The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0263-5577.htm

Exploring organizational culture for information security management

Shuchih Ernest Chang
Institute of Electronic Commerce, National Chung Hsing University, Taichung, Taiwan, Republic of China, and
Chin-Shien Lin
Department of Business Administration, National Chung Hsing University, Taichung, Taiwan, Republic of China

Abstract

Purpose – This paper aims to examine the influence of organization culture on the effectiveness of implementing information security management (ISM).

Design/methodology/approach – Based on a literature review, a model of the relationship between organizational culture and ISM was formulated, and both organizational culture characteristics and ISM effectiveness were measured empirically to investigate how various organizational culture traits influenced ISM principles, by administrating questionnaires to respondents in organizations with significant use of information systems.

Findings – Four regression models were derived to quantify the impacts of organizational culture traits on the effectiveness of implementing ISM. Whilst the control-oriented organizational culture traits, effectiveness and consistency, have strong effect on the ISM principles of confidentiality, integrity, availability and accountability, the flexibility-oriented organizational culture traits, cooperativeness and innovativeness, are not significantly associated with the ISM principles with one exception that cooperativeness is negatively related to confidentiality.

Research limitations/implications – The sample is limited to the organizational factors in Taiwan. It is suggested to replicate this study in other countries to reconfirm the result before adopting its general implications. Owing to the highly intrusive nature of ISM surveys, a cautious approach with rapport and trust is a key success factor in conducting empirical studies on ISM.

Practical implications – A culture conducive to information security practice is extremely important for organizations since the human dimension of information security cannot totally be solved by technical and management measures. For understanding and improving the organization behavior with regard to information security, enterprises may look into organizational culture and examine how it affects the effectiveness of implementing ISM.

Originality/value – A research model was proposed to study the impacts of organizational factors on ISM, after a broad survey on related researches. The validated model and its corresponding study results can be referenced by enterprise managers and decision makers to make favorable tactics for achieving their goals of ISM – mitigating information security risks.

Keywords Data security, Information systems, Organizational culture

Paper type Research paper

Industrial Management & Data Systems
Vol. 107 No. 3, 2007
pp. 438-458

0263-5577
DOI 10.1108/02635570710734316

1. Introduction

While information systems pervasively underpin the enterprises which have the growing dependence on smooth and sound operations of their information systems, the issues of information security become more and more important, especially

for businesses in electronic commerce environment (Kankanhalli *et al.*, 2003; Galanxhi-Janaqi and Nah, 2004; Kim and Leem, 2005; Shih *et al.*, 2005; Kefallinos, *et al.*, 2006). As a matter of fact, information security management (ISM) has evolved into a popular area of interest for practitioners and academics (Eloff and von Solms, 2000; Hong *et al.*, 2003; Foltz *et al.*, 2005; Huang *et al.*, 2006). When large amounts of data are stored and processed in electronic form, the misgiving of information security has also raised due to the inherent vulnerability of information technology (Chiu and Chen, 2005). According to the 2004 CSI/FBI Computer Crime and Security Survey (CSI/FBI, 2004), while the attacks of computer systems or misuse of these systems had been slowly and steadily decreasing over years, both the average reported annual loss per firm and the average reported loss per incidence were not decreasing. This trend might result from the fact that organizations have focused their computer security practice largely on technical issues like encryption/decryption, access controls, and intrusion detection system in recent years. Nevertheless, the report suggests that economic, financial and risk management aspects of computer security have become more and more important concerns to today's organizations, and such concerns are complements to, rather than substitute for, the technical aspects of computer security. As organizations increasingly invest, construct and implement information security systems, the issue of assuring employees' commitment and understanding of the objectives of information security has become increasingly important.

Deal and Kennedy (1982) indicated that the culture was the single most important factor accounting for success or failure of an organization. Organization culture is the media between management and organizational behavior, and different companies usually have different organizational cultures. Since, the organizational culture would certainly influence the operation activities of an enterprise and the effectiveness of an enterprise's information security practice, the managers should regard organizational culture as an important factor for supporting and guiding ISM practice. While information security is a major concern facing every organization, engaging security practices in the organizational culture proactively and spontaneously for day-to-day operations could positively affect the success of the organization (Vroom and von Solms, 2004). Although the staff may be just one of several factors in achieving the goals of information security practice, human behavior is relatively difficult to control. This research is targeted to study the influence of organizational culture on ISM, by conducting research on various organizational culture traits (including cooperativeness, innovativeness, consistency, and effectiveness) and their relationships with ISM principles (including confidentiality, integrity, availability (CIA), and accountability). The objective of this study is to find out how organizational culture influences ISM effectiveness, to discuss the relationships between organizational culture traits and ISM principles, and to identify what kind of culture is conducive to ISM implementation. The research result can be used not only to identify key organizational culture traits related to ISM implementation, but to derive guidelines and best practices for enterprise managers and decision makers to make the correct tactics for achieving their goals of ISM practice – mitigating information security risks.

2. Literature review

2.1 Information security management

Given the integral role of information technology in today's enterprises, information security has to be a key component in modern enterprise planning and management. This entrenchment of security was also driven by the increasing growth of electronic transactions, and fueled partly by the internet as electronic commerce proliferated with the growth of networks. The goal of information security is to ensure the CIA of information as well as information processing resources (Ryan and Bordoloi, 1997; Chou *et al.*, 1999; Chang and Ho, 2006). Bishop (2003) also stated that computer security rested on CIA. In general, information security concluded from broad surveys deals with CIA. ISM is used to protect all valuable information assets and mitigate various risks to information coming from all aspects of the organization's environment by applying the security technology and management process.

According to a broad survey conducted by *Information Security Magazine* (2002), the most pressing problems on information security, based on data collected from 2,196 information security practitioners, are malicious code (31 percent), securing authorized users (23 percent), IT and telecomm (15 percent), unauthenticated users (11 percent), and organizational management (9 percent). The survey result also shows that most information security problems are caused by the negligence of people, rather by attack events. Therefore, it is important to train and manage the problem-prone people. An acceptable level of information security can only be introduced and maintained if the correct set of security controls is identified, implemented and maintained. Identifying a reasonably effective set of security controls can be a very complicated and resource-intensive process, which requires special resources and expertise most companies do not possess. Therefore, there exists an urgent demand for ISM standards, which offer guidelines to organizations by identifying and introducing a set of controls conducive to an acceptable level of information resource protection. BS 7799, a UK standard on ISM published in February 1998, is a comprehensive set of controls comprising best practices in information security (BS 7799-1, 1999). Part 1 of BS 7799 was adopted as the international standard ISO17799/IEC17799 in December 2000. ISO 17799 reinforces the three traditional principles of information security – CIA – as an effective information security program (Kenning, 2001). Complying with this internationally recognized standard is growing in importance. Although BS 7799 does not mean absolute security, it provides a common basis for companies to develop, implement, and measure security management practice and helps to reduce the predictable risk. Such ISM standards serving as the common basis can provide companies with confidence for inter-company trading, collaborations, subcontracting, and procurement of IT services or products.

