INFORMATION SECURITY CULTURE (ISC): IMPACT ON INFORMATION SECURITY PRACTICES

Lim Joo Soon[1], Goay Syan Lim[2]

ABSTRACT

Employee behaviour has a significant impact on information security. Information security culture (ISC) that regulates acceptable employee behaviour in relation to information security is therefore important. Although a large body of literature calls for the cultivation of ISC to shape information security related behaviour of employees, nevertheless, there is little research investigating ISC that enables the implementation of information security. This study addresses the unsupported claim that there is an important relationship between ISC and the success of the implementation of security practices. The findings suggest that security practices can be successfully implemented within eight ISC characteristics. Investigation of these ISC characteristics from a security perspective is a significant step towards future empirical research aimed at understanding the relationship between ISC and the accomplishment of systematic improvement of security practices. The research and practical implications of these findings are presented, and future research areas are discussed.

Keywords: *Information security culture (ISC), behaviour of employees, ISC characteristics, implementation of security practices,*

Introduction

Insiders in organizations have often been reported as a threat to the security of information and are regarded as a major concern in the implementation of information security practices (Lim, Ahmad, Chang, & Maynard, 2010; Workman, Bommer, & Straub, 2008). According to Richardson (2007), insider threat was cited by 59 percent of respondents, overtaking virus attacks as the most reported security incident in the annual CSI Computer Crime and Security Survey. Recent studies support this new trend (Furnell & Thompson, 2009). This signifies the need to look at human behavior within organizations. Additionally, researches show that within organizations, it is security culture that has an impact on employees' behaviors in relation to implementation of information security. Security culture has this impact because it is a set of shared security values, beliefs, and practices

[1] Dr. Lim Joo Soon is a Superintendent of Police at Legal Division, the Department of Protective Security, Royal Malaysia Police

[2] Goay Syan Lim is a Director of Advanced Protective Engineering Sdn. Bhd

that shape and direct the attitudes and behaviors (Ramachandran, Srinivasan, & Tim, 2008). Several researchers have therefore suggested that the impact of security culture in influencing the security behavior of employees must be considered (Thomson, von Solms, & Louw, 2006; B. Von Solms, 2000).

Information security culture remains among the top ranked concerns of information security researchers and industries' practitioners over the last decade (Lim, et al., 2010; Ramachandran, et al., 2008). Many academic researchers argue that ISC is vital in protecting organizational information and that security behavior should be cultivated in the routine activities of each employee as a way forward in improving information security problems (Dhillon, 2007; B. Von Solms, 2000). For industry practitioners, the Organization for Economic Co-operation and Development (OECD) Council and SANS have peculiarly depicted the guidelines for propelling for a culture of information security (OECD, 2003, 2004, 2005; SANS, 2005) for the same purpose.

Whilst many organizations recognize the significance of ISC in information security behavior, however, many researchers have discovered that the ISC in these organizations had not offered enough support to security practices. For example, Helokunnas and Kuusisto (2003) found that none of the small to medium sized enterprises in their studies had completely embedded an ISC and Knapp et al., (2006) found that security training is not an integral part of most organizations. These findings indicate more empirical work is needed to investigate the ISC characteristics that offer support to security practices.

Generally, ISC has been examined in view of various concepts and models of organizational theory. It has been explored from the perspective of Schein's (1992) three layered model (Schlienger & Teufel, 2002, 2003; Veiga & Eloff, 2009); Habermas's theory (Kuusisto, Nyberg, & Virtanen, 2004); organizational behaviors (Martins & Eloff, 2002; Veiga & Eloff, 2009); and Detert Schroeder, & Mauriel's (2000) model. Although such concepts and models are useful and offer better apprehension of ISC, we conclude from our analysis that little work has investigated ISC characteristics that are contributing for the effectuation of information security practices in organizations.

The above discourse results to the following research question: **what are the security culture characteristics that are contributing to information security practices in organizations?** As there is limited literature on this topic, this study decides to research this question using a case study methodology. The rest of the paper is divided into four sections. First, we have a critical review on previous relevant research on ISC, pointing out the gap in existing approaches. Second, we rationalize the methods used to research this gap. Third, this study discusses the results of the case studies. Fourth, this study offers ISC characteristics for information security practices. In the final section, this study discusses the contributions, and concludes by discussing future research in the area.

Relevant Literature

This section presents an overview of the relevant literature including a summary of ISC, the issues of ISC, and adaptation of Lim et al's (2012) model as an analytical framework.

Information Security Culture

There are plethora definitions for information security culture. It has been defined as the totality of human attributes such as behaviors, attitudes, and values that protect all kinds of organizational of information (Dhillon, 1997, 2007). Others have proposed that ISC should abide all activities in a way that information security becomes an intrinsic aspect in daily activities of every employee (Schlienger & Teufel, 2002, 2003; Thomson, et al., 2006; B. Von Solms, 2000). ISC exists when every organization member is aware of the relevant risks and preventive measures, to improve the information security (OECD, 2002). Although ISC has been defined from different perspectives, there seems to be a consensus that organizations need ISC to protect information.

