# Assessing the Level of I.T. Security Culture Improvement: Results from Three Australian SMEs

Leanne Ngo, Wanlei Zhou, Ashley Chonka
Deakin University
lengo, wanlei, ashley @deakin.edu.au

Jaipal Singh
Curtin University of Technology
J.Singh @cbs.curtin.edu.au

*Abstract*- Transitioning towards an improved I.T. security culture that fosters desired I.T. security behaviour and attitudes in individuals is pertinent to any organizational I.T. security strategy. To improve the current I.T. security culture of an organization and its members, an initial assessment covering four core questions was necessary to determine how much of an improvement was needed. The assessments and data collection techniques and corresponding results and findings are presented and discussed. The implications of this research will be of great benefit to both practitioners wanting to improve I.T. security culture and awareness in their organization, and will help to fill the lack empirical research within the academic field of I.T. security.

## I. INTRODUCTION

Protection of information and information systems resources by online security threats have been a growing concern in Australia. In the 2006 Australian Computer Crime and Security Survey (ACCSS) published by the Australian Emergency Response Team (AusCERT), total average annual losses for electronic attacks, computer crime, and computer access misuse or abuse increased by a staggering 63% to $241,150 per organization compared to 2005. The 2004, 2005 and 2006 ACCSS surveys, reports inadequate staff training in computer security management, poor security culture within organizations and changing the user's behaviour and attitudes towards security were all consistently apparent in the past three consecutive ACCSS surveys as key contributing factors towards losses incurred by organizations [1-3]. AusCERT has called for increased efforts to be made at the organizational level and through computer security initiatives that benefit the broader Australian community. The survey had suggested a lack of security culture and good human behaviour and attitudes towards security as impediments to the success of overall organizational security efforts. Despite every attempt by humans to be careful and vigilant in their practice, natural human tendencies tend to fail on their behalf.

The Australian Government has implemented many initiatives to combat online security. In 2006, the Australian E-security National Agenda (ESNA) established a secure and trusted electronic operating environment for both the public and private sectors within Australia. One of the priorities of ESNA was to enhance the protection of home users and SMEs from electronic attacks and fraud. As a result, a $13.6 million package of initiatives over four years was announced to improve online security home users and small businesses from online attacks and fraud. In mid-2008, the 'Stay Smart Online' program was established as part of the Australian Government's initiative to help online security home users and small businesses. The 'Stay Smart Online' program is centered on providing information and advice on securing their computer, transacting online, protecting children from unsuitable websites and email, and providing information and advice for small business safety. The initiative concentrates on raising online security awareness of home users and SMEs with the intention to improve the security of online behaviours and computer defenses.

The need to concentrate on improving security culture to foster good security behaviour and attitudes of individuals within organizations is important. Although technological solutions can solve some information security problems, even the finest technology cannot succeed if humans do not interact and approach these resources appropriately because human security problems cannot be solved with technical solutions alone. The ultimate success of any effort to secure information resources depends largely on the behaviour and attitudes of users involved because humans are the ones interacting with our systems, services, information and information technology.

Results and findings from this study will benefit both practitioners and academics in the field. Practitioners can use the findings to help assess their level of I.T. security establishment and identify their current I.T. security culture as well as determine how much of an improvement is needed to reach their desired I.T. security culture. On the academic side, the project will fill in the gaps of the descriptive and empirical research in the area of I.T security culture.

## II. LITERATURE REVIEW: I.T. SECURITY CULTURE

The term information technology security culture can be initially separated into three terms information technology security and culture. Information technology security refers to

978-1-4244-4649-0/09/$25.00 ©2009 IEEE 

the strategies and techniques used by organizations to protect information and technology. Information can encompass stored data, printed or data in transit, intellectual data, knowledge, and to simply anything that could be used to establish meanings of. Technology includes the equipment, tools and facilities that information is attached to. The term culture has not yet been mentioned and will be discussed next.

Culture is a complex concept and has been researched thoroughly in the management literature. The current consensus in the literature is that culture cannot be explained in its entirety, despite many research undertakings in the area. Therefore, this paper describes only organizational culture, not culture as a whole.

