Inf Technol Manag
DOI 10.1007/s10799-015-0252-2

The impacts of organizational culture on information security culture: a case study

Mincong Tang[1] · **Meng'gang Li**[2] · **Tao Zhang**[3]

© Springer Science+Business Media New York 2015

Abstract Information security cannot rely solely on technology. More attention must be drawn to the users' behavioral perspectives regarding information security. In this study, we propose that a culture encouraging employees to comply with information policies related to collecting, preserving, disseminating and managing information will improve information security. Information security culture is believed to be influenced by an organization's corporate culture (or organizational culture). We examine how this occurs through an in-depth case study of a large organization. We present a relationship map for organizational culture and information security practices. Six propositions are drawn from the findings of our interviews and discussions. Managerial insights, such as how to measure an organization's information security culture and subsequently determine what perspective(s) is important for the organization to improve, are also discussed.

Keywords Organizational culture · Information security · Security culture · Case study

✉ Mincong Tang
mincong@bjtu.edu.cn

Meng'gang Li
morganli@vip.sina.com

Tao Zhang
zhangtao@abp.gov.cn

[1] International Center for Informatics Research, Beijing Jiaotong University, Beijing, China

[2] China Center for Industrial Security Research, Beijing Jiaotong University, Beijing, China

[3] State Administration of Radio, TV and Films, Beijing, China

1 Introduction

Today, information is regarded as a critical asset for organizations. Like electricity, business cannot operate without information [2]. However, with the rapid development of information technologies, particularly the widespread use of the Internet, business transactions and information processing are more vulnerable than ever for threats and risks both external and internal to an organization [22]. Mcllwraith [18] reported that two to three percent of a company's profit may possibly be lost due to information security issues. According to the China National Computer Network Emergency Response Center (CNCERT), over 50,000 oversea IPs participated in attacking 8.9 million hosts in China in 2011. Among these controlled hosts, 99.4 % of the IPs were from the United States and approximately 75 % of the IPs were disguised as websites of Chinese domestic banks. These numbers are surprising. The overall situation appears bleak for companies' information security problems. Occurrences of these hacks make companies realize the immense importance of solving information security problems.

Through a comprehensive literature review on information security research, we found that before the 2000s, academics and practitioners conducted many studies on information security research, many of which focused on technical perspectives. However, since the millennium, people gradually realize that information security cannot be achieved solely through applying technology. The 'human factor' has been raised as a more critical issue by an increasing number of researchers, although it is often ignored by practitioners. Regardless of how advanced the technologies are, without an insufficient consciousness of information security by employees, great loss might occur in companies where employees are unconscious of risks

Published online: 18 November 2015

and regard it as unimportant to unintentionally disclose confidential information. Thus, it is critical for companies to establish employees' consciousness of responsibility and develop their information security culture (ISC). As a subset of an organization's corporate culture (or organizational culture), information security is characterized as having a shared belief, recognition and value system, thus formulating normalized thinking and behavior modes, and is believed to help an organization achieve its objectives in information security management (ISM).

The remainder of this paper is organized as follows. First, we present a summary of the existing literature on organizational culture, ISM and their relationships; from this discussion, we formulate the theoretical foundations of our study. Research gaps are also indicated in this section. Next, based on the findings of existing literature, we propose a theoretical model that illustrates the relationships between organizational culture and ISC from a 'practice' perspective. As we aim to propose a theory for ISC research, we conduct an in-depth case study of a large company in China to examine the detailed relationships. Finally, we summarize our qualitative findings and provide future directions for ISC research.

2 Literature review

2.1 Organizational culture

Every organization has a particular culture, which consists of a set of assumptions, values and norms and directs the activities within an organization. Organizational culture has been defined in various ways and ascribed to numbers of identifiable value sets, such as management styles, reward systems, communication styles, and manners of decision making, all of which help to define an organization's character and norms. Hofstede et al. [11] defined organizational culture as "the manifestation of practices or behaviors evolving from the shared values in the organization", which implies that organizational culture refers to practices or the more observable perspectives of culture. Scholars have developed various models for measuring organizational culture with the aim to differentiate organizations along the lines of the dominant values guiding organizational behaviors.

