that we succeeded in obtaining complete data from only 126 firms, the number of observations was not large enough to make broad generalizations. Second, the cross-sectional nature of the data

limited our ability to imply causality. Cautions must be exercised when interpreting the findings. Third, use of a single informant from each firm was also a limitation: possible over-reporting or underreporting of certain phenomenon may have occurred as a result of the top executive's personal and role characteristics.

The theory adopted in this study is heavily driven by the resource-based view and results of the study ratify that IS human, relationships and infrastructure resources have profound effects on a firm's information security. However, little is known about the implementation process and critical factors that affect the effectiveness of these resources at organizations. Different theoretical views can be taken (i.e. institutional or power theories) to examine this issue. Specifically, it would be interesting to scrutinize how organizations develop human resources that are both technically and managerially competent in enhancing information security. Moreover, future studies could explore effective methods for the development of good information security infrastructure that fits the unique organizational security features and business needs. Specifically, issues such as the adoption, use, and continuance of information security architectures could be investigated. Research can also be conducted to examine the relevancy and applicability of the components of the architectures to different organizational environments. Additionally, the issue of employee compliance is still a major concern even the security resources are in place. Studies looking into the managerial mechanisms that encourage compliance may offer valuable insights on employee compliance with requirements and practices of information security management architectures.

6 Conclusions

Drawing on the resource-based view, this study developed and empirically tested the impacts of IS resources on a firm's information security. Analyses based on 126 firms support the hypothesized relationships in the model. The comprehensive resource-based scheme used in the study extends and enriches the extant information security research that is largely anecdotal. This study highlights the importance of the human resources, relationship, and infrastructure assets that a firm possesses in enhancing its information security. In general, this study shows that a firm's human, relationships, and security infrastructure influence the level of information security of a firm. But when closely examining the impact of IS resources on each information security component, the findings suggest that the effects of IS resources on information security is not monolithic but multiform. Based on the results, guidelines are suggested for organizations to effectively allocate limited organizational resources to advance level of information security.

Appendix

Information Technology Technical Skills

Our IT department is skilled in

1. multiple programming languages.
2. system analysis and design.
3. operating information systems.
4. maintaining information systems.
5. diagnosing information systems problems.

IT Technology Management Skills

Our IT department is able to

1. align IT investments with long-term business needs.
2. develop technical solutions to solve business problems.
3. align IT strategies with our organization's business strategies.
4. understands the business environment where our organization is situated.
5. understands our organization's business plans.
6. understands the business goals of our organization.

Internal Relationship

Our IT department and other business units (i.e. finance, production, marketing)

1. share intelligence related to information security. *
2. understand each other's working environments.
3. trust each other.
4. rarely have conflicts.
5. resolve conflicts through communications and mutual adjustment.
6. work closely with each other.

External Relationship

Our IT department and business partners (i.e. customers and suppliers)

1. rarely have conflicts.*
2. share intelligence related to information security.
3. respond our information security needs in a timely manner.
4. trust each other.
5. have good relationships.

Information Security Technology Architecture

The software and hardware equipments in our company can effectively

1. control network security.
2. control user access rights.
3. control data access.
4. encrypt or decrypt data.
5. store data.
6. prevent malicious intrusion.
7. generate log analysis reports.

Information Security Management Architecture
In our company,

1. the information security objectives are well defined.
2. the responsibility for information user is well defined.
3. the information properties are well classified.
4. security training is well planned.
5. the use of information property is well regulated.
6. the procedure of data process is well regulated.
7. the process of data access is well defined.
8. the process of managing security events is well defined.
9. the process of information systems development is well defined.
10. the process of information systems maintenance is well defined.
11. the continuity of systems operation is well managed.

Information Confidentiality
Data in our company

1. can only be accessed by authorized personnel.
2. is protected from disclosure.
3. is protected from break-in.
4. is protected from unauthorized access.
5. is protected from compromising.
6. is protected from making public.
7. is protected from exposure.

Information Integrity
After being stored or transmitted, the content of the information is

1. correct.
2. accurate.
3. reliable.
4. consistent compared to the original data.
5. consistent in format compared to the original data.

Information Availability
Data in our company is readily

1. retrieved.
2. accessed.
3. obtained.
4. accessed when needed.*

Note:* Item dropped

References

Agarwal, R., & Karahann, E. (2000). Time flies when you're having fun: cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665–694.

Anderson, J. M. (2003) Why we need a new definition of information security. *Computers & Security, 22*(4), 308–313.

Armstrong, J. S., & Overto, T. S. (1977). Estimating non-response bias in mail surveys. *Journal of Marketing Research, 14*(3), 396–402.

