2005

Understanding transition towards information security culture change

Leanne Ngo

Wanlei Zhou

Matthew Warren

Understanding Transition towards Information Security Culture Change

Leanne Ngo
Wanlei Zhou
Matthew Warren
School of Information Technology
Deakin University
mln@deakin.edu.au
wanlei@deakin.edu.au
mwarren@deakin.edu.au

Abstract

Transitioning towards an information security culture for organisations has not been adequately explored in the current security and management literature. Many authors have proposed how information security culture can be created, fostered and managed within organisations, but have failed to adequately address the transition process towards information security culture change, particularly for small medium enterprises (SMEs). This paper aims to (1) recapitulate key developments and trends within information security culture literature; (2) explore in detail the transition process towards organisational change; (3) adapt the transition process with respects to the key players involved in transition and propose a transition model for information security culture change; and (4) consider how this model could be used by managers and employees of Australian SMEs. A major intention of this paper is to provide academic researchers and practicing managers with an understanding of the transition process towards achieving information security culture change within SMEs.

Keywords

Information Security Culture, Transition Process, Change Management, SMEs.

INTRODUCTION

The environment is more dynamic than ever, computers are pervasive and boundaries are becoming less visible. We have seen a number of web technologies, networked based applications, telecommunications and wireless mobility come to light. These new technologies signify constant changes and more revolutions, and as a consequence of these changes, the dimensions of information security – once a single disciplinary area – have become multifaceted and convoluted (Ngo and Zhou 2005). As a result, organisations need to increase their information security capability to respond creatively to new challenges and to ensure survival in this new age.

Over the past half-century we have seen many approaches, safeguards and countermeasures developed, practiced and learned within organisations. We have seen technical approaches to security, which often focus on using computer systems' facilities for security. We have seen the involvement of management, such as providing governance and support for information security initiatives and the use of standards, certifications and measurements schemes for benchmarking and compliance checking. Furthermore there have been institutionalised efforts to safeguard and control the human aspects of information security (von-Solms 2000). Now, the focus is on establishing an information security culture.

In a short amount of time the security and management literature has produced several key ideas regarding how organisations can establish, foster and manage information security culture. However, none seem to address the transition process towards information security culture change and furthermore, how organisational members such as managers and employees may be affected by this transition. This paper represents research in progress which will use the proposed methodology to assist managers and employees of Australian SMEs in understanding the value of transition towards information security culture change.

This paper is composed in the following order – Section one (this section) introduces the problem and motivation for this research. Section two summarises the key developments in information security culture research. Section three explains the transition concept, including the transition process, how it differs to *change* as well as individual transition. Section four, our methodology is explained. Section five, we propose our transition model and consider how it can be used by managers and employees of Australian SMEs. Limitations and future research, as well as, conclusions are discussed in sections six and seven respectively.

INFORMATION SECURITY CULTURE

Research on information security culture has been predominantly focused on two areas. First, defining information security culture and second, institutionalising information security culture. These research and developments are elaborated here.

Defining Information Security Culture

Information security culture is often explained using a variety of theories and established principles from other research areas. This is because information security culture is a new and emerging area of research, thus making use of other theories as a basis for research appears logical. Theories belonging to organisational behaviour (Leach 2003; Stanton, Stam, Mastrangelo and Jolton 2004; Vroom and von-Solms 2004) and management (Parker 2002; Stanton, Stam, Guzman and Caledra 2003; Stanton *et al.* 2004) through to communication (Schlienger and Teufel 2003; Roth 2004) and established principles of psychology (Schein 1985; Kabay 1993) have been used as a basis for information security culture research.

Information security culture is part of the organisational culture (Schlienger and Teufel 2003). Culture relates to the way in which things are done in organisation (Martins and Eloff 2001) and thus, relating to the behaviour and attitude of people. Martins *et al.* (2001) defines information security culture as the assumptions of which types of information security behaviour are accepted and encouraged by the employees of the organisation. Whereas, Schlienger *et al.* (2003) affirms that information security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee. Therefore, information security culture can be understood as how things are done (i.e. accepted behaviour and actions) by employees and the organisation as a whole, in relation to information security.

Institutionalising Information Security Culture

The second predominated area of information security culture research is Institutionalisation. This usually involves three main processes. These processes include establishing, fostering and managing information security culture.