In this study, we choose Hofstede's framework to measure organizational culture as it is relatively easy to map onto organizational issues, such as ISM practices. Furthermore, Hofstede's data show that different organizations within the same national culture can be distinguished by their daily practices and not by their values, which is in opposition to Schein's work. We believe that this finding is consistent with and supportive of this study.

2.2 Organizational culture and information security management

According to Deal and Kennedy [5], culture is believed to be the single most important factor accounting for the success or failure of an organization. Organizational culture certainly influences the behaviors of employees and the activities of the entire organization. Thus, an organization's ISM practices are to be supported and guided by its organizational culture. In a comprehensive literature review conducted by Leidner and Kayworth [17], IT behaviors that require organizational or management changes, such as adopting, managing, and using information technologies, are often resisted by people who do not want to change accustomed practices and subsequently run into trouble. According to Lacey [16], ISM practices are easily resisted by employees if there is a lack of motivation for changing their daily habits [13]. As noted by many researchers, information security is mainly a managerial issue rather than a technical one; without a deep change in its organizational security culture, an organization cannot achieve effectiveness in ISM. Thus, many studies have been conducted to determine ideal forms of organizational culture to facilitate organizations in carrying out ISM. Through two case studies, Kokolakis et al. [14] found that organizations with a coherent culture, which is characterized as employees following a code of practice or ethics, will be able to implement and adopt IS policies more easily. Chang and Lin [3] reported that controlling organizational culture significantly influences ISM in terms of confidentiality, integrity, and availability, whereas flexible organizational culture is not significantly associated with ISM except insofar as cooperativeness negatively relates to confidentiality. In their survey, Herath and Rao [9] suggested that intrinsic and extrinsic motivators significantly influence security behaviors, whereas certainty of detection was found to be significant and severity of punishment has a negative effect on security behavior intentions. Kraemer et al. [15] examined human and organizational factors in computer and information security: factors such as management and organization are identified as significant players in ISM. By applying protection motivation theory (PMT) and the theory of planned behavior (TPB), Ifinedo [12] empirically tested whether subjective norms (organizational culture) positively influence the behavioral compliance intentions, in terms of information security policy adherence, of employees, which produced positive results. Hedström et al. [7] argued that as organizations apply multiple forms of rationality in organizational actions, value conflicts must be caused. Thus, a value-based compliance model is useful in ISM, as it considers the managers and employees' rationalities. In the discussion above, we can see a clear relationship between organizational culture and ISM practices.

2.3 Information security culture

An increasing number of studies have indicated that the establishment of an ISC in an organization is necessary for effective ISM practices. According to Schlienger and Teufel [19], a security culture "encompasses all socio-cultural measures that support technical security measures", which helps to establish trust among the actors of an organization and becomes a part of the organizational culture. Helokunnas and Kuusisto [8] proposed ISC as a system consisting of a framework that includes the standardization, certification and measurement of information security and contains employees' attitudes toward, knowledge about and mental models of information security. Thomson et al. [20] reported that information security must be integrated with organizational culture to achieve protection of information assets. According to Kanungo et al. [13], organizations must mold the information security behaviors of employees. Such molded information security behaviors formulate a balanced ISC that can direct individual and group behaviors. Through a questionnaire survey, Veiga et al. [21] first validated an assessment instrument for ISC. The instrument includes the dimensions of ISC, including ISM, performance management, performance accountability, communication, governance and capability development. Unfortunately, few studies have expanded upon their research. One possible reason might be that there is a lack of consistency between what the authors defined as an ISC and the common understanding in the existing literature of organizational culture. In contrast, information security is a well-known branch of organizational culture; however, the specifics of how information security and organizational culture are related remain unclear. As proposed by Crossler et al. [4], cultural studies are one of the future directions of behavioral information security research. Therefore, we are motivated to conduct this study. In summarizing the discussion above, we believe that there is a necessity for a clear and measurable framework to justify the detailed relationship between the elements (or dimensions) of organizational culture and those of ISC that practitioners can apply to guide their daily ISM practices.