Examinations of the relationship between ISC and security practices incline to be adaptations of Schein's (1992) three-layered cultural model, assessing underlying assumptions, espoused values, and artifacts (Schlienger & Teufel, 2003; Van Niekerk & Von Solms, 2006; Vroom & von Solms, 2004); adaptation of Denison's (1990) and Cameron & Freeman's (1991) organizational culture studies, to examine the relationship between ISC and information security management (Chang & Lin, 2007); and adaptation of Detert et al., (2000)'s framework, to explore the ISC (Ruighaver, Maynard, & Chang, 2007).

Researches utilizing Schein's (1992) model, Denison (1990), Cameron & Freeman (1991), and Detert et al's (2000) model offer an improved understanding of the relationship between ISC and security practices, nevertheless, these studies only derived from few case studies, more research is still needed to perform in order to provide a clear aspect of the security culture characteristics that enable security practices to occur in organizations, and thus it is here we focus on our own investigations.

The Concerns of Information Security Culture

Lim, Chang, Ahmad, and Maynard (2012) utilized Ruighaver et al., (2007)'s conceptual framework to investigate the cultural characteristics underlying information and then relating it to security practices to see the extent and nature of the relationship between them. Ruighaver et al (2007)'s conceptual framework consists of eight cultural characteristics underlying information security and it is synthesized from a series of case studies performed adopted Detert et al., (2000)'s organizational culture model (Chia, Maynard, & Ruighaver, 2002; Chia, Maynard, & Ruighaver, 2003; Koh, Ruighaver, Maynard, & Ahmad, 2005; Maynard & Ruighaver, 2006; Tan, Ruighaver, & Ahmad, 2003). Lim et al's (2012) framework consists of eight security culture characteristics underlying information security as follows:

a. Security decision making should rely on facts and rationality that security is important

b. Improving information security requires a long-term commitment

c. Proper security systems and processes motivate employee to adhere to security policies and procedures.

d. Organizations must make continuous changes to improve information security.

e. Employees should be involved in improving the overall organization's information security.

f. Collaboration and cooperation are necessary for effective information security.

g. A shared security vision and shared security goals are critical for effective information security.

h. Information security needs should be determined by external and internal requirements.

Lim et al's (2012) offers a better understanding of the security culture characteristics for security practices to occur in organizations, however, Lim et al., (2012)'s framework was derived from only two case studies. Therefore, more case studies are needed to further validate security culture characteristics.

Lim et al's (2012) as an Analytical Framework

The study utilized Lim et al's (2012) framework because it was progressed and derived on empirically findings based on Ruighaver et al., (2007)'s conceptual framework. This study aims to progress by conducting more case studies and triangulate with more interviewees to validate ISC characteristics. The details of eight dimensions of culture characteristics are as follows:

a. **Security decision making should rely on facts and rationality that security is important**. The primary idea behind this value is that any system based on cause and effect requires measurement and data to make improvements (Lim, et al., 2012). In organizations, this could take the form of security penetration test, external and internal audit, which indicates the security measures that would improve the protection of organizational information. Top management should make security decisions based on facts and scientific findings. Security managers must inform senior management about the importance of information security because their beliefs about the importance of security are often more important than the beliefs of end-users (Shedden, Ahmad, & Ruighaver, 2006).

b. **Security decision making should be driven by a long-term commitment.** The fundamental idea behind this value is that organizations should be driven by a long term commitment that maintains the organizations' long-range security mission and goals (Lim, et al., 2012). This value helps to decide if leaders adopt long term planning and or focus on the here-and now (Denison & Mishra, 1995). Most of the organizations found to implement on ad-hoc basis rather than long term planning to improve the security practices in prior literature in information security (Ruighaver, et al., 2007; Wood, 2000). However, information security practitioners should be cautioned that short term management commitment, may have little long term impact (Straub & Welke, 1998).

c. **Proper systems and processes in place to improve information security.** The primary idea behind this value is that proper system and process in place in organizations are able to motivate people to safeguard organizational information (Lim et al 2012). This value reminds the importance of focusing on processes rather than people as the source of most errors. This is consistent with Adams & Sasse (1999)'s finding where the majority of users were security conscious, so long as they perceived the need for security behaviours. It means that management should alert employees on the importance and requirement of protecting organizational information. Most of the employees will be intrinsically motivated to comply if they work in an environment without fear and have good systems in place.

d. **Continuous changes to improve information security.** The primary idea behind this value is that organizations require making continuous changes to protect organizational information (Lim et al 2012). Past literature found that most organizations, which have lower security requirements tend to react rather than proact whereas, those organizations which have a high security requirement choose to remain static over change (Ruighaver, et al., 2007). However, the differences between organizations and the fact that their security requirements are different should not prevent organizations from continuously improving the protection of information security (Siponen & Willison, 2009). Information security should be improved continuously as information security is dynamic and multidimensional in nature (Ozkana & Karabacaka, 2010)

e. **Employees' involvement in security activities to improve information security.** The primary idea of this value is that involvement of employees in security activities is imperative in the protection of organizational information (Lim et al 2012). Whilst many organizations are repeatedly found to merely present a brief overview of security during induction (Ruighaver, et al., 2007), however, it is important to alert employees on their role and responsibilities in security matters. It is imperative to make employees feel responsible by involving them in security activities (Lim et al., 2012).

