2009

Exploring the Relationship between Organizational Culture and Information Security Culture

Joo S. Lim
University of Melbourne

Shanton Chang
University of Melbourne

Sean Maynard
University of Melbourne

Atif Ahmad
University of Melbourne

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2017

Exploring the Relationship between Organizational Culture and Information Security Culture

Joo Soon Lim, Shanton Chang, Sean Maynard & Atif Ahmad
Department of Information Systems
The University of Melbourne
Australia
Email: jslim@pgrad.unimelb.edu.au; slwc@unimelb.edu.au
Email: seanbm@unimelb.edu.au; atif@unimelb.edu.au

Abstract

Managing Information Security is becoming more challenging in today's business because people are both a cause of information security incidents as well as a key part of the protection from them. As the impact of organizational culture (OC) on employees is significant, many researchers have called for the creation of information security culture (ISC) in organizations to influence the actions and behaviour of employees towards better organizational information security. Although researchers have called for the creation of ISC to be embedded in organizations, nonetheless, literature suggests that little past research examining the relationship between the nature of OC and ISC. This paper seeks to explore the relationship between the nature of OC and ISC and argues that organizations that have a medium to high security risk profile need to embed the ISC to influence employee actions and behaviours in relation to information security practices. In addition, this paper also introduces a framework to assist organizations in determining the extent to which the desired ISC is embedded into OC.

Keywords

Information security, information security culture, information security policy, organizational culture

INTRODUCTION

Information security problems in organizations have been linked to employee behaviour (Thomson, von Solms, & Louw, 2006; Siponen & Oinas-Kukkonen, 2007; Workman, Bommer, & Straub, 2008) Information Security Forum, November 2000 reported that as many as 80% of major security failures could be the result of poor security behaviour by staff instead of poor security solutions (Leach, 2003). These findings are supported by recent studies where major threat to information security is caused by careless employees who do not comply with organizational information security policies and procedures (Pahnila, Siponen, & Mahmood, 2007; Siponen & Oinas-Kukkonen, 2007; Workman et al., 2008). Therefore, senior management must recognize that information security can no longer solely rely on technical and physical controls. Consequently, several researchers have called for an examination of organizations' culture as a way forward in solving information security problems (Von Solms, 2000; Schlienger, T. & Teufel, 2002, 2003b; Siponen, 2005; Ruighaver, Maynard, & Chang, 2007)

Why do we need to understand OC? OC typically defined by academics as a set of shared values, beliefs, assumptions and practices that shape and direct members attitude and behaviour in the organizations (Denison, 1990; Schein, 1992; Cameron & Quinn, 1999). Therefore, understanding OC may be useful in looking at how employees' behaviour may impact on security practices for a number of reasons. Schein (1992) posited that OC is a powerful, underlying and often unconscious force that establishes employees' behaviours. Thus, the relationship between OC and employees' behaviours should be considered when implementing security practices because it impacts on how employees behave in organizations (Thomson et al., 2006).

Unlike OC as defined by Schein (1992), ISC is "the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds" (Dhillon, 1997). Dhillon (1997) further stressed that if security culture is not prevalent in organizations, it will be problems to maintain the integrity of the organizations and also to protect the technical systems of the organizations. Since 1996, many authors have suggested that ISC needs to be integrated with the OC to guide employee behaviour in maintaining information security (James, 1996; Dhillon, 1997; Andress & Fonseca, 2000; Breidenbach, 2000; Von Solms, 2000). In a recent study, Ramachandran, Srinivasan, & Tim (2008) also identified information security culture (ISC) as the employees' security related beliefs, values, which manifest in employee's actions and behaviours in protecting organizational information.

Through examining the definitions of OC and ISC, there is an argument can be made that the concepts of ISC and OC may be interrelated. Although many researchers have called for the creation of ISC to be embedded into organizations,

nonetheless, a thorough review of the literature suggests that little past research has studied the relationship between the nature of OC and ISC. This paper fills in the gap by exploring the nature of relationship between OC and ISC.

The purpose of this paper is twofold. First, this paper seeks to explore the nature of relationship between OC and ISC. Second, the paper intends to develop the conceptual framework which may assist organizations in determining the extent to which ISC is embedded into OC. Furthermore, this framework may offer suggestions for organizations moving to the desired level of ISC to influence employees' security related actions and behaviours in protecting organizational information according to organizations' priorities.

