# COMPARATIVE STUDY: THE RELATIONSHIP BETWEEN ORGANIZATIONAL CULTURE AND INFORMATION SECURITY CULTURE

**Lim Joo Soon**[1]

## ABSTRACT

*Employee behavior has been identified to be a major problem in managing Information Security as people are both a cause of information security incidents as well as a key part of the protection from them. The culture of the organization to a large extent shapes the behaviour of individuals and groups in organizations. As such, many researchers have called for the creation of information security culture (ISC) in organizations to influence the actions and behaviours of employees to better protect organizational information. Although researchers have called for the creation of ISC to be cultivated in organizations, however, little past research examining the relationship between organizational culture (OC) and ISC. Therefore, this paper fills in the gap by examining the relationship between OC and ISC and contends that organizations that have a medium to high security risk profile need to cultivate the ISC to influence employee actions and behaviours to protect organizational information. Additionally, this paper also develops a framework to help organizations in determining the levels of the desired ISC cultivated in organizations.*

***Keywords:*** *Organizational Culture, Information Security, Information Security Culture, Information Security Policy.*

## INTRODUCTION

Employee behaviour has been identified to be a key problem in managing organization's information security (Lim, Chang, Ahmad, & Maynard, 2012; Lim & Lim, 2014; M. Siponen & Oinas-Kukkonen, 2007; Workman, Bommer, & Straub, 2008). The annual CSI Computer Crime and Security (2007) Survey reported that insider threat was cited by 59 percent of respondents, surpassing virus attacks as the most reported security incident (Richardson, 2007). These findings are consistent with the findings of recent studies where major threat to information security is caused by careless employees who failed to comply with information security policies and procedures in organisations (Lim, et al., 2012; Lim & Lim, 2014; M. Siponen & Oinas-Kukkonen,

[1] Dr Lim Joo Soon is a Superintendent of Police at Royal Malaysia Police Force. Email: unimelbourne.lim@gmail.com.

2007; Workman, et al., 2008). As such, top management must accept that information security should consider other measures beside technical and physical controls. Subsequently, many researchers have demanded an examination of organizations' culture to solve information security problems (Lim, et al., 2012; Lim & Lim, 2014; Ruighaver, Maynard, & Chang, 2007; M. Siponen, 2005; Von Solms, 2000)

The call for an examination of OC to solve information security is because the culture of the organization to a large extent shapes the behaviour of individuals and groups in organizations. There are plethora definitions of OC. It is 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; Detert, Schroeder, & Mauriel, 2000; Hofstede & Hofstede, 2005; Schein, 1992). Logically, understanding OC may be helpful in understanding how employees' behaviour may impact on security practices to better protect organizational information. Schein (1992) contended that OC is a powerful, underlying value and has huge impact on employees' behaviours. Therefore, the relationship between OC and ISC should be considered because ISC impacts on how employees behave in relation to the implementation of security practices in organizations (Lim, Ahmad, Chang, & Maynard, 2010; Lim, et al., 2012; Thomson, von Solms, & Louw, 2006).

Like OC, past literature indicates that there are many definitions of ISC. ISC has been defined by Dhillon (1997) as "the totality of patterns of behaviour in an organization that contributed to the protection of information of all kinds". Dhillon (1997) further asserted that if security culture is not widespread in organizations, it will be a problem to maintain the integrity of the organizations and also to protect the technical systems of the organizations. Since 1997, many researchers have suggested that ISC needs to be cultivated into OC to guide employees behaviour in implementing information security (Dhillon, 1997; Schlienger & Teufel, 2002; Von Solms, 2000). In a more recent study, Lim (2012) defined ISC as the shared beliefs, values, behaviours, and actions held by employees in relation to the implementation of information security to protect organizational information.

Discussion on the definitions of OC and ISC need to be further enhanced and analysed. It is reasonable to argue that the concepts of ISC and OC may be interrelated. While many researchers have demanded for the creation of ISC to be cultivated into OC, nevertheless, a careful review of the past literature indicates that little has studied the relationship between the OC and ISC. As such this paper bridges the gap by examining the nature of relationship between OC and ISC.