Information security related research should not merely attempt to go into technical details of security systems or technologies, because they will change with time (Sanderson and Forcht, 1996). It is fair to say that information security is a social and organizational problem since technical systems have to be operated and used by people. A solid security product alone cannot protect an organization without a good management policy and implementation. It is affirmed that information security is not primarily a technical problem but a business or management problem (Dutta and McCrohan, 2002; Kankanhalli *et al.*, 2003; von Solms and von Solms, 2004; Chang and Ho, 2006).

2.2 Organizational culture

The concept of organizational culture was adapted from anthropology for organization management research. Almost every scholar has his/her special attitude of mind for culture, and different scholars have different definitions of organization culture (Bali *et al.*, 1999). Douglas (1985) pointed out that organization culture was the emergent result of the continuing negotiations about values, meanings and proprieties between the members of that organization. Based on two basic categorizing dimensions including the internal/external orientation and the flexibility/control orientation, Quinn and Spreitzer (1991) developed a typology for identifying and classifying organizational culture into four types: group culture, developmental culture, hierarchical culture, and rational culture. They also stated an important fact that normally organizations are likely to have attributes and values reflecting all four types of organizational culture. Based on Quinn and Spreitzer's competing values framework of organizational culture, Boggs (2004) categorized organizational culture into four types (clan culture, hierarchy culture, ad hocracy culture, and market culture), for examining the implementation of total quality management. Denison *et al.* (2004) also classified organizational culture into four types according to four cultural traits (mission, consistency, adaptability and involvement) derived from effective organizations. It is noted that these four different cultural traits are related to different criteria of effectiveness. In this research, we adopted an approach of using various culture traits to examine the influence of organizational culture upon the effectiveness of implementing ISM.

2.3 Organizational culture and information security management

Culture is a critical factor for firms to continue living, since it drives the organization and its actions. Many corporate security articles point out that security is primarily a management issue, instead of a technology one, because technology is one part of security, but without a deep change in organization security culture which directly affects security practices, buying security product will brings little safety (von Solms and von Solms, 2004). Guiding how employees think, act, and feel, culture is somewhat like "the operating system" of the organization (Hagberg and Heifetz, 1997). It is concluded that the culture paradigm is inextricably linked to existing practices and roles in an organization (Allen and Fifield, 1999). Initiatives in adopting new information technology, conducting business process re-engineering, and implementing organizational or management changes frequently run into trouble, because people do not want to change what they have got used to, and lack of motivations to change their habits (Cooper, 1994; Allen and Fifield, 1999; Cooper, 2000; Melton, *et al.*, 2006). Since, new security policies often conflict with the way employees have done their jobs for years, implementing policy-based security plan will be extremely challenging. Consequently, exploring various traits of organizational culture for facilitating businesses in carrying out ISM, and building shared values, beliefs and norms for ISM based on the concept of organizational culture are critically important and highly interesting for both researchers and practitioners. Since, there is litter research working on the relationship between organization culture and ISM, our study tried to fill in the gap to find out such relationship by investigating how various types of organization culture influence the effectiveness of implementation ISM practice.

3. Research methodology

3.1 Research framework

Our model for evaluating ISM is based on various characteristics of organizational culture. Attributes for describing the organizational culture include cooperativeness, innovativeness, consistency and effectiveness. These attributes were used to create hypotheses for evaluating the CIA principles of ISM. Other than CIA, accountability was identified by previous researches as another important principle of ISM. The accountability for information security must be spelled out clearly and shared by all employees (von Solms and von Solms, 2004). Without a framework of accountability for information security, it will be difficult for organizations to progress further for an effective implementation of information security policies (Gaunt, 2000). Corporate accountability for materials sent and downloaded by employees on their own initiatives is also an important issue (Higgins, 1999). In an organization, accountability is necessary to be able to find a person or persons accountable for their actions (Borglund, 2005). Therefore, accountability is incorporated into our research framework as yet another ISM principle. The proposed research framework shown in Figure 1 shows the relationships between organizational culture and ISM.

3.2 The variables

Based on prior studies about organizational culture (Cameron, 1991; Quinn and Spreitzer, 1991; Denison *et al.*, 2004; Boggs, 2004), our study used the two categorizing dimensions, including the internal/external orientation and the flexibility/control orientation shown in Figure 2, to categorize the characteristics of organizational culture into four constructs: cooperativeness, innovativeness, consistency and effectiveness. Descriptions of these constructs are as follows:

(1) The first culture trait falls into the upper left corner of the two-dimensional model of organizational culture, and it is named cooperativeness in our study. This trait emphasizes the internal and flexibility orientations, and focuses primarily on cooperation, information sharing, trust, empowerment, and team work. The organization emphasizing cooperativeness is typically a friendly

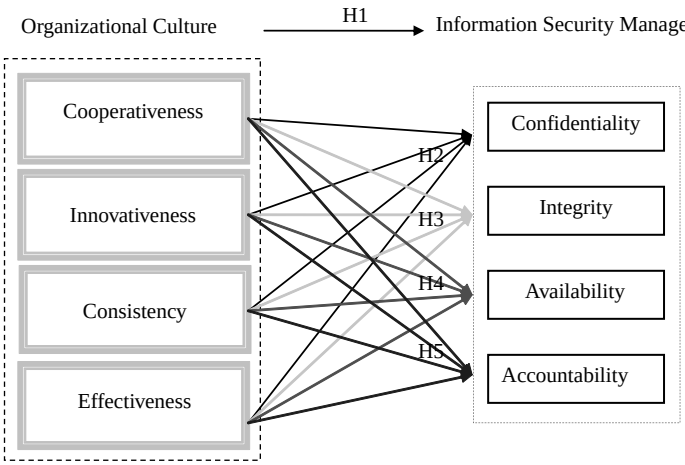


Figure 1.
The conceptual framework

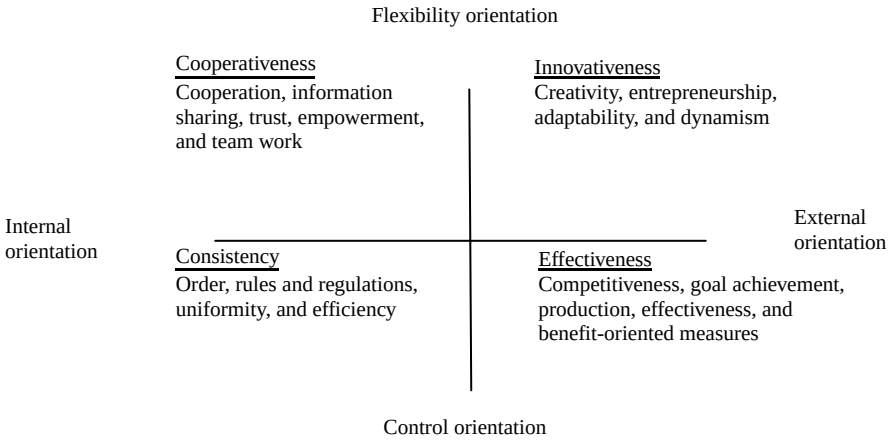


Figure 2.
The model of organizational culture traits

place where its members share information and trust one another just like an extended family.