The rest of the paper is devised into four sections. First, we review previous relevant research on OC and ISC, highlighting the shortages of existing advances. Second, we review and summarise the relationship between OC and ISC. Third, we provide a conceptual framework developed from the literature. In the final section, we make the conclusions, we mention the contribution to body of knowledge and implications to practice, then we discuss research limitation, and at last, we propose the future research direction.

LITERATURE REVIEW

The Impact of Organizational Culture

OC culture refers to the systems of shared beliefs and values that develops within an organization and guides the behaviours of its members to maintain suitable patterns of social systems to form a coordinated behaviour to survive in the dynamic environment (Denison, 1990; Schein, 1992). OC is forms by the behaviours of dominant organizations members like founders and top management (Schein, 1992).

Table 1 - The Organizational Culture Framework (Detert et al., 2000)

1. The basis of truth and rationality in the organization Decision making should rely on factual information and the scientific method. Focuses on the degree to which employees believe something is real or not real and how truth is discovered.
2. The nature of time and time horizon The concept of time in an organization has baring in terms of whether the organization adopt long term planning, strategic planning and goal setting, or focus and reacting on a short time horizon.
3. Motivation Employees are intrinsically motivated to do quality work if the system supports their efforts. Management should identify whether manipulating others' motivation can change effort or output of employees
4. Stability versus change/innovation/personal growth Organizations that are risk-taking always stay innovative with a push for constant, continues improvement. Risk-averse organizations tend to be less innovative, with little push for change.
5. Orientation to work, task, and co-workers The main important issues here is the responsibility employees feel for their position and how they are educated in terms of their roles and responsibility.
6. Isolation versus collaboration/cooperation Cooperation and collaboration (internal and external) are necessary for a successful organization. In some organizations, collaboration is often viewed as a violation of autonomy.
7. Control, coordination, and responsibility A shared vision and shared goals are necessary for organizational success. All employees should be involved in decision making and in supporting the shared vision
8. Orientation and focus-internal and/or external An organization may decide to have internal orientation focusing on people and processes within organization or emphasize on external orientation focusing on external competitive environment, or have combination of both.

Robbins (1989) argued that OC serves a number of functions within organizations. They include a boundary setting role that makes distinctions between organizations. OC facilitates the generation of employees' commitment to organizations and, it enhances social systems stability. According to Robbins (1989) OC helps to bind the organization members by providing accepted standards and rules. It acts as a sense-making and control mechanism that guides and shape attitudes

and behaviours of employees. This paper is interested in the last function of OC and seeks to focus on OC's consequences on organizations' member behaviour. The following section briefly describe why we choose Detert et al (2000)'s framework.

Detert, et al (2000) found that there has been little effort to synthesize the general dimensions of OC, and to identify which of these culture dimensions most related to the change programs to improve in important human and organizational effects. Subsequently, Detert, et al (2000) reviewed the existing repeated emerged OC and developed a set of eight overarching, descriptive dimensions of culture. They linked it to a comprehensive set of values and beliefs that represent the "culture backbone" of successful Total Quality management (TQM) adoption and found the framework explicated well the TQM's framework. The eight dimensions of OC are briefly described in Table 1.

While there are many general frameworks and models of organizational culture available, Detert et al (2000)'s framework was chosen because it review over twenty-five multiconcept frameworks that include Measuring Organizational Culture (Hofstede, Neuijen, Ohayv et al., 1990), Organizational Culture and Leadership (Schein, 1992), and Competing Values (Cameron & Freeman, 1991). We believe and convinced that it consolidated existing organizational culture dimensions compactly into eight descriptive dimensions as in Table 1.

Information Security Culture

The importance of security culture has attracted many researchers in this domain to understand it comprehensively. For example, James (1996) argued that ISC requires imbedding security and protection considerations into OC and management mind-set. Von Solms (2000) suggested "a culture of information security to be created in a company by instilling the aspects of information security to every employee as a natural way of performing his or her daily job" (p618) (Oost & Chew, 2007). In the same vein, Schlienger and Teufel (2002) proposed that "security culture should support all activities in such a way, that information security becomes a natural aspect in daily activities of every employee" (p7). Several authors also argued that ISC is vital in ensuring organizational information security (Vroom & von Solms, 2004; Thomson et al., 2006).

