Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2010 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2010

Embedding Information Security Culture Emerging Concerns and Challenges

Joo Soon Lim
The University of Melbourne, jslim@pgrad.unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Shanton Chang
The University of Melbourne, slwc@unimelb.edu.au

Sean Maynard
The University of Melbourne, seanbm@unimelb.edu.au

EMBEDDING INFORMATION SECURITY CULTURE EMERGING CONCERNS AND CHALLENGES

Joo Soon Lim, Department of Information Systems, The University of Melbourne, Victoria, Australia, jslim@pgrad.unimelb.edu.au

Atif Ahmad, Department of Information Systems, The University of Melbourne, Victoria, Australia, atif@unimelb.edu.au

Shanton Chang, Department of Information Systems, The University of Melbourne, Victoria, Australia, slwc@unimelb.edu.au

Sean Maynard, Department of Information Systems, The University of Melbourne, Victoria, Australia, seanbm@unimelb.edu.au

Abstract

The behaviour of employees has been identified as a key factor in the protection of organizational information. As such, many researchers have called for information security culture (ISC) to be embedded into organizations to positively influence employee behaviour towards protecting organizational information. Despite claims that ISC may influence employee behaviours to protect organizational information, there is little empirical work that examines the embedding of ISC into organizations. This paper argues that embedding ISC should not only focus on employee behaviour, but rather in a holistic manner, involve everyone in the organization. The argument is developed through case studies in two organizations based on semi structured interviews of respondents, observations, and documents analysis from each organization. The results show that the challenges of embedding ISC are not as simple as changing employee behaviour and technical aspects of security. Rather, the more challenging problem is how to embed ISC in a holistic manner that includes senior management support and involvement to instil awareness through mandatory training with a clear assignment of responsibility and constant enforcement of security policies and procedures. We believe that the findings will provide researchers in ISC with a broader view of how ISC can be embedded in organizations.

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

1 INTRODUCTION

Human behaviour is recognised as a major problem in the implementation of information security practices in organizations (Pahnila, Siponen, & Mahmood, 2007; Siponen & Oinas-Kukkonen, 2007; Workman, Bommer, & Straub, 2008). Employees are often found to be careless and are often unaware of security directives, failing to comply with organizational information security policies and procedures. This may be caused by organizations possessing weak information security culture.

As such, researchers have called for the creation of ISC to help organizations to influence employee behaviour in order to better protect organizational information (Von Solms, 2000; Schlienger & Teufel, 2003; Ruighaver, Maynard, & Chang, 2007; Veiga & Eloff, 2009). Similarly, a recent study contended that managing information security culture is becoming more challenging in today's business because people are both a cause of information security incidents as well as playing a key part in the protection of organisational assets (Lim, Chang, Maynard, & Ahmad, 2009).

Many researchers have called for the creation of ISC, however these studies do not elaborate further on how to embed ISC within the organisation. Helokunnas & Kuusisto (2003) found that none of the firms had fully embedded ISC into organizations during information security assessments in Small Medium Enterprises in Tampere region in Finland. In addition, Lim et al., (2009) also claim that there seems to be inconsistency between calls for creation of ISC and actual security practices. These findings indicate further research is still needed to understand how ISC could be embedded into organizational culture (OC).

Therefore, this paper aims to bridge the gap in literature by examining how ISC can be embedded into OC. In this paper we argue that research in ISC is limited in that it does not provide details on how ISC is embedded into OC. This paper explores in depth how ISC is embedded into OC in two organizations. The paper will review the literature in the area briefly, justify the methods, discuss the results of the case studies, discuss the contributions and limitations, and conclude by discussing further research directions in the area.

2 LITERATURE REVIEW

2.1 Information Security Culture

Organizational culture refers to "shared values, beliefs, and behaviours that shape and direct members attitude and behaviours in organizations" (Hofstede, Neuijen, Ohayv, & Sanders, 1990; Schein, 1992). Information Security Culture can be defined as "the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds" (Dhillon, 1997) or as what is done in organizations in relation to information security practices (Martins & Eloff, 2002; Veiga & Eloff, 2009). Others point out that information security is a management problem, claiming that ISC is still new and complex, and therefore it can not be fully defined (Ruighaver et al., 2007).