(2) The second culture trait, which falls into the upper right corner of the two-dimensional model of organizational culture, is named innovativeness in our study. Innovativeness can be characterized by the external and flexibility orientations in the model of organization culture traits, with a focus on creativity, entrepreneurship, adaptability, and dynamism. The company emphasizing innovativeness supports a fully creative and dynamic environment.

(3) The third culture trait, consistency, occupies the lower left part of the model shown in Figure 2, and emphasizes the internal and control orientations. It focuses on order, rules and regulations, uniformity, and efficiency. The company emphasizing consistency is typically a formalized and regular organization.

(4) The last culture trait representing the lower right part in our two-dimensional culture model is named as effectiveness in our study. This trait emphasizes external and control orientations, with a focus on competitiveness, goal achievement, production, effectiveness, and benefit-oriented measures. The company emphasizing effectiveness is primarily a result-oriented and benefit-oriented organization.

The four constructs of organization culture were operationalized using 26 items, adapted from several instruments (Cameron, 1991; Quinn and Spreitzer, 1991; Denison *et al.*, 2004; Boggs, 2004), for measuring the culture of a company by the organization characteristics, character of leader, organizational clime, and management style. As a matter of fact, these 26 questionnaire items include eight items for cooperative trait, six items for innovative trait, six items for hierarchical trait, and six items for effective trait.

This study divided the ISM construct into four components including CIA and accountability (Figure 1), as suggested by various prior studies (Chou *et al.*, 1999; Dhillon and Backhouse, 2000; Bishop, 2003; von Solms and von Solms, 2004). The four variables used in this study as indicators to ISM principles are described below:

(1) Confidentiality for restricting data access to those who are authorized.

(2) Integrity for maintaining the values of the data stored and manipulated, such as maintaining the correct signs and symbols.

(3) Availability for the systems, used by an organization, remaining available when they are needed.

(4) Accountability for holding employees fully accountable for their conduct related to information security. Organizations can enforce accountability by educating employees about their information security policies, and establishing disciplinary practice and procedures.

The four ISM variables were operationalized using 19 questionnaire items, where five items were for confidentiality, five items for integrity, three items for availability, and six items for accountability. All these questionnaire items were adapted from security control measures contained in BS 7799 Part 1, and every questionnaire item was formulated to assess the effectiveness of ISM practice on a specific ISM principle (CIA, or accountability).

3.3 The hypotheses

Organization culture can be regarded as a pattern of beliefs and expectations shared by organization members, and these beliefs and expectations produce norms that powerfully shape the behavior of individuals, groups, or organizations (Schwartz, 1981). Organizational culture may also include the ideas shared by the people of the organization and communicated between each other (Szilagyi and Wallace, 1987). Generally speaking, organization culture not only is a critical factor for an organization to continue living but drives the organization and its actions including particularly the practice of protecting information resources. It is stated that the way information is managed and used is very much a product of the culture and management style of an organization (Owens *et al.*, 1995). Winn Schwartau, the founder of Interpact Inc. (which is a security awareness firm in Seminole, Florida), stated that the challenge for many awareness programs was the corporate culture, and William Malik, a Vice President and Research Area Director for information security at Gartner, also pointed out that a business would have good security if its corporate culture was correct. The culture of an organization may have huge impact on the security of information, and this could be negative or positive. It is imperative that the culture of an organization reflects a positive attitude to information security throughout the whole organization (Vroom and von Solms, 2004). Based on the above mentioned prior researches and expert opinions, the following hypotheses are posited:

H1. There are significant relationships between organizational culture and ISM.

H2. There are significant relationships between organizational culture and confidentiality.

H3. There are significant relationships between organizational culture and integrity.

H4. There are significant relationships between organizational culture and availability.

H5. There are significant relationships between organizational culture and accountability.

3.4 Sample and procedure

Empirical data was collected through a survey of using questionnaire. The survey subjects were targeted on companies in various industries including financial services, computer and peripherals, consumer electronics, logistics and services, healthcare, food industry, and others. The key informants were senior managers or equivalent (such as senior staffs, strategists and technologists with management experience), and they were supposed to have experience and/or knowledge in information technology. The questionnaire was developed from an integrated process referencing the results from literature review and the research framework. In addition to the questionnaire items for collecting demographic information, the questionnaire contained two parts: one for the evaluation of organizational culture and the other for the evaluation of ISM practice. The demographic statistics-related questionnaire items cover gender, education, the age of the company, seniority of service, number of employees in company, department, job level and industry.

Every questionnaire item was measured on a seven-point Likert scale, ranging from "strongly disagree" (extremely unimportant) to "strongly agree" (extremely important). To ensure that the question items could be understood and measured validly, a pretest was conducted in a small group. The pretest adopted the exploratory factor analysis to analyze the collected data and to make sure all items were appropriately grouped into expected common (latent) factors. Based on the comments received from the pretest, modifications were made to the questionnaire items for improving its readability before it was used in the formal survey. In addition, to ensure that the instrument possessed acceptable reliability and validity, five questionnaire items (two items for the evaluation of organizational culture and three items for the evaluation of ISM effectiveness) were deleted from the original questionnaire. Finally, the formal questionnaire (Appendix) was used by confirmatory factor analysis to analyze collected data. Survey data were evaluated for their adequacy and construct validity, and the hypotheses were tested using correlation and regression analyses.