Generally speaking, ISC is often studied from various concepts and models of organizational culture. Based on awareness maturity (Von Solms, 2000); Detert's et al (2000)'s framework (Chia, Maynard, & Ruighaver, 2002); Schein 1992's three-layer model (Schlienger, T. & Teufel, 2003a; Zakaria & Gani, 2003; Thomson et al., 2006); shared values (Helokunnas & Kuusisto, 2003); organization behavior (Martin, 2003); human resource management for education and learning (Leach, 2003; Van Niekerk & Von Solms, 2006); socio technical perspective (Stanton, Stama, Mastrangelob et al., 2005); and Hall's taxonomy (Tejay & Dhillon, 2005) as cited by Ramachandran et al (2008). Although such frameworks provide better understanding on ISC, they present a broad and scattered theoretical field. They create some confusion when trying to review (Oost & Chew, 2007), and lacking of integration across different areas of focus (Sneza, Sharman, & Matthew, 2006). In addition most of the past research simply mentioned the importance of OC in general terms and they do not really look into the relationship between the natures of OC and ISC in depth.

This paper adopts Detert et al. (2000)'s framework. The comprehensiveness of Detert et al., (2000)'s framework convinced (Chia et al., 2002) adopting it to explore and understand organizational security culture. They carried out case studies to show that the identified topics can be used for assessing and developing information security culture for an organization. Subsequently, they used this framework to further perform several case studies to explore the security culture within a few organisations with different levels of security (Chia et al., 2002; Chia, Maynard, & Ruighaver, 2003; Tan, Ruighaver, & Ahmad, 2003; Koh, Ruighaver, Maynard et al., 2005; Maynard & Ruighaver, 2006; Shedden, Ahmad, & Ruighaver, 2006). They found that this framework explained well the level on organization's security culture. However, these case studies performed are in small scale and mostly concentrate on problem of end-users not the relationship between OC and ISC.

In a more recent study, Ruighaver et al., (2007) reviewed and synthesised the resulting insights of the case studies abovementioned and they believe that Detert et al (2000)'s framework adopted to explore ISC is essential and useful. In view of the relevancy and comprehensiveness of Detert et al (2000)'s framework as described above, it is convinced and justified that this paper adopts the framework to explore the relationship between the nature of OC and ISC.

The Challenges of Embedding Information Security Culture

The findings from previous research show that ISC is still not embedded into organizations. Past literature indicates that the key challenges of embedding ISC in organizations are: ISC is not an integral part of OC, difficulty in getting sufficient budget for security activities, locus of responsibility, organizational motivation towards implementing security measures, and the different perceptions towards security risk.

- Not Integral Part of OC

Knapp, Marshall, Rainer et al., (2006) found that information security is not an integral part of most OC. Management of security risks still not prevalent and not comprehensive in the training in most organizations. Furthermore, employees incline to treat information security as troublesome and often resist new policies and associated controls. These findings call for further research as Chia et al., (2003) argued that without an OC to support, the enforcement of these policies would not be optimal.

- Difficulty in Getting Budget

  There is a problem getting sufficient budget from top management in implementing information security practices. For example, Shedden et al., (2006) found organizations are inclined to treat security spending as a cost, and often fight to gain funding for security initiatives. Straub (1986) argued that there is evidence that organizations will only adopt security functions after a major loss from a security incident .Security concern will remain low if there is no major loss due to lack of security. Along the same line, Keefe (1983) found that computer security function may continue difficult to get support from management.

- Locus of Responsibility

  Information security measures are often carried out by only a small group of people. Some researchers found evidences to suggest that only small group is involved in planning, managing and implementing security and lack of social participation in their case study organizations (Chia et al., 2002; Koh et al., 2005)

- Organizational Motivation

  Maynard & Ruighaver (2006) found evidence to suggest that there are number of organizations forced to conform to external audit and government regulation. Therefore, the implementation of security policies may not have derived from a belief in the importance of security practices but a result of external requirements. Hence, employees tend to consider information security as inconvenience and new policies and associated controls are often met with resistance.

- Perceived Risk Profile

  Many companies believe that a security threat level does not warrant financial investment or could reduce efficiency and productivity. As such, they still refuse to apply compulsory automated controls measures (Ong, Tan, Tan et al., 1999).