Establishing a security culture means to change the current culture to a more security conscious one. This may involve altering the behaviour and attitudes of people to be security aware. This may also involve an examination of the current culture in the organisation to highlight areas that require greatest attention for change. Research on changing organisational culture towards a security conscious culture were researched by Schlienger *et al.* (2003), Kuusisto, Nyberg and Virtanen (2004), Roth (2004) and Vroom *et al.* (2004).

Fostering a culture takes time (Kuusisto *et al.* 2004). The authors explain that if the values of each subject (i.e. individuals, the whole organisation and society) are unified, then a unified culture can be formed in less than a few years. However, if the subjects are not unified, then the process can take significantly longer. von-Solms and von-Solms (2004) asserts the importance of properly structured and organised security policies, but more so, the effective communication and education of these policies to employees, otherwise the chances that they will manifest in company culture are minimal.

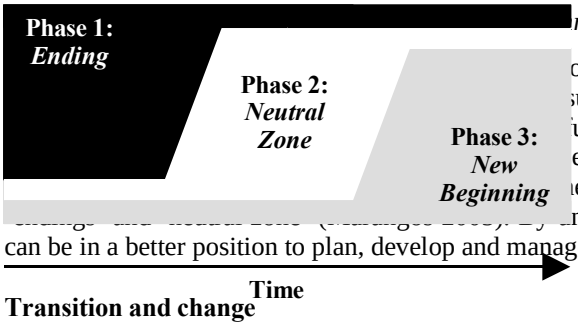
Research focused on managing information security culture is reflected in Schlienger's *et al.* (2003) work, who presents an information security culture management cycle adapted from an internal marketing concept. The authors state that security culture is very similar to internal marketing in terms of promoting certain values, corporate goals and philosophies within an organisation.

From our review of the literature on information security culture research, none seem to address the transition towards information security culture change. Much of the key research is focused on establishing, fostering and managing information security culture without fully understanding the transition required for information security culture change to take place. In particular, information security culture research based on organisational change theory has failed to mention the transition process as an aid to facilitate change. Since creating an information security culture involves changing the current culture to a security conscious culture we need to understand the transition process that organisations, managers and employees go through. In the management literature, transition management has been discussed as a facilitator in assisting organisational change (Bridges 2003). We address this major research gap in this paper.

THE TRANSITION CONCEPT

According to Bridges (2003), a leader in the study of transition management, understanding the transition process can assist towards successful organisational change. A successful transition requires the completion of three phases: (1) Ending; (2) Neutral zone; and (3) New Beginning. However, these phases are not separate stages with clear boundaries. The process of transition involves changeover, as dominance is passed on from one stage

to the next. As a result, one can be in more than one of these phases at the same time. Bridges's (2003) transition process is illustrated in Figure 1.



ree-phase transition process

or to starting something new, you have to end what used to suade people to let go of the past and move on. Phase two is using time in the transition phase (Bridges 2001; St-Amour e three ends with a new beginning. Beginnings can only be em to, and when they have been preceded by well-managed nderstanding each phase of the transition process managers can be in a better position to plan, develop and manage the transition process.

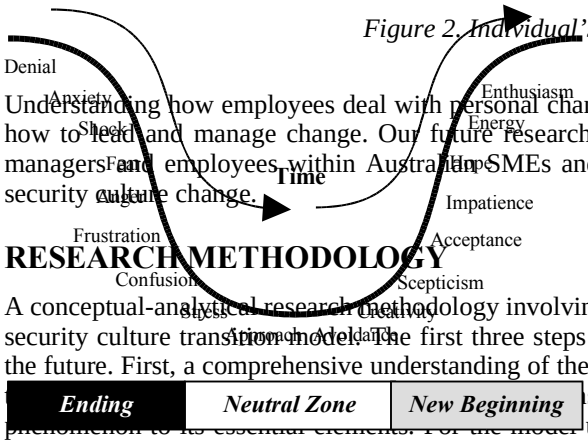
Transition and change

Change causes transitions, and transition begins with an ending (Bridges 2003). Transition means coming to terms with the new environment in which organisations and employees find themselves. Change is not the same as transition (Harvard Business School 2003). These two concepts are separate and should not be confused. Consider this analogy. If change requires letting go of one's hand in order to take hold of another to cross a ditch, then the gap in between - where you are left floating in that nowhere place - is the transition. Change requires people to behave or react in a new and different manner (Iacovini 1993). Change may (time and again) require us to sacrifice something that we have grown accustomed to (Bridges 2003; McGreevy 2003; Magee *et al.* 2005). Change focuses on beginnings; beginning a new process, a new system, a new way of doing things. Whereas, transition, starts with endings such as ending a job, an office, and hence, a way of doing things (Bridges 2003).