3 The research framework

In this section, we elaborate on the relationship between organizational culture and ISC. We define ISC as the manifestation of ISM practices or information security behaviors evolving from the shared values and beliefs in information security within an organization. This definition is consistent with Hofstede's definition of organizational culture. In the following discussion, we first present the dimensions of Hofstede's organizational culture framework, with which we will examine the role of organizational culture in ISM practices. We then decompose ISC into four dimensions: employees' behavioral compliance with information security policies (Compliance), an organization's communication to employees concerning information security (Communication), an organization's actions in response to employee violation of ISM (Accountability), and the positioning of information security within an organization (Governance). We believe that these four dimensions integrate human, organizational and technological views into ISM as proposed by Werlinger et al. [23]. For the purpose of this study, we aim to propose a theory of the relationships between organizational culture and ISC. Thus, the case study method is applied.

3.1 Hofstede's organizational culture framework

According to Hofstede et al. [11], organizational culture can be described with six dimensions of practices: *process oriented versus results oriented, employee oriented versus job oriented, parochial versus professional, open system versus closed system, loose versus tight control* and *normative versus pragmatic.*

Process oriented versus results oriented explores the differences between a concern with means and a concern with goals [10]. This dimension typically refers to the innovativeness and risk-taking of an organization. Process-oriented organizations have relatively conservative attitudes toward innovations and their associated risks, thus exerting minimal effort and preferring the use of existing methods, whereas results-oriented organizations encourage the use of innovative techniques for the survival and growth of the organization.

Employee oriented versus job oriented explores the differences between a concern for people and a concern for accomplishing the job [10]. In an employee-oriented organization, employees feel that the organization should take care of their personal problems and welfare, whereas in job-oriented organizations, employees believe that their organization is only concerned about completing jobs and not about their personal affairs.

Parochial versus professional compares how employees derive their identity from the organization or from their job type [10]. In a parochial organization, workers believe that when hiring new employees, companies should consider their social and family backgrounds along with their capabilities and that companies should also take care of their employees' futures. Conversely, in a professional organization, workers believe that their company should only consider employees' capabilities and leave their private affairs out of the scope of consideration.

Open system versus closed system refers to the communication climate of an organization. In an open system

organization, employees are eager to share their experience and information in support of one another—they are open with new hires and outsiders alike. However, in a closed system organization, new employees need more time to feel comfortable and accepted—the organization and its more tenured employees are felt to be closed and secretive [10].

Loose versus tight control deals with the rules, policies and structure (hierarchy) of an organization. Organizations with a tight control culture place a strict emphasis on following the rules and policies. They are highly cost-conscious, and meeting times are punctually kept. In contrast, in loose control organizations, employees do not primarily consider costs, and meeting times are only approximately kept [10].

Normative versus pragmatic deals with the popular notion of "customer orientation" [10]. Normative organizations place more emphasis on following the correct procedures than on the results, whereas pragmatic organizations emphasize meeting the customer's needs and consider results to be more important than following correct procedures.

According to Hofstede [10], these six dimensions are derived from perceptions of the daily practices of organizations and their employees, which is consistent with our definition of ISC. Thus, we apply Hofstede's six dimensions of organizational culture in our study to conduct the analysis.

3.2 Four proposed dimensions of information security culture

Following the comprehensive literature review, we propose that ISC includes the following dimensions of ISM practices:

- *Compliance*: this dimension mainly refers to employees' behavioral compliance with information security policies, particularly in terms of their willingness to change their working practices to ensure the security of information assets, their commitment to information security policies, and their beliefs concerning adequate information protection.
- *Communication*: this dimension refers to how an organization explains its information security policies to employees, how it informs employees of the personal impacts of information security changes, and its expectations of employees regarding information security.
- *Accountability*: this dimension refers to an organization's response to employee violation of information security policies, which includes the actions an organization will take if employees do not obey its information security policies, whether employees feel safe at the organization, and whether employees are held accountable when they violate the organization's rules/policies of ISM.
- *Governance*: this dimension includes the positioning of information security at an organization, the management's obedience to information security policies, the controls placed on information security assets, and the management-level perception of the importance of information security.

3.3 A framework of the relationship between organizational culture and information security culture

Based on the discussions above, we propose a framework for elaborating the relationship between organizational culture and ISC, as shown in Fig. 1.