Armstrong, C. P., & Sambamurthy, V. (1999). Information technology assimilation in firms: the influence of senior leadership and IT infrastructures. *Information Systems Research, 10*(4), 304–327.

Bagchi, K., & Udo, G. (2003) An analysis of the growth of computer and internet security breaches. *Communications of AIS, 12*(46), 684–700.

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares approach to causal modeling: personal computer adoption and use as an illustration. *Technology Study, 2*(2), 285–324.

Benantar, M., & Guski, R. (1996). Access control systems: from host-centric to network-centric computing. *IBM Systems Journal, 35* (1), 94–113.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly, 24*(1), 169–196.

Bovee, M. W., Srivastava, R. P., & Mak, B. (2001). A conceptual framework and belief function approach to assessing overall information quality. *Proceedings of the 6th International Conference on Information Quality*, *18*(1), 51–74, Cambridge, MA.

Broadbent, M., & Weill, P. (1997). Management by maxim: how business and IT managers can create IT infrastructures. *MIT Sloan Management Review, 38*(3), 77-92.

Budiarto, Shojiro, N., & Masahiko, T. (2002). Data management issues in mobile and peer-to-peer environments. *Data & Knowledge Engineering, 41*(2/3), 183-204

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.

Byrd, T. A., Lewis, B. R., & Turner, D. E. (2004) The impact of IT personnel skills on IS infrastructure and competitive IS. *Information Resources Management Journal, 17*(2), 38-62.

Campbell, K., et al. (2004). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Cash, J. I., & Konsynski, B. R. (1985). IS redraws competitive boundaries. *Harvard Business Review, 63*(2), 134–142.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28–46.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345–361.

Cheng, E. C. (1999). An object-oriented organizational model to support dynamic role-based access control in electronic commerce applications. *Proceedings of the 32nd Hawaii International Conference on System Sciences*, 1–9.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), 7–16.

Chin, W. W., & Gopal, A. (1995). Adoption intention in GSS: relative importance of beliefs. *Data Base Advances, 26*(2/3), 42–63.

Cohen, P., Cohen, J., Teresi, J., Marchi, M., & Velez, C. N. (1990). Problems in the measurement of latent variables in structural equations causal models. *Applied Psychological Measurement, 14*(2), 183–196.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communication of the ACM, 43*(7), 125–128.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communication of the ACM, 43*(7), 125–128.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: an alternative to scale development. *Journal of Marketing Research, 38*(2), 269–277.

Dutta, A., & Mccrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45* (1), 67–87.

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling.* Akron: The University of Akron.

Feeny, D. F., & Willcocks, L. P. (1998). Core IS capabilities for exploiting information technology. *MIT Sloan Management Review, 39*(3), 9–21.

Ferraiolo, D. F., Sandhu R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and Systems Security, 4*(3), 1–51.

Finne, T. (2000). Information systems risk management: key concepts and business processes. *Computers & Security, 19*(3), 234–242.

Flowerday, S., & Von, S. R. (2005). Real-time information integrity= system integrity+ data integrity+ continuous assurance. *Computers & Security, 24*(8), 604–613.

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

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.

Gunter, K (2000). Authorization in COBRA security. *Journal of Computer Security 8*(2&3), 89–108

Hair, J. A., et al. (1992). Fawn hematology and survival following tick infestation and theileriasis. *Journal of Agricultural Entomology, 9*(4), 301–319.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Grablowwsky, B. J. (1998). *Multivariate data analysis*, 5th edn. New York: Macmillan.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal, 38*(2), 472–484.

Hinde, S. (2002). Security surveys spring crop. *Computers & Security, 21*(4), 310–321.

Hong, K. S., et al. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243–248.

Hulme, H. (2002). Businesses keep spending on security. *Information Week* (January 28).

Jarvenpaa, S. L., & Leidner, D. E. (1998). An information company in Mexico: extending the resource-based view of the firm to a developing country context information. *Systems Research, 9*(4), 342–361.

Joshi, J. B. D., et al. (2001). Security models for Web-based applications. *Communications of the ACM, 44*(2), 38–44.

Kankanhalli, A., et al. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154.

Keil, M., Mann, J., & Rai, A. (2000). Why software projects escalate: an empirical analysis and test of four theoretical models. *MIS Quarterly, 24*(4), 631–664.

Kleinbaum, D. G., Kupper, L., & Muller, K. E. (1988). *Applied Regression Analysis and other multivariable methods*, 2nd edn. Boston: PWS-Kent.

Laudon, K. C., & Laudon, J. P. (2000). *Management information systems*, 6th edn. New Jersey: Prentice Hall.