According to [4] there are three levels of culture within an organization: artefacts, espoused values, and basic assumptions and values. The basic assumptions and values are difficult to recognize due to existing at the unconscious level. It is, however, the core elements of organizational culture as it consequently expresses the espoused values. Espoused values are collective values, norms and knowledge of the organization which affect the behaviour of organizational members. The artefacts are at the surface and are difficult to interpret. Artefacts are visible organizational policies and processes which are based on the expressions of such norms and values. These three levels are interconnected and form the overall organizational culture.

In [4], the authors define organizational culture as 'the basic tacit assumptions about how the world is and ought to be that a group of people are sharing and that determines their perceptions, thoughts, feelings, and, their overt behaviour'. In basic terms, organizational culture refers to 'the way things are done in the organization' [5]. It is the unwritten rules and the assumptions of how things get done.

Every organizational culture is different to the next organization [6]. For example, Organization A may highly value and freely promote 'innovative thinking' from their employees, whilst Organization B may be more conservative and frown upon these sort of beliefs and behaviours. Every organization also has specific information security procedures, which are adhered to and built-in to the daily operational work environment that will develop as a piece of the organizational culture. An example of such a procedure is to keep a 'clean-desk' policy by storing away sensitive company information or to change passwords three months.

I.T. security culture could be understood as a set of principles influencing attitudes and behaviours of individuals, groups and the whole organization concerning I.T security. An organization may have has many pre-existing cultures in parallel forming part of the overall organizational culture. I.T security culture is one such pre-existing culture to support the broad organizational culture. I.T. security culture encompasses all socio-cultural measures and support technical security measures within an organization, so that information security becomes a natural aspect in the daily activities of every employee. Further, I.T. security culture are the assumptions of which types of I.T. security behaviour are accepted and encouraged by the employees of the organization [7-9].

I.T. security related principles may include maintaining confidentiality, integrity and availability of information within an organization. These sets of principles are values and assumptions relating to I.T. security that are shared and manifested by members of a group. Once group attitudes and behaviour begins to alter it would influence the individual employees approach to I.T. security, and likewise have an eventual effect on the overall organization.

## III. BACKGROUND: IT SECURITY CULTURE TRANSITION (ITSECT) MODEL

Our study on I.T. security culture improvement includes a development and implementation of the I.T. Security Culture Transition (ITSeCT) Model [10-12] to help SMEs and their employees transition towards an improved I.T. security culture. The model was implemented and evaluated in three Australian SMEs. An overview of each SME is provided in Table I.

TABLE I: OVERVIEW OF THREE AUSTRALIA SMES

| | **SME#1 Printing** | **SME#2 Timber** | **SME #3 Hi-Tech** |
|---|---|---|---|
| **Industry** | Billing and Printing | Timber Wholesaler | Hi-Tech Cameras |
| **Service Areas** | Australia, New Zealand & Asia | Australia-wide | Australia-wide |
| **Client Range** | SMEs and local government | Building companies and retailers | Defence, Universities, Oil & mining companies |
| **No. of Staff** | 80+ | 70+ | 10 |

The goals of the ITSeCT Model are to:

- provide an overall framework for implementing programs to help Australian SME and their staff transition towards IT security culture improvement;
- help facilitate the understanding of the transition process towards IT security culture improvement within managers and employees;
- help to identify the current IT security culture of Australian SMEs and their staff, and further, identify areas of IT security culture improvement;
- provide the foundation for further opportunities to implement practical steps for improving I.T. security culture through transition.

Benefits of the ITSeCT model are:

- the model being ideal for Australian SME due to staff hierarchy consisting of two levels – managers and employees.

- three simple phases providing a comprehensive step-by-step guide for managers and employees for improving IT security culture;
- two parties involved: managers and employees. Roles and responsibilities are defined in each phase of the transition process.

Before the ITSeCT model could be implemented and considered for evaluation in the three Australian SMEs, an initial assessment was considered to determine what improvements were needed.

