2007

Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia

S. Dojkovski
Deakin University, sneza.dojkovski@deakin.edu.au

Sharman Lichtenstein
Deakin University, sharman.lichtenstein@deakin.edu.au

Matthew J. Warren
Deakin University, matthew.warren@deakin.edu.au

FOSTERING INFORMATION SECURITY CULTURE IN SMALL AND MEDIUM SIZE ENTERPRISES:

AN INTERPRETIVE STUDY IN AUSTRALIA

Dojkovski, Sneza, Deakin University, 221 Burwood Rd, Burwood, Melbourne, Australia, 3125, sneza.dojkovski@deakin.edu.au

Lichtenstein, Sharman, Deakin University, 221 Burwood Rd, Burwood, Melbourne, Australia, 3125, sharman.lichtenstein@deakin.edu.au

Warren, Matthew John, Deakin University, 221 Burwood Rd, Burwood, Melbourne, Australia, 3125, matthew.warren@deakin.edu.au

Abstract

By having an effective organisational information security culture where employees intuitively protect corporate information assets, small and medium size enterprises (SMEs) could improve information security. However, previous research has largely overlooked the development of such a culture for SMEs, and the national context in which SMEs operate. The paper explores this topic and provides key findings from an interpretive Australian study based on a literature review, two focus groups and three case studies. A holistic framework is provided for fostering an information security culture in SMEs in a national setting. The paper discusses key managerial challenges for SMEs attempting to develop such a culture. The main findings suggest that Australian SME owners do not provide sufficient support for information security due to insufficient awareness of its importance and may also be affected by national attitudes to risk. The paper concludes that Australian SME owners may benefit from adopting a risk-based approach to information security and should be educated about the potential strategic role of information technology and information security. The paper also identifies the value and difficulty of promoting a behavioural and learning approach to information security to complement traditional technological and managerial approaches. Implications for theory and practice are discussed.

Keywords: information security culture, small and medium size enterprises

1 INTRODUCTION

The contribution of insiders to organisational information security risk is well reported. Highlighting the significance of this class of risk are recent figures revealing that employee misuse and abuse of internet services comprise twenty - fifty per cent of all internet incidents (AusCERT 2005; CSI/FBI 2005; ISBS 2006). In response, many companies have developed an interest in cultivating *intuitive* — rather than *enforced* — employee adherence to information security policy, processes and procedures (Dhillon 2001). Such companies are interested in the institutionalisation of information security practices as information security culture, here defined as the set of employee assumptions about what is, and is not, acceptable in relation to information security (Martins & Eloff, 2001). The potential value of adopting a socio-cultural approach to information security management was recently highlighted by Galletta and Polak (2003). Their study revealed that peer and supervisory culture may be highly influential in the management of internal internet misuse and abuse. However, while progress has been made globally in the enculturation of information security, more is needed (Ernst & Young 2006).

To assist companies in establishing an information security culture, experts have identified various approaches based on policy, awareness, training and education (Lichtenstein & Swatman 2001; Furnell et al. 2000; Schlienger & Teufel 2003). However, managerial initiatives alone will not significantly influence employee behaviour (Rosanas & Velilla 2005) and new conceptual frameworks are needed that identify and integrate complex behaviour modification and cultural change. Supporting the need for further research in this area, the Editor-in-Chief of the respected *Computers & Security* journal observed recently that the human factor in information security deserves greater research attention (Schultz 2005).

Turning to organisations whose information assets are least protected, experts suggest that small and medium size enterprises (SME) are particularly disadvantaged in the development of secure employee behaviour (Dimopoulos et al. 2004; Furnell et al. 2000; Helokunnas & Iivonen 2003; Taylor & Murphy 2004). We suggest that developing a strong information security culture in SMEs may address many of the behavioural issues that underpin information security breaches in such companies. We further note that existing conceptual frameworks for developing information security culture are preliminary and fragmented, and mainly based on considerations for large organisations rather than catering to the special characteristics of SMEs.

In addition, the national environment has been overlooked by existing frameworks. In a recent Australian survey, forty percent of respondent companies identified information security culture as a key concern (AusCERT 2005). This paper reports key findings from a study conducted in the Australian SME context, where a medium size business has between 20 and 200 full-time employees, and a small business has less than 20 full-time employees (ABS, 2001).

The paper explores the fostering of an information security culture in SMEs in a national setting (Australia). The topic was explored by conducting a literature review, two focus groups, and three case studies of small businesses. The remainder of the paper is organised into five sections. In the first section, we review previous research on information security culture, highlighting the shortfalls of current approaches, particularly for SMEs and national environments. In the second section, we summarise the research design employed for the study. In the third section, we provide a holistic conceptual framework developed from the study. The fourth section provides a discussion of the key challenges faced by SME managers and, in the context of Australia, the role of the Australian Government (federal and state). Fifth, conclusions are drawn, research limitations discussed, and future research directions proposed.