First, this paper aims to examine the nature of relationship between OC and ISC. Second, the paper plans to develop the conceptual framework which may assist organizations in determining the desired ISC levels in organization. Additionally, this

framework may provide suggestions for organizations in enhancing to the desired level of ISC to influence employees' shared security beliefs, values, behaviours and actions to protect organizational information according to the security needs. The rest of the paper is divided into four sections. First, the author reviews prior relevant literature on OC and ISC, highlighting the gap in existing advances. Second, the author reviews and summarises the relationship between OC and ISC. Third, the author provides a conceptual framework synthesised from the past literature. In the final section, the author makes the conclusions; the author discusses the contributions, and concludes by discussing further research direction in the area.

## ORGANIZATIONAL CULTURE

There are plethora definitions of culture. Ouchi and Johnson (1978) define culture as how things are done around here. Various researchers, however, have defined culture as the system of shared beliefs, values, customs, behaviours and artefacts, which members of the society or organisation use to cope with their world and with one another. OC creates both stability and adaptability by being the glue that holds the organisation's members together (Schein, 1992).

Thus far, the culture perspective has focused on the basic values, beliefs, and assumptions that are present in organisations (Schwartz & Davis, 1981; Denison, 1990; O'Reilly, 1996; Buch & Wetzel, 2001; Kropp, 2004). These underlying values have an influence on the behaviour of organisational members, as people rely on these values to guide their decisions and behaviours (Schein, 1992; 2004). From the prior research, the majority of researchers have taken the functional sociological perspective (Hofstede, 1980; Denison, 1990; Schein, 1992; Brown, 1998; Cameron & Quinn, 1999a; Detert et al., 2000). Culture has been treated as a permanent set of values, beliefs, and underlying assumptions that exemplify organisations and their members. The adoption of these definitions is important to distinguish the concept of organisational culture from organisational climate. Organisational climate refers to more temporary attitudes, and perceptions on the part of individuals (Denison, 1996).

Similarly Robbins (1989) has taken the functional sociological perspective and argued that OC serves a number of functions within organizations, which includes a boundary setting role that makes distinctions between organizations. OC facilitates the generation of employees' commitment to organizations and, it enhances social systems stability. Furthermore, Robbins (1989) contended that OC helps to bind the organization members with accepted norms and values. OC also works as a sense-making and control mechanism that guides and shapes employees' beliefs, values, behaviours, and actions in organizations.

From the discussion above, while there seem to be multiple definitions of OC, but most researchers agree that culture consists of some combination of artefacts, values and beliefs, and underlying assumptions that organisational members share about appropriate behaviour (Schein, 1992; Denison, 1996; Detert et al., 2000). OC refers to the theme that connects the beliefs and behaviours in the synthesized, helps employees make sense of the functioning of the firm and provides norms for their behaviour in the firm. This paper is interested in the function of OC that works as a sense-making and control mechanism that guides and shape employees beliefs, values, behaviours, and actions in organizations. This paper intends to focus on OC's consequences on organizations' members behaviour. The next section briefly describe why the author chooses Detert et al (2000)'s framework.

There has not been much work and effort to synthesize the dimensions of OC, and to categorize which of these culture dimensions most associated with the change programs to improve in employees and organizational effects (Detert, et al., 2000). Subsequently, Detert, et al (2000) synthesized the frequently emerged OC and developed a set of eight overarching, descriptive dimensions of culture. They connected it to a set of values and beliefs that represent the "culture backbone" of successful Total Quality Management (TQM) adoption and found that the framework explained well the TQM's framework. The eight dimensions of OC are described in Table 1 below.

**Table 1: The Organizational Culture Framework**

| No. | Dimensions | Descriptions |
|---|---|---|
| 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/ personel growth | Organizations that are risk-taking always stay innovative with a push for constant, continues improvement. Riskaverse organizations tend to be less innovative, with little push for change. |

**Table 1: The Organizational Culture Framework *(Cont.)***

| No. | Dimensions | Descriptions |
|---|---|---|
| 5. | Orientation to work, task, and coworkers | 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. |

Source: Detert, et al., 2000

Although past literature provides many general frameworks and models of organizational culture, Detert et al (2000)'s framework was preferred because it synthesised over twenty-five multi-concept frameworks that comprise Measuring Organizational Culture (Hofstede, Neuijen, Ohayv, & Sanders, 1990), Organizational Culture and Leadership (Schein, 1992), and Competing Values (Cameron & Freeman, 1991). The author believes and convinced that it fused existing organizational culture dimensions solidly into eight descriptive dimensions as in Table 1.