f. **Collaboration and cooperation to improve information security.** The primary idea behind this value is that organizations' stakeholders need to collaborate and cooperate in improving organizational information (Lim et al., 2012). Previous literature repeatedly found that many organizations' security planning was handled by a small group of specialists and often left to the IT department (Fitzgerald, 2007). These findings are not surprising as security is still seen to be highly technical and requires special expertise to deal with it.

g. **A shared security vision and security goals.** The primary idea behind this value is that there should have a shared security vision and goals among departments in improving organizational information (Lim et al., 2012). This value signifies the beliefs in the power of coordinated action. The principle of this value is that individuals should be willing to sacrifice some autonomy for the benefit of the organization (Detert, et al., 2000). This idea requires that all organization members understand the organization's vision and are agreeable to align their actions accordingly (Lim et al., 2012). Senior management needs to connect information security to the success or failure of the organization, reminding employees that information leakage could shut down the company (Stan, 2007).

h. **External and internal focus to improve security.** The primary idea of this value is that organizations should have a balance between internal and external focus in improving organization's security levels (Lim et al., 2012). Whilst others are focused on external constituents, customers, competitors and dynamic environment (Denison, 1990). Previous literature shows that some organizations are forced to conform to external audit and government requirements instead of intending to improve organization's security (Ruighaver, et al., 2007). For external focus, it should comprise technology changes, customer requirements, and threats besides regulatory requirements, whereas, internal focus should consist of proper security controls, raising awareness through mandatory ongoing security training, communication and having feedback mechanism in place (Lim et al 2012).

We have reviewed Lim et al's (2012) eight cultural dimensions and we intend to determine if these ISC characteristics are actually associated to security practices as claimed, through empirical testing. To this end, we consider some companies with high security profile and associated security practices to see if the ISC characteristics are present.

Research Methodology

This study adopted multiple case study methodology to expose the research questions that investigate the cultures characteristics regulating the implementation of security practices (Walsham, 1995; Yin, 1994). This approach is particularly suitable as it captivates the organizational dynamics of the phenomenon (Klein & Myers, 1999). Additionally, it is more proper to examine the underlying complexity of the development by interpreting the shared understanding of the stakeholders (Klein & Myers, 1999).

Altogether, 18 semi-structured interviews were conducted with 16 interviewees including staff from two government agencies as shown in Table 1. The interviews focused on the involvement of the interviewees during the implementation of information security. On average each of these interviews lasted for about 45 minutes. Additional sources of data, including on-site observation and documentation also provided useful insight into the implementation processes.

Data analysis was performed in parallel with data collection. The analysis was conducted iteratively - cycling between empirical data, the theoretical framework, and the related literature as proposed by (Eisenhardt, 1989). Based on the collected data, the interview transcripts were used to prepare a detailed case description, containing a summary of the Organisational Culture (OC) characteristics that support the implementation of security practices. Data was validated with several individuals who are familiar with the OC as well as with security practices and the entire data analysis process was repeated multiple times to case study development (Klein & Myers, 1999; Yin, 1994).

Table 1. Demographic of Case Organizations

Case	Environment	Number of Employees	Informants	Interview Duration
Organization A	Government	5,000	Principal Assistant Director of Operation, Assistant Director of IT (2)*, IT Security Officer, IT Officer, Assistant Director of Training, Head of Personnel Record, Assistant Registrar of Record, Personnel Record Clerk, Physical Security Officer, Head of Protective Security, and Supervisors of Records Department (11 persons-12 interviews)	> 45 minutes each
Organization B	Government_ ICT security	302	Head of Security Management & Business Practices (SMBP) (2)*, Head of Outreach Dept, Head of Government Engagement, Head of Human Resource, and head of professional training. (5 persons- 6 interviews)	> 45 minutes

(2)* indicates the interviewee was interviewed two times

Case Description

Background of the Governmental Organization A

Organization A is a governmental organization employing over 5,000 employees providing a range of services. Being a governmental organization, the role of the security function is to protect the confidentiality, integrity and availability (CIA) of information for senior management to make executive decisions.

Security Culture at the Governmental Organization A

Evidence-based decision making - Top management believed in the importance of information security in protecting organisational information. Security decisions were based on the outcomes of internal and external audits. As a public-sector agency, Organization A was subjected to be regulated by Malaysian Administrative Modernisation and Management Planning Unit (MAMPU). To show the importance of information security, top management formed the ICT Steering Committee to oversee ICT-related matters at Organization A. In addition, top management also translated their security beliefs by installing the Intelligence Access Control & Intrusion Systems (IACIDS) with an electric power fence to deter and detect unauthorised access to the building.

Long-term plan - The long-term plan of Organization A was to implement its ICT Security Policy and to increase manpower in the IT Division. The IT Division had heavy workloads from various departments and was facing a shortage of manpower. Therefore, its long-term plan was to implement Organization A's ICT Security Policy and to provide security training and awareness programs to every employee.

Proper systems and processes - Organization A implemented IACIDS to improve control of access to the buildings. The IACIDS was integrated with a power fence and CCTVs on the fence to control and monitor access and intrusion to the building. In addition, there was a metal detector (scanner and X-ray detector) for visitors entering the complex. Additionally, Organization A performed integrity screening, i.e. background checks, on all employees before they were recruited into Organization A. In addition, all employees were required to sign a non-disclosure agreement twice a year to prevent them from divulging sensitive information.