4 The case study

We use a case study approach because the focus of this study is to answer "how" questions [24]. Moreover, we cannot manipulate the behaviors of those involved. Thus, the purpose of this study is to explore and enrich the understanding of the relationship between organizational culture and ISC, with the eventual aim of building a theory explaining how organizational culture influences ISC. Of course, the use of only a single case reduces the generalizability of the findings. However, the rich data found in our single case study provide an excellent foundation for the inductive process of theory building.

In IS research, case studies pose considerable problems in terms of ensuring sufficient rigor and reliability [1]. To ensure an adequate level of reliability in this study, we introduce multiple respondents from the same company who work in different departments and have different backgrounds. Additionally, we asked these respondents to review and evaluate the research results. Of course, it is always better to include more companies and conduct multiple case studies. However, given our circumstances, this is impossible due to limited resources. Nevertheless, we were able to collect a considerable amount of data for our analysis. Our case study concerns a large manufacturing firm in the garment industry. The garment industry is one of the most representative industries of China, and the company we studied is the largest garment manufacturing firm in China; with over 30 years of history, it evinces the change of China's economic reform and opening-up. It is the main OEM for many major international brands, including Nike, Adidas, Ralph Lauren, and Tommy

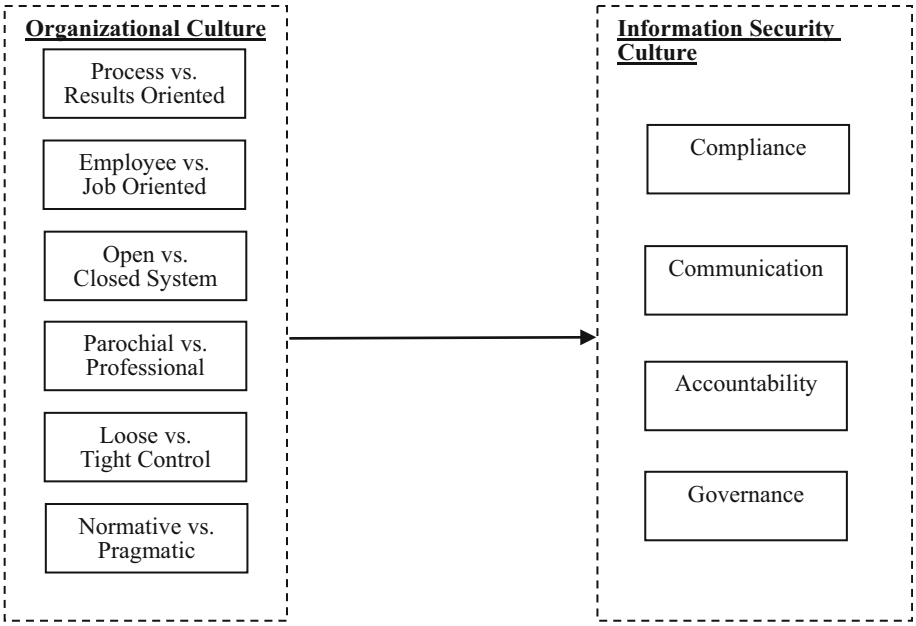

Fig. 1 The research framework

Hilfiger. It developed from a small factory into a large corporation with over 50,000 workers in mainland China. Its management also developed from a family-run enterprise into an internationally standardized corporation. We spent 6 months with the company to collect case data while providing management consultancy services. Through our early study of this company, we believe that it characterizes many features of Chinese manufacturing firms and can be positioned as a classic representative of the Chinese garment industry. Thus, we ultimately chose this company for the purpose of our study.

4.1 Research questions and case data collection

As suggested by Eisenhardt [6], it is important to define the research question(s) when building a theory from case studies. Based on the comprehensive literature review and early-stage interviews with top management in the company, we proposed the following research questions for our study:

> Research question 1: Can the culture of an organization significantly influence its employees' behaviors/practices when considering its information assets (namely, its information security culture)?
> Research question 2: If the answer to question 1 is yes, how can we interpret the impacts of organizational culture on information security culture? By applying Hofstede's framework, how will each dimension of organizational culture influence information security culture in terms of compliance, communication, accountability and governance?