With the lesson learned from their failure in conducting empirical study related to ISM, Kotulic and Clark (2004) suggested a slow and cautious approach with research effort focusing on a few selected firms with whom the researcher had developed an excellent rapport and trust, especially for studies that were either under-researched or of a sensitive nature. Based on their suggestions, our survey was designed and conducted with caution in order to achieve an acceptable response rate and collect enough data for statistical significance. First, to improve the willingness of targeted respondents in cooperation with the survey, a social networking approach was adopted to go through various sources of personal and professional relationships. For example, we were able to get quite a few responses through the assistance from EMBA students of our university. Secondly, about three days before our questionnaire was sent to the targeted respondents in 196 companies, an e-mail message and/or a courtesy telephone call was made to clearly and briefly inform every targeted respondent that the nature of our survey was exclusively for academic research. Third, every targeted respondent was notified in advance that the questionnaire was designed and tested to make sure it could be completed in about 10-15 minutes. Finally, about three days after the questionnaire was sent, follow-up telephone calls were made to improve the response rate.

4. Empirical findings

After a total of 108 respondents were gathered, invalid and incomplete survey results were identified and discarded. Overall, 87 usable copies of questionnaire were collected and used for analysis. Among 87 usable respondents, 57.5 percent were male, and 42.5 percent were female. In terms of education level, 18.4 percent owned master degree or above, 55.2 percent were college graduates, and 26.4 percent did not have bachelor degree. About 40.2 percent usable questionnaires were from senior managers and 59.8 percent from senior staff with information technology experience and/or knowledge. About 54 percent of usable respondents worked for companies with 400 or fewer employees, and the remaining 46 percent were with more than 400 employees. Of those respondents, 33.3 percent worked for companies in financial industry, 20.6 in electronic/electrical or computer industry, 20.7 percent in service sectors, and 25.5 percent in other areas such as manufacturing, healthcare, food industry, etc.

The descriptive statistics including the mean value and standard deviation (SD) for the collected valid survey results are listed in Tables I and II, where Table I covers the items for the evaluation of organizational culture and Table II covers the items for the measurement of ISM practice.

Factor analysis was applied in data analysis to measure construct validity and to find out the sets of correlated variables. There are some rules to measure whether the data in

Factor	Questionnaire item	Mean	SD	*N*
Cooperativeness	Cooperativeness_1*	4.4713	1.7107	87
	Cooperativeness_2*	4.2184	1.6595	87
	Cooperativeness_3*	4.6897	1.3751	87
	Cooperativeness_4*	4.2644	1.3932	87
	Cooperativeness_5*	4.5402	1.4612	87
	Cooperativeness_6*	3.9540	1.3802	87
	Cooperativeness_7*	4.7586	1.5992	87
	Cooperativeness_8*	4.5402	1.5686	87
Innovativeness	Innovativeness_1*	4.4138	1.7689	87
	Innovativeness_2*	4.4023	1.4743	87
	Innovativeness_3*	4.5977	1.4584	87
	Innovativeness_4*	4.7816	1.4095	87
	Innovativeness_5*	4.3218	1.5439	87
	Innovativeness_6*	4.1494	1.5366	87
Consistency	Consistency_1*	4.6092	1.4970	87
	Consistency_2*	4.5057	1.5912	87
	Consistency_3*	4.7701	1.4603	87
	Consistency_4*	5.0920	1.2260	87
	Consistency_5*	4.4713	1.5390	87
	Consistency_6*	4.6782	1.5514	87
Effectiveness	Effectiveness_1*	4.7126	1.5545	87
	Effectiveness_2*	4.7586	1.4704	87
	Effectiveness_3*	4.3563	1.5248	87
	Effectiveness_4*	4.3908	1.5579	87
	Effectiveness_5*	5.0000	1.1813	87
	Effectiveness_6*	4.8276	1.3742	87

Note: *Refer to Appendix for the descriptions of questionnaire items

Table I.
The descriptive statistics for the measurement of organization culture

Factor	Questionnaire item	Mean	SD	*N*
Confidentiality	Confidentiality_1*	5.1954	1.6554	87
	Confidentiality_2*	5.5747	1.2997	87
	Confidentiality_3*	5.4368	1.3092	87
	Confidentiality_4*	5.4598	1.2276	87
	Confidentiality_5*	5.3333	1.4994	87
Integrity	Integrity_1*	5.1839	1.5442	87
	Integrity_2*	4.9885	1.6030	87
	Integrity_3*	4.5747	1.5894	87
	Integrity_4*	5.2414	1.3722	87
	Integrity_5*	4.8046	1.5465	87
Availability	Availability_1*	5.0345	1.4179	87
	Availability_2*	5.4713	1.0548	87
	Availability_3*	5.1609	1.3966	87
Accountability	Accountability_1*	5.1034	1.4145	87
	Accountability_2*	5.0230	1.2387	87
	Accountability_3*	4.4828	1.5542	87
	Accountability_4*	4.8506	1.4429	87
	Accountability_5*	4.9195	1.4485	87
	Accountability_6*	5.1494	1.3341	87

Note: *Refer to Appendix for the descriptions of questionnaire items

Table II.
The descriptive statistics for the measurement of information security management

this study is sufficient for factor analysis. The greater the Kaiser-Meyer-Olkin (KMO) criteria value is, the more communal the factors are, and the data would be more suitable for factor analysis (Kaiser, 1974). In this study, the KMO values for all constructs were acceptable and the corresponding results of Bartlett's test of sphericity were significant (Table III). Table IV shows the correlations between each pair of these variables. One more important test is to assure the discriminant validity, which refers to that the indicators for different constructs should not be so highly correlated as to lead one to conclude that they measure the same thing. It is recommended that discriminant validity is demonstrated when the estimated correlations of the factors that underlie sets of indicators supposed to measure different constructs are not excessively high (>0.85) or excessively low (<0.1) (Kline, 1998). The construct correlation matrix listed in Table IV indicated that the estimated correlations, ranged between 0.317 and 0.827, were acceptable, and the test of discriminant validity was also satisfied Thus, the construct validity was assured and the correlation among variables was suitable for factor analysis.

Construct	Number of items	Cronbach's α	KMO	Bartlett's test of sphericity
Cooperativeness	8	0.903	0.839	Significant
Innovativeness	6	0.892	0.839	Significant
Consistency	6	0.885	0.829	Significant
Effectiveness	6	0.848	0.883	Significant
Confidentiality	5	0.875	0.815	Significant
Integrity	5	0.717	0.726	Significant
Availability	3	0.673	0.628	Significant
Accountability	6	0.865	0.850	Significant

Table III.
Cronbach's coefficient (α) of the construct

	Coop.	Inno.	Cons.	Effi.	Conf.	Intg.	Avai.	Acct.
Coop.	1							
Inno.	0.750 (*)	1						
Cons.	0.646 (*)	0.664 (*)	1					
Effi.	0.643 (*)	0.730 (*)	0.827 (*)	1				
Conf.	0.317 (*)	0.452 (*)	0.613 (*)	0.602 (*)	1			
Intg.	0.395 (*)	0.366 (*)	0.558 (*)	0.572 (*)	0.772 (*)	1		
Avai.	0.350 (*)	0.407 (*)	0.544 (*)	0.567 (*)	0.747 (*)	0.717 (*)	1	
Acct.	0.439 (*)	0.414 (*)	0.584 (*)	0.567 (*)	0.773 (*)	0.780 (*)	0.681 (*)	1