## INFORMATION SECURITY CULTURE

Information security culture is crucial to support and guide security practices to improve organisations' information security (Dhillon, 1997; Lim, et al., 2010; Lim, et al., 2012; MikkoSiponen & Willison, 2009; Von Solms, 2000). Information security is most efficient when management of information security are entirely woven into the organisational culture (Allen & Westby, 2007). Culture will develop and uphold the bonds between people, technology, and processes. In time, the culture of information security will prevail when it becomes natural employee behaviour in relation to improving the organisation's information security.

Past literature claims that security culture is still a new and emerging area of research (Ruighaver et al., 2007; Ramachandran et al., 2008). It was late in the twentieth century that researchers (Dhillon, 1995; James, 1996; Chia et al., 2002a) began to recognise the importance of a sufficient security culture in improving organisations' information security. Over the past decade, security culture has been among the top concerns of researchers and practitioners in the domain of information security (Oost & Chew, 2007). For example, Von Solms (2000)'s institutionalisation wave aimed to create a security culture so that it could become part of natural employee behaviour to improve organisations' information security.

The significance of ISC from discussion above has drawn many researchers in information security to comprehend it comprehensively. For example, Von Solms (2000) contended that "a culture of information security to be cultivated in organizations 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). Similarly, 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 (Lim & Lim, 2014; Ruighaver, et al., 2007). Broadly speaking, ISC is often examined from different concepts and models of organizational culture. Based on Detert et al., (2000)'s framework (Lim, et al., 2010; Lim, et al., 2012; Ruighaver, et al., 2007);

Schein 1992's three-layer model (Thomson, et al., 2006; Van Niekerk & Von Solms, 2009; Zakaria & Gani, 2003); shared values (Helokunnas & Kuusisto, 2003); human resource management for education and learning (Van Niekerk & Von Solms, 2006); and Hall's taxonomy (Tejay & Dhillon, 2005) as adopted by Ramachandran et al (2008). While these frameworks and models offer better understanding on ISC, they demonstrate a broad and scattered theoretical field. They generate some confusion when trying to review (Lim, Chang, Maynard, & Ahmad, 2009; Oost & Chew, 2007). Additionally most of the past literature briefly mentioned the importance of OC in general and they do not examine in depth into the relationship between the nature of OC and ISC.

To examine the relationship between the nature of OC and ISC, this article adopts Lim et al (2012)'s security culture framework. The framework is evolved from Detert et al., (2000)'s OC framework. The comprehensiveness of Detert et al., (2000)'s OC framework convinced (Chia, Maynard, & Ruighaver, 2002) adopting it to explore organizational security culture. Chia et al., (2000) performed case studies to demonstrate that the identified dimensions can be used for assessing and cultivating ISC in organizations. Subsequently, they adopted the framework to carry out several

case studies to examine the security culture in a few organisations (Chia, et al., 2002; Chia, Maynard, & Ruighaver, 2003; Koh, Ruighaver, Maynard, & Ahmad, 2005; Maynard & Ruighaver, 2006; Ruighaver, et al., 2007). They established that the framework explicated well the different levels of ISC in organizations. Nevertheless, they merely performed small scale case studies and mostly concentrate on problem of end-users not the relationship between OC and ISC.

Therefore, Lim et al (2012) advanced their findings by performing more case studies focusing on the nature of ISC characteristics rather than on problem of end-users. Lim et al., (2012) reviewed and synthesised the resulting insights of the case studies above mentioned and they believe that Detert et al (2000)'s framework adopted to explore ISC is useful and vital in understanding ISC. In consideration of the exhaustiveness of Lim et al., (2012)'s security culture framework, it is convinced and justified that this paper adopts the framework to explore the relationships between the nature of OC and ISC. The eight dimensions of ISC are described in Table 2 below.