With these two research questions in mind, we conducted the case study and analyzed the data collected from the company. There were three stages to our interviews. In the first stage, we invited top management, mid-level managers and regular employees from different departments to participate. There were no specific questions, and we recorded their opinions of this study. During this stage, we had three meetings with these three types of interviewees. All interviewees from top and middle management had more than 10 years of experience with the company, and two of the top management respondents were the cofounders of the company. For the common staff members, some were from production lines, others were administrative employees, and all of them had worked with the company for over 5 years. Thus, these interviewees were believed to know the company well. The purpose of these meetings was to gain an understanding of the knowledge possessed by the people in this company regarding their daily practices (which can later be interpreted as elements of organizational culture and ISC). In the second stage, we presented an open-ended questionnaire with questions concerning the organizational culture and ISC, all of which were open-ended—the participants were required to answer the questions in a descriptive manner. With this information, we conducted a qualitative analysis and prepared the materials for future discussions. In the third stage, we asked the executive director of the company to arrange a focus group meeting, the participants of which were representatives from the three types of interviewees. During the meeting, we presented the outline and summary of the findings from the first two stages of the study. Subsequently, the participants discussed and

presented their opinions of the findings. The content of this meeting was recorded for future analysis.

4.2 Case data analysis

As described above, there were three stages to our case study. Thus, our case data analysis will be conducted in an inductive manner corresponding to the three stages of the data collection.

In the first stage, twelve persons were interviewed, and they were open about discussing the current practices of their company from their perspectives. To avoid collecting unrelated or unnecessary information, we intentionally provided questions that fall within the scope of this study. Instead of asking the respondents'agree or disagree' questions, we decomposes the original Likert-scale questions into 'what' and 'how' (i.e., open-ended) questions. For example, one of the original questions for '*process versus results oriented'* is "People feel comfortable with unfamiliar situations", which we changed into "Could you please describe how people deal with new situations" and led them into a discussion. Through such a decomposition, the interviews become sufficiently open, and the respondents talked about their daily operations and practices related to information and security management as well as their daily practices in general, which have been implicitly elaborated by the dimensions of organizational culture in this study.

In the second stage, we provided an entire set of the questions, which included those on organizational culture and information security practices. All of these questions were open-ended, and the respondents needed to provide answers that reflected their daily practices and routines. We do not suggest that these questions on organizational culture and information security practices explain everything to be elucidated. For example, the four sets of questions on information security practices are all relevant for describing the main scope of the ISC. However, we do not aim to obtain completeness but conciseness: it is sufficient to use the four sets, and there is no necessity to use more to explain most of what occurs.

In the third stage, which was held 1 month after the second stage was completed, three representatives, including the executive director, were invited to participate in a focus group meeting. In the meeting, we first presented our findings from the first and second stage interviews. For the discussion results, we used a relational diagramming technique to causally interrelate the six dimensions of organizational culture and the four dimensions of ISC. We also considered the directions of impacts among these factors. We attempted to arrive at a relational structure that could explain how organizational culture influences ISC, which is the focus of this study. In the following discussion, we present our theory of how the dimensions of organizational culture influence those of information security practices (or ISC). The relationships elaborated in Fig. 2 are the findings from the discussion and examination of the results from our analysis of the interview data. Based on the research framework (Fig. 1), we summarize the relationships as shown in Fig. 2.

5 Discussion

In this section, we present six preliminary research propositions resulting from this exploratory study for further investigation in subsequent research. We refer to these as propositions because they are not ready to be tested as hypotheses. This is a common phenomenon from case studies because generalization is always problematic, and our case is not suggested as a possible one for generalization. However, we believe that further research following these propositions should be able to produce more generalizable findings.

Proposition 1 *The dimension of organizational culture Process versus Results Oriented will influence Information Security Culture in terms of Compliance and Communication. Process-oriented culture, which is characterized as 'more conservative toward innovations and associated risks', is believed to lead to increased compliance with information security management policies and rules. In terms of communication, it mainly refers to how organizations explain and disseminate information security policies and rules to employees. Thus, in a process-oriented organization, it is believed that the organization will develop routines to involve and inform employees of its information security policies.*

Proposition 2 *The dimension of organizational culture Employee versus Job Oriented will influence information security culture in terms of compliance and accountability. In an employee-oriented organization, employees are more likely to be taken care of by the company. Thus, employees are more likely to comply with rules and policies, including those related to information security management. Regarding accountability, employee-oriented organizations will consider more options when responding to employee violations of information security management.*