Continuous change and improvement - Acknowledging the problem of a manpower shortage and faced with heavy workloads, Organization A took the necessary steps to improve the situation. Its direction was modernisation and organisational reinforcement, which focused on structural improvements, streamlined work procedures and systems, acquiring equipment through the usage of computers and ICT and adopting the latest management techniques.

Employees' involvement - Organization A formed an ICT steering committee, which included representatives across departments to oversee ICT projects. Although the implementation of security practices was not done in a holistic manner that included every employee, it involved a number of departments in trying to ensure the effectiveness of security practices to improve the organisation's information security. The departments involved were the IT Division; the Physical Security Department; the Protective Security Department and the HR Department.

Collaboration and cooperation - The implementation of security practices and enforcement of security policy were collaborative between the IT Division; the Physical Security Department; the Protective Security Department and the HR Department. For instance, the IT security officers and the protective security officers performed random checks on the content of USBs. Collaboration and cooperation also took place between the Physical Security Department and the Protective Security Department on the issuing of access cards to employees and visitors.

A shared security vision - Organization A's vision was to be a leading governmental agency of integrity, competency and commitment to working with the community. Although there was no written shared security vision at that time, in order to achieve integrity and competency, Organization A through communication shows the importance of information security via e-broadcasts or intranet to its employees to protect organisational information.

Internal and external focus - At Organization A, top management focused more on the core business rather than information security. Being a public-sector agency, Organization A was regulated by MAMPU. It understands the importance of maintaining its reputation to gain public confidence and respect. Internally, it had enhanced the protection of organisational information by implementing IACIDS, integrated with the electric power fence and CCTVs on the fence to control and monitor access and intrusions to its buildings.

Background of the Governmental Organization B

Organization B was a governmental organisation assigned to look after information security-related matters in Malaysia. Organization B had obtained certification of Information Security Management Systems (ISMS), ISO 27001. At the time, Organization B was one of the agencies promoting ISMS in the country. It emphasised the importance of ISMS, as it is one of the main enablers to ensure information security that can help achieve business goals. At Organization B, every employee knows their responsibility to work together to continuously maintain ISMS certification.

Security Culture at the Governmental Organization B

Evidence-based decision making - Being ISMS ISO 27001 certified, Organization B was required to find the root cause of any problem related to security matters.

ISMS is a risk-based standard and as such the security controls in place were based on the outcomes of risk assessment. Furthermore, one of the requirements of being ISO certified is to find out how, why, when and what are the risks, impacts and vulnerabilities prior to taking any corrective and preventive actions in relation to information security. In addition, Organization B also conducted quarterly online information security awareness level assessments. From the assessment, it gauged all employees' levels of awareness; no one was exempted from the assessment.

Long-term plan - Being the agency safeguarding Malaysia's cyberspace and the agency promoting best practices to the private and public sector, organization B has put in place a long-term plan to improve organisation's information security. For example, Organization B had obtained ISMS certification since 2008, and has continued to maintain the certification. Furthermore, in 2008 it had been tasked with developing a culture of information security in private and public agencies, as well as end users.

Proper systems and processes - There was an Information Security Management Council (ISMC) at Organization B. All security-related matters had to go through the ISMC. The ISMS held regular meetings to discuss security issues and made decisions on the issues raised. Moreover, to help employees comply with security policies and procedures, it organised training sessions and talks about how to manage information security issues. As an ISMS certified organisation, hiring of personnel had to strictly comply with the information security standard, including background checks.

Continuous change and improvement - Risk assessment was carried out annually at Organization B. When there were new findings that require some measures be changed, it changed accordingly. There was a procedure and capability for incident handling that looked into incidents reported and made changes accordingly. Organization B had avenues to monitor vulnerability, its department called MYCERT, which studied and monitored new trends and changes to certain applications, e.g. Microsoft applications. Subsequently, it studied the impact on its business and discussed in a steering committee the necessary changes in response to news trends.

Employees' involvement - Information security was everyone's responsibility at Organization B. All employees at Organization B were empowered to be involved in security activities. Employees were provided with sufficient information about ISMS and employees were also encouraged to report to the Security Management Best Practices Department (SMBP) regarding the violation of security policies and procedures. For instance, employees were empowered to take a photo of the person who violated security policies and procedures and submit a report, even if the person who violated security policy was the head of a department. Another example was the placement of cameras, CCTV, and biometrics' entries and employee feedback and suggestions were taken into consideration as to the placement of these gadgets but not stated in the ISO 27001.

Collaboration and cooperation - There was good collaboration and cooperation amongst departments at Organization B. For example, when the Outreach Department was involved in giving a talk about information security, other departments provided help in preparing presentation materials and presentation slides. At Organization B, when there was a non-compliance issue, the officers from SMBP rendered help to the particular department to comply with the security policy, going through it with each member of the department to assist them in complying with security policies and procedures.

A shared vision - Although Organization B had obtained ISMS certification, it had to maintain its certification to remain an information security reference point. Senior management was very serious about this, and as such this had been stressed in every meeting. At Organization B, every department set its own departmental goal aligned with the corporate mission and goal, which was heavily related to information security. For example, it had a security training program whereby it encouraged all staff to participate together. This program was stated in the Key Performance Index (KPI) of all employees and would be evaluated at the end of the year.