**Table 2: The Security Culture Framework**

| No. | Dimensions | Descriptions |
|---|---|---|
| 1. | Evidence-based decision making | Decision-making should rely on factual information, not on opinion. Organisations should make security decisions that are driven by data and analysis. |
| 2. | Long-term plan | Organisation's information security should be driven by longterm stable improvement goals. Short-term sacrifices especially in employees' efforts and time may be necessary. |
| 3. | Proper systems and processes | Organisations need to provide proper systems and processes to motivate employees to adhere to security policies and procedures. This value notes the importance of focusing on processes rather than people as the source of most errors. Employees will be intrinsically motivated to do a good job if they work in an environment without fear and have good systems in place. |
| 4. | Continuous change and improvement | Top management and employees in the organisations should devote time and energy to make things better. This is a neverending process. People should be willing to take risks associated with making change. |
| 5. | Employee Involvement | Organisations should involve employees in improving information security. Organisations should empower employees with real responsibilities so to create a sense of ownership and initiative. Top management should consider employee feedback in making security decisions |

**Table 2: The Security Culture Framework *(Cont.)***

| No. | Dimensions | Descriptions |
|---|---|---|
| **6.** | Collaboration and cooperation | Organisations should engage all departments to improve information security. There are ongoing collaborative work security practices across departments. Employees should not be left to do their own work but also cooperate to improve organisational information. |
| **7.** | A shared security vision | Organisations should have a shared security vision that is agreed upon and all staff members should work together to achieve the agreed shared vision. |
| **8.** | Internal and external focus | Organisations should have a balance of internal and external focus in relation to information security. The underlying value of this dimension is that organisations should focus on internal processes and external requirements to improve information security. |

Source: Lim, et al., 2012

## The Issues of Information Security Culture

Past research indicates that ISC is still not prevailing in most of the organizations (Lim, et al., 2010; Lim, et al., 2009). Prior literature indicates that the key issue of cultivation of ISC in organizations is ISC is not an integral part of 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 (K.J. Knapp, Marshall, Rainer, & Ford, 2005; K.J. Knapp, Marshall, Rainer, & Ford, 2006).

IT department and information security teams are also facing problems in getting sufficient allocations from senior management in implementing information measures. Often, organizations are treating security spending as a cost (Shedden, Ahmad, & Ruighaver, 2006). Along the same line, there is indication that organizations will only implement security measures after a major loss from a security incident (Straub, 1986) .Security concern will remain low if there is no major loss due to lack of security.

Prior literature also found that organizations often engage a small group of people in implementing information security measures. Several researchers found indication to suggest that only a small group is involved in information security management and governance and lack of social participation in their case study organizations (Koh, et al., 2005; Lim, et al., 2010; Lim, et al., 2009)

From the above prior literature, it demonstrates that organizations have still not fully cultivated ISC. Since ISC is still new and emerging, the authors conclude that organizations need to understand the nature of ISC to cultivate in organizations. From the review, the author concludes that reference to OC has found its way into research of ISC. Past literature in ISC often give emphasis on the importance and connection of OC. Nevertheless, the relationship and importance of OC provided often lack of details and do not focus on fundamental cultural characteristics. The obvious conclusion is that careful attention must be paid to OC in order to cultivate ISC successfully. The question remains, what type of cultural environment would be more conducive to develop ISC to influence employees' behaviour to protect organizational information?

## THE RELATIONSHIP BETWEEN OC AND ISC

Over the past decade, security culture has been among the top concerns of researchers and practitioners in the domain of information security (Lim, et al., 2010; Lim, et al., 2009; Oost & Chew, 2007). Past researchers have contended that security culture is important in influencing employees' behaviour in implementing security practices to protect organizational information and should be part of the routine activity of each employee (Lim, 2012; Lim & Lim, 2014; Thomson, et al., 2006; Von Solms, 2000). Several researchers suggested that ISC should be part of OC and support all activities dealing with information in organizations (Schlienger & Teufel, 2003; Thomson, et al., 2006; Von Solms, 2000) For practitioners, the Organization for Economic Cooperation and Development (OECD) Council and SANS have passed special guidelines for developing a culture of information security to improve security practices (OECD, 2002, 2003, 2004, 2005; SANS, 2005). While past researchers have called for ISC to be part of OC, nevertheless little has provided the details of the nature of relationships between the two.

