ACIS 2010 Proceedings

Australasian (ACIS)

2010

Enabling Information Security Culture: Influences and Challenges for Australian SMEs

Sneza Dojkovski
Deakin University, sneza.dojkovski@hotmail.com

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

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

Recommended Citation

Dojkovski, Sneza; Lichtenstein, Sharman; and Warren, Matthew J., "Enabling Information Security Culture: Influences and Challenges for Australian SMEs" (2010). *ACIS 2010 Proceedings*. 61.
http://aisel.aisnet.org/acis2010/61

Enabling Information Security Culture:

Influences and Challenges for Australian SMEs

Sneza Dojkovski
School of Information Systems
Deakin University
Burwood, Australia
Email: sneza.dojkovski@hotmail.com

Sharman Lichtenstein
School of Information Systems
Deakin University
Burwood, Australia
Email: sharman.lichtenstein@deakin.edu.au

Matthew J. Warren
School of Information Systems
Deakin University
Burwood, Australia
Email: matthew.warren@deakin.edu.au

Abstract

An effective information security culture is vital to the success of information systems governance, risk management and compliance. Small and medium size enterprises (SMEs) face special challenges developing an information security culture as they may lack the information security knowledge, skills and behaviours of large organisations. This paper reports the main findings from an interpretive study of key influences enabling an effective information security culture for Australian SMEs. The paper provides a framework depicting external and internal influences on SME information security culture and a set of key challenges in the Australian context. The findings highlight that SME owner attitudes and behaviour – in turn influenced by government involvement - strongly influence information security culture for Australian SMEs. A surprising finding is the potential influence of the Australian culture. Practical and theoretical implications are discussed.

Keywords

Information security; Information security culture; Small and Medium Size enterprises

INTRODUCTION

Information security is a vital element in the governance, risk management and compliance of organisational information systems. Recent surveys reveal a significant insider threat (BIS 2008; PWC 2008; Richardson 2009) where employees, ex-employees and contractors have succumbed to email phishing attacks, leaked confidential business information via social media and engaged in excessive personal web use, among other information technology (IT) misuses. Increasingly experts advocate a behavioural response to such threats (Martinez-Moyano, Rich, Contrad, Andersen and Stewart 2008; Warkentin and Willison 2009), seeking to institutionalise good employee information security practices as an *information security culture* by cultivating and reinforcing desired employee behaviours. Behavioural approaches are supported by recent research suggesting that the absence of an effective information security culture enables insider misuse (Kraemar and Carayon 2007) while its presence reduces it (D'Arcy and Greene 2009).

Despite a growing research stream on the facilitation of an information security culture, scholars have largely ignored the special needs of Small and Medium-Size Enterprises (SMEs), especially within a national context. A recent survey of information security in Australian and New Zealand SMEs highlighted inadequate resourcing for information security management, particularly worker information security skills, budget and time (Symantec 2009). In addition the influence of national culture on an information security culture may be particularly relevant to SMEs. Links between national culture and organisational culture have previously been drawn (Van Muijen and Koopman 1994) while national culture has been shown to influence individual ethical decision-making (Vitell, Nwachukwu and Barnes 1993). Such cultural effects may be highly relevant to SMEs which lack the expertise to make informed information security decisions. There is a need for focused research on the facilitation of an effective information security culture for SMEs in a national context. Such research will help address the literature gap and provide guidance for SMEs seeking to develop such a culture.

This paper 1) develops a framework of key influences on information security culture for Australian SMEs, and 2) identifies key challenges for Australian SME managers and government agencies for developing an effective information security culture. The paper reports findings from an interpretive research study conducted in the Australian SME environment. The Australian Bureau of Statistics defines a medium-size Australian business as one with 20 and 200 full-time employees, and a small business as one with less than 20 full-time employees (ABS 2001). Australia was the site of the study as first its SMEs report the under-protection of information resources and significant insider misuse (for example, Symantec 2009). Second, the researchers resided in Australia at the time of study and had immediate access to a selection of Australian SMEs and to IT consultants who provide IT support services to Australian SMEs. The study incorporated a literature review, two focus groups, and three case studies of small Australian businesses.

The paper proceeds with a literature review that explores potential influences on an information security culture in organisations of all sizes and provides a background to information security in SMEs, focusing on the Australian context. Next, the paper outlines the research methodology. Key findings are presented and implications for theory and practice discussed. The paper concludes with research limitations, suggestions for future research and final insights.

THEORETICAL FOUNDATIONS

Potential Influences on Information Security Culture

This section reviews representative literature on information security culture and identifies important potential influences on the development of information security culture for organisations of all sizes.