## IV. I.T. Security Culture Assessment

An assessment was conducted at each SME to determine how much of an 'improvement' was needed to improve the I.T. security culture of the SME and its employees. This led to the development of four core questions:

1) *What is the level of I.T. security establishment in the SME?*
2) *What is the desired I.T. security culture of the SME and employees?*
3) *What is the current I.T. security culture of the SME and employees?*
4) *What 'improvements' are needed to transition towards an improved I.T. security culture?*

To answer these core questions, an assessment comprising of two parts was conducted in each of the three SME: 1) Preliminary Assessment - aims to answer the first two questions and 2) Primary Assessment - aims to answer the third question. The findings from the combined three questions are summarized and answers the forth core question.

### A. Preliminary Assessment

A preliminary assessment of each SME was conducted to answer questions one and two. The following four data collection techniques were used:

- *Informal Interviews*: provided background understanding of the SME such as main business operations, number of employees, business goals, I.T. security goals, I.T. security roles and responsibilities and current I.T. security controls and measures. The staff member in charge of the I.T. and systems within each SME was interviewed.
- *Observations:* were conducted to get a sense of the I.T. security behaviour in the workplace as well as aid in the development of the questionnaire in the following primary assessment.
- *Document Analysis:* was conducted to review company policies, procedures and guidelines related to I.T. security.
- *I.T. Security Controls Checklist*: to determine the type of I.T. security controls and strategies within each SME. The I.T. security controls checklist is based on the recommended list contained within the ISO/IEC 27002:2007. The checklist is grouped under three levels of I.T security establishment categories: 1) technical, 2) management and 3) organization. The three stages of I.T security establishment were based on the work of [13]'s I.T. security evolution in a company. Each new stage includes the characteristics of the preceding category and hence, the further up an organization is, the more established it is in I.T. security.

The results of the above preliminary assessment will help to provide insights to the level of I.T. security establishment and the desired I.T. security culture of each SME. The results are presented later in this paper.

### B. Primary Assessment

The primary assessment provides insight to the third question pertaining to the 'current' I.T. security culture of each SME and employees. The following two data collection techniques were used:

- *Questionnaire*: The paper-based seven-point likert scale questionnaire was distributed to SMEs members to explore current individual and organizational attitudes and values towards various I.T. security areas. The questionnaire is composed of two parts: 1) ten questions sourcing I.T security attitudes, and 2) Demographic information about the respondent.
- *Follow-up semi-structured interview:* was conducted to seek deeper views of the findings gathered from the questionnaire.

The next section presents the results and findings of previously mentioned assessments and is composed in the order of the four core questions.

## V. Results of I.T. Security Culture Assessment

### A. Question #1: What is the Level of I.T. Security Establishment in the SME?

The results of the informal interviews, observations, document analysis and the I.T. Security Control Checklist conducted provided insights to the level of I.T. security establishment of each SME. The level of I.T. security establishment outcomes of each SME is depicted on the I.T. Security Establishment Model [14] in Fig. 1. Note that each new stage in the model includes the characteristics of the preceding category and hence, the further up an organization is, the more I.T. security established it is. There are seven separate establishment levels throughout the three technical, management and organization categories. These seven I.T. security establishment levels are explained as follows based on the preliminary assessment conducted in each participating SME.

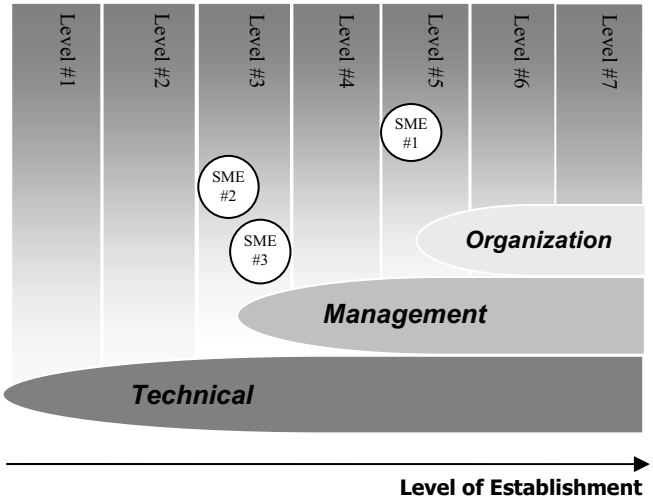
- *Level #1 Technical Controls 'Initiative':* Companies in this position have either installed 'off-the-shelf' products that came with in-built security features such as userIDs and passwords and firewalls, or have not given much thought to the basic technology available