It seems that there is inconsistency between the calls for the creation of ISC and the findings from the previous researches. For example information security implementation is still does not have full support of OC in terms of getting sufficient budget from management, only a small technical group of people is involved who participates in information security implementation, lacking of management support, and information security risk not in the training schedule.

In summary, reference to OC has found its way into research on ISC. Case studies in ISC repeatedly emphasize the importance and linkage of OC. However, the linkage and importance of OC often with little further elaboration and do not focus heavily on underlying cultural factors. The obvious conclusion is that careful attention must be paid to OC in order to embed ISC successfully. The question remains, what type of cultural environment would be more conducive to influence employees' behaviour for ISC embedding?

THE RELATIONSHIP BETWEEN OC AND ISC

For years, ISC remains as one of the top-ranked concerns of academic researchers and industry practitioners. For example, the Organization for Economic Co-operation and Development (OECD) Council has particularly passed the guidelines for a culture of information security in (OECD, 2002, 2003, 2005). Subsequently, many researchers suggested that ISC should be part of OC and support all activities dealing with information in organizations (Von Solms, 2000; Schlienger, T. & Teufel, 2002, 2003b). Other argued that a utopian ISC would be where employees of the organizations follow information security guides of the organizations voluntarily as part of the OC (Vroom & von Solms, 2004; Thomson & von Solms, 2005; Thomson et al., 2006).

Literature shows that there are three type of relationship between OC and ISC. Type 1: ISC is separated from OC; Type 2: ISC is a subculture of OC; and Type 3: ISC is embedded into OC. Type 1 relationship is the situation where information security is not an integral part of most OC (Chia et al., 2002; Knapp, Marshall, Rainer et al., 2004). Often, organizations members is not involved or at the very minimum level with security implementation in organizations (Chia et al., 2002; Koh et al., 2005). Organizations members have very little knowledge and do not feel that it is their responsibility in security problems. Organizations often tend to view security spending as a cost, and often struggle to gain funding for security initiatives (Shedden et al., 2006). The nature of relationship is the situation where organizations' ISC is totally separate from the OC. The organizations security awareness is low. This is the situation where the information security activity is only taken care by the IT department.

Organizations in type 2 relationship indicate the situation where organizations members within department are more aware of security requirement; intermittent training for security is carried out as adherence to the requirement of management. Management begins to pay more attention towards the implementation of information security practices. However, there is still less interdepartmental coordination in handling organizations information security. Moreover, only small group of people participate or involve in security measures carry out in organizations (Chia et al., 2002). The ISC of organizations is a mix of security subcultures, each accommodating the needs associated with the responsibilities and tasks of the respective professional groups (Ramachandran et al., 2008). ISC is a subculture of OC. The situation is where certain value has been accepted by a very particular group such as accounting department or human resource department.

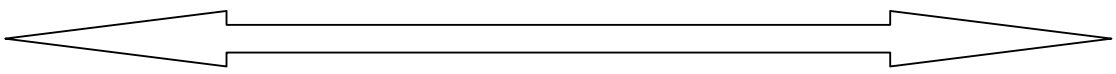
Organizations in type 3 relationship indicate the situation where the organizations' security practices is the responsibility of all members. Implementation of security measures is in a holistic manner and has a relatively high level of involvement. In addition, there are regular updates on security policy. Members of organizations feel ownership of information and they are motivated to adhere to the security policy. ISC is embedded into OC. This nature of relationship is the situation where information security awareness unconsciously becomes daily routine activities (Von Solms, 2000; Vroom & von Solms, 2004; Thomson & von Solms, 2005; Thomson et al., 2006). All members of organization accept the values that ISC will enable thereby allowing organizations to make better decisions in organizational information security.