ISC remains among the top ranked concerns of academic researchers and industry practitioners. Several researchers have argued that ISC is vital in ensuring organizational information and should be part of the routine activity of each employee (Von Solms, 2000; Schlienger & Teufel, 2003; Thomson, von Solms, & Louw, 2006). For industry practitioners, the Organization for Economic Co-operation and Development (OECD) Council has specially documented the guidelines for moving towards a culture of information security (OECD, 2003, 2005).

The key challenges of embedding ISC in organizations are (Lim et al (2009)): ISC is typically not an integral part of OC, security managers frequently have difficulty in getting sufficient budget from senior management to implement information security practices, information security measures often involve a small group of people, organizations are typically forced to conform to external audit and government regulation rather than belief in the importance of security practices in protecting

organizational information. These findings indicate that empirical work is still needed to examine why organizations still do not take actions to embed ISC into OC to protect organizational information.

ISC is often studied using various concepts and models of organizational theory. For example it has been researched from the perspectives of Schein (1992)'s three layers model (Schlienger & Teufel, 2003) ; Detert et al (2000)'s frameworks (Chia, Maynard, & Ruighaver, 2002); organizational behaviour (Martins & Eloff, 2002; Veiga & Eloff, 2009); conceptual frameworks (Alnatheer & Nelson, 2009; Lim et al., 2009); and management and economical science (Van Niekerk & Von Solms, 2009). Although such concepts and models are valuable and provide further understanding in ISC, however, they do not provide details on how to embed ISC into organizations. Organizations still need appropriate frameworks and processes to embed ISC into OC (Van Niekerk & Von Solms, 2009).

2.2 Embedding of Information Security Culture

The purpose of this study is to examine how organisations embed ISC into OC to influence employee behaviour to better protect organizational information. This study uses Lim et al., (2009)'s framework. This framework was derived from past literature combined with cultural views by (Fitzgerald, 2007). The framework captures three types of relationships between OC and ISC. These relationships are: ISC is not part of OC, ISC is a subculture of OC, and ISC is completely embedded into OC.

The framework proposes that the extent to which ISC is embedded in OC depends on senior management involvement in security practices, assignment of security responsibilities, security policies enforcement, security awareness, security training, and allocation of security budget. The following section discusses each of the abovementioned activity.

2.2.1 Senior Management Involvement

Senior management involvement is essential in implementing information security practices. Hone & Eloff (2002) posit that employees will adhere to security policies and procedures if senior management shows concern for it. Similarly, Dutta & McCrohan,(2002) assert that organizational computer security starts with senior management support and not with firewalls. This is further confirmed by recent research that shows that senior management commitment to security is vital in promoting compliant and proactive security conscious users (D'Arcy & Greene, 2009). In short, senior management must show support by active participation in security activities.

2.2.2 Assignment of security responsibilities

Assignment of responsibilities refers to the person or department that is responsible for ensuring the compliance of information security policies. Researchers contend that information security polices need to clearly delineate the responsibilities of every one in organization to protect organizational information (Baskerville & Siponen, 2002; Doherty & Fulford, 2006). However, past researchers found evidence to suggest that only a small group of people is involved in security activities (Chia et al., 2002). It suggests that further research is still needed to understand why organizations only assign security responsibility to a small group of people.

2.2.3 Enforcement of security policies

Information security policy may be one of the most important controls to protect organizational information. The main objective of security policy is to influence and direct the actions and behaviours of organization members (Höne & Eloff, 2002). Security policy also helps to develop ISC by specifying what is acceptable or unacceptable behaviour in relation to security practices (Thomson et al., 2006). However, Chia et al., (2002) point out that organizational culture support is needed for its development, implementation, and compliance. Their findings show the importance of ISC in the context of security policy enforcement towards achieving an optimal level of compliance.