Proposition 3 *The dimension of organizational culture Open versus Closed System will influence information security culture in terms of communication and accountability. In an open-system organization, new employees find it easy to feel comfortable and accepted, and inter-employee conversations are more open. Thus, it will be easier for management to explain information security*

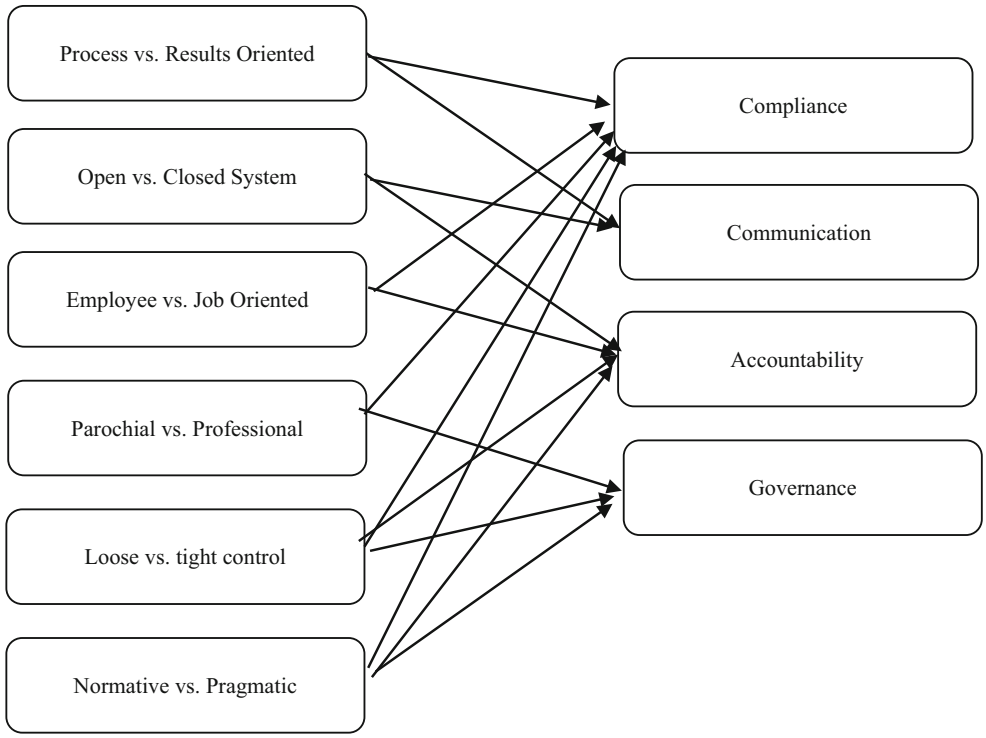

Fig. 2 Causal relationships between organizational culture and information security culture

management policies and rules to their employees. It is also easier for employees to accept personal impacts when information security affairs have to change. Regarding an organization's response to employee violations of information security management policies, open-system organizations can be less strict, whereas closed-system organizations might take severe measures.

Proposition 4 *The dimension of organizational culture Parochial versus Professional will influence information security culture in terms of compliance and governance. Employees of a parochial organization identify themselves as members of that organization, whereas in professional organizations, employees only identify themselves with their professions. It is believed that in parochial organizations, employees are more likely to comply with rules and policies, including those related to information security. Conversely, professional organizations will place information security in a more important position, as it would be a 'profession' for such an organization.*

Proposition 5 *The dimension of organizational culture Loose versus Tight Control will influence information security culture in terms of compliance, accountability and governance. In a loose control organization, rules and policies are not taken strictly. Thus, employees are more likely to be less obedient to information security management policies, and they may believe it to be less serious when violating the related rules and policies. Regarding the positioning of information security management, loose control organizations are also believed to position it as less important, even at the management level. This dimension is important and dangerous for information security management compared with the other dimensions of organizational culture.*

Proposition 6 *The dimension of organizational culture Normative versus Pragmatic will influence information security culture in terms of compliance, accountability and governance. In a normative organization, the procedures are critical, whereas a pragmatic organization will use its best effort to fulfill the customers' needs. Thus, it is believed that employees in normative organizations are more likely to obey the rules and policies. When violating rules, employees are more likely to be held accountable for such behaviors in normative organization. With regard to the positioning of information security management, management in a normative organization is also believed to perceive employee obedience to information security policies and rules as more important.*

6 Conclusions and future research

This study suggested that organizational culture impacts ISC. We attempted to illustrate the relationship between the two cultures by proposing the causal linkages above.