Interestingly, these three relationship types match the organization cultural views toward information security proposed by (Fitzgerald, 2007). He pointed out that organization cultural views toward information security can be view simplistically as high, moderate, and low. They are briefly described below:

- High. Senior management brings information security into the discussion on new projects. Periodic updates on information security are made to the company board of directors. Employees are aware of the importance of information security and they know how and who to report whenever incidents happened. Yearly budgets are set up with funding levels to endure an ongoing security program. Senior leadership treats security to be a business risk reducer and strongly keeps on security efforts through participation, funding, and authorisations.
- Moderate. Employees have received some training on information security. Information security role has been assigned to a person as suggested by regulator or auditor. Security policies are created by IT department but, it may not have strong support. Employees do not know where they are located. Senior management has typically assigned the job of information security to the Chief Information Officer. An individual is assigned for information security and mainly consists of security administration operational activities like password resets and account creation of account for new employee.
- Low. Typically, information security policies may be created by coping but not serious in enforcing them. Usually, these policies will be issued by a memo whenever an incident has taken place like no sharing password. Although senior management knows that information security is important, nonetheless it assigns the same level of importance as making sure that computer is running. There is no special fund for information security and is usually part of a budget for IT support.

FRAMEWORK OF THE RELATIONSHIP BETWEEN OC AND ISC

Information security culture continues to grow in importance as more and more organizations rely on interconnectivity and information to gain competitiveness in this dynamic environment. Therefore, organizations need an ISC to guide the actions and behaviours of employees in protecting organizations' information. The understanding from literature and the cultural views by Fitzgerald (2007) constitutes three natures of relationships between OC and ISC as depicted in Table 2. They can be considered in continuum ranging from ISC not part of OC to ISC embedded completely into OC as depicted in Figure 1 below:



ISC is not part of OC ISC embedded completely into OC

Figure 1- The continuum of ISC embedding in organizations

Table 2: Framework of the Relationship between OC and ISC

Nature of Relationship	Organizational Culture (OC)	Employees Beliefs, Actions and Behaviours (ISC)	Probable Consequences
Type 3 relationship: where ISC is embedded into OC. (Von Solms, 2000; Schlienger, T. & Teufel, 2002; Thomson et al., 2006) **High** (Fitzgerald, 2007)	**Management Involvement:** Management bring security matters and strategy into board meeting. Updates are made on a periodic basis to the company board of directors **Locus of Responsibility:** Management involves every member of organizations. **Information Security Policy**: Created in holistic manners. In addition, there are regular updates on security policy. **Education/Training:** Management make the awareness program compulsory for all the employees. **Budget Practice:** Management allocates budget for security activities annually.	**Responsibility:** Always adhere to the security procedures and guides **Participation:** Employees undergo periodic security training, awareness programme C**ommitment:** Employees feel responsible and ownership of information. **Motivation:** Motivated and committed towards security matters **Awareness/Know how:** Know how and who to deal with when facing security problems	**Risk Vulnerability:** Low **Awareness:** Employees are highly aware and concern about security matters in organization. **Responsibility:** Security is every employee's business **Security Practices:** Holistic manners. Unconsciously become daily routine activities **Investment for security practices:** High cost in implementing security activities
Type 2 relationship: where ISC is a subculture of OC (Dutta & McCrohan, 2002; Ramachandran et al., 2008). **Moderate** (Fitzgerald, 2007)	**Management Involvement:** Management typically delegates understanding of information security matters to CIO. **Locus of Responsibility**: Management starts to empower security matters to head of dept. **Information Security Policy**: Created within IT department and may not have widespread support or knowledge of where they are located **Education/Training:** Management starts to pay attention to awareness. People receive some training of information security **Budget Practice:** Management acts promptly towards expenses pertaining security activities	**Responsibility:** Adhere to security matters as a requirement of management **Participation:** Employees are involved in security matters in own dept. Less interdepartmental coordination. **Commitment:** Responsible and committed in security matters for own dept. **Motivation:** Employees are motivated in security matters in own dept. **Awareness/Know how:** Know how and who to deal with when facing security problems within dept.	**Risk Vulnerability:** Medium **Awareness:** Employees are aware of security matters within their own dept **Responsibility:** Employees are responsible for security matters within own dept. **Security Practices:** Security is employees' routine activities within own dept. **Investment for security activities:** Medium cost in implementing security activities
Type 1 relationship: where ISC is separated from OC (Chia et al., 2002; Knapp, Marshall, Rainer et al., 2004; Shedden et al., 2006) **Low** (Fitzgerald, 2007)	**Management Involvement:** Management intuitively knows that information security is important, but it assigns the same level of importance as ensuring that computer is up **Locus of Responsibility:** Management assigns all the security responsibility to IT department. **Information Security Policy**: Created by copying without the means to enforce them. Usually issued by a memo. **Education/training** Low awareness. Management does not emphasize on security training. **Budget Practice:** Usually part of a budget for IT support.	**Responsibility:** Do not care and not responsible towards security matters **Participation:** Employees are not involved in security matters **Commitment:** Employees leave it to IT dept. Always bypass security procedures. **Motivation:** Employees are not motivated in dealing with security matters **Awareness/Know how:** Do not know what to do when facing with security problems	**Risk Vulnerability:** High **Awareness**: No awareness in security matters **Responsibility:** Only IT dept is responsible for security matters **Security Practices:** Not a routine activity of employees **Investment for security activities:** Low cost in implementing security activities