2 THEORETICAL FOUNDATIONS

This section reviews representative contemporary literature on information security culture, information security for SMEs, and information security culture within Australian SMEs. As introduced earlier, the development of information security culture is an attempt to addresses the insider misuse threat in companies, as revealed by many studies and experts (c.f. Dhillon 2001; Magklaras & Furnell 2004). Employees may ignorantly or negligently contribute to information security risks – for example, by unwittingly retrieving spam electronic mail, opening virus e-mail attachments, or dismissing information security threats as unimportant in comparison with other needs such as usability (Besnard & Arief 2004). In a recent survey (McAfee 2005), findings of insider misuse included:

- Twenty-one per cent of workers allowed family and friends to use company laptops and personal computers for internet access;
- Fifty-one per cent of workers connect their own devices or gadgets to their company personal computer;
- Sixty per cent of workers stored personal content on their company personal computer;
- Ten per cent of workers downloaded prohibited content at work;
- Sixty per cent of workers stored personal content on their company personal computer.

In response, many companies in developed countries have implemented a range of managerial and technical measures within an overall information security management program based on policies, procedures and practices. However increasingly, information security culture is considered a way to embed appropriate security practices. Next, we review representative published literature on information security culture.

2.1 Information Security Culture

Experts have previously proposed conceptual frameworks for information security management that include information security cultural development based on management initiatives of policy, awareness, training, and education (c.f. Knapp et al. 2006). In recent years, several dedicated frameworks for information security culture have emerged, based on: organisational culture and the measurement of information security culture (Schlienger & Teufel 2003); shared values (Helokunnas & Iivonen 2003), stages of information security awareness maturity (von Solms 2000); inputs associated with the development of individual, group and organisational levels of information security enculturation (Martins & Eloff 2001); socio-technical perspective on information security (Stanton et al. 2004); persuasive prescriptive awareness approach based on morals and ethics (Siponen 2000); informal methods of enculturation (Vroom & von Solms 2004); key concepts of organisational culture (Zakaria & Gani 2003); personnel capabilities (Furnell & Clarke 2005); organisational learning (van Niekerk & von Solms 2003) and a multifaceted approach (Chia et al. 2002).

While such frameworks are clearly valuable, they portray a fragmented theoretical field, lacking in integration across the different areas of focus. Furthermore, they do not address the special information security challenges encountered by SMEs, or the national context, each of which we now briefly review using representative literature.

2.2 Information Security in SMEs

SMEs in developed countries generally have a weak understanding of information security, security technologies and control measures, and neglect to carry out risk assessments or develop security policies (Dimopoulos et al. 2004; Gupta & Hammond 2005; Helokunnas & Iivonen 2003; ISBS 2006). This may be because SMEs lack the funds, time and specialised knowledge to coordinate information security or offer adequate information security awareness, training and education (Furnell et al. 2000;

Dimopoulos et al. 2004; Gupta & Hammond 2005). However, the literature suggests a quite different explanation, as now discussed.

According to published reports, SME owners are not supportive of information security in terms of budget or time, thus impacting the level of security awareness and security technology. For example, Johnson and Koch (2006) recently found that home-based SMEs will not pay for security. In business, while SMEs often use power surge protectors, they are unlikely to deploy encryption, firewalls, access control technologies and dial-back modems (Gupta & Hammond 2005). Gupta and Hammond further point out that, lacking specialised knowledge of security technologies, SMEs often retain the security technologies with which they are already familiar and which therefore offer immediate convenience. Further, by giving higher prioritisation to other business tasks, SMEs only occasionally review their information security needs. Moreover, with fewer breaches, there will be fewer reports to business owners and thus information security may appear even less important and attract less management attention and support (Gupta & Hammond 2005). Finally, prior research suggests that SMEs do not perceive IT as linked to business strategy and may extend their belief to security technologies which are therefore less likely to command owner respect (O'Halloran 2003). Indeed, recent research highlights a need to link information security with information systems strategic planning and thus company goals (Doherty & Fulford 2006).

2.3 Information Security in Australian SMEs

The Australian context is of particular interest to this research. In thirty-one per cent of Australian SMEs, it is the business owner who makes the buying decision for information technologies (IT) (Hallett 2004). In a recent Symantec study of IT use in Australian SMEs, three of the top four IT concerns reported were security-based – viruses (twenty-one per cent), security (thirteen per cent), Internet speed (thirteen per cent) and spam filtering (twelve per cent) (ZDNet Australia 2004). However, the Symantec study found that most SMEs spent less than ten per cent of their IT budget on information security technology. Twenty-nine per cent of the companies explained as their reason for low spending that IT security was not viewed as a priority, twenty-five per cent cited inadequate time to attend to IT security, and twenty per cent reported having restricted budgets for IT security. While ninety-five per cent of the responding businesses had antivirus software installed, only sixty-four percent used firewall software and only forty-three per cent used spam filters.