First, managers may play important roles. Managerial actions help shape cultural norms for information security behaviour through the articulation of organisational information security goals and expected employee security behaviours (Thomson, Von Solms and Louw 2006). Through awareness, education and training activities, managers communicate the importance of information security and related employee responsibilities (Furnell and Clarke 2005). However managers will be even more influential if they take the time to learn about the information security challenges faced by employees (Albrechtsen and Hovden 2009). Other managerial strategies can also be useful. For example, a change-management program could help bring about an information security culture (Chia, Maynard and Ruighaver 2002; Martins and Eloff 2002; Van Niekerk and Von Solms 2003).

Learning and knowledge sharing activities can enable an information security culture. Van Niekerk and Von Solms (2003) suggest that information security learning should be targeted at the individual level with understanding spreading from individuals to collective and organisational levels. Knowledge gained through practice and reflection also facilitates organisational learning (Thomson, Von Solms and Louw 2006).

Personal and interpersonal worker traits such as trust, ethics and values are important influences (Myyry, Siponen, Pahnila, Vertianen and Vance 2009). When managers model appropriate information security behaviours, trust increases and employees are more likely to comply with policies and procedures (Martins and Eloff 2002). Trust can also increase when security responsibilities are delegated (Chia, Maynard and Ruighaver 2002). Martins and Eloff (2002) suggest that managerial policies, procedures and expectations can help employees become aware of organisational standards for key ethical issues.

Information Security for SMEs

SMEs can lack the expertise and resources required to manage information security well. Without specialised information security expertise a small firm does not fully understand information security risks and controls and is unlikely to perform risk assessments or develop information security policies (Dimopoulos, Furnell, Jennex and Kritharas 2004; Gupta and Hammond 2005; Helokunnas and Iivonen 2003). An SME can lack the resources required to coordinate and implement information security or offer security awareness, training and education (Furnell, Gennatou and Dowland 2000; Dimopoulos, Furnell, Jennex and Kritharas 2004; Gupta and Hammond 2005; Lee and Larson 2009). E-learning could be helpful to keep information security education costs down. However Leary and Berg (2007) note that small businesses lack the infrastructure and other essential resources (such as time) to support e-learning. The researchers point to the lost opportunity costs of denying workers e-learning activities. Gupta and Hammond (2005) explain that SMEs lack specialised knowledge of information security technologies and, with one eye on limited resources, may elect to retain outdated security technologies.

Security technologies are not taken up by SMEs in comparison with large organisations. O'Halloran argues that SME owners do not see the link between business strategy and IT and may extend this belief to security technologies (O'Halloran 2003). Some SME owners assess the availability of external IT support before electing to implement security software (Lee and Larson 2009). Some owners even doubt that they will benefit from security technologies (Lee and Larson 2009).

Gupta and Hammond (2005) provide additional insight into SME neglect of information security management. First, as a result of prioritising other business tasks, SME owners only review information security needs occasionally. Further, with fewer information security breaches than large organisations, there will be fewer incident reports produced and read. Thus information security may appear even less important and attract less attention and support from SME owners.

Information Security for Australian SMEs

As mentioned earlier a recent survey of information security management in Australian and New Zealand SMEs highlighted the main concern as inadequate resourcing (Symantec 2009). Key challenges were a lack of employee skills (40 percent), lack of time (38 percent) and budget restrictions (37 percent). Key threats were system breakdown or hardware failure (69 percent); natural or onsite disasters (49 percent); human error (47 percent); lost or stolen mobile devices (45 percent); deliberate sabotage by employees (39 percent), out–of–date security solutions (38 percent) and improper security policies (37 percent). In many cases basic safeguards were missing. For example, 43 percent of SMEs lacked an anti-spam solution, 45 percent did not backup their desktop PCs, and 39 percent lacked antivirus protection. Australia has a moderate appetite for risk according to Hofstede's (1991) cultural dimension of uncertainty avoidance and it is possible that the results of the survey partly reflect the risk posture as well as the resourcing issue.

The state of information security in Australian SMEs also relates to governmental efforts. New agencies have emerged to promote information security awareness among Australian SMEs using initiatives such as StaySmartOnline (2010). Such promotion includes annual national security awareness programs offered to SMEs across Australia and an online community forum.

The above review suggests that Australian SMEs would benefit from a framework depicting the key influences for enabling information security culture at SMEs, integrating the complexities of behaviour modification and cultural change with important management initiatives. The framework should accommodate the special needs of SMEs operating in a national context.

RESEARCH METHODOLOGY AND DESIGN

Understanding complex socio-organisational influences on information security culture in SMEs involves understanding how people think, feel and behave, suggesting an interpretive approach would be the most effective (Walsham 1995). As we believe that knowledge is socially constructed, we felt that seeking the meanings that people give to organisational information security concepts would best identify and resolve "truths" about key influences. An interpretive approach can be useful for discovering new insights as it is flexible and can be adapted as new opportunities emerge.