Our case analysis shows that Hofstede's framework was suitable for explaining the relationship between organizational culture and ISC. Furthermore, we believe that the four proposed dimensions of ISC could be a practical measure. This study provides a supportive foundation for future research, which must produce generalized findings to provide detailed practical guidelines for practitioners as well as insights for academics in relevant fields. Future research could be deployed in at least two directions: one to validate a measure for ISC and the other to develop an exploratory model to empirically test the impact of organizational culture on ISC. Moreover, there are revised or possible additional dimensions that could be constructed for the proposed ISC framework of this study.

Acknowledgments This study is part of the projects 'Research on China Industrial Security Index' (No. B09C1100020) and "Industrial Security Engineering Research" (No. 239010522) funded by the Ministry of Education, China. We appreciate the supportive comments from the reviewers.

References

1. Akkermans H, van Helden K (2002) Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors. Eur J Inform Syst 11(1):35–46
2. Carr NG (2003) It doesn't matter. Harv Bus Rev 41(9):5–12
3. Chang S, Lin C (2007) Exploring organizational culture for information security management. Ind Manag Data Syst 107(3):438–458
4. Crossler R, Johnston A, Lowry P, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. Comput Secur 32(1):90–101
5. Deal T, Kennedy A (1982) Corporate cultures: the rites and rituals of organizational life. Addison-Wesley, Boston
6. Eisenhardt K (1989) Building theories from case study research. Acad Manag Rev 14:532–550
7. Hedström K, Kolkowska E, Karlsson F, Allen JP (2011) Value conflicts for information security management. J Strateg Inf Syst 20:373–384
8. Helokunnas T, Kuusisto R (2003) Information security culture in a value net. In: IEEE Engineering management conference, 2003. IEMC'03. Managing technologically driven organizations: the human side of innovation and change, pp 190–194
9. Herath T, Rao H (2009) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 47(2):154–165
10. Hofstede G (1998) Identifying organizational subcultures: an empirical approach. J Manage Stud 35(1):1–12
11. Hofstede G, Neuijen B, Ohayv D, Sanders G (1990) Measuring organizational cultures: a qualitative & quantitative study across twenty cases. Adm Sci Q 35(2):286–316
12. Ifinedo P (2012) Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 31(1):83–95
13. Kanungo S, Sadavarti S, Srinivas Y (2001) Relating IT strategies & organizational culture: an empirical study of public sector units in India. J Strateg Inf Syst 10(1):29–57
14. Kokolakis S, Karyda M, Kiountouzis E (2005) The insider threat to information systems and the effectiveness of ISO17799. Comput Secur 24(6):472–484
15. Kraemer S, Carayon P, Clem J (2009) Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput Secur 28(3):509–520
16. Lacey D (2010) Understanding and transforming organizational security culture. Inf Manag Comput Secur 18(1):4–13
17. Leidner D, Kayworth T (2006) A review of culture in information systems research: toward a theory of information technology culture conflict. MIS Q 30(2):357–399
18. Mcllwraith A (2006). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Gower Publishing Company, Burlington
19. Schlienger T, Teufel S (2003) Information security culture - from analysis to change. S Afr Comput J 31:46–52
20. Thomson K, von Solms R, Louw L (2006) Cultivating an organizational information security culture. Comput Fraud Secur 2006(10):7–11
21. Veiga A, Martins N, Eloff J (2007) Information security culture-validation of an assessment instrument. S Afr Bus Rev 11(1):147–166
22. Vroom C, Von Solms R (2004) Towards information security behavioral compliance. Comput Secur 23(3):191–198
23. Werlinger R, Hawkey K, Beznosov K (2009) An integrated view of human, organizational, and technological challenges of IT security management. Inf Manag Comput Secur 17(1):4–19
24. Yin RK (2003), Applications of case study research, 2nd edn. Sage, Thousand Oaks