The state of information security in Australian SMEs is also a result of national and cultural influences. Australian information security coordination programs for businesses have recently deteriorated with the demise of the National Organisation for the Information Economy (NOIE) (Warren 2003). The politically motivated decision resulted in the closure of government departments dedicated to promoting the use of technology and raise security awareness among Australian SMEs. Such promotion included several national security awareness programs extended to business owners across Australia. A national risk appetite may also be involved, with a recent study of internet banking adoption in Australia revealing significant security risk-taking, which may be lower in other countries (Lichtenstein & Williamson 2006).

Emerging from the above review, a fresh conceptual framework is needed that identifies and integrates the complexities of behaviour modification and cultural change with management initiatives and that accommodates the special characteristics of SMEs operating in a national context.

3 METHODOLOGY AND RESEARCH DESIGN

Building a conceptual framework to guide the development of information security culture necessarily involves considering how people think and behave. Seeking to gain deeper 'rich picture' understandings of key influences on information security culture, we chose a qualitative, interpretivist approach to study this topic. We believe that knowledge and truth are socially constructed with

multiple conflicting versions of reality to be found. Interpretive research is advantageous for the serendipitous discovery of new evidential data and insights because of its flexible approach.

The study was conducted in four phases and particularly explored small businesses - that is, firms with less than 20 employees (ABS 2001). In *Phase One*, a preliminary conceptual framework was developed by reviewing and synthesising relevant literature, using the subjective-argumentative approach of Galliers (1992). In *Phase Two*, a focus group was conducted in November 2005 to collect initial data to explore and enhance the framework. Focus groups can be useful for theory exploration and theory validation in electronic business topics where multiple stakeholder types are involved (Lichtenstein & Swatman 2003). The initial focus group was conducted with four information technology (IT) consultants in Geelong, a semi-rural city in south-east Australia in the state of Victoria. Participants provided IT services, including security services, to small businesses in the local Geelong region. Participants were asked questions relating to potential influences on the development of information security culture in Australian SMEs. Specifically, participants were asked about SME awareness of information security, the challenges that SMEs face in fostering an information security culture, and the feasibility of the preliminary framework. Focus group data was transcribed and analysed using an adapted inductive grounded approach based on (Glaser 1992). Findings from the focus group were used to help develop questions for the next phase, and to confirm the value of the preliminary framework.

In *Phase Three*, conducted in 2006, three interpretive case studies were conducted. A case study approach was selected as it can enable the researcher to investigate in-depth issues in context and build theory (Eisenhardt 1989). Multiple case studies were conducted as there was some concern that findings from a single case may be unique to that organisation in such an unexplored topic area. Three cases were investigated as findings were similar by the third study, suggesting that there was no special need for further case studies (Darke et al. 1998). The cases were chosen according to the theoretical sampling strategy of Eisenhardt (1998) in order to develop understandings about the theory being explored. We elected to study three small businesses, again in the region of Geelong. Fictional names are hereafter used as company names for confidentiality reasons. One company comprised an engineering consultancy with twenty employees ("ConsultEng"). A second company comprised an IT service provider with three employees ("ServIT"). A third firm comprised an IT service provider with five employees ("ProvIT"). These three firms were selected for three main reasons. First, as small regional (rather than city-based) firms, the three companies represented the less advantaged companies of Australia. Second, the three firms did not profess to have effective information security cultures at the time of study. Third, as technical firms, some employees possessed an understanding of information technologies, thus enabling more specific issues relating to information technologies to surface.

Eight employees in total were interviewed by the first author– four at ConsultEng, one at ServIT (the owner) and three at ProvIT. In each case, ordinary employees as well as business owners were interviewed, except at ServIT where only the business owner was interviewed. Interviews were semi-structured single interviews of around one and a half hour's duration. The researcher also gathered background documents of organisational structure and information technology strategy. All three companies did not possess formal information security documents so none were collected.

Definitions of key terms were provided and questions were based on the preliminary framework. Five groups of questions were asked, probing: (1) managerial issues (policy, procedures, benchmarking, risk analysis, budget, management, response, training, education, awareness, change management); (2) behavioural issues (responsibility, integrity, trust, ethicality, values, motivation, orientation; personal growth); (3) electronic learning (e-learning), cooperation, collaboration and knowledge sharing; (4) individual and organisational learning; (5) ethical, national and organisational culture. The complete question set can be obtained from the first author.