Table 2 is the framework derived from the past literature and cultural views by (Fitzgerald, 2007) . Basically, first column shows that it contains three natures of relationships and its relationship can be considered continuum ranging from ISC not part of OC to ISC embedded completely into OC.

Second column of Table 2 shows the organizational culture towards information security practices in organizations. Again, the level of management participation and supports in terms of setting up security strategy, assignment of responsibility, participation, provision of training, and establishment of budget can be ranged from low to high.

Third column indicates the employees' action and behaviours in relation to information security practices. At the level where ISC is separated from OC, employees do not care and responsible towards security matters. Employees do not involved in security matters and they always leave the security issues to IT department. They do not know how to do and what to do when facing with security issues. At the opposite extreme where ISC is completely embedded into OC, the employees always adhere to information security policies, and procedures. Employees undergo periodic security training programme. They feel responsible and ownership of information and committed toward security matters. They know what to do and whom to report to when facing security problems.

The fourth column demonstrates the probable consequences that organizations facing depending on their current position in Table 2. Those organizations where ISC is separated from OC may have lowest costs in implementing security measures, but, at the same time they are facing highest vulnerability. On the other hand, organizations where ISC is completely embedded into OC may have the lowest risk vulnerability, and involving high costs in implementing security measures.

Theoretically, in order to embed ISC in OC in Table 2, all the organizations members must accept the importance of ISC. If these values are proven to be able to guide employees' actions and behaviours in relation to information security practices then it will strengthen organizational values and became an integral part of work practices in protecting organizations' information. Tipton (2007) also argued that with the proper focus, organizations can move quickly from low to high security cultural levels.

However, this is not the case from the past literature which found that information security is still not an integral part of OC (Knapp et al., 2006). Also, there is none of the firms had reached the institutionalization wave of the information security during information security assessments in Small Medium Enterprises in Tampere region in Finland (Helokunnas & Kuusisto, 2003). Question remains why ISC still not completely embedded into organizations.

CONCLUSION

Each organization has different priorities, and the current organizational culture may decide the desired level of ISC (Fitzgerald, 2007). However, real security culture lies in the security related beliefs, values, which manifest in employee's actions and behaviours towards information security problems (Stan, 2007). Therefore, organizations need to carefully think about the desired level of ISC to influence their employees' behaviour to protect organizational information. The effectiveness of an information security program has to depend on the behaviour of people (Stan, 2007).

This paper explored the nature of relationship between OC and ISC and conceptually developed a framework of the relationship between ISC and OC. It focused on how organizations should increase the embedding of ISC into OC. The ISC and OC relationship framework may assist organizations in determining the extent to which ISC is embedded into OC. This framework offer suggestions for organizations moving to the desired level of ISC to enhance employees' security related actions and behaviours in protecting organizational information according to organizations' priorities. Nonetheless, one must also remember that ISC is always regarded as a complex system and it take times to develop. It can only be developed over time by influencing employees' related beliefs, values and behaviours.

Theoretically, we believe that this paper has provided better understanding of the relationship between OC and ISC and contributed to existing ISC knowledge and research. Practically, the framework of relationship between OC and ISC offer suggestions for organizations moving to the desired level of ISC to influence employees' related security actions and behaviours in protecting organizational information.

The main limitation of a framework that is derived from existing literature is that it is not fully tested and may defer from industry to industry. Furthermore, the derivation of this framework does not take into consideration of different industries. Literature shows that different industries tend to differ in terms of their requirement for information security needs (Jung, Han, & Lee, 2001; Yeh & Chang, 2007). Similarly, several researchers also found that financial organizations undertake more hindrance efforts and have stronger deterrent than other industries (Kankanhalli, Teo, Tan et al., 2003; Davamanirajan, Kauffman, Kriebel et al.,2006). In contrast, manufacturing firms only focus on internal

operations and thus require lower strategy-level IS application (King, 1994). This low strategy-level IS application also means low security measures.