2.2.4 Security Awareness

Security awareness is not training. Awareness programs teach employees to be conscious about information security policies and procedures. Past researchers suggest that investing in security awareness and culture is more effective than in security policies (Straub, D. W. & Welke, 1998; Knapp, K.J., Marshall, Rainer, & Ford, 2006). Although security awareness is widely accepted to raise employees consciousness in security matters, however, recent research still found that employees are not aware of security policies and procedures (Pahnila, Siponen, & Mahmood, 2007) Their findings indicate that awareness programs are still not been effectively carried out in organizations. This paper argues that organizations may not achieve high level of ISC if there is little awareness among employees.

2.2.5 Security Training

Security training is important in order to raise the awareness of organizational information. Organizational members must be trained to handle security problems (Straub, D. W. & Welke, 1998). In the United States, a National Security Telecommunications and Information Systems Security Committee (NSTISSC) directive established the requirement for all federal agencies to develop and implement education, training, and awareness programs for national security systems (Hentea, Dhillon, & Dhillon, 2006). However, recent research shows that training is still not part of most of the OC (Knapp, K.J. et al., 2006). We argue that senior management has to be convinced and educate of the importance of training in raising employees' awareness.

2.2.6 Allocation of Security Budget

Information security managers have always found it difficult to get adequate funding from senior management. Senior management may continue to be reluctant to commit resources to the security function as (Keefe, 1983). In a more recent study, Shedden, Ahmad, & Ruighaver (2006) found that organizations are inclined to treat security spending as a cost, and often struggle to gain funding for security implementation. The finding suggests that there is a need for security managers to educate and convince senior management that without sufficient allocation, it is almost impossible to have effective information security practices in place.

3 METHODOLOGIES

We adopt a case study approach to gain a better understanding of how organizations embed ISC into OC. The application of case study research to this phenomena is appropriate in a new and emerging area as it is a research strategy that allows for an in-depth exploration in a particular setting (Benbasat, Goldstein, & Mead, 1987; Yin, 1999). Interview protocols were developed based on various issues identified from literature.

We selected two organizations from different industries with expected medium to high level of security risks profile, awareness and knowledge. Participants were selected from senior management and employees who are involved in information processing. The organizations demographics are shown in Table 1.

Organization A is a finance company employing over 5,500 employees providing a diverse range of financial services. The role of the security function in organization A is to protect information risks and organizational reputation. Being a financial institution, organization A is required by regulations to protect customer information and privacy. In addition the security functions must also protect organizational reputation to retain competitiveness.

Organization B is a governmental organization employing over 96,000 employees 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 financial institution and governmental organizations, both have high risk profiles and need to have a high level of ISC to influence employee behaviours towards protecting organizational information.

	Organization A (Finance)	Organization B (Government)
Number of employees	5,500	96,000
Number of Interviewees	8	10
Experience (years)	1-28	4-34
Job Titles	CIO, IT Security Manager, IT Development Manager, HR Manager, Head of Learning and Development, Security and Financial Crime Manager, Business Information Risks Officer (BIRO), Administration Clerk.	Principal Assistant Director of Operation, Assistant Director of IT, IT Security Officer, Assistant Director of Training, Head of Personnel Record, Assistant Registrar of Record, Personnel Record Clerk, Physical Security Officer, Head of Protective Security, Supervisor of Records Department
Expected Organization Security Awareness Level	Medium to high	Medium to high

Table 1: Demographics

Data was collected from organization A (8 participants) and organization B (10 participants) via semi structured interviews. The participants are highlighted in Table 1 above. Organizational information security policies and enforcement guidelines were provided for review by organization A and organization B.

Interviews were recorded and transcribed to transform the collected information with the aim of extracting useful data and facilitate findings. The output of the information was qualitative in nature, therefore the appropriate method by which to accurately identify the correct concepts and themes in the qualitative data collected is through pattern matching (Miles & Huberman, 1994). Patterns codes represent the sets of emergent codes that the researcher develops during data analysis. It helped in reducing the large volume of data into a smaller number of analysis units. Information collected from document analysis and observation also analysed using the same approach.

4 CASE STUDY RESULTS AND DISCUSSIONS

Our goal was to investigate how organizations embed ISC into OC to influence members' behaviours towards protecting organizational information. This section includes discussion of senior management support and involvement, locus of responsibilities, enforcement of security policies, security awareness, security training, and allocation of budget uses Lim et al (2009)'s framework (Section 2.2) to enable reader to observe the emerging concern and challenges of embedding ISC into OC.