Internal and external focus - There was a balance in internal and external focus at Organization B. Being an ISMS-certified agency, it was subject to an audit by the certification body and to comply with all the requirements. Being an agency safeguarding the cyberspace of Malaysia, it was not only involved in the promotion of information security to school children, and the community at large, but also dealt with Critical National Information Infrastructure (CNII) and other law agencies. So these internal and external requirements played a significant role in its decision making.

Table 2. The Key ISC Characteristics Identified at the Organization A and Organization B

ISC characteristics underlying information security	Exemplar evidence of security culture at Governmental Organization A	Exemplar evidence of security culture at Governmental Organization B
Security decision making should rely on facts and rationality that security is important.	"*When there is any incident. Let say we have found out that this person has misused his power by releasing any information from certain station, we will write in to ask explanation and write in to the officer in charge and tell them to remind their men not to misuse their power. We acted based on evidence.*" (source: Supervisors of Records Dept)	"*Usually because we are ISO compliance, we need all the hard facts and data to support any decision that we make. So there is the process in this organization for decision making*" (source: Head of Outreach Dept)
Improving information security requires a long-term commitment	"*Planning of ICT programs is accordance to various guidelines and planning. We have our ICT steering committee to monitor all the projects that are implemented in this organization. Besides, we also have ISP (ICT Security Policy) that are drafted/ reviewed every 5 years which consists of representatives from all the departments.*" (source: Asst Director of IT)	"*I think it is for the entire life time of the corporation because we have ISMS, and that shows our commitment to information security and our name also reflects our roles and responsibilities.*" (source: Head of Security Management & Business Practices)
Proper security systems and processes motivate employee to adhere to security policies and procedures.	"*The IACIDS system is integrated with power fence. It means that we could trace any intrusion with our CCTV. Also, it means that our complex is more secured and under control. IACIDS also comes with anti pass back function, meaning that if one comes in through point A, he has to go out through point A. We can always play back our CCTV to check or monitor to see if there is any person who came in without a valid pass*" (source: Physical Security Officer)	"*We have intranet system and there is a template for you to report in case of emergency. You can immediately report by phone or email or whatever. Also, we have a suggestion box and if you don't want to disclose your name, anonymous, you can send to CEO to voice out your opinion or whatever you feel that you need to tell the organization to improve*" (source: Head of Security Management & Business Practices)

ISC characteristics underlying information security	Exemplar evidence of security culture at Governmental Organization A	Exemplar evidence of security culture at Governmental Organization B
Organizations must make continuous changes to improve information security.	*"We have put up Disaster Recovery Centre (DRC) under the 9th Malaysia Plan, unfortunately there was no allocation. Again we put it up under the 10th Malaysia Plan where we want to have one DRC for all the systems. Nevertheless, we already have the DRC for those critical systems like PRS s and BIOFIS. We yet to have the DRC for all the other systems ."* (source: IT Security Officer)	*"I think that this is one of the requirements under ISMS, where we should demonstrate continuous improvement. Not only ISMS, but quality management is a continuous improvement. It is common to these three standards, quality management, ISO 27001 and environment standard. They require continuous improvement."* (source: Head of Professional Training)
Employees should be involved in improving the overall organization's information security	*"Information security is the responsibility of each and every one in this organization. E-broadcast is an application that can be accessed by computer at HQ and others states. There is no reason for people to say they are not aware about the security policy. We always make use of e-broadcast to involve our personnel besides sending the order physically through signal and circulars"* (source: Assistant Director of IT)	*"The employee, what normally we do is, regardless what discipline they come from, they have to go to a formal class of the information security management and best practices awareness course. At the same time we measure their knowledge by having quizzes quarterly and they must have a minimum pass for the test. That is how we can monitor or improve their knowledge and experience."* (Source: Head of Professional Training)
Collaboration and cooperation are necessary for effective information security.	*"Technically, the IT department will be handling the issues of ID and password but it depends on the owner of the system. Let us say in the Narcotic system, the application must go to the Narcotic Department and it has to instruct the IT Department to issue the ID and password. We are only the administrator. It should be a collaboration and cooperation among departments.* (source: Principal Assistant Director of Operation)	*"Information management security council/committee comprises of all the head of departments. This committee will have quarterly meetings chaired by the CEO or COO."* (source: Head of Security Management & Business Practices)

ISC characteristics underlying information security	Exemplar evidence of security culture at Governmental Organization A	Exemplar evidence of security culture at Governmental Organization B
A shared security vision and shared security goals are critical for effective information security.	*"Indeed, information security is the responsibility of all. It is indeed the case and practically it must also be the same. Information security is not only subjected to the ICT department. In other words, the protection of information breaches should be a shared goal for all departments."* (source: Assistant Director of IT)	*"Apart from ISMS, our culture in this organization also focus on information security because we are an organization that is certified under ISO 27001. So, everything we do, we adhered to the standard. Everything even how we manage our people, and assets .They are all based on the information security standard that I just mentioned. "* (source: Human Resource Manager)
Information security needs should be determined by external and internal requirements.	*"The main objective is to protect information security. MAMPU has Pemantauan Rangkaian ICT Sektor Awam (*PRISMA*) or Malaysian Government ICT Network Monitoring. PRISMA will alert the relevant agencies if they detect any attempts to penetrate into that agency's system.. We have to make improvement to protect our information upon suggestions made by MAMPU."* (source: IT Security Officer)	*"We are not only dealing with school children, and community at large. We are dealing with law enforcement agencies, with CNII (Critical National Information Infrastructure) and their requirements and all these requirements play a significant role in our decision. "* (source: Human Resource Manager)