According to Lim et al., (2009), prior literature indicates that there are three types 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 cultivated into OC. Lim et al (2009) further contends that Type 1 relationship is the situation where information security is not an integral part of most OC. In this relationship, often, organizations members are not involved or at the very minimum level with security implementation in organizations (Chia, et al., 2002; Koh, et al., 2005). Senior management mainly gives priority to train IT personnel in information security related matters and non IT personnel have very low level of awareness in relation to security problems. Senior management seldom allocate sufficient budget for security activities and often assume security activities as a cost rather than investment (Shedden, et al., 2006). Type 1 relationship

is the situation where organizations' ISC is totally separate from the OC. This is the situation where the information security activity is only taken care by the IT department (Lim, et al., 2009).

As for Type 2 relationship, organizations' employees have higher level of awareness towards security requirement; intermittent training for security is carried out as adherence to the requirement of management (Lim, et al., 2009). Senior management are more interested and pay more attention to the implementation of information security initiatives. However, Lim et al., (2009)'s argued that there is still less interdepartmental collaboration and cooperation in dealing with organizational information security. Furthermore, senior management merely engage a small group of people to participate in security measures (Chia, et al., 2002; Lim, et al., 2009). In this Type of relationship, ISC is a mix of security subcultures, each obliging the needs of the respective professional groups (Ramachandran, et al., 2008). ISC is a subculture of OC. Lim et al (2009)'s argues that the situation is where certain value has been acknowledged by a particular group (for example accounting department or human resource department) on the importance of ISC in protecting departments' information.

For Type 3 relationship, organizations' security initiative is carried out in a holistic manner, and it is a responsibility of all employees. Organizations' employees are made compulsory to attend security training and security policies are reviewed and updated from time to time (Lim, et al., 2009). ISC is cultivated into OC and organizations members feel responsible and they are motivated to comply with the security policies and procedures. This type of relationship is where information security awareness becomes daily routine activities of employees (Lim, et al., 2009; Thomson & von Solms, 2005; Thomson, et al., 2006; Von Solms, 2000). Organizations' members recognize that ISC will help organizations to make better decisions in relation to information security.

Interestingly, Lim et al (2009) synthesised and found that these three relationship types match the organization cultural views on information security proposed by (Fitzgerald, 2007). According to Fitzgerald (2007), the organization cultural views towards information security can be considered as high, moderate and low. These cultural views can be described as below:

- High – Top management discusses information security projects during meetings. Information security team briefs information security matters to the board of directors. Organizations employees have a high level of security awareness and know how in relation to information security related matters. There are sufficient budget allocated for information security initiatives.

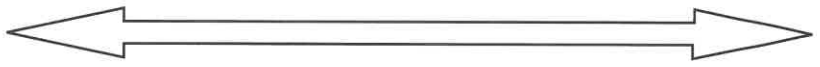
Top management knows the importance of information security and treats security as a business risk reducer.

- Moderate – Organization employees have a medium level of security awareness and have participated in security awareness programs and trainings. There is a specific assignment of security role and responsibility as required by a regulator or auditor. IT department is responsible for developing security policies and it may not necessarily communicate to other departments. Top management has assigned the Chief Information Officer to be responsible for information security related matters.

- Low – Top management has never discussed information security projects during meetings. Organization members have low level of security awareness and they would leave the security problems to IT department. Security policies and procedures may be created but are not serious in enforcing them. Typically, IT department will send out security policies by memo to organization members whenever there is a security incident. Top management may know information security is important, however, they are more concern about the operational aspects of computers. Top management will not allocate a budget for information security initiatives.