4.1 Senior management support and involvement

Organization A is a finance company and it adopted the BIRO structure framework to implement and enforce the information group security policies and group guides. Senior management appointed the Chief Operating Officer (COO) as Chief Information Security Officer (CISO) to demonstrate the seriousness in implementing information security practices. Implementation of information security in organization A has always been top down according to the manager of IT development:

> *Yes, in fact the BIRO structure is headed by CISO, he is one of the top management. So he will assure that this program or whatever initiatives we do will come from the top to the low level. Therefore it has some buy-in. we do have top management support in that sense. CISO is actually the COO of company*

Organization B is a government organization that has a hierarchical organizational structure. Senior management did not appear to understand the importance of the IT division and information systems functions. Furthermore, there was no full time Information Technology Security Officer (ITSO) appointed to handle security matters as stated by Assistant Director of IT:

> *Ideally IT should has its own department. Then we could have special committee for IT, and then ITSO and CIO are assigned specifically. But what is happening now is IT division is one of the eight divisions under Logistic Department and Logistic Department is one of the eight Departments under this organization. We don't have the full time ITSO and we only appoint officers to perform as ITSO besides their actual role and responsibilities. The answer is we don't have full time ITSO.*

In addition, there was less involvement from management from organization B as responded by Head of Protective Security:

> *So I am doing my part in my office, respective supervisors must play their role. Imparting the knowledge, sharing information, supervise the personnel under us,. but now only 10% of line managers doing the same thing.*

Results from organization B confirm Fitzgerald (2007)'s cultural view towards information security and Straub, & Welke (1998)'s findings where information security continue to be ignored by senior management and management tends to leave the security responsibility to the IT department. In contrast, organization A had no problems in getting management support and involvement. Senior management involvement is essential in implementing information security practices. Ruighaver et al., (2007) point out that information security is a management problem and security culture reflects how management handles this problem. Without senior management support and involvement, it is difficult to imagine how organization B will achieve a high level of ISC

4.2 Assignment of Security Responsibilities

The security training and awareness program of organization A is managed by the Learning and Development Department. BIRO and DBIRO across organization taking charge of enforcement of security policies. The IT security department was overseeing all IT security matters. The Security and Financial Crime Manager responded as follows when we asked who is responsible for conducting awareness program:

> *For the awareness program we have information security awareness training which is conducted by Learning and Development, our training unit.*

Further evidence of the clear assignment of responsibility came to light when we asked about who is responsible for overall risks. The IT security Manager responded:

> *As manager of information systems, E-Risk and compliance, it is very specialized section; I look after the complinace of IT whether is from the central bank of from the group. Only compliance of IT compliance because we also have the risk department who is in charge of overall risks.*

The security officer of organization B focused more on physical security rather than on information security. In addition, there was no full time ITSO. The training department was more on coordinating courses from others departments and there wasn't any security training and awareness program ever conducted in organization B as explained by Assistant Director of Training:

> *We are more on coordinate course from various training institutions and departments. If IT division feels that information security is very important, why don't they inform us? Then we will implement. They don't inform us. Security of*

computer should be from them, I don't have the expertise and I don't have the knowledge also. If they said important then we can arrange.

As there was no clear assignment of security responsibility, IT division ended up not being able to focus on security matters as stated by the Assistant Director of IT:

IT may not be able to organize awareness program as we are limited in resources. We don't have enough times to train users. We even haven't trained users in application systems. So we hope that users in this organization understand their responsibility in looking after the digital information.

The findings from organization A are in line with the contention of past researchers where a good security policy should clearly assign the responsibilities to various departments and individuals (Whitman, M.E., 2004; Whitman, M. E., 2008). Furthermore, a clear assignment of security responsibility may enable employees to better perform and develop their own work practices (Dhillon & Backhouse, 2001). In contrast, organization B greatly relied on the IT division on security matters, however, it was unable to cope due to heavy workloads. Lack of clear assignment of security responsibilities may jeopardise the protection of organizational information.