Table IV.
The result of correlation analysis

Notes: *Correlation is significant at the 0.01 level (2-tailed); coop., cooperativeness; inno., innovativeness; cons., consistency; effi., effectiveness; conf., confidentiality; intg., integrity; avai., availability; acct., accountability

The reliability of construct was checked using Cronbach's coefficient (α) for each component. As shown in Table III, all components had acceptable reliability since their Cronbach's α measures were between 0.673 and 0.903. According to the guideline indicated by Nunnally and Bernstein (1994), the value of 0.7 or above is an acceptable reliability coefficient, but sometimes slightly lower thresholds are used in the literature (Koch *et al.*, 2005; García-Morales *et al.*, 2006). Indeed, all above mentioned test results suggested that measurement model exhibited adequate construct reliability and validity.

Four regression models were used to quantify the effects of various traits of organizational culture on ISM principles: CIA, and accountability. The models can be expressed as regression equations in the following form:

$$y = \beta_0 + \beta_1 \chi^1 + \beta_2 \chi^2 + \beta_3 \chi^3 + \beta_4 \chi^4 + \mu$$

The dependent variable measures various ISM principles, while the independent variable are χ^1 (cooperativeness), χ^2 (innovativeness), χ^3 (consistency), and χ^4 (effectiveness). Ordinary least squares regression results are shown in Table V.

For testing *H2*, a regression analysis was conducted to check the relationship between organizational culture and confidentiality. The result showed that:

$$\text{Confidentiality} = -0.266^{*}\chi^1 + 0.130\chi^2 + 0.435^{**}\chi^3 + 0.318\chi^4$$

$$(F(87) = 15.651,\ \ p = 0.000,\ \ \text{and}\ \ R^2 = 0.433).$$

For testing *H3*, a regression analysis was conducted to check the relationship between organizational culture and integrity. The result showed that:

$$\text{Integrity} = 0.087\chi^1 - 0.196\chi^2 + 0.275\chi^3 + 0.432^{*}\chi^4$$

$$(F = 11.649,\ \ p = 0.000,\ \ \text{and}\ \ R^2 = 0.362)$$

For testing *H4*, a regression analysis was conducted to check the relationship between organizational culture and availability. The result showed that:

	Dependent variable			
	Confidentiality	Integrity	Availability	Accountability
Constant	-1.63×10^{-16} (0.083)	-4.98×10^{-17} (0.088)	-1.77×10^{-16} (0.087)	1.50×10^{-16} (0.089)
Cooperativeness	−0.266* (0.132)	0.087 (0.140)	0.113 (0.139)	−0.073 (0.142)
Innovativeness	0.130 (0.144)	−0.196 (0.153)	−0.112 (0.152)	−0.006 (0.155)
Consistency	0.435** (0.153)	0.275 (0.163)	0.344* (0.162)	0.266 (0.165)
Effectiveness	0.318 (0.164)	0.432* (0.174)	0.292 (0.173)	0.398* (0.177)
F	15.651	11.649	12.034	10.664
R^2	0.433	0.362	0.370	0.342

Notes: *$P < 0.05$, **$P < 0.01$, ***$P < 0.001$

Table V.
The result of regression analysis

$$\text{Availability} = -0.073\chi^1 - 0.006\chi^2 + 0.266\chi^3 + 0.398^*\chi^4$$

$$(F = 10.664, p = 0.000, \text{ and } R^2 = 0.342).$$

For testing *H5*, a regression analysis was conducted to check the relationship between organizational culture and accountability. The result showed that:

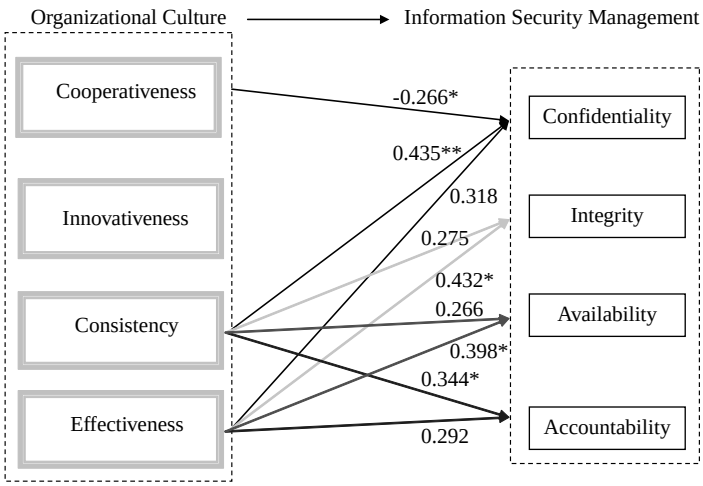
$$\text{Accountability} = 0.113\chi^1 - 0.112\chi^2 + 0.344^*\chi^3 + 0.292\chi^4$$

$$(F = 12.034, \ p = 0.000, \text{ and } R^2 = 0.370).$$

It is concluded that there are significant relationships between organizational culture and ISM. Hypothesis *H1* was therefore substantiated. The result of regression analysis is shown in Figure 3, which shows the relationships between organization culture and ISM.

In terms of the relationship between the ISM principle of confidentiality and various organizational culture traits, we found that cooperativeness was negatively related to confidentiality. The characteristics of cooperativeness are cooperation, information sharing, trust, empowerment, and team work. Curry and Moore (2003) found that the sharing of information in the healthcare environment was often hampered by a perceived need for confidentiality. Cooperativeness can be fostered in an organization for sharing information internally, but it is difficult in holding the principle of confidentiality in such an information sharing environment. Effectiveness and consistency have positive effect on confidentiality. Innovativeness is characterized by the external and flexible orientations, and it is possible that an organization characterized by innovativeness would find a low level of confidentiality in ISM implementation.

As for the relationship between the ISM principles of integrity, availability and accountability and the various organizational culture traits, we found that both effectiveness and consistency had positive effects on the ISM principles of integrity,



Notes: *P<0.05, **P<0.01

Figure 3.
The result of regression analysis

availability and accountability, but there were no significant relationships between the other two flexibility oriented organizational culture traits (i.e. cooperativeness and innovativeness) and these ISM principles. It is possible that organization characterized by these two flexibility oriented culture traits would find a low level of ISM implementation upon integrity, availability and accountability. It is derived from our study result that control oriented culture traits (effectiveness and consistency) would have strong effect on all ISM principles (CIA and accountability), and flexibility oriented cooperativeness and innovativeness are not significantly associated with the ISM principles with an exception that cooperativeness is negatively related to confidentiality.