Individual Transition Process

People within the organisation are also going through their own psychological transitions (Iacovini 1993; St-Amour 2001; Harvard Business School 2003). Figure 2 shows an adaptation of an individual transition process and the psychological experiences as suggested by St-Amour (2001) during each transition phase.

Figure 2. Individual's Psychological Process



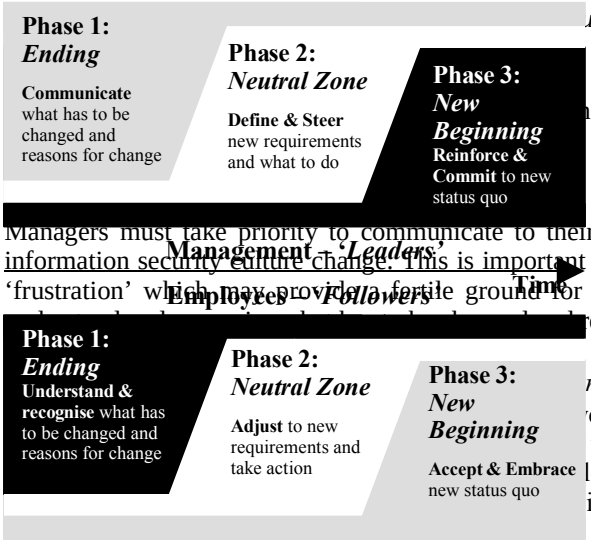
Understanding how employees deal with personal change can provide a potent reference for managers regarding how to lead and manage change. Our future research will explore the psychological transition experiences of managers and employees within Australian SMEs and how this may affect the transition towards information security culture change.

RESEARCH METHODOLOGY

A conceptual-analytical research methodology involving a series of five steps is used to construct the information security culture transition model. The first three steps have been completed, whilst the last two are planned for the future. First, a comprehensive understanding of the phenomenon through an extensive survey of the literature sition process was conducted. Secondly, a reduction of the phenomenon to its essential elements. For the model used in this work, only the transition process required for information security culture change and how it will affect the management and employees of SMEs were considered. Thirdly, the first-cut model was devised. The plan for the fourth stage is to verify and validate the model by presenting it to the management and employees of Australian SMEs for our present research. In the fifth stage, the plan is to refine the model from the feedback provided.

OUR MODEL: INFORMATION SECURITY CULTURE TRANSITION MODEL

This paper proposes a transition model based on Bridges's (2003) transition framework that is intended to assist Australian SMEs in transitioning towards information security culture change. According to Bridges's (2003) transition process, there appears to be two main players for successful transition to occur – leaders and followers, and therefore, managers and employees, respectively. The model is shown in Figure 3. The model highlights the respective roles and responsibilities of managers and employees. The first has the role of overseeing and managing the process and the latter, adapts and accepts the transition. The staff hierarchy in Australian SMEs consists predominantly of two levels – the managers and general employees, therefore, making our transition model ideal for discussion.



urity Culture Transition Model

ed in detail with reference towards information security

Managers must take priority to communicate to their employees what has to be changed and the reason for information security culture change. This is important as employees may experience 'shock', 'fear', 'anger' and 'frustration' which may provide a fertile ground for insider threats. Therefore, it is crucial for employees to reason for change. This requires the following:

r whom – Chia, Maynard and Ruighaver (2002) argues that e can not have security at all. Managers need to explain the why a security conscious culture is needed. The potential longer be ignoring security threats, no longer see security as interacting with IT/IS without security in mind.

- *Give people information on a continuous basis* – Employees need to know why there is a sudden interest in establishing information security culture. Ideally, managers can outline that the old ways of doing things such as the current 'non-security' minded behaviour and attitudes are no longer acceptable. Managers can explain why this is so, (e.g. the current way is no longer appropriate for the organisation's business and security goals). Managers may need to emphasise the implications of such ignorance of security (e.g. monetary and operational loss to the organisation).