Qualitative content analysis techniques were employed in each case to analyse the data. Each case was analysed as follows. One of the researchers inductively discovered coded categories over iterative

readings of the case interview transcripts, drawing on the earlier preliminary framework to help identify categories which were later grouped into final themes. A second researcher conducted an independent analysis and the two sets of themes were compared, seeking reliability. The two sets of themes were similar, and so were integrated. Data from organisational documents were employed as triangulation to establish internal validity. A cross-case analysis established that case findings were markedly similar on key points, which were used to revise the framework and enhance the set of managerial challenges from Phase Two. Samples of the analysis may be obtained from the first author on request.

In Phase Four, a focus group with four participants was held in 2006 to validate the conceptual framework. Geelong-based participants included an IT services consultant to SMEs, an Australian (and international) IT security expert, a small business owner, and an IT services employee from a medium size organisation. As mentioned earlier, focus groups are highly useful for theory validation (Lichtenstein & Swatman 2003). The focus group was of three hours duration and involved validation of (1) the revised framework from Phase Three, and (2) the set of managerial challenges from Phase Two. The revised framework was drawn on a white board and participants, led by a moderator, discussed each element of the framework and how the elements related to one another. Small but valuable changes to the framework were proposed, considered and resolved at the session. The framework was revised during the session, and the final framework is presented in the next section. The set of key managerial challenges from Phase Three was confirmed and later enhanced by a qualitative content analysis conducted in a similar way to the analysis of the initial focus group in Phase One. The set of challenges are also discussed in a later section.

4 FINDINGS: CONCEPTUAL FRAMEWORK

In figure 1, we provide an issue-based conceptual framework for fostering information security culture in Australia, derived from the four phases of the study. In this section, the framework is described, and also discussed in terms of prior theory where relevant. First, three external influences are described: national and ethical culture; government initiatives; and vendors.

National and Ethical Culture: National cultures may affect organisational information security culture and this possibility should be considered by government initiatives (see below). Societal ethics may also have an impact. In addition, ethical standards can differ between countries. Previous research on information security culture for large and small organisations has ignored these key influences, with one exception. It has been pointed out that value nets of companies sharing relevant knowledge can strengthen information security culture (Helokunnas & Kuusisto 2003). According to the researchers, different nations and companies have their own values and cultures and by working together, the interaction of the values and cultures can promote effective information security in each region or firm.

Government Initiatives: Governments (federal and state) can play key support roles including, in an Australian context, the distribution of information security awareness brochures to SMEs and the conduct of national SME information security benchmarking. To assist Australian organisations, sample security risk scenarios can be developed from existing information security resources. These can be couched in terms of asset loss protection in order to better appeal to SMEs. Initiatives should also be targeted to the national context. For example, Australia has a laissez-faire culture and thus brochures and other initiatives should be targeted at addressing this "risk-accepting" characteristic. This influence has generally not been previously identified for either large organisations or small. However, Martins and Eloff (2001) proposed benchmarking as useful for large organisations which, of course, have the resources, including know-how, to carry it out.

Vendors: Information security technology vendors play key roles. They may provide information security awareness, but they may also provide trustworthiness to SME firms which otherwise might

feel they are being sold unnecessary hardware and software. This influence has not been previously identified for either large organisations or SMEs.

The next set of influences is internal to an SME: leadership/corporate governance; organisational culture; managerial; individual and organisational learning; organisational security awareness; review/evaluate.

Leadership/Corporate Governance: SME owners must demonstrate leadership in organising managerial measures, acting as a role model for information security, taking initiative to find out about information security, and developing corporate governance structures to provide adequate assurance of information security. The value of leadership was noted for large organisations by Dutta and McCrohan (2002), but has not been previously identified for SMEs.

Organisational Culture

The local organisational culture will affect the information security culture. For example, an open culture promotes casualness in approach to information security. This influence has not previously been identified for either large organisations or SMEs.

Managerial

First, information security policies and procedures direct required and acceptable employee security-oriented behaviour, as also suggested by Martins and Eloff (2001) for larger firms. It is noted, however, that while SMEs in the study did not believe they needed formal policies, focus group participants felt it important that they have them. Greater awareness and the results of a risk analysis were seen as key for assuring SMEs that formal policies and procedures are truly needed. Second, SMEs should be guided by the results of a process of asset loss protection which can stem from a scenario-based risk analysis sourced from external accessible content. Martins and Eloff (2001) previously proposed this influence as important for large organisations however it is a new finding for SMEs. Third, a budget should be allocated for information security, particularly in SMEs where proper resource provision may easily be overlooked. Such a budget will enable cultural initiatives such as training to be resourced. Martins and Eloff (2001) have previously suggested that budget has an influence on large organisations. Fourth, procedures that respond to information security incidents will help emphasise the importance of information security to employees; this has also been suggested by (OECD 2002) more generally. Fifth, SMEs will be helped by regularly assessing their information security culture. This factor has not been previously proposed. Sixth, the contract of employment, or employee handbook where no contract exists, can offer incentives and stipulate penalties regarding employee information security conduct, thus influencing employee motivation. All managerial processes must be regularly assessed.