Law, K., & Wong, C. S. (1999). Multidimensional constructs in structural equation analysis: an illustration using the job perception and job satisfaction constructs. *Journal of Management, 25*(2), 143–160.

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.

Lee, Y. W., et al. (2004). Process-embedded data integrity. *Journal of Database Management, 15*(1), 87–103.

Lindell, M. K., &Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114–121.

Maccallum, R. C., & Browne, M. W. (1993). The use of causal indicators in covariance structure models: some practical issues. *Psychological Bulletin, 114*(3), 533–541.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: a resource-based analysis. *MIS Quarterly, 19*(4), 487–505.

Mckenney, J. L. (1995). *Waves of change: business evolution through information technology.* Cambridge: Harvard Business School Press.

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*, 283–294, Minneapolis, MN.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623–656

Piccoli, G., & Ives, B. (2005) Review: IT-dependent strategic initiatives and sustained competitive advantage: a review and synthesis of the literature. *MIS Quarterly, 29*(4), 747–776.

Podsakoff, P. M., MacKenzie, S. B, Lee, J.-Y., & Podsakoff, N. P. (2003). Common method bias in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.

Power, R. (2002). Computer crime and security survey. *Computer Security Issues and Trends, 8*(1), 1-28.

Priem, R. L., & Butler, J. (2001). Is the resource-based "view" a useful perspective for strategic management research? *Academy of Management Review, 26*(1), 22–40.

Ravichandran, T., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: a resource-based perspective. *Journal of Management Information Systems, 21*(4), 237–276.

Ray, G., Muhanna, W., & Barney, J. (2005). Information technology and the performance of the customer service process: a resource-based analysis. *MIS Quarterly, 29*(4), 625–651.

Ross, J. W., Beath, C. M., & Goodhue, D. L. (1996). Develop long-term competitiveness through IT assets. *MIT Sloan Management Review, 26*(2), 31–42.

Schultz, E. E., et al. (2001). Usability and security an appraisal of usability issues in information security methods. *Computer & Security, 20*(7), 620–634.

Shih, S. C., & Wen, H. J. (2003). Building e-enterprise security: a business view. *Information System Security, 12*(4), 41–49.

Straub, D. W. (1990). Effective IS security: an empirical study. *Information Systems Research, 1*(3), 255–276.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly, 14* (1), 45–60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

Swanson, E. B. (1994). Information systems innovation among organizations. *Management Science, 40*(9), 1069–1092.

Tickle, I. (2002) Data integrity assurance in a layered security strategy. *Computer Fraud & Security, 2002*(10), 9–13.

Twitchell, G. D. (2004). Infrastructure of electronic information management. *Information Services and Use*, *24*(4), 195–208.

Velissarios, J., & Santarossa, R. (1999). Practical security issues with high-speed networks. *Journal of High Speed Networks, 8*(4), 311–325.

Vermeulen, C., & Von Solm, R. (2002). The information security management toolbox—taking the pain out of security management. *Information Management & Computer Security, 10*(2/3), 119–125.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*, 371–376.

Wang, R. Y., Reddy, M. P., & Kon, H. B. (1995). Toward quality data: an attribute-based approach. *Decision support system, 13*(3/4), 349–372.

Wang, R. Y., Strong, D. M., & Beyond, A. (1996). What data quality means to data consumers. *Journal of Management Information Systems, 12*(4), 5–34.

Weill, P., Subramani, M., & Broadbent, M. (2002). Building IT infrastructure for strategic agility. *Sloan Management Review, 44* (1), 57–65.

Yi, M. Y., & David, F. D. (2003). Developing and validating an observational learning model of computer software training and skill acquisition. *Information Systems Research, 14*(2), 146–169.

Zhang, C. N., & Yang, C. (2003). Integration object oriented role-based access control model with mandatory access control principles. *Journal of Computer Information Systems, 43*(3), 40–50.

Kuo-chung Chang is an assistant professor of the Department of Information Management at Yuan Ze University, Taiwan, R.O.C. He received his Ph.D. from the University of South Carolina, U.S.A. His current research focuses on IS project management, information systems outsourcing, and knowledge management. His work has been published in journals such as Information and Management, Information and Software Technology, and Industrial Management and Data Systems.

Chih-ping Wang currently is a division manager in Everenergy Corporation, a leading solar cell manufacturer in Taiwan. Mr. Wang holds an M.B.A. in Information Management from Yuan Ze University, Taiwan, R.O.C. He is experienced in system programming and management. His research focuses on the information security. He can be reached at wang.cp@gmail.com