5. Implications

Since, flexibility oriented culture traits are not positively associated with ISM principles, if the organizational culture of a company is flexibility oriented, it is unfavorable for the development of ISM in that company. Managers of such organizations need to understand the ISM disadvantage resulting from their flexibility oriented culture, and carefully lead their organizations with suitable counter measures, such as the proactively and carefully designed instructions and directions. We also found that control oriented culture traits (effectiveness and consistency) are significantly and positively associated with the ISM principles. Though control oriented culture is conducive to the development of ISM, unduly control will indirectly discourage information sharing among staffs. However, it is found that forming an atmosphere and culture of sharing is extremely important for enterprises in the knowledge economy to achieve the goal of creating business value through the utilization of intangible knowledge (Yeh *et al.*, 2006). For those organizations with strategic needs for encouraging staff to share their valuable information, experience, and idea, managerial controls conducted with caution to ensure and enhance the effectiveness of information security will play an important role in such organizations.

The culture of an organization can be built or changed by important factors of culture, such as norms, beliefs, values, and expectations. For the purpose of information security, organization leaders can make appropriate choices and adopt various approaches to shape the culture of their organizations, and eventually foster an environment conducive to the success of information security initiatives. For instance, organizations with flexibility oriented cultures may not support a favorable environment for information security practice, and therefore, it would be more imperatively desirable for managers of such organizations to identify and utilize information security technologies and corresponding implementation and management measures to enforce all ISM principles: CIA and accountability. Especially, for those cooperativeness oriented organizations, paying special attentions to confidentiality related initiatives is needed to assure positive (or at least to minimize undesirable) ISM outcomes according to our research findings that cooperativeness negatively affects confidentiality.

Various important factors of culture can shape human behaviors not only at intra-organizational level but also across inter-organizational partners. Thus, the same efforts described above should be applied to all related business counterparties, although both the assessed prerequisites and the important factors of culture may be different from those of various organizations at intra-organizational level.

Understanding the cultures of partner stakeholders can play important role in critically spelling the difference between the success and failure of ISM initiatives at inter-organizational level.

The development of information security can be represented and categorized into three waves: technical wave, management wave, and institutionalization wave (von Solms, 2000). Nowadays, information security is no longer a pure technical issue, and it requires top management's involvement in establishing or appointing policies, procedures, organization structures, staff and managers to improve information security. Other than the technical and management waves, the institutionalization wave is to cultivate information security as an organizational culture and in such a way that information security becomes a natural aspect of the daily activities of all members of an organization. A culture of information security is extremely important for organizations since the human dimension of information security cannot totally be solved by technical and management measures.

6. Conclusion

Security is a major concern in electronic commerce and knowledge economy, a higher level of perceived security leads to higher customer satisfaction and trust (Huang *et al.*, 2004; Flavián and Guinalíu, 2006), and a higher level of customer satisfaction can eventually create more transaction opportunities and benefit the businesses (Sudaporn and Ogenyi, 2004). The enterprises invest more and more in information security system, due to the fact that the virus and hacker attacks have become the vogue in recent years. However, this upsurge has been slowing down in 2005, partly because the cost of information security system is very expensive and it is difficult for enterprises to keep up with the huge increasing expense needed. While the information security systems are still fundamentally important, it has become more and more important for enterprises to pay attentions to the management of information security, which has the ultimate goal of designing and implementing information security strategies in an efficient and effective way.

Since, all technical security products need to be operated and managed by people, a technical security solution alone cannot protect an organization without a good security management policy and practice. A good practice of information security strategies between intra-organization and inter-organization partners can be supported and facilitated by information security systems and technologies, but it is not assured by them. Information security technology is necessary but not sufficient for successful ISM, whether at the intra-organizational level or across inter-organizational partners. Therefore, enterprises should adopt an integrated strategy combining both information security and organization culture aspects, and focusing not only on the "outside" artifacts and behavior patterns which are visible and audible, but on the "inside" human nature, activity and relationships which are hidden and mostly unconscious. The efficiency and effectiveness of the "outside" aspect of information security requires the "inside" aspect of an organization culture which is embedded in the values and beliefs of information security shared by all units at all levels in an organization. As a common faith and practice of each member in an organization, the implementation of an integrated information security practice and organizational culture would eventually reduce the damage of major events of information security. Overall, an appropriate and effective ISM implementation requires a combination of

favorable organizational culture, competent information security technology, and the management's supportive attitude toward information security.

Vroom and von Solms (2004) integrated the concept of the levels of organizational behavior and the organization culture model proposed by Schein (1985) to show how organizational culture influenced the organizational behavior at each level of an organization. For understanding and improving the organization behavior at each level in regard to information security, enterprises may look into organizational culture and examine how it affects information security practice. The first step for achieving the objectives of information security is to assess cultural prerequisites for ISM specifically. For instance, different subgroups within an organization may have some organizational culture traits in common, but also experience a sub-culture unique to some particular subgroup. Such a variation of the organizational culture in subgroups might ultimately affect the organizational culture as a whole. Our research contributes to a better understanding of the relationships between various organizational culture attributes and the effectiveness of ISM implementation (as detailed in previous sections covering empirical findings and implications). A better understanding of such relationships can provide a better picture of how to make information security initiatives succeed.

Before ending this paper, it is perhaps appropriate to suggest some directions for future research. Since, this study is the first known research for investigating the influence of organizational culture attributes (traits) upon the effectiveness of ISM, exploring the influence of other culture factors, such as different culture attributes or different culture types, upon the effectiveness of ISM may help us better understand the relationship between organizational culture and ISM. Since, our empirical study analyzed data collected from organizations in Taiwan, it would be interesting and valuable to conduct similar surveys in other regions for comparative studies. Furthermore, we plan to extend our study in the future by increasing the number of sampled companies, including other organizational factors such as top management support, and investigating how the effectiveness of ISM practice influences organizations upon their performance in various areas such as competition edge, customer satisfaction, corporate image, credibility, trust, and reputation.

References

Allen, D.K. and Fifield, N. (1999), "Re-engineering change in higher education", *Information Research*, Vol. 4 No. 3, available at: http://informationr.net/ir/4-3/paper56.html

Bali, R., Cockerham, G. and Bloor, C. (1999), "MISCO: a conceptual model for MIS implementation in SMEs", *Information Research*, Vol. 4 No. 4, available at: http://informationr.net/ir/4-4/paper61.html

Bishop, M. (2003), "What is computer security?", *IEEE Security and Privacy*, Vol. 1 No. 1, pp. 67-9.