## FRAMEWORK OF THE RELATIONSHIP BETWEEN OC AND ISC

In this interconnected world, more and more organizations are connected to internet to gain competitiveness in the dynamic environment. As such more organizations are vulnerable and exposed themselves to be attacked by hackers as the internet was originally conceived as an open, loosely linked computer network that enables unscrupulous hackers and scam artists to intercept and change the information. Therefore, information security culture continues to grow in importance 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 3. They can be considered in continuum ranging from ISC is not part of OC to ISC fully cultivated into OC as depicted in Figure 1 below:



ISC is not part of OC ISC cultivated fully into OC

**Figure 1: The continuum of ISC cultivating in organizations**

**Table 3: Framework of the Nature of Relationships between Organizational Culture and Information Security Culture**

| Organizational Culture (OC) | Information Security Culture (ISC) | Nature of Relationship | Probable Consequences |
|---|---|---|---|
| 1. The basis of truth and rationality in the organization - **Decision making should rely on factual information and the scientific method.** | 1. **Evidence-based Decision making** – Decision making in information security related matters should rely on factual information and driven by data. | **Type 3 relationship**: where ISC is cultivated into OC. (Lim, et al., 2009; Thomson, et al., 2006; Veiga& Eloff, 2009; Von Solms, 2000)<br><br>High (Fitzgerald, 2007) | **Risk Vulnerability**: Low<br>**Security Awareness**: Employees are highly aware and concern about Information security matters in organization.<br><br>**Responsibility**: Security is every employee's business.<br>**Security Prac tices**: Implement in holistic manners and unconsciously become employees daily routine activities<br>**Investment for security practices:** High cost in implementing security activities |
| 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, or focus and reacting on a short time horizon.** | 2. **Long term plan** - Organisation's information security should be driven by longterm goals. Short-term sacrifices especially in employees' efforts and time may be necessary. | | |
| 3. Motivation- **Employees are intrinsically motivated to do quality work if the system supports their efforts.** | 3. **Proper systems and processes** -Organisations need to provide proper systems and processes to motivate employees in adhering to security policies. | **Type 2 relationship**: where ISC is a subculture of OC (Dutta & McCrohan, 2002; Lim, et al., 2009; Ramachandran, et al., 2008).<br><br>Moderate (Fitzgerald, 2007) | **Risk Vulnerability**: Medium.<br><br>**Security Awarenes**:s: Employees are aware of security matters within their own department.<br><br>**Responsibility**: Employees are responsible for security matters within own department. |
| 4. Stability versus change /innovation/ personal growth – **Organizations that are risk-taking always make improvement. Risk-averse organizations tend to be less innovative, with little push for change.** | 4. **Continuous change and improvement** - Top management and employees should continuously improve information security and to take risks associated with making change. | | **Security Practices**: Security activity is employees' routine activities within own department. Investment for security activities: Medium cost in implementing security activities. |

Source: Author, 2012.

**Table 3: Framework of the Nature of Relationships between Organizational Culture and Information Security Culture *(Cont.)***

| Organizational Culture (OC) | Information Security Culture (ISC) | Nature of Relationship | Probable Consequences |
|---|---|---|---|
| 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.** | **5. Employees involvement** - Organisations should empower and involve employees with responsibility in information security. Employees' feedback should be considered. | **Type 1 relationship**: where ISC is separated from OC (Chia, et al., 2003; K. J. Knapp, Franklin, Marshall, & Byrd, 2009; Lim, et al., 2009)<br><br>Low (Fitzgerald, 2007) | **Risk Vulnerability**: High<br><br>**Security Awareness**: Low level of awareness towards security matters.<br><br>**Responsibility**: Only IT department is responsible for security matters.<br><br>**Security Practices**: Purely leave it to IT department. Security activity is not a routine activity of employees.<br><br>**Investment for security activities**: Low cost in implementing security activities |
| 6. Isolation versus collaboration/ cooperation - **Cooperation and collaboration are necessary for a successful organization.** | **6. Collaboration and cooperation** - Organisations should engage all departments to improve information security. | | |
| 7. Control, coordination, and responsibility - **A shared vision and shared goals are necessary for organizational success.** | **7. A share security vision** - Organisations should have a shared security vision for all employees working together to achieve the agreed shared vision. | | |
| 8. Orientation and focus- internal and/or external - **An organization may decide to focus on people and processes within organization or emphasize on external competitive environment, or have combination of both.** | **8. Internal and external focus** - Organisations should have a balance of internal process and external requirement to improve information security to protect organizational information in this dynamic business world. | | |

Source: Author, 2012.