Future research should populate and validate the components of the framework by conducting case studies to explore the security culture within few organisations from different industries with different levels of security. Future research also should look into change programs of how to move from low level of ISC to high level of ISC to influence employees' security related actions and behaviours in protecting organizational information.

REFERENCES

Andress, M., & Fonseca, N. (2000). Manage People to Protect Data. *Infoworld, 22*(46), 48.

Breidenbach, S. (2000). *How Secure Are You*. Information Week 2000;800:71-8

Cameron, K. S., & Freeman, S. (1991). Cultural Congruence, Strength and Type: Relationships to Effectiveness. . *Research in Organizational Change and Development, 5*, 23-58.

Cameron, K. S., & Quinn, R. E. (1999). *Diagnosing and Changing Organizational Culture.* Reading: Addison-Wesley.

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). *Understanding Organizational Security Culture.* In Proceedings of PACIS2002. Japan, 2002, Japan.

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2003). *Understanding Organisational Security Culture. In: Hunter Mg, Dhanda Kk, Editors. Information Systems: The Challenges of Theory and Practice.*, Las Vegas, USA: Information Institute; 2003.

Davamanirajan, P., Kauffman, R. J., Kriebel, C. H., & Mukhopadhyay, T. (2006). Systems Design, Process Performance, and Economic Outcomes in International Banking. *Journal of Management Information Systems 23*(2), 65-90.

Denison, D. R. (1990). *Corporate Culture and Organizational Effectiveness*. New York: Wiley (New York).

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A Framework for Linking Culture and Improvement Initiatives in Organisations. *Academy of Management Review, 25*(4), 850-863.

Dhillon, G. (1997). *Managing Information System Security*. Houndmills, Basingstoke, Hampshire: Macmillan Press LTD.

Fitzgerald, T. (2007). Building Management Commitment through Security Councils, or Security Council Critical Success Factors. In H. F. Tipton (Ed.), *Information Security Management Handbook* (pp. 105-121). Hoboken: Auerbach Publications.

Hall, E. T. (1959). *The Silence Language Anchor Books*. Garden City, NY.

Helokunnas, T., & Kuusisto, R. (2003). *Information Security Culture in a Value Net.* In Engineering Management Conference, 2003. IEMC'03. Managing Technologically Driven Organizations: The Human Side of Innovation and Change.

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring Organizational Cultures: A Qualitative and Quantitative Study across Twenty Cases. *Administrative Science Quarterly, 35*(2), 286-316.

James, H. L. (1996). Managing Information Systems Security: A Soft Approach. *IEEE*.

Jung, B., Han, I., & Lee, S. (2001). Security Threats to Internet: A Korean Multi-Industry Investigation. *Information & Management, 38*, 487-498.

Keefe, P. (1983). Computer Crime Insurance Available-for a Price, . *Computerworld,* 20-21.

King, W. R. (1994). Organizational Characteristics and Information Systems Planning: An Empirical Study. *Information Systems Research*, 75-109.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information Security: Management's Effect on Culture and Policy. *Information and Computer Security, 14*(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2004). *Top Ranked Information Security Issues.* In The 2004 International Information Systems Security Certification Consortium (ISC)2 Survey Results., Alabama: Auburn University.

Koh, Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). *Security Governance: Its Impact on Security Culture*.

Kropp, R. (2004). The Importance of Organisational Culture. *Advanced Management Sciences, Inc.*

Leach, J. (2003). Improving User Security Behaviour. . *Computer & Security, 22*(8), 685-692.

Martin, A., & Eloff, J. (2003). *Information Security Culture.* In Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt.

Maynard, S. B., & Ruighaver, A. B. (2006). *What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality.* In Proceedings of the fifth annual security conference, Las Vegas, Nevada USA.

Mohr, J. J. (1996). The Management and Control of Information in High Technology Firms. *The Journal of High technology Management Research, 7*(2), 245-268.