4.3 Enforcement of Information Security Policies

As mentioned in Section 4.1, Organization A adopted group security policies and group guides and these policies and guides were enforced by BIRO and DBIRO across organization as stated by Business Information Risks Officer (BIRO):

We do have DBIRO, these are checkers that we have nominated them across the organization. So they are actually being our people to actually make sure that everyone conforms to the clear desk policy.

Enforcement of security policy in organisation A was an ongoing activity. When we asked the BIRO how often desks are checked according to the clean desk policy, the BIRO stated:

Meaning that DBIRO have to perform clear desk check once a week after office hour. Then they report their findings and submit to us every month. The number of desk checks and the number of breaches they have found. They have to send us the reports.

In contrast, organization B did not adopt any documented security policies. Instead it adopted orders of logistic department, security orders from security department, and security policies drawn by Malaysian Administrative Modernization and Management Planning Unit (MAMPU) as explained by the Assistant Director of IT:

In actual fact we don't have security policy in our organization yet. We are in the process of developing security policy. However, we are making use of existing guides and procedures like Logistic's orders, MAMPU's orders and orders from security office

He was very confident that members of the organization were aware of the security policies as it is advertised via e-broadcast, and the organization's intranet. However, the response from the Assistant Registrar of Record was:

I don't know about any information security policy, But I know that we have to login using user id and password.

The result showed that organization A adopted group security policies and guides, and the enforcement of security policies was an ongoing activity. In contrast, organization B did not adopt proper documented security policies. David (2002) asserts that policy must be enforced to make it effective. Without the enforcement, "A policy may become a 'paper tiger' with no 'teeth' " (Knapp, K. J., Franklin, Marshall, & Byrd, 2009). The lack of security awareness in Organization B did not assist enforcement.

4.4 Security Awareness

Organization A considered awareness to be a very important matter in relation to security practices as explained by the Security and Financial Crime Manager. It made sure that the awareness program was highly promoted and communicated to organization members:

> *So, everyone needs to be aware. So, that is why awareness need to be taken seriously and efforts from the bank has to be pretty good rolled out. So, that is why almost every month you will see programs undertaken by bank and of course to be implemented by DBIRO and there are lots of communication to the staff on information risk.*

In contrast, organization B did not have an awareness program. The only time employees were exposed to security matters was when they attended application programs as explained by the Assistant Director of IT:

> *We don't have awareness program but we will touch on security whenever there is courses organized by IT department.....We can only incorporate it together with other application programs. This is the time where we create awareness on the security of password, and computer handling.*

When we queried the Head of Protective Security on awareness in organization B, he responded:

> *They don't even care of security. From our inspection, the result shows that when they go out during break, they never locked the door. All the files scattered on the desks. Even the classified document, and cupboard are left opened.*

Our results indicated that the awareness program was conducted in a holistic manner and it was an ongoing activity in organization A. However, there was no specific awareness program in organization B; instead, it was only incorporated with other application programs. Security awareness is raising consciousness within the organization of the threats to its well being and the role employees play in mitigating those threats (Manjak, 2006). Thus, it is difficult to believe that organization B will achieve effective ISC without the awareness among its personnel.

4.5 Security training

In organization A, training is conducted by the Learning and Development Department. Every new employee must go through an induction program within three months of joining the organization. When asked if security is covered during the induction program, the administration's clerk responded:

> *Under the induction course, we were trained how to protect our information, not to share information with others even though we are in the same department..I attended both application and security.*

In addition, security training was an ongoing and mandatory requirement for every member including the Chief Executive Officer of the organization as the administration's clerk explained:

Annually is compulsory, is mandatory thing again for the existing staff. Everyone must go through a specific e-learning. For example information risk, compliance .

Surprisingly, there was no security training in organization B; the training department was more on coordinating courses as explained by Assistant Director of Training:

We handle the entire course in this organization but base on request....We never conducted any module on security of computer. I don't think we have. We don't have but we have introduction to computer module-word processing.

The results showed that security training in organization A was mandatory, and involved everyone in organization. In contrast, organization B had no security training and only incorporated in application programs. Past researchers and practitioners stress that security training is important to improve security awareness (Wipawayangkool, 2009). Without appropriate security training, it is difficult to raise security awareness of employees in organization B. This paper argues that security training should be made mandatory to everyone as Furnell (2007) asserts that an effective security culture cannot be achieved without appropriate attention to security awareness, training and education for staff.