Boggs, W.B. (2004), "TQM and organizational culture: a case study", *The Quality Management Journal*, Vol. 11 No. 2, pp. 42-52.

Borglund, E. (2005), "Operational use of electronic records in police work", *Information Research*, Vol. 10 No. 4, available at: http://InformationR.net/ir/10-4/paper236.html

BS 7799-1 (1999), *Information Security Management – Part 1: Code of Practice for Information Security Management*, British Standards Institute, London.

Cameron, K.S. (1991), "Culture congruence strength and type: relationship to effectiveness", *Research in Organizational Change and Development*, Vol. 5, pp. 23-58.

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-61.

Chiu, R-K. and Chen, J.C.H. (2005), "A generic service model for secure data interchange", *Industrial Management & Data Systems*, Vol. 105 No. 5, pp. 662-81.

Chou, D.C., Yen, D.C., Lin, B. and Cheng, P.H-L. (1999), "Cyberspace security management", *Industrial Management & Data Systems*, Vol. 99 No. 8, pp. 353-61.

Cooper, R.B. (1994), "The inertial impact of culture on IT implementation", *Information & Management*, Vol. 27 No. 1, pp. 17-31.

Cooper, R.B. (2000), "Information technology development creativity: a case study of attempted radical change", *MIS Quarterly*, Vol. 24 No. 2, pp. 245-76.

CSI/FBI (2004), *CSI/FBI Computer Crime and Security Survey 2004*, Computer Security Institute, San Francisco, CA, available at: www.gocsi.com/

Curry, A. and Moore, C. (2003), "Assessing information culture – an exploratory model", *International Journal of Information management*, Vol. 23 No. 2, pp. 91-110.

Deal, T. and Kennedy, A. (1982), *Corporate Culture: The Rites and Rituals of Corporate Life*, Addison-Wesley, New York, NY.

Denison, D.R., Haaland, S. and Goelzer, P. (2004), "Corporate culture and organizational effectiveness: is Asia different from the rest of the world?", *Organizational Dynamics*, Vol. 33 No. 1, pp. 98-109.

Dhillon, G. and Backhouse, J. (2000), "Information system security management in the new millennium", *Communications of ACM*, Vol. 43 No. 7, pp. 125-8.

Douglas, M. (1985), *Measuring Culture: A Paradigm for the Analysis of Social Organization*, Columbia University Press, New York, NY.

Dutta, A. and McCrohan, K. (2002), "Management's role in information security in a cyber economy", *California Management Review*, Vol. 45 No. 1, pp. 67-87.

Eloff, M.M. and von Solms, S.H. (2000), "Information security management: an approach to combine process certification and product evaluation", *Computers & Security*, Vol. 19 No. 3, pp. 698-709.

Flavián, C. and Guinalíu, M. (2006), "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site", *Industrial Management & Data Systems*, Vol. 106 No. 5, pp. 601-20.

Foltz, C.B., Cronan, T.P. and Jones, T.W. (2005), "Have you met your organization's computer usage policy?", *Industrial Management & Data Systems*, Vol. 105 No. 2, pp. 137-46.

Galanxhi-Janaqi, H. and Nah, F.F-H. (2004), "U-commerce: emerging trends and research issues", *Industrial Management & Data Systems*, Vol. 104 No. 9, pp. 744-55.

García-Morales, V.J., Llorens-Montes, F.J. and Verdú-Jover, A.J. (2006), "Antecedents and consequences of organizational innovation and organizational learning in entrepreneurship", *Industrial Management & Data Systems*, Vol. 106 No. 1, pp. 21-42.

Gaunt, N. (2000), "Practical approaches to creating a security culture", *International Journal of Medical Informatics*, Vol. 60 No. 2, pp. 151-7.

Hagberg, R. and Heifetz, J. (1997), *Corporate Culture: Telling the CEO the Baby is Ugly*, Hagberg Consulting Group, San Mateo, CA, available at: www.hcgnet.com/research.asp?id = 6

Higgins, H.N. (1999), "Corporate system security: towards an integrated management approach", *Information Management & Computer Security*, Vol. 7 No. 5, pp. 217-22.

Hong, K-S., Chi, Y-P., Chao, L.R. and Tang, J-H. (2003), "An integrated system theory of information security management", *Information Management & Computer Security*, Vol. 11 No. 5, pp. 243-8.

Huang, J.-H., Yang, C., Jin, B.-H. and Chiu, H. (2004), "Measuring satisfaction with business-to-employee systems", *Computer in Human Behavior*, Vol. 20 No. 1, pp. 17-35.

Huang, S-M., Lee, C-L. and Kao, A-C. (2006), "Balancing performance measures for information security management", *Industrial Management & Data Systems*, Vol. 106 No. 2, pp. 242-55.

Information Security Magazine (2002), "2002 ISM survey: does size matter?", *Information Security*, September, available at: http://infosecuritymag.techtarget.com/2002/sep/2002survey.pdf

Kaiser, H. (1974), "An index of factorial simplicity", *Psychometrika*, Vol. 39 No. 1, pp. 31-6.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y. and Wei, K.K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139-54.

Kefallinos, D., Lambrou, M.A. and Sykas, E.D. (2006), "Secure PKI-enabled e-government infrastructures implementation: the SYZEFXIS-PKI case", *Electronic Government: An International Journal*, Vol. 3 No. 4, pp. 420-38.

Kenning, M.J. (2001), "Security management standard – ISO 17799/BS 7799", *BT Technology Journal*, Vol. 19 No. 3, pp. 132-6.

Kim, S. and Leem, C.S. (2005), "Enterprise security architecture in business convergence environment", *Industrial Management & Data Systems*, Vol. 105 No. 7, pp. 919-36.

Kline, R.B. (1998), *Principles and Practice of Structural Equation Modeling*, The Guilford Press, New York, NY.

Koch, A.L., Arfken, C.L., Dickson, M.W., Agius, E. and Mitchelson, J.K. (2005), "Variables associated with environmental scanning among clinicians at substance abuse treatment clinics", *Information Research*, Vol. 11 No. 1, available at: http://InformationR.net/ir/11-1/paper244.html

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information & Management*, Vol. 41 No. 5, pp. 597-607.

Melton, C.E., Chen, J.C.H. and Lin, B. (2006), "Organisational knowledge and learning: leveraging it to accelerate the creation of competitive advantages", *International Journal of Innovation and Learning*, Vol. 3 No. 3, pp. 254-66.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory*, McGraw-Hill, New York, NY.