'All quotes were transcribed verbatim from the audio-taped interviews'

Discussion

Security Decision Making Should Rely on Facts And Rationality

Although both organizations, A and B believe in the importance of information security, their beliefs stem from different concerns and perspectives. Organization A's beliefs are rooted in the need to prevent security incidents, whereas, Organization B wants to maintain as the leading government agency in safeguarding the national's cyberspace and as a reference point in regard to information security. To improve information security, Organization A has appointed a steering committee to oversee its ICT projects in general and information security in particular. As for Organization B, it believes, as a matter of priority, that providing a secure cyberspace is critical in gaining customers trust. Consequently, it was working towards the maintaining of ISMS, ISO 27001 to prove to the customers that it is capable of protecting and safeguarding national cyberspace from intrusion by unauthorized users.

The belief that facts and data should form the backbone of decision making has long been supported in organizational culture literature. What is seen as rational and true enables employees to make decisions (Reynolds, 1986; Saphier & King, 1985). The primary idea behind this value is that any system based on cause and effect requires measurement and data to make improvements. In practice, this could take the form of security penetration test, external and internal audit, which indicates the security measures that would improve the protection of organizational information.

While different companies have different beliefs and concerns, however, achieving optimal security for that organization's particular situation will still be important (Ruighaver, et al., 2007). Security managers must educate senior management about information security as their beliefs about the importance of security are often more important than the beliefs of end-users (Shedden, et al., 2006). This study proposes that no matter what kind of beliefs that organizations hold, organizations should make security decisions based on facts and scientific findings.

Long-Term Commitment to Improve Security

As an organization that maintains peace and order of the country, organization A has applied to increase manpower of its IT department so that it will have sufficient manpower to conduct security awareness training, and to enforce information security policy. Additionally, top management has also appointed an ICT steering committee to monitor all the projects that is implemented in this organization. For Organization B, the long term strategy is to maintain the accreditation of ISMS to prove to other agencies that it is capable in safeguarding national's cyberspace and it is a leading agency in relation to information security.

The value of long term commitment helps determine if leaders adopt long term planning and or focus on the here-and now (Denison & Mishra, 1995). As for Reynolds, the difference in time horizon for goal setting is "ad hockery versus planning" (Reynolds, 1986). Previous information security literature show that most of the organizations found to have implement on ad-hoc basis rather than long term planning to improve security practices (Ruighaver, et al., 2007; Wood, 2000). But, implementers should be cautioned that short programs, just like short term management commitment, may have little long-term impact (Straub & Welke, 1998).

This study proposes that organizations should be driven by a long term commitment that supports the organizations' long-range security mission and goals. For example, organizations should invest in electronic learning module systems that enable every employee to undergo ongoing security awareness and training no matter where they are, rather than only focus on a small number of employees in a physical class.

Proper Security Systems and Processes

Organization A understands the importance of employees' motivation by implementing proper security systems and processes. It introduces the IACIDS so that employees adhere to the access systems and it also allows the officer in charge to check up the log whenever the need arises. As for Organization B, there is a mechanism in place where all employees can write in to the CEO directly to provide suggestions improving the protection of organizational information or to report any wrongdoing or non-compliances of employees to the CEO.

This value indicates 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; in contrast, they will be de-motivated by extrinsic rewards stemming from performance of processes they do not control (Deming, 1986). However, recent research has shown that when individuals are rewarded for achieving an absolute, normative, or graded level of performance, intrinsic motivation is enhanced (J. Cameron, Pierce, Banko, & Gear, 2005).

This value believes that people want to do a good job, but are often discouraged by the systems in which they work. For example, lack of communication and reporting mechanisms can lead to many unreported errors. Similarly, Adams & Sasse (1999) postulate that it is important to challenge the view that users are never motivated to behave in a secure manner. They found that the majority of users were security conscious, as long as they perceived the need for the behaviors. Therefore, this study proposes that organizations should have proper systems and processes to educate employees on the importance of safeguarding organizational information.

Continuous Changes to Improve Security

Organization A constantly made changes to improve security. New measures would be taken upon recommendation from the auditors or changes of technology. It would then review and update security policies and procedures based on the new measures and communicate results to employees. As for Organization B, it continues to learn from the findings and recommendations from auditors to improve the protection of information security.

This value represents a mindset in which the state of information security is never 'good enough' and is found in organizations where processes and products are continuously studied for improvement. This idea is reflected in Deming's 14 points as 'improve constantly and forever, systems of production to improve quality and productivity..' (Deming, 1986). However, some individuals are open to change, whereas others are said to have a high "need for security" (Hofstede, Neuijen, Ohayv, & Sanders, 1990).