4.6 Allocation of Security Budget

In terms of allocation of security budget, Organization A used to have a problem when it was not centralised at regional level. But since it became centralised, every decision was decided by senior management at the group level. Therefore, there was no budget issue in organization A as the IT Security Manager indicated:

We used to have because last time is not so centralised from regional level. So every country, whatever they think is useful they buy. So now for the past three to five years they want everything to be done at group level, which is good because every country use the same tool, equipment, software, and hardware. So you know everybody is practising the same technology. Monitoring and tracking everything is the same. So now the budget will come from region, Head Quarter.

In contrast, Organization B was facing difficulties in getting sufficient budget to implement security practices as explained by Assistant Director of IT:

We don't have Disaster Recovery Contigency (DRC) for the entire systems yet. However, we already have the DRC for those critical systems. We have put up under 9th Malasyia Plan, unfortunately there was no allocation.

Further evidence of the allocation funds can be seen from absence of much needed encryption:

We don't encrypt yet. It is only user id and password on the operating sysems. We don't have allocation for hard disk encryption

The result showed that organization B struggled with getting sufficient funds to implement their information security practice. The lack of allocated budget caused the delay in implementation of security practices in organization B. This supports Straub (1986)'s findings where it has to take a major loss from security incidents to initiate administration function. Moreover, senior management needs to be convinced that sufficient budget is important to implement security practices. In this regard, Johnson & Goetz (2007) suggest that one of the possible ways is showing the management you are fixing the business problem rather than telling them what security is doing.

In summary, the case studies illustrated the merits of adopting Lim et al 2009's framework to investigate how organizations embed ISC into OC. The results showed that organization A had full management support and involvement by allocating sufficient resources and material in implementing

security practices. There is clear assignment of security responsibilities in conducting awareness program; security training; and ongoing enforcement of security polices and guides. The results supported (Goodhue & Straub, 1991)'s findings that financial firms tend to invest more in security than other firms. First, they rely heavily on information for business operations; second, losses from information abuse can be very large; and third, reputation is important to their business.

In contrast, organization B had less management support and involvement in implementing security practices. It did not have its own documented policies. Moreover, there was no clear assignment of security responsibility. As a result, its IT division lacked resources in providing a proper awareness program and security training. These results supported (Dzazali, Sulaiman, & Zolait, 2009)'s findings where only 13% Malaysian Public Service (MPS) at Level 4 maturity and 1% at Level 5 when they evaluated the information security maturity level of information landscape of the MPS organizations. The following section discusses the findings of the case studies and relate the findings to Lim et al. (2009)'s framework.

The following Table 2 summarises how Lim et al. (2009)'s framework might be a useful way of understanding how deeply the ISC of an organization is embedded into its OC. It represents a starting point for examining the ISC of an organization.

Factors that Contribute to ISC	**Organization A**	**Organization B**
Management Support and Involvement towards Security	High levels of support and active involvement	Low support and low involvement
Locus of Security Responsibilities	Responsibilities clearly assigned	Responsibilities not assigned
Enforcement of Security Policy	BIRO support for enforcement	Low enforcement
Security Awareness	High	Low
Security Training	Mandatory at all levels	Only for specific applications
Allocated Budget for Security	Allocated budget is evident	No allocated budget
Nature of Relationship between ISC and OC	**ISC is completely embedded into OC**	**ISC is a subculture of OC**

Table 2: The level of ISC embedded into Organization A and Organization B

5 CONTRIBUTIONS AND LIMITATIONS

This paper offers contributions to the body of knowledge and practice. Given the majority of current research in this area is conceptual and promotes embedding of ISC into OC without providing supportive empirical evidence, this paper offers some empirical evidence regarding the embedding of ISC into OC. For practitioners, the results pinpoint the importance of senior management support and active involvement in ensuring the embedding of ISC into OC. These findings are particularly important as they highlight the main concerns and challenges of embedding ISC into OC. Results suggest that lack of management support and involvement in implementing in information security practices will affect all security activities in organization.