to protect them. Furthermore, companies in this position are vulnerable to many I.T. security threats and hence are exposed at a high level to attacks or inappropriate information resource usage by their staff. Companies should give more thought to how data and information should be backed-up, encryption of sensitive information and/or automatic monitoring and logging of user activities.

- *Level #2 Technical Controls 'Developing':* At this stage, companies start to see the benefits of implementing an array of technical controls to combat I.T. security. Reasons for not implementing further controls may be due to 'lack of' funding, management support, I.T. security knowledge and/or value in investing in I.T. security. Furthermore, companies typically see technical controls as their way to combat against I.T. security, hence, which in turn provide them with a false sense of security since I.T. security is more than just implementing technical controls. Companies will continue to strive towards continuously seeking other technologies to combat I.T. security issues as they see the value in investing in technological controls. Realisation that I.T. security is more than implementing technical measure will see the company progress further.
- *Level #3 Technical Controls 'Established' and Management Controls 'Initiative':* Companies at this stage will not only strive towards continuously seeking other technologies to combat I.T. security issues, but also start to look into establishing formal policies and processes to manage I.T. security. At this stage, management would have expressed some level of concern for I.T. security and there would be some level of support from management. Furthermore, companies would like to see I.T. security controls more manageable and formalized. Working towards assessing and analysing risk helps to identify a range of information assets held within the company. It will also help to establish the level of risk of each information asset and anticipate its likely impact upon the company in the event of damage/breach. Furthermore, establishing an I.T. security policy for which to base the foundations of how I.T. security should be managed ought to be the next steps in the company's I.T. security initiatives.
- *Level #4 Management Controls 'Developing':* The realizations of the detrimental affects of I.T. security issues are apparent with management. Therefore, concern for I.T. security, and support and commitment from management is demonstrated here. I.T. security policy should be reviewed if not yet established. Once an I.T. security policy is developed then work will be required to communicate the policy to staff so they are aware of its existence and hence, encourage compliance to policy. Establishing an I.T. security awareness and education program will make staff aware of I.T. security and encourage proper security behaviour. Companies may look into setting up an I.T. security team if necessary or look at defining and allocating I.T. security roles and responsibilities to staff members. Management should stay abreast to current laws and regulations relating to data and information protection and privacy. Incident response planning should be considered to lay out the process for recording and dealing with I.T. security incidents. Looking forward, companies should start thinking about business continuity planning. Business continuity planning provides companies to plan for the continuity of the business after an unpleasant event/disaster. Having an additional disaster recovery plan, will provide the company with procedures to get back on track after a disaster.
- *Level #5 Management Controls 'Established' and Organization Controls 'Initiative':* In this stage, various management controls are considered and the company should start to consider organizational-wide controls that will benefit everyone throughout the company. The first thing to establish in the organization stage is to realize that I.T. security is an organizational-wide effort involving everyone within the company. The understanding that everyone is responsible for I.T. security and that it requires an organizational-wide effort are important first steps to this stage. This may begin with decentralizing I.T. security responsibilities to general staff members. Furthermore, work is needed in improving the overall I.T. security awareness of individuals and companies and hence, improves the whole company culture and individual culture of security.
- *Level #6: Organization Controls 'Developing':* At this stage, management controls are established and the overall I.T. security focus is on organizational-wide security. Here, adhering to standards the priority. Having I.T. security processes conform to an I.T. security standard will give management the peace of mind that due diligence has been considered. Developing further, is seeking certifications for I.T. security processes that have been implemented and using certified I.T. security products to provide a degree of security assurance.
- *Level #7 Organization Controls 'Established':* At this stage, organizational-wide I.T. security culture and awareness are well enforced through the organization. Companies are looking further to improve I.T. security on continuous basis. This may include measuring their I.T. security efforts via reviews and constant refinements, as well as, measuring up against standards, policies and other companies. Striving for continuous improvement will see the company constantly finding different ways to surpass its current I.T. security efforts.