Past literature found that most organizations, which have lower security requirements have a propensity to be reactive rather than proactive, whereas, those organizations, which have a high security requirement favor stability over change (Ruighaver, et al., 2007). However, the differences between organizations and the fact that their security requirements are different (Siponen & Willison, 2009) should not prevent organizations from continuously improve the protection of information security. This study proposes that improvement of information security should be ongoing as information security is dynamic and multidimensional in nature (Ozkana & Karabacaka, 2010; Basie Von Solms, 2001).

Employees' Involvement to Improve Security

Organization A involves employees in information security through E-Broadcast and also through the participation of organization's members in steering committee. Every employee is given a username and password to access to security policy and procedures. As for Organization B, it placed great emphasis in raising employees' security awareness; every employee from driver to CEO is required to take the assessment test.

This idea represents the importance of involving all employees in decision making. Some individuals view work as an end in itself. For these people, work has a 'task focus', and the fundamental concern is on work accomplishment and productivity (O'Reilly, Chatman, & Caldwell, 1991). In contrast, some people view social relationship as more important than productivity (Reynolds, 1986). However, it is advocated that TQM values should focus on both process improvement and results (Detert, et al., 2000) .

Many organizations are often found to merely provide a brief overview of security during induction (Ruighaver, et al., 2007). However, this study proposes that employees should be made to feel responsible by involving in security activities. Thus, it is important to involve and educate employees on their role and responsibilities in security matters. According to (LaRose, Rifon, & Enbody, 2008) when involvement is low, individuals are likely to take mental shortcuts (heuristics), and when involvement is high, users are likely to elaborate by thinking arguments through, provided they have clear information and are not distracted from reflection.

Collaboration and Cooperation to Improve Security

In organization A, IT department collaborates with all departments in protecting organizational information. For example IT department will only generate usernames and passwords to user as instructed by the owner of systems at each department. IT is responsible for computer security, and information risk is the responsibility of the owner of the systems. For Organization B, there is a comprehensive collaboration among all departments; for example, employees from other departments are always required to help the outreach department in educating school children and public on cyber security.

Collaboration represents primary beliefs about the nature of human relationships and how work is effectively accomplished (Denison & Mishra, 1995; Schein, 1992). For some organizations, work must be completed by individuals. In these organizations, teamwork or collaboration will be viewed as violation of individual autonomy (Detert, et al., 2000). In contrast, many organizations now face tasks that are sufficiently complex that no individual can accomplish them alone. These organizations will go after collaboration than individuals (Briggs, Kolfschoten, Gert-Jan, & Douglas, 2006).

Prior research show that most of the organizations' security planning was found to be handled by a small group of specialists and often left to IT department (Fitzgerald, 2007; Lim, Chang, Maynard, & Ahmad, 2009). These findings are not surprising as security is still seen to be highly technical and requires special expertise to deal with it. As information security is a dynamic and multidimensional discipline (Basie Von Solms, 2001), this study propose that organizations should attempt to collaborate with all departments to participate in security activities to improve the protection of organizational information.

A Shared Security Vision and Security Goals

Organization A is a governmental organization providing range of services. Being a governmental organization, the role of the security function is to protect the confidentiality, integrity and availability (CIA) of information for senior management to make executive decisions. As for Organization B, it always want to maintain as a number one information security agency that safeguard the national's cyberspace. It always work hard to maintain the accreditation of ISMS to prove to other agencies that it is capable to provide services in relation to information security related matters.

This value represents the beliefs in the power of coordinated action. For this value, individuals should be willing to sacrifice some autonomy for the sake of the organization (Detert, et al., 2000). A shared vision and shared goals require that all staff members know and understand the organization's vision and are willing to align their actions accordingly. These values is what Deming terms 'adopt a constancy purpose' in total quality management (Deming, 1986).

Top management needs to connect information security to the success or failure of the organization, helping employees understand that information leakage could close the company (Stan, 2007). This may be attained by providing security training to raise employees' security awareness. Furthermore, senior management should discuss the security strategy and planning during the board meeting and have an annual budget for security activities (Fitzgerald, 2007) and "a goal should be to make information security a common theme in discussion around the water cooler" (Stan, 2007). This study proposes that organizations should set out the security vision and goals and communicated to every employee in the organization.

External and Internal Focus to Improve Security

Being a government organization, Organization A is required to be regulated by MAMPU. Similar to Organization A, Organization B is also regulated by MAMPU and ISMS auditors, which is responsible for the accreditation of ISMS. Organization B needs to maintain the accreditation of ISMS as it wants to prove to its customers that it is capable in providing advice on information security related matters and it is a number one reference point in relation to information security matters in Malaysia.

The primary value of this dimension is that organizations should focus on internal processes and external requirements to improve information security. Some organizations assume that the key to organizational success is to focus on people and processes within the organization (Detert, et al., 2000). While others are focused on external constituents, customers, competitors and dynamic environment (Denison, 1990). In contrast, TQM philosophy is customer driven and actively cooperate with community, suppliers and external parties (Dean & Bowen, 1994).

Past literature shows that some organizations are forced to conform to external audit and government requirements rather than with intention to improve organization's security (Ruighaver, et al., 2007). As information security is multi dimensional and dynamic, this study advocates that organizations should have a balance between an internal and external focus to improve organization's security levels. The external focus should include technology change, customer requirements, and threats besides regulatory requirement, whereas, internal focus should include proper security controls, raising awareness through mandatory ongoing security training, communication and feedbacks mechanism in place. This study proposes that organizations should have focus on internal processes and external requirements in improving information security.