The above Table 3 is the framework developed from the prior literature and cultural views by (Fitzgerald, 2007). Principally, first column shows the eight overarching, descriptive dimensions of frequently emerged OC prior to 2000. As mentioned above, there has not been much work and effort to synthesize the dimensions of OC, and to categorize which of these culture dimensions most associated with the

change programs to improve in employees and organizational effects (Detert, et al., 2000). Subsequently, Detert, et al (2000) synthesised the frequently emerged OC and developed a set of eight overarching, descriptive dimensions of culture.

Second column of Table 3 shows the ISC characteristics that are conducive for information security practices to occur in organizations. Lim et al., (2012) found that organizations that cultivate these eight cultural characteristics tend to implement information security practices in a more holistic manner (Lim, et al., 2012). They argue that organizations need to have a shared security visions that are widely shared among employees so that these employees are aware about the importance of information security. Additionally, top management should make security decisions based on evidence and should involve all departments across the organization to continuously improve information security. The security measures in place should base on internal and external requirements to improve the protection of organizational information. From Table 3, the third column shows that it contains three types of relationships. The nature of relationships that can be considered as continuum ranging from ISC is not part of OC (Type 1 relationship) to ISC but is cultivated completely into OC (Type 3 relationships).

The fourth column suggests the probable consequences that organizations may face depending on their current position in Table 3. Those organizations where ISC is separated from OC may allocate a small budget in implementing security initiatives; however, they are encountering with highest vulnerability. In contrast, organizations where ISC is fully cultivated into OC may have the lowest risk vulnerability; nevertheless, they have to invest a substantial amount of money in implementing security measures.

Theoretically, in order to cultivate ISC into OC in Table 3, organization employees must understand and recognize the importance of ISC in influencing employees' behaviours in protecting organizational information. Once organizations accept the importance of ISC, then ISC will become an integral part of work practices among employees. This will in turn help in influencing employees' behaviours in relation to information security matters. Tipton (2007) posited that with the proper focus, organizations can move from low to high security cultural levels.

## CONCLUSION

Every organization has different requirements and priorities in protection of organizational information, and the present OC may decide the desired level of ISC (Fitzgerald, 2007; Lim, et al., 2012; Lim, et al., 2009). However, actual security culture

depends on the security related beliefs, values, which manifest in employee's actions and behaviours towards information security matters (Lim, et al., 2009; Stan, 2007). As such, organizations need to cautiously consider the actual desired level of ISC to influence employees' behaviour to better protect organizational information. The effectiveness and success of any information security programs have to depend on the behaviour of people towards these programs (Lim, et al., 2009; Lim & Lim, 2014; Stan, 2007).

This paper filled in the gaps by examining the nature of relationship between OC and ISC and conceptually developed a framework of the relationship between ISC and OC. It concentrated on how organizations should improve the level of ISC into OC. This framework may offer organizations to decide the extent to which ISC is cultivated into OC. This framework provides suggestions for organizations to raise the desired level of ISC to influence employees' security related behaviours to better protect organizational information according to organizations' security needs. However, one must not forget that ISC is always considered as a complex issue and it requires time and continuous effort of all employees to develop. It can only be cultivated over time by making it as employee routine activities.

From a theoretical development point of view, the author believes this paper has developed a much-needed empirical insight by providing a better understanding of the relationship between OC and ISC. Additionally this paper has also contributed to current ISC knowledge and research. Practically, the developed framework of relationship between OC and ISC provides suggestions for organizations to elevate to the desired levels of ISC to positively influence employees' behaviours in relation to security related matters in organizations.

Like most of the research, this paper has its limitation. The main limitation of a framework is that it is derived from existing literature that is not tested and may not be consistent from industry to industry. Additionally, the development 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 (Lim, et al., 2009; Yeh & Chang, 2007). In the same light, several researchers also found that financial institutions undertake more efforts and have stronger deterrent than other industries (Davamanirajan, Kauffman, Kriebel, & Mukhopadhyay, 2006; Lim, et al., 2009). On the other hand, manufacturing firms merely focus on internal operations and thus require lower strategy-level IS application that only require low security measures (King, 1994; Lim, et al., 2009).

The author suggests that future research should populate and validate the components of the framework by performing more case studies to further understand the relationship between OC and ISC from different industries with different levels of

security. Also, future research should explore change programs for organizations to assist top management and employees to move from low level of ISC to high level of ISC so as to influence employees' behaviours in relation to information security related matters for better protection of organizational information.