As shown in Fig 1. of the level of I.T. security establishment for each SME, SME #1 Printing is the furthest in the I.T. security establishment model being in *Level #5: Management Controls 'Established' and Organization Controls 'Initiative'*. Whilst, SME #2 Timber and SME #3 Hi-Tech are both located in *Level #3: Technical Controls 'Established' and Management Controls 'Initiative'*. Also, note that SME #3 Hi-Tech is further ahead in Level #3 than SME #2 Timber because SME #3 Hi-Tech had recorded more *management* controls whilst a lower number of controls were recorded for SME #2 Timber.

Fig. 1. I.T. Security Control Establishment Level Outcomes of SMEs




The I.T. security establishment levels for each SME were presented in this section. In the next section, the next core question which provides insights to the desired I.T. security culture of each SME is explored next.

### *B. Question #2: What is the desired I.T. security culture of the SME and employees?*

Semi-structured interviews were used to collect data relating to company background to establish ground and more importantly, to determine the desired I.T. security culture of each SME. The interviews were conducted face-to-face on-site at each SME. Each interview went from 30 minutes to an hour. One person from each SME, who holds the designated I.T. security role in the company, was interviewed. Each Interviewee was asked to provide comments on their desired I.T. security culture for the organization. SME #1 Printing interviewee responded, *"When staff thinks and breathe I.T. security. Full Stop."* When asked to elaborate, the interviewee referred to the need for staff responsibility and staff knowing how to protect and handle data and information resources. The following excerpts were taken from the interview transcript when the interviewee was asked to elaborate further,*" Staff taking responsibility…", "Everyone treating data and information like their own."* and *"…being able to differentiate between sensitive data and not so sensitive data."* Further comments made by the interviewee related to desired I.T. security behaviours by staff and enforcing the company policy, *"Getting into the habit of locking down their workstations when they are a way from their machine even to get up to get a cup of coffee…they should know how easily it is for someone to come along and use account on their machine."*and*"…also we have a company policy stipulating proper use of I.T facilities – staff should know this…and abide by it."* SME #1 Printing interviewee's comments concluded with a desire for staff to be constantly aware of I.T. security at all times *"…I suppose always having I.T. security at the back of their minds."*

SME #2 Timber interviewee's response to their desired I.T. security culture is *"when everyone knows what to do and not always relying on the 'I.T guy' to look after the I.T system."* The interviewee had divulged that the company had suffered from a recent virus outbreak disrupting company operations for several days. Desired I.T. security related staff behaviour included *"thinking twice before double-clicking on an .exe file in emails."* Elaborated responses made concentrated on staff responsibility, staff knowing how to use I.T. resources safely and understanding the risks and impact I.T. security incidents. Excerpts of responses include *"know how to deal with new I.T security threats...being aware of the dangers"* and *"…recognizing the risks associated with their carelessness can result in major consequences to the company…".*

SME #3 Hi-Tech interviewee's desired I.T. security culture is when staff *"abides by the I.T. security policy as stated in our company policy".* Similarly to SME #1 Printing and SME #2 Timber, further elaborated comments were associated with staff responsibility, enhancing I.T. security knowledge and understand how to protect and handle data and information resources in the company. The following comments were provided when asked to elaborate, *"staff knowing how to safely protect and handle company data, documents and equipments they use at work…knowing the risk involved…", "…[staff]takes responsibility…"* and *"Where every employee has basic I.T. security literacy to understand the importance I.T security".*

From the findings of the interviews, five common desired I.T. security culture themes are apparent including:

1. *Staff take on board and shares the responsibility of I.T. security* - staff make I.T security a personal responsibility and everyone's responsibility;
2. *Basic I.T. security literacy* - staff to make security conscious decisions on how to protect and handle data and information resources as well as how to respond to new threats;
3. *Staff abiding by I.T. security related company policy* - staff behaving and approaching security compliant to company policy;
4. *Pro-active I.T. security attitude* - staff having a receptive, predictive and unified attitudes toward I.T. security; and
5. *I.T. security is second nature* - staff being constantly aware of I.T. security at all times.