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Adopted as a Recommendation of the OECD Council at Its 1037th Session on 25 July 2002*. Retrieved 9 March, 2009

OECD. (2003). *Implementation Plan for OECD Guides for the Security of Information Systems and Networks: Towards a Culture of Security (02-July-2003)*. Retrieved 9 March 2009, from http://www.oecd.org/dataoecd/23/11/31670189.pdf

OECD. (2005). *The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries (16-December-2005).* Retrieved 9 March 2009, from www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

Ong, T.H.,Tan, C.P.,Tan,Y.T., & Ting, C. *Snms-Shadow Network Management System. In Symposium on Network Computing and Management.*, 1-9 (1999).

Oost, D., & Chew, E. (2007). *Investigating the Concept of Information Security Culture*: UTS: School of Management Working Paper: No. 2007/6.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' Behavior Towards Is Security Policy Compliance.* In Proceedings of the 40th Hawaii International Conference on System Sciences - 2007, Hawaii.

Ramachandran, S., Srinivasan, V. R., & Tim, G. (2008). *Information Security Cultures of Four Professions: A Comparative Study.* In Proceedings of the 41st Hawaii International Conference on System Sciences - 2008, Hawaii.

Robbins, S. P. (1989). *Organizational Behavior: Concepts, Controversies, and Applications* (Fourth Edition ed.). New Jersey: Prentice Hall.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational Security Culture: Extending the End-User Perspective. *Computers & Security, 26*(1), 56-62.

Schein, E. H. (1992). *Organizational Culture and Leadership*: San Francisco: Jossey-Bass,.

Schlienger, T., & Teufel, S. (2002). *Information Security Culture - the Social-Cultural Dimension in Information Security Management.* In IFIP TC11 International Conference on Information Security, Cairo, Egypt.

Schlienger, T., & Teufel, S. (2003a). *Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture.* In 14th International Workshop on Database and Expert Systems Applications (DEXA'03).

Schlienger, T., & Teufel, S. (2003b). *Information Security Culture - from Analysis to Change*.

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2006). *Risk Management Standard-the Perception of Ease of Use.* In Proceedings of the fifth annual security conference, Las Vegas, Nevada, USA.

Siponen, M. (2005). Analysis of Modern Is Security Development Approaches: Towards the Next Generation of Social and Adaptable Iss Methods. *Information and Organization, 15*(4), 339-375.

Siponen, M., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions *SIGMIS Database, 38*(1), 60-80.

Sneza, D., Sharman, L., & Matthew, J. W. (2006). Fostering Information Security in Small and Medium Size Enterprises (pp. 1560-1571).

Stan, S. (2007). Beyond Information Security Awareness Training: It Is Time to Change the Culture. In H. F. Tipton (Ed.), *Information Security Management Handbook* (pp. 555-565). Hoboken: Auerbach Publications.

Stanton, J. M., Stama, K. R., Mastrangelob, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *Computer and Security, 24*(2), 124-133.

Straub, D. (1986). Deterring Computer Abuse: The Effectiveness of Deterrent Countermeasures in the Computer Security Environment. Bloomington, IN: Indiana University School of Business, .

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2003). *Incident Handling: Where the Need for Planning Is Often Not Recognised*.

Tejay, G., & Dhillon, G. (2005). Developing Measures of Information Security, *The Fourth Workshop on e-Business (WeB 2005)*. Las Vegas.

Thomson, K., & von Solms, R. (2005). Information Security Obedience: A Definition. *Computers & Security, 24*(1), 69-75.

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an Organizational Information Security Culture. *Computer Fraud & Security, 2006*(10), 7-11.

Tipton, H. F. (2007). *Information Security Management Handbook* Hoboken Auerbach Publications.

Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework *Information Security South Africa (ISSA), Johannesburg , South Africa*.

Von Solms, B. (2000). Information Security -- the Third Wave? *Computers & Security, 19*(7), 615-620.

Vroom, C., & von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computers & Security, 23*(3), 191-198.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Security Journal: A Global Perspective, 16*(6), 315-331.

Workman, M., Bommer, W., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior*.

Yeh, Q. Y., & Chang, J. T. (2007). Threats and Countermeasures for Information Systems Security: A Cross-Industry Study. *Information & Management, 44*, 480-491.

Zakaria, O., & Gani, A. (2003). *A Conceptual Checklist of Information Security Culture.* In 2nd European Conference on Information Warfare and Security, Reading, UK.

COPYRIGHT