The primary limitation of this paper is the dimensions of ISC is mainly based on Lim et al., (2009)'s framework and Fitzgerald (2007)'s cultural views of security culture. We believe that additional dimensions like monitoring and control, communication, integrity, and regulatory requirement can be added in future research as Ruighaver et al., (2007) assert that information security culture is too complex to be covered by a single framework or model. Also, due to sensitivities involved in information security, we were only able to obtain their information security policy for a short amount of time.

6 CONCLUSION

Many researchers have called for embedding of ISC into OC to influence employee behaviour towards protecting organizational information. This paper examines how organizations embed ISC into OC. Case study strategy was used to investigate two organizations. The results highlight the main concerns and challenges of embedding ISC into OC.

We have illustrated through case studies that the challenges of embedding ISC into OC are not as simple as changing employee behaviours and the technical aspects of security. The results demonstrate that ISC does not operate in isolation. The roles of senior management, the delineation of responsibilities, the enforcement processes, the awareness program and training, and allocation of budget of organizations in relation to security practices are ways of expressing ISC that can make every member in the organizations believe that ISC is embedded into OC to protect organizational information. We believe that the findings have contributed to ISC research, particularly on how ISC is embedded into OC.

References

Alnatheer, M., & Nelson, K. J. (2009). A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.

Baskerville, R., & Siponen, M. (2002). An Information Security Meta-Policy for Emergent Organisations. *Logistics Information Management, 15*(5/6), 337-346.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly, 11*(3), 369-385.

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

D'Arcy, J., & Greene, G. (2009). *The Multifaceted Nature of Security Culture and Its Influence on End User Behavior.* In IFIP TC 8 International Workshop on Information Systems Security Research.

David, J. (2002). Policy Enforcement in the Workplace. *Computers & Security, 21*(6), 506-513.

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

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

Dhillon, G., & Backhouse, J. (2001). Current Directions in Is Security Research: Towards Socio-Organizational Perspectives. *Info Systems J, 11*, 127-153.

Doherty, N. F., & Fulford, H. (2006). Aligning the Information Security Policy with the Strategic Information Systems Plan. *Computers & Security, 25*(1), 55-63.

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

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information Security Landscape and Maturity Level: Case Study of Malaysian Public Service (Mps) Organizations. *Government Information Quarterly, 26*(4), 584-593.

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. (2007). Ifip Workshop-Information Security Culture. *Computers & Security, 26*(1), 35-35.

Goodhue, D. L., & Straub, D. W. (1991). Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security. *Information & Management, 20*, 12-27.

Höne, K., & Eloff, J. H. P. (2002). What Makes an Effective Information Security Policy? *Network Security, 2002*(6), 14-16.

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

Hentea, M., Dhillon, S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Information Technology Education, 5*.

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.

Johnson, M. E., & Goetz, E. (2007). Managing Organizational Security: Embedding Information Security into the Organization. *IEEE Security & Privacy*, 16-24.

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

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. (2006). Information Security: Management's Effect on Culture and Policy. *Information and Computer Security, 14*(1), 24-36.

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

Manjak, M. (2006). *Obstacle to Educating Employees* SANS Institute

Martins, A., & Eloff, J. (2002). *Information Security Culture.* In IFIP TC11 International Conference on Information Security, Cairo, Egypt

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook.* . Thousand Oaks, USA: Sage.

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

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

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

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

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

Schlienger, T., & Teufel, S. (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.* In Proceedings of the fifth annual security conference, Las Vegas, Nevada, USA.

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

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

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

Van Niekerk, J. F., & 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. *C o m p u t e r s & S e c u r i t y 29*, 196-207.

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

Whitman, M. E. (2004). In Defense of the Realm: Understanding the Threats to Information Security. *International Journal of Information Management, 24*(1), 43-57.

Whitman, M. E. (2008). *Security Policy: From Design to Maintenance.* (Vol. 11): Armonk, N.Y. .

Wipawayangkool, K. (2009). Security Awareness and Security Training: An Attitudinal Perspective.

Yin, R. K. (1999). Enhancing the Quality of Case Studies in Health Services Research. *Health Services Research, 34*(5), 1209-1224.