Owens, I., Wilson, T.D. and Abell, A. (1995), "Information and business performance: a study of information systems and services in high-performing companies", *Information Research*, Vol. 1 No. 2, available at: http://informationr.net/ir/1-2/paper5.html

Quinn, R.E. and Spreitzer, G.M. (1991), "The psychometrics of the competing values culture instrument and an analysis of the impact of organization culture on quality of life", *Research in Organizational Change and Development*, Vol. 5, pp. 115-42.

Ryan, S.D. and Bordoloi, B. (1997), "Evaluating security threats in mainframe and client/server environments", *Information & Management*, Vol. 32 No. 3, pp. 137-46.

Sanderson, E. and Forcht, K.A. (1996), "Information security in business environment", *Information Management & Computer Security*, Vol. 4 No. 1, pp. 32-7.

Schein, E. (1985), "Coming to a new awareness of organizational culture", *Sloan Management Review*, Vol. 25 No. 2, pp. 3-16.

Schwartz, B. (1981), *Vertical Classification: A Study in Structuralism and the Sociology of Knowledge*, University Chicago Press, Chicago, IL.

Shih, D-H., Sun, P-L. and Lin, B. (2005), "Securing industry-wide EPCglobal network with WS-security", *Industrial Management & Data Systems*, Vol. 105 No. 7, pp. 972-96.

Sudaporn, S. and Ogenyi, O. (2004), "The store loyalty of the UK's retail consumers", *The Journal of American Academy of Business, Cambridge*, Vol. 5 Nos 1/2, pp. 503-9.

Szilagyi, A.D. and Wallace, M.J. (1987), *Organizational Behavior and Performance*, 5th ed., Scott, Foresman and Company, Glenview, IL.

von Solms, B. (2000), "Information security – the third wave?", *Computers & Security*, Vol. 19 No. 7, pp. 615-20.

von Solms, B. and von Solms, R. (2004), "The 10 deadly sins of information security management", *Computers & Security*, Vol. 23 No. 5, pp. 371-6.

Vroom, C. and von Solms, R. (2004), "Towards information security behavioral compliance", *Computers & Security*, Vol. 23 No. 3, pp. 191-8.

Yeh, Y-J., Lai, S-Q. and Ho, C-T. (2006), "Knowledge management enablers: a case study", *Industrial Management & Data Systems*, Vol. 106 No. 6, pp. 793-810.

Further reading

Hung, Y-C., Huang, S-M., Lin, Q-P. and Tsai, M-L. (2005), "Critical factors in adopting knowledge management systems for the pharmaceutical industry", *Industrial Management & Data Systems*, Vol. 105 No. 2, pp. 164-83.

Appendix. Questionnaire items

Organization culture

Cooperativeness_1: Managers empower their staff.
Cooperativeness_2: Managers treat all staff as their big family members.
Cooperativeness_3: Employees are loyal and trust one another.
Cooperativeness_4: Your company encourages employees to actively participate all company activities and events.
Cooperativeness_5: Employees are devoted to protect their organization.
Cooperativeness_6: Employees are trusted by their managers, and can participate in the decision making process.
Cooperativeness_7: It is very harmonious amongst employees, and your company is treated like a big family.
Cooperativeness_8: Your company pays attentions to human resource development, employees' morale, and team work.
Innovativeness_1: Managers have courage to make innovation and take risk.
Innovativeness_2: Managers actively lead the staff to grow and innovate.
Innovativeness_3: Managers have vision and insights to create new business opportunities.
Innovativeness_4: Employees always have to face challenges and they can learn and grow from the challenges.
Innovativeness_5: Your company pays attentions to the uniqueness of employees and encourages the innovation from employees.
Innovativeness_6: Your company is willing to take risks, and it is indeed an ambitious and energetic organization.
Consistency_1: Managers set up clear goals and demand employees to carry out the goals strictly.
Consistency_2: Your company always has formal and strict rules for employees to follow.

Consistency_3: The operation of your company emphasizes stability and conservative culture. It does not allow any confusion.
Consistency_4: Your company pays attentions to efficiency and performance for achieving the goals.
Consistency_5: Your company is stable and offers job security to employees.
Consistency_6: Your company is a systematic organization where each employee has clear duty, and its operations are well defined with clear rules to follow.
Effectiveness_1: Managers emphasize working efficiency and acts effectively.
Effectiveness_2: Managers pay attentions to achieve good work performance and reach the goal, regardless of personal feelings.
Effectiveness_3: The critical success factor of your company is its good productivity.
Effectiveness_4: Your company pays attentions to work efficiency. Every department and employee must compete with its peer for better efficiency.
Effectiveness_5: Your company pays attentions to maintaining its competition advantages.
Effectiveness_6: Your company pays attentions to employees in terms of increasing their efficiency and pursuing their accomplishment.

Information security management

Confidentiality_1: Your company enforces security controls (such as the cryptographic system) to protect sensitive information and proprietary/business secrets.
Confidentiality_2: Unauthorized employees are prohibited from accessing company's information resources.
Confidentiality_3: Employees must follow company policy and regulations when releasing or transmitting information.
Confidentiality_4: Your company has well implemented security practices to protect important information from stolen by malicious intrusions (such as break-in, Trojans, and spy-wares).
Confidentiality_5: Information security measures are implemented in your company to prevent sensitive information from unauthorized disclosure.
Integrity_1: Your company constantly updates information resources and regularly creates information backups.
Integrity_2: Your company regularly conducts risk assessment and updates security plans to reduce the probability of loss of information.
Integrity_3: When acquiring important information from the information sources or business partners, employees will store it into the company's database.
Integrity_4: Your company has security controls (such as change management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion).
Integrity_5: The database is periodically reconciled and regularly maintained in your company to increase the accuracy and reliability of information.
Availability_1: Your company pays attentions to lower down the probability of information system breakdown and information service disruption.
Availability_2: There are well established information access control procedures in your company, to make sure that for any particular information resource only authenticated users with right privileges can access such resource.
Availability_3: A legitimate user with business needs can access company information at anytime and at anyplace.
Accountability_1: In your company, there is a clear procedure to discipline employees who violate organizational security policy and regulations.
Accountability_2: Your company provides good information security training and education to employees.

Accountability_3: In your company, labels and warning signs about information security are clearly posted on computers and communication equipments.

Accountability_4: A matching management structure with various roles and responsibilities has been set up in your company to maintain a sound information security practice and respond to information security incidents.

Accountability_5: Your company sets up proper information security controls, and employees follows information security protocols, norms, and regulations related to these controls.

Accountability_6: Your company routinely conducts information security audits and maintains historical records/data of information misuse or intrusion attempts.

Demographic items

- gender;
- education;
- job title/level;
- seniority of service;
- department;
- the age of the company;
- number of employees in company; and
- industry sector.

Corresponding author
Shuchih Ernest Chang can be contacted at: eschang@dragon.nchu.edu.tw