Individual and Organisational Learning

E-learning, training and education are potentially valuable initiatives for developing information security culture for SMEs, as also found for larger firms by (Furnell & Clarke 2005; Furnell et al. 2004; Siponen 2000). Knowledge sharing, cooperation and collaboration were found important to learning at individual and organisational levels in order to develop information security culture. The importance of these processes has not been previously identified for large organisations or SMEs. Learning processes must be assessed regularly.

Organisational Security Awareness

Marketing of information security – in particular, informal awareness measures that support the formal awareness provided externally – is essential. Brown bag lunches and wall posters were mentioned as examples. Formal and informal awareness measures have been previously suggested for SMEs by Furnell and colleagues (2004). However, the researchers did not separately allocate formal and informal measures. This framework clearly assigns formal activities as external responsibilities and informal activities as internal responsibilities. Awareness measures should be persuasive, as proposed by Siponen (2000) more generally. Awareness processes must be assessed regularly.

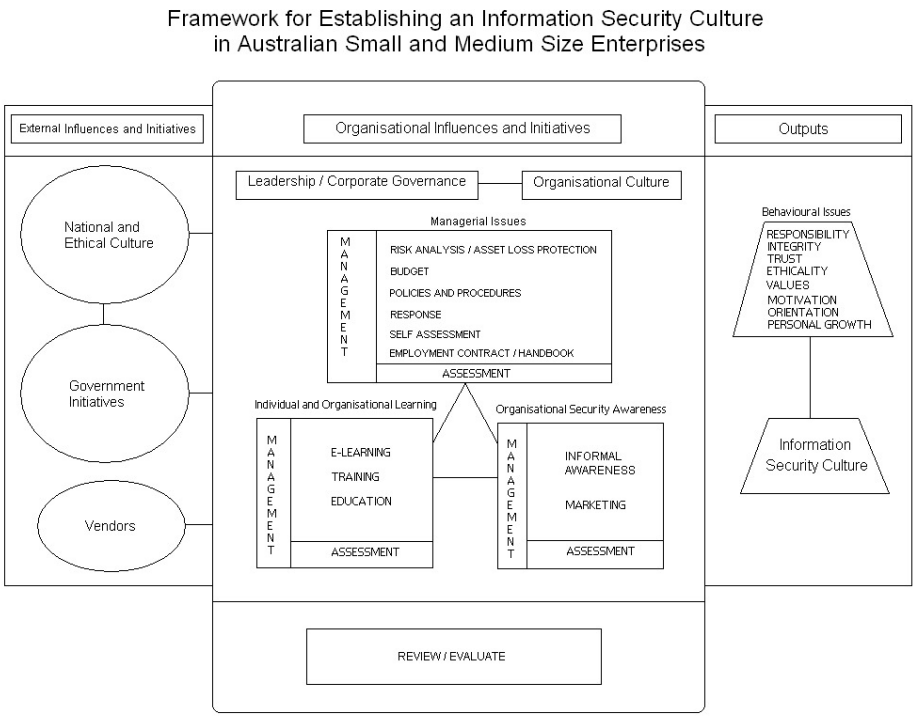

Figure 1: Framework for fostering information security culture in SMEs

Review/Evaluate: SMEs should regularly review and evaluate the measures adopted in order to continuously improve. This finding has been made previously for information security management programs (for example, Lichtenstein & Swatman 2001).

Behavioural: A range of external and internal initiatives can develop desirable behavioural traits of responsibility, integrity, trust and ethicality. According to Dhillon and Backhouse (2001) for large organisations, internal management initiatives must achieve this transformation, however the framework developed in our study (see figure 1) allocates responsibilities also to external agencies such as government and vendors and acknowledges the role of national and societal/ethical culture. Developing intrinsic motivation is important and can be assisted by internal and external initiatives. Siponen (2000) also noted the importance of intrinsic motivation but did not focus on SMEs nor allocate this responsibility to both internal and external roles. An organisational orientation and the promotion of personal growth may be helpful as also suggested for effective organisational cultures in general by Detert and colleagues (2002).