Phase 2: 'Neutral Zone'

For employees progressing directly from an old culture, the transition towards a security conscious culture also represents an important phase of moving from an unknown area to a known area with increased responsibilities, independence and freedom. Managers must define new requirements and steer their employees in the right direction. Employees will need to adjust to these requirements and take action if a transition into the next stage is to be achieved. This requires the following:

- *Redefine new requirements* – this is the stage whereby managers define a set of new requirements for which an information security culture change is to surface. Employee participation may mean less confusion and decrease ambiguity. As a result, employees will benefit, as they are contributing and know where to go in the transition towards change.
- *Establish temporary solutions* – Reviewing security policies and procedures so it aligns with future security and business goals. If there are no security policies or procedures in place, this is a good opportunity to create some. Alignment with a generic baseline information security standard may allow for measurement and benchmarking. Establish information sessions to clarify any ambiguity.
- *Establish a communication channel* – Schlienger *et al.* (2003) recommends managers should attempt to 'sell' information security awareness. This may involve utilising different marketing strategies and determining the most appropriate type of channels of information delivery.
- *Enhance creativity and learning* – establish focus groups that allow managers and employees to discuss the transition and allow for questions and answers to reduce confusion. Allow employees to participate and contribute towards raising information security awareness for themselves, among each other and for the organisation.

Phase 3: 'New Beginning'

As transition ends with a new beginning – the beginning of information security culture change. Managers must be ready to reinforce and commit to the new status quo, whilst employees begin to accept and embrace it. Bridges (2003) advises that to make a new beginning, people need to understand the four P's: the purpose, a picture, the plan, and a part to play. This requires the following:

- *The purpose* – Managers should go over the problems again and reinforce why the old ways of doing things had to end and the benefits of information security culture change.
- *The picture* – Managers should explain and provide an overall vision regarding what the organisation is hoping to establish after completing the transition.

- *The plan* – Managers should consider devising a transition plan towards information security culture. This plan should outline the incremental steps required towards change.
- *The part to play* – Managers should make sure that each employee in the organisation has a role to play and have responsibilities that they are accountable for. Allocating roles to employees will provide them with first-hand knowledge on real security problems facing the organisation. Given that employees are taking part in the transition process, there will be higher chances of them embracing the new culture and hence, be ready to accept it.

This work proposed an information security culture transition model based on Bridges's (2003) transition framework that can be used by managers and employees of Australian SMEs for transitioning towards information security culture change.

LIMITATIONS AND FUTURE RESEARCH

Key findings in both the 2004 and 2005 Australian Computer Crime and Security survey showed the top security management challenges for organisations were due to inadequate staff training in computer security management and poor security culture within organisations as the top vulnerabilities reported. Furthermore, changing the user's behaviour and attitudes towards security were also highlighted as key challenges (AusCERT 2004; AusCERT 2005). As a result, the authors plan to validate and refine our transition model by seeking feedback from managers, IT professionals and general employees of Australian SMEs. Until this is performed, the model will remain incomplete, and hence, the suitability of the model in practice will not be known. Future research project will focus on this research gap to promote information security awareness and establish an information security culture within Australian SMEs.

Recent research by Sarriegi, et al (2005) conducted an empirical field study assessing security management in SMEs. Their results showed that various organisations are at different levels within the security management evolution with regard to their implemented security systems. This might provide an interesting area to consider for future research in identifying at which stage of the security management evolution Australian SMEs are currently at. This will allow for the consideration of how big of a change that Australian SMEs are ready to undergo and to assist in transitioning towards information security culture change.

Furthermore, future research will explore the individual psychological transition experiences of managers and employees within Australian SMEs and how their personal experiences may affect the transition towards information security culture change. This paper has mentioned, for example, that the Ending phase of the individual psychological transition process may be seen as a fertile ground for developing potential insider threats due to individuals experiencing shock, fear, anger and frustration during this phase. Hence, knowing the psychological experiences of individuals may allow for a better understanding of how employees deal with personal change, and which can provide a strong reference for managers about how to lead and manage change.

CONCLUSION:

Transition is the adjustment, development and change experienced by people within organisations when progressing towards achieving a particular change. Understanding the transition process is crucial for successful organisational information security culture change. Furthermore, identifying the key roles of management and employees in the transition process will allow for better understanding of their respective responsibilities.

The purpose of this paper was to highlight to managers and academia the importance of understanding the transition process required for information security culture change. This paper recapitulated the key developments within information security culture research and commented on the lack of reference to the transition towards change in the literature. This paper also put forward a transition model outlining the roles of leaders and followers and their respective responsibilities in each of the transition phases. The model was developed based on key information security culture research and Bridges's (2003) transition process framework.

REFERENCES:

COPYRIGHT