## REFERENCES

Cameron, K., & Freeman, S. (1991). Cultural congruence, strength and type: relationships to effectiveness. *Research in Organizational Change and Development, 5*, 23-58.

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

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2003). *Understanding organisational security culture. Information Systems: The Challenges of Theory and Practice, Hunter MG and Dhanda KK (eds)*, Information Institute, Las Vegas, USA.

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. [Article]. *Academy of Management Review, 25*(4), 850-863. Dhillon, G. (1997). *Managing information system security*. Houndmills, Basingstoke, Hampshire: Macmillan Press LTD.

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. [Article]. *California Management Review, 45*(1), 67-87.

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.

Helokunnas, T., &Kuusisto, R. (2003). *Information security culture in a value net.* Paper presented at the Engineering Management Conference, 2003. IEMC'03. Managing Technologically Driven Organizations: The Human Side of Innovation and Change.

Hofstede, G., & Hofstede, G. J. (2005). *Cultures and Organisations: Software and the Mind.* United States of America: McGraw-Hill.

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.

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

Knapp, K. J., Franklin, M. R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2005). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

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.

Koh, K., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). *Security Governance: Its Impact on Security Culture.* Paper presented at the Proceedings of the 3rd Australian Information Security Management Conference, Perth.

Leach, J. (2003). Improving user security behaviour. *Computer & Security, 22*(8), 685-692.

Lim, J. S. (2012). *Defining the relationship between information security culture and information security practices.* Unpublished PhD thesis, The University of Melbourne Australia.

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). *Embedding Information Security Culture - Emerging Concerns and Challenges*. Paper presented at the 14th Pacific Asia Conference on Information Systems.

Lim, J. S., Chang, S., Ahmad, A., & Maynard, S. B. (2012). Towards an Organizational Culture Framework for Information Security Practices. In G. Manish, W. John & S. Raj (Eds.), *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions* (pp. 296315). Hershey, PA, USA: IGI Global.

Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). *Exploring the Relationship between Organizational Culture and Information Security Culture.* Paper presented at the 7th Australian Information Security Management Conference, SECAU Security Congress 2009, Perth, Western Australia.

Lim, J. S., & Lim, G. S. (2014). Information Security Culture: Impact On Information Security Practices. *Journal of Public Security and Safety 2*(2/2014), 91-117.

Martin, A. E., J. (2003). *Information Security Culture.* Paper presented at the 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.* Paper presented at the Proceedings of the Fifth Annual Security Conference, Las Vegas, Nevada USA.

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. (2004). Business and Advisory Committee to the OECD. Security your business: A companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security. Retrieved 9 March, 2009, from http://www.iccwbo.org/home/e_business/securing_your_business.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 ,00.html

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

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

Richardson, R. (2007). 2007 CSI Computer Crime & Security Survey. Retrieved 9 March 2009, from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

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 enduser perspective. *Computers & Security, 26*(1), 56-62.

SANS. (2005). Developing a Security-Awareness Culture-Improving Security Decision Making 1-22.

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.* Paper presented at the IFIP TC11 International Conference on Information Security, Cairo, Egypt.

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

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2006). *Risk Management Standard-the perception of ease of use.* Paper presented at the 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.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

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. W. (1986). Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment. Unpublished Doctoral Dissertation. Indiana University School of Business.

Tejay, G., &Dhillon, G. (2005). *Developing Measures of Information Security*. Paper presented at the The Fourth Workshop on e-Business (WeB 2005).

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. [doi: DOI: 10.1016/S1361-3723(06)70430-4]. *Computer Fraud & Security, 2006*(10), 711.

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*.

Van Niekerk, J., & Von Solms, R. (2009). Information security culture: A management perspective. *Computers & Security, In Press, Corrected Proof*.

Veiga, A. D., & Eloff, J. H. P. (2009). A framework and assessment instrument for information security culture. *Computers & Security 29*, 196-207.

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

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 crossindustry study. *Information & Management, 44*, 480-491.

Zakaria, O., & Gani, A. (2003). *A conceptual Checklist of Information Security Culture.* Paper presented at the 2nd European Conference on Information Warfare and Security, Reading, UK.