5 FINDINGS: KEY MANAGERIAL CHALLENGES

The study highlighted six key managerial challenges, which we discuss in this section. First, for reasons including lack of specialised information security knowledge, absence of an IT manager position and minimal reports of breaches, Australian SME owners lack an adequate understanding of the importance of information security to their business. This finding supports reports in other contexts by (Dimopoulos et al., 2004; Gupta & Hammond 2005; Helokunnas & Iivonen 2003; ISBS 2006) as

reviewed earlier. As a result, SME owners take a *reactive*, rather than *proactive*, stance to information security.

One possibly fruitful avenue suggested by this study is to persuade SME owners to undertake a formal scenario-based risk analysis/information asset protection process. Recent findings from information security surveys have highlighted a strong correlation between the formal process of risk assessment and expenditure on information security (ISBS 2006). Interestingly, experts have also recently proposed a business-based holistic risk analysis process in order to broaden and raise the information security issue to a business strategic alignment concern (Gerber & von Solms 2005). The results of a risk analysis may motivate a proactive stance toward information security management.

Second, and related to the first challenge above, our findings highlight that Australian SME owners do not understand the strategic value of IT to their business. A recent UK study (O'Halloran 2003) similarly found that UK SMEs do not understand how IT may add value to the business. *Security technologies are therefore viewed as business costs rather than strategic enablers.* The challenge in Australia – and other countries with similar findings – is to change this perception for SME owners. In Australia, the study suggests this can best commence with a range of government (federal and state) initiatives.

Third, a prerequisite for developing information security culture in SMEs is the development and communication of related policies, procedures and responsibilities. As many experts and studies have noted, most SMEs in developed countries lack such policies (e.g. Dimopoulos et al. 2004; Gupta & Hammond 2005; ISBS 2006) while the case companies found them unnecessary. However, both focus groups were emphatic that formal policies were essential. Again, persuading SMEs to undertake a scenario-based risk analysis process may help to motivate policy creation. Assistance in developing suitable policy guidelines could also be provided by conducting research into the special information security policy needs of SMEs. A related, important requirement is the provision of appropriate informal awareness activities to make the policies, procedures and responsibilities known to employees.

Fourth, the study has identified that cooperation, collaboration, sharing of knowledge and electronic learning for Australian SME employees are potentially valuable activities. This finding was also suggested by the recent ISBS (2006) survey where businesses noted the value of sharing information security experiences. Currently, no communities exist to support Australian SME employees in understanding and addressing information security issues, although such communities exist in some other countries such as the US.

Fifth, the development of strong employee values was considered by all participants to be an impossible challenge. While experts have noted the importance of values-based behaviour for developing strong information security cultures in organisations of all sizes (Dhillon & Backhouse 2000; Helokunnas & Kuusisto 2003; Martins & Eloff 2001; Schlienger & Teufel 2003), this study highlights that such development is a special challenge for SMEs. The study further found that recruiting people who already possess strong values is the only effective approach.

Finally, in a national context, the study highlights the key challenge of overcoming the Australian laissez-fair attitude toward information security concerns.

6 CONCLUSION

This paper has provided an integrative issue-based conceptual framework for developing an effective information security culture in SMEs in a national context. The key challenges in enabling Australian SMEs to develop an information security culture have been highlighted as a result of the study. Both the framework and its challenges reveal numerous new insights which, while they cannot immediately be generalised to other national or international contexts, contribute to existing limited theory in this emerging area, as discussed in the previous two sections.

The findings have also broken new ground in theories on fostering information security culture for Australian SMEs by highlighting the important facilitating role of business owner support. The findings suggest that (1) external provision of information technology and information security education and awareness for Australian SME owners, (2) external initiatives such as the development of scenario-based approaches that highlight the importance and relevance of information security, and benchmarking of other Australian SMEs, are potentially valuable ways to develop business owner support. Australian SMEs must be persuaded of the need to invest in information security in a variety of ways and Government (federal and state) and IT security vendors have key roles to play here. Finally, the findings have highlighted the negative influence of a laissez-faire Australian attitude to information security exemplified by the popular Australian catchcry "She'll be alright, mate." The findings will also provide guidance to managers and external agencies (governments and vendors) in the provision of improved initiatives, thus contributing to practice.

The final validating focus group noted that the conceptual framework can be applied in practice to assist Australian SMEs in developing and maintaining information security culture. Participants proposed that the framework's implementation would need to commence with a range of government initiatives which would provide the impetus for business owner support and proactivity in carrying out and overseeing the internal processes.