The next section explores the current I.T. security culture of each SME and the subsequent section aims to provide insights in to how much of an improvement is needed to transition towards the desired I.T. security culture.

### C. *Question #3: What is the Current I.T. Security Culture of the SME and Employees?*

A questionnaire and follow-up semi-structured interviews was conducted to collect data on the current I.T. security culture of each SME and their members. A discussion summarising the current I.T. security culture of each SME is presented at the end of this section.

We extended the questionnaire structure in the work of [15] seeking individual and company's perception on I.T security. We added a forth sub-section to determine whether the staff is aware of availability or implementation of the I.T. security control in the company. Therefore, each questionnaire question has four sub-questions seeking:

1) *Personal view* – seeking respondent's individual perception;
2) *Company's view* – seeking the company's perceptions;
3) *Responsibility view* – seeking what the respondent's would do if they were in charge of I.T. security and held accountable; and
4) *I.T. security acknowledgement* – seeking whether the respondent is aware of the existence of the I.T. security control in the company.

The quadruplet will give interesting insights and fulfil gaps between the individuals' and company's perception, as well as, offer a didactic impact, since the respondent has to reflect upon the best solution if they were in authority. It also provides insights to whether the I.T. security controls are known by the respondents to be currently in practice by the company.

The questionnaire questions sought responses using a seven-point likert scale to provide a more accurate view of their attitudes and perceptions [16]. See question example in Fig. 2.

Fig. 2 Example of Questionnaire Question

| **Q1. IT security company policy should be readily available to all** | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **1 VSD** | **2 SD** | **3 D** | **4 50/50** | **5 A** | **6 SA** | **7 VSA** |
| a) *Personally*, my view is … | □ | □ | □ | □ | □ | □ | □ |
| b) *The Company's* view is … | □ | □ | □ | □ | □ | □ | □ |
| c) If I was *responsible*, than my view is… | □ | □ | □ | □ | □ | □ | □ |
| d) *Currently*, this is happening … | □ | □ | □ | □ | □ | □ | □ |

The questionnaire response rate from SME #1 Printing was 70 percent 85 percent from SME #2 Timber and 80 percent from SME #3 Hi-Tech. Hence, the total questionnaire response rate across all three SME is 75 percent.

Questionnaire findings uncovered that I.T. security was not a priority in all three SME and not much effort was made in managing and implementing it effectively. SME #1 Printing and SME #3 Hi-Tech both have company policy with related I.T. security content, where as SME #2 Timber did not have any policy documented. The company policy of SME #3 Hi-Tech was stored in the General Managers' office and hence, awareness of its existence was forgotten by employees. Company policy document of SME #1 Printing is reviewed on an annual basis but communication of updates was not directly made to employees, but instead only published on the Intranet. SME #3 Hi-Tech did not have a set period to review company policy. SME #2 Timber did not have any related I.T. security policy. Management for all three SME felt that I.T. security was not one of its top priorities. Further, there were no explicit expectations that are stated in company policy regarding I.T. security behaviour in the organization. However, management had some sort of outlook of how employees should behave as indicated in their interview responses. Furthermore, management was unsure whether their company had an acceptable level of I.T. security in the organization. Although SME #1 Printing and SME #3 Hi-Tech had not had any reports of external security breaches, there were indications of internal security breaches.

In summary, basic I.T. security knowledge, communication, commitment and direction from managers is needed to increase I.T. security awareness in the workplace. This will in turn establish ideal I.T. security attitudes and behaviours from employees as well as lessen employee confusion regarding who is responsible for I.T. security. The fact that everyone is responsible for I.T. security should be made clear and communicated throughout the company.

### D. *Question #4: What 'improvements' are needed to transition towards an improved I.T. security culture?*

This section will discuss and present improvements toward the desired I.T. security culture of the SME. The findings culminated from the informal interviews, I.T. security control checklist, observation, content analysis, questionnaire and follow-up interviews, and are summarized and presented as ways that the three SME could improve their I.T. security culture.