Future Research

As every organization has different security needs and requirements, therefore we need to understand if there is an ideal security culture characteristic for all organizations and industries. Additionally, we have to investigate whether we need to match a security management structure to a culture, or change a culture according to the needs of security, or any acceptable combinations. Subsequently, we still need more future development and validation studies of measuring approaches and instruments will be required. Furthermore, what we also need is more on longitudinal studies of culture change in relation to information security. Cross studies can only tell us to a limited extent what is important and what is changeable. The framework offers an important step toward future empirical research aimed at understanding the relationship between security culture, and the implementation of systematic improvement of information security practices.

Conclusion

This study addressed existing equivocalness in the type of security culture characteristics enabling the implementation of information security practices in organizations. The study does so by conceptualizing through the ISC literature. The study articulates Lim et al (2012)'s conceptual framework of security cultural values which, argues will facilitate the implementation of security practices in organizations. The study tested it empirically through two case studies and made some appealing findings.

These case studies offer much-needed empirical penetration by providing a security culture framework for the implementation of security practices from a theoretical development perspective. Although previous researches have studied ISC, little is known about the security culture characteristics for information security practices. This security culture framework has provided an improved understanding of the security culture characteristics. This study also makes a contribution to ISC literature by extending existing knowledge based on the Lim et al., (2012)'s model as an analytical framework. This framework offers a vocabulary for framing experiences of ISC development.

As for security practitioners, this study assists in offering security culture characteristics that are conducive for security practices to occur in organizations. These cases demonstrate the importance of the role of top management in information security management, especially how to create the culture of security to mould employees' behaviors and gain employees' commitment to improve the protection of organizational information. Moreover, this framework could also provide the management in distinguishing the technical and non-technical controls in relation to employees' security behaviours.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. *Communication of the ACM, 42*(12), 41-46.

Briggs, R., Kolfschoten, G., Gert-Jan, V., & Douglas, D. (2006). *Defining Key Concepts for Collaboration Engineering.* Paper presented at the Americas Conference on Information Systems, AMCIS 2006 Proceedings, Acapulco, Mexico

Cameron, J., Pierce, W. D., Banko, K. M., & Gear, A. (2005). Achievement-Based Rewards and Intrinsic Motivation: A Test of Cognitive Mediators. *Journal of Educational Psychology 97*(4), 641-655.

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

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(No. 3), 438-458.

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.

Dean, J. W., & Bowen, D. E. (1994). Management theory and total quality: Improving research and practice through theory development. *Academy of Management Review, 19*, 392-418.

Deming, W. E. (1986). *Out of the crisis* Cambridge, MA: MIT Center for Advanced Engineering Study.

Denison, D. R. (1990). *Corporate culture and organizational effectiveness*. New York: Wiley (New York).

Denison, D. R., & Mishra, A. (1995). Toward a theory of organizational culture and effectiveness *Organ Sci, 6*, 204-224.

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.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. River Street, Hoboken, NJ: John Wiley & Sons, Inc.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review *Academy of Management Review, 14*(1), 57-74.

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.

Furnell, S., & Thompson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, 5-10.

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., 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.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretative field studies in information systems. . *MIS Quarterly, 23*(1), 67-94.

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.

Kuusisto, R., Nyberg, K., & Virtanen, T. (2004). *Unite security culture: May a unified security culture be plausible.* Paper presented at the Proceedings of the 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting Personal Responsibility for Internet Safety. *Communications of the ACM 51*(3), 71-76.

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 M. Gupta, J. Walp & R. Sharman (Eds.), *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions* (pp. 296-315). Pennsylvania, United States: 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.

Martins, A., & Eloff, J. (2002). *Information Security Culture.* Paper presented at the IFIP TC11 International Conference on Information Security, 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.

O'Reilly, C. A., Chatman, J. R., & Caldwell, D. F. (1991). People and Organizational Culture: A Profile Comparison Approach to Assessing Person-Organization Fit. *The Academy of Management Journal, 34*(3), 487-516.

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 Commitee 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_1_1_1,00.html

Ozkana, S., & Karabacaka, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management, 30* 567-572.

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.

Reynolds, P. D. (1986). Organizational culture as related to industry, position, and performance: A preminary report. *Journal of Management Studies, 23*(3), 333-345.

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

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

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

Saphier, J., & King, M. (1985). Good seeds grow in strong cultures. *Educational Leadership, 43*(6), 67-74.

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., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management 46*, 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.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469.

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2003). *Incident handling: where the need for planning is often not recognised.*

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), 7-11.

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

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.

Von Solms, B. (2001). Information Security -- A Multidimensional Discipline. *Computers & Security, 20*(6), 504-508.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Walsham, G. (1995). Interpretive Case Studies in IS research." Nature and method. *European Journal of Information Systems 4*, 74-81. .

Wood, C. C. (2000). Integrated approach includes information security. [Article]. *Security: For Buyers of Products, Systems & Services, 37*(2), 43-44.

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*.

Yin, R. K. (1994). *Case study research: design and methods* (2nd ed.). Thousand Oaks, CA: Sage Publications.