The findings from this paper have several important limitations:

- The study is interpretive, and the findings are based on only two focus groups of Australian SMEs, and three case studies of Australian small businesses. We have argued that the findings suggest a national influence on the development of information security culture, however there is an opposing argument suggesting that a study conducted only in Australia cannot provide evidence of national influence. There is a need for replicating the study in another country. It would also be useful to conduct further interpretive studies in Australia to further explore the framework and challenges.
- The framework lacks specific elements applicable only to SMEs (as distinct from large businesses). We suspect that some of the included elements are more strongly influential in SMEs, such as national culture. Future research can explore this avenue.
- The framework lacks detailed processual guidelines to enable its application. Future research might consider developing an internal change management process to implement processes suggested by the framework.
- The study focused on investigating technical SMEs which employed some staff with technical knowledge. While these companies lacked information security cultures, and were therefore suitable for study, non-technical SMEs may have more severe issues, suggesting a need for stronger external support. Such non-technical companies might be suitable subjects for future in-depth interpretive case studies.
- The framework was developed in the Australian context. Clearly, other countries may be interested in the potential value of the framework, which should therefore be explored in other national settings.

To conclude, the trend in research and practice to promote organisational information security culture has been to expect organisations to become proactive on their own. While large organisations may have the resources — including the awareness and know-how — to do so, this study teaches us that SMEs need external support in order to develop the necessary proactivity to promote and support information security culture internally.

REFERENCES

AusCERT (2005) 2005 Australian Computer Crime and Security Survey, AusCERT.

ABS (2001) 1321.0 - Small Business in Australia, 2001,Australian Bureau of Statistics.

Besnard, D. & Arief, B. (2004) Computer Security Impaired by Legitimate Users, *Computers & Security, 23*, 253-264.

Chia, P.A., Maynard, S.B. & Ruighaver, A.B. (2002) Exploring Organisational Security Culture: Developing A Comprehensive Research Model, in *Proceedings of IS ONE World Conference*, Las Vegas.
Computerworld (2005) Viruses: The New Weapon of Choice for Workplace Violence Offenders, *Computerworld*, August 22.
CSI/FBI (2005) Tenth Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute, USA.
Darke, P., Shanks, G. & Broadbent, M. (1998) Successfully Completing Case Study Research: Combining rigour, relevance and pragmatism, *Information Systems Journal, 8*(4), 273-289.
Detert, J., Schroeder, R. & Mauriel, J. (2000) A Framework For Linking Culture and Improvement Initiatives in Organisations, *The Academy of Management Review, 25*(4), 850-863.
Dhillon, G. (2001) Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns, *Computers & Security, 20*(2), 165-172.
Dhillon, G. & Backhouse, J. (2001) Current Directions in Information Systems Security Research: Toward Socio-Organizational Perspectives, *Information Systems Journal, 11*(2), 127-153.
Dimopoulos, V., Furnell, S.M., Jennex, M. & Kritharas, I. (2004) Approaches to IT Security in Small and Medium Enterprises, in *Proceedings of the 2nd Australian Information Security Management Conference 2004*, Perth, Australia.
Doherty, N.F. & Fulford, H. (2006) Aligning the Information Security Policy with the Strategic Information Systems Plan, *Computers & Security, 25*(2), 55-63.
Dutta, A. & McCrohan, K. (2002) Management's Role in Information Security in a Cyber Economy, *California Management Review, 45*(1), Fall, 67-87.
Eisenhardt, K. (1989) Building Theories from Case Study Research, *Academy of Management Review, 14*(2), 532-550.
Ernst & Young (2006) 2006 Global Information Security Survey, Ernst & Young.
Furnell, S.M., Gennatou, M. & Dowland, P.S. (2000) Promoting Security Awareness and Training within Small Organisations, in *Proceedings of the 1st Australian Information Security Management Workshop*, Deakin University, Geelong, Australia.
Furnell, S.M. & Clarke, N.L. (2005) Organisational Security Culture: Embedding Security Awareness, Education and Training, in *Proceedings of the 4th World Conference on Information Security Education (WISE 2005)*, Moscow, 67-74.
Furnell, S., Warren, A. & Dowland, P.S. (2004) Improving security awareness and training through computer-based training, in *Proceedings of the 3rd World Conference on Information Security Education (WISE 2004)*, Monterey, California.
Galletta, D.F. & Polak, P. (2003) An Empirical Investigation of Antecedents of Internet Abuse in the Workplace, in *AIS SIG-HCI Workshop*, Seattle, December, 2003.
Galliers, R.D. (1992) Choosing Information Systems Research Approaches, In R.D. Galliers (Ed) *Information Systems Research: Issues, Methods and Practical Guidelines*, Blackwell Scientific Publications, Oxford, 144-162.
Gerber, M. & von Solms, R. (2005) Management of risk in the information age, *Computers & Security, 24*(1), 16-30.
Glaser, B.G. (1992) *Emergence Versus Forcing: Basics of Grounded Theory*, Mill Valley, CA, Sociology Press.
Gupta, A. & Hammond, R. (2005) Information systems security issues and decisions for small businesses, *Information Management & Computer Security, 13*(4), 297-310.
Hallett, T. (2004) SMEs increasingly tech-savvy, ZDNet Australia, 21 September.
Helokunnas, T. & Iivonen, I. (2003) Information Security Culture in Small and Medium Size Enterprises, Seminar Presentation, Institute of Business Information Management, Tampere University of Technology, Finland.
Helokunnas, T. & Kuusisto, R. (2003) Information security culture in a value net, in *Proceedings of the 2003 IEEE International Engineering Management Conference (IEMC 2003)*, Albany, New York, USA, 2-4 November 2003, pp. 190-194.
ISBS (2006) Information Security Breaches Survey 2006, Department of Trade and Industry, UK.