An improved culture means enhanced attitudes, behaviours, values and beliefs working towards building compliant behaviour. The list of recommendations below is aimed to improve I.T. security culture of staff by focusing on developing I.T. security compliant attitudes, behaviours and sensitivity to privacy as well as makes I.T. security second nature to staff and assumed throughout their daily work. Key improvement considerations for the SME to transition towards a desired I.T. security culture include:

- Senior management support and commitment;
- Properly structured and organized security policies procedures and guidelines;
- Provide basic I.T. security awareness, training and education program;

- Clearly define roles and responsibilities;
- Establish policy compliant behaviour;
- Stay abreast of current and changing laws and regulations;
- Focus on product security and standards;
- Exploit technology effectively; and
- Measure and review security efforts.

The above points are recommended for participating SME to improve their I.T. security culture.

## VI. CONCLUSION

This paper provided an assessment strategy and data collection techniques for assessing the level of I.T. security culture improvement in Australian SMEs. Four core questions seeking 1) the level of I.T. security establishment, 2) the desired I.T. security culture, 3) the current I.T. security culture and 4) the improvements needed to transition towards an improved I.T. security culture were explored in three participating Australian SMEs. The results and findings of the three participating SME showed different levels of I.T. security establishment, common themes between the desired I.T. security culture, differences and similarities in the current I.T. security culture, and a list of recommendations for I.T. security culture improvement for Australian SME to transition towards an improved I.T. security culture.

## REFERENCES


[1] AusCERT *2004*, *2004 Australian Computer Crime and Security Survey*, AusCERT, Accessed: May 2009, http://www.auscert.org.au.

[2] AusCERT *2005*, *2005 Australian Computer Crime and Security Survey*, AusCERT, Accessed: May 2009, http://www.auscert.org.au.

[3] AusCERT *2006*, *2006 Australian Computer Crime and Security Survey*, AusCERT, Accessed: May 2009, http://www.auscert.org.au/.

[4] E. H. Schein, *Organizational Culture and Leadership*, 2d Ed ed. San Francisco: Jossey-Bass, 1992.

[5] O. Lundy and A. Cowling, *Strategic Human Resource Management*. London: Routledge, 1996.

[6] S. P. Robbins, B. Millett, R. Cacioppe, and T. Waters-Marsh, *Organizational Culture*, 2nd ed: Prentice Hall, 1998.

[7] S. Ramachandran, S. V. Rao, and T. Goles, "Information Security Cultures of Four Professions: A Comparative Study," presented at Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, 2008.

[8] A. B. Ruighaver, S. B. Maynard, and S. Chang, "Organizational security culture: Extending the end-user perspective." *Computers & Security Computers & Security - Computers & Security*, vol. 26, pp. 56-62, 2007.

[9] K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: management's effect on culture and policy," *Journal of Information Management & Computer Security*, vol. 14, pp. 24 - 36, 2006.

[10] L. Ngo, *IT Security Transition Process*. Hersheym, PA: IGI Global Encyclopedia, 2008.

[11] L. Ngo, W. Zhou, and M. Warren, "IT Security Culture Transition Process," in *Encyclopedia of Information Ethics and Security*, M. Quigley, Ed.: Information Science Reference, IGI Gobal, 2007, pp. pages: 319-325.

[12] L. Ngo, W. Zhou, and M. Warren, "Understanding Transition towards Information Security Culture Change," presented at The 3rd Australian Information Security Management Conference, Perth, Australia, 2005.

[13] B. von-Solms, "Information Security - The Third Wave?," *Computers & Security*, vol. 19, pp. 615 - 620, 2000.

[14] L. Ngo, W. Zhou, and M. Warren, "Social Engineering," presented at Australasian Conference on Information Security and Privacy, Australia, 2006.

[15] T. Schlienger and S. Teufel, "Information Security Culture - From Analysis to Change," presented at 3rd Annual Information Security South Africa Conference, Johannesburg, South Africa, 2003.

[16] P. Jarvinen, "Research Questions Guiding Selection of an Appropriate Research Method," University of Tampere 2004.