Johnson, D.W. & Koch, H. (2006) Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, IEEE Society Press.

Knapp, K.J., Marshall, T.E., Rainer, R.K. & Ford, F.N. (2006) Information Security: Management's effect on culture and policy, *Information Management & Computer Security, 14*(1), 24-36.

Lichtenstein, S. & Williamson, K. (2006) Understanding Consumer Adoption of Internet Banking: An Interpretive Study in the Australian Banking Context, *Journal of Electronic Commerce Research*, *7*(2), 50-66.

Lichtenstein, S. & Swatman, P.M.C. (2001) Effective Management and Policy in E-business Security, in *Proceedings of Fourteenth Bled Electronic Commerce Conference,* Bled, Slovenia.

Lichtenstein, S. & Swatman, P.M.C. (2003) The Potentialities of Focus Groups in e-Business Research: Theory Validation, in *Seeking Success in e-Business: a Multi-disciplinary Approach, Proceedings of IFIP TC8/WG 8.4 Second Working Conference on E-business: Multidisciplinary Research and Practice*, June 9-11, 2002, Copenhagen, Denmark: Kluwer Academic Publishers.

Magklaras, G. & Furnell, S. (2004) The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users, *2004 International Information Warfare Conference*, Perth, Australia.

Martins, A. & Eloff, J.H.P. (2002) Information Security Culture, in *Proceedings of the International Conference on Information Security*, Cairo, Egypt.

McAfee (2005) The Threats Within, McAfee.

OECD (2002) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Report, Organisation for Economic Co-operation and Development.

O'Halloran, J. (2003) ICT business management for SMEs, *Computer Weekly*, December 11. .

Rosanas, J.M. & Velilla, M. (2005) The Ethics of Management Control Systems: Developing Technical and Moral Values, *Journal of Business Ethics, 53*, 87-96.

Schlienger, T. & Teufel, S. (2000) Information Security Culture: The Socio-cultural Dimension in Information Security Management, in *Proceedings of 17th International Conference on Information Security*, Kluwer Academic Publishers, USA.

Schlienger, T. & Teufel, S. (2003) Information Security Culture - From Analysis to Change, in: J. Eloff, H. Venter, L. Labuschagne and M. Eloff, (Eds.) *IS South Africa -Proceedings of ISSA 2003, 3rd Annual IS South Africa Conference*, Johannesburg, South Africa.

Schultz, E. (2005) The Human Factor in Security, *Computers & Security, 24*, 425-426.

Siponen, M.T. (2000) A Conceptual Foundation for Organisational Information Security Awareness, *Information Management & Computer Security, 8*(1), 31-41.

Stanton, J.M., Stam, KR., Mastrangelo, P.R. & Jolton, J. (2004) Analysis of end-user security behaviors, *Computers & Security*, *24*, 124-133.

Taylor, M & Murphy, A. (2004) SMEs and eBusiness, *Journal of Small Business and Enterprise Development, 11*(3), 280-289.

van Niekerk, JC & von Solms, R. (2003) Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach, in *Proceedings of ISSA 2003:3rd Annual IS South Africa Conference*, Johannesburg, South Africa, 9-11 July 2003.

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

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

Warren, M.J. (2003) Australia's Agenda for E-Security Education and Research, in *Proceedings of TC11 / WG11.8 Third Annual World Conference on Information Security Education (WISE3)*, Naval Post Graduate School, Monterey, California, USA.

Zakaria, O. & Gani, A. (2003) A Conceptual Checklist of Information Security Culture, in *Proceedings of 2nd European Conference on Information Warfare and Security*. University of Reading, UK, 30 June – 1 July 2003.

ZDNet Australia (2004) SMBs reluctant to open wallets for IT security, *ZDNet Australia*, 16 June.