The research study was conducted in four phases and explored information security culture for Australian small businesses - that is, firms with less than 20 employees (ABS 2001). In *Phase One*, a preliminary conceptual framework of influences was developed from a literature review and synthesis. In *Phase Two*, the perspectives of four IT consultants who provide IT services to Australian SMEs were explored in an exploratory focus group. The consultants are based in Geelong, a semi-rural city in south-east Australia in the state of Victoria. They provide IT services, including security services, to small businesses in the region. They were asked questions about potential influences on the development of information security culture in Australian SMEs. The questions related to SME awareness of information security, the challenges that SMEs face in fostering an information security culture, and the feasibility of the preliminary framework. The focus group data were later transcribed and analysed by two researchers working independently. Themes (key influences) were identified qualitatively and inductively and compared between the two researchers, with very similar results found. By integrating the two researchers' findings, key influences were identified. An initial set of challenges for SMEs was also developed by using the same techniques.

In *Phase Three*, three interpretive case studies of small businesses in the Geelong region were conducted. Fictional company names are employed hereafter 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"). The firms were selected for three main reasons. First, as small regional (rather than city-based) firms, the three companies represented less advantaged Australian companies. Second, the three firms claimed to lack effective information security cultures. Third, as they were technical firms, some employees possessed an understanding of information technologies, enabling issues relating to information technologies to surface.

Eight employees were interviewed: four at ConsultEng, one at ServIT and three at ProvIT. In each case ordinary employees and 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. Key documents were collected including background documents of organisational structure and IT strategy. The companies lacked formal information security documents including security policies and therefore none were collected. Questions were asked based on the preliminary framework developed after the literature review and exploratory focus group. The questions probed managerial, behavioural, learning and cultural influences. The question set is available on request.

Qualitative content analysis techniques were employed to analyse the interview transcripts. A second researcher conducted an independent analysis and the two sets of themes were compared for reliability assurance. The two sets of themes were very similar and thence integrated. Internal validity checks were performed by analysing organisational documents. A cross-case analysis established that the findings from each case study were consistent. The framework of key influences was revised accordingly and the set of key challenges resulting from Phase Two was updated.

In *Phase Four* a confirmatory focus group was conducted to confirm the framework and set of managerial challenges. The four participants comprised an IT services consultant to SMEs, an Australian (and international) IT security expert, a small business owner and an IT services employee for a medium size organisation. The diversity supported debate and the remaining contentious issues were identified. Small but valuable changes to the framework were proposed, considered and resolved. The final framework (Figure 1) is presented in the next section. The set of key challenges from Phase Three was confirmed and later enhanced by the results of a content analysis of the focus group transcript. The challenges are discussed in a later section.

FRAMEWORK FOR ENABLING INFORMATION SECURITY CULTURE AT SMES

Figure 1 depicts the final framework for developing information security culture in Australian SMEs. Below we briefly describe the components of the framework and support them with sample participant quotes. First, three external influences are described: national and ethical culture; government initiatives; and IT vendors.

National and Ethical Culture

> "When it comes to computer security, the old Aussie saying applies of, 'She'll be right, mate!'... 'that'll be right! It's not causing any major wreck. Let's just leave it alone!' … the trouble is, it *is* broken. They [SME owners] just don't see it yet." [IT consultant]

National culture may affect SME information security culture and should be addressed by government initiatives (see below). Societal ethics may also have an impact as ethical standards can differ between cultures.

Government Initiatives

> "I think there's an issue with governments not promoting IT security." [Owner, ServIT]

Government agencies can play key supporting roles to help facilitate information security culture for SMEs, such as conducting national SME information security benchmarking. Another possible initiative is the development of information security risk scenarios based on existing information security resources. These can be couched in terms of asset loss protection in order to persuade SME owners to invest in information protection:

> "if they [SMEs] were to take ... their customer information, their payroll information, the obligations to the Australian Taxation Office to hold information for 'x' number of years, and then say, ' This is all valuable information to me and I can lose it, courtesy of all these [security] vulnerabilities'.. then the cost issue [of implementing controls] kind of goes away." [IT consultant].

Initiatives should also be targeted to the national context. Australia has a moderate risk posture and thus brochures and other initiatives should be targeted at addressing this attitude.

Vendors

IT vendors often provide IT security software for their SME clients thereby providing information security awareness. They may aim to deliver IT services well and so gain the trust of SME owners. Later when recommending new IT security software to SMEs, their trusted advice will then not be perceived as a sales ploy but rather as a required information resources protection measure:

> "[SMEs feel that] the external source [IT vendor] is perhaps looking after their own pocket ... getting in there to offer the security to be getting some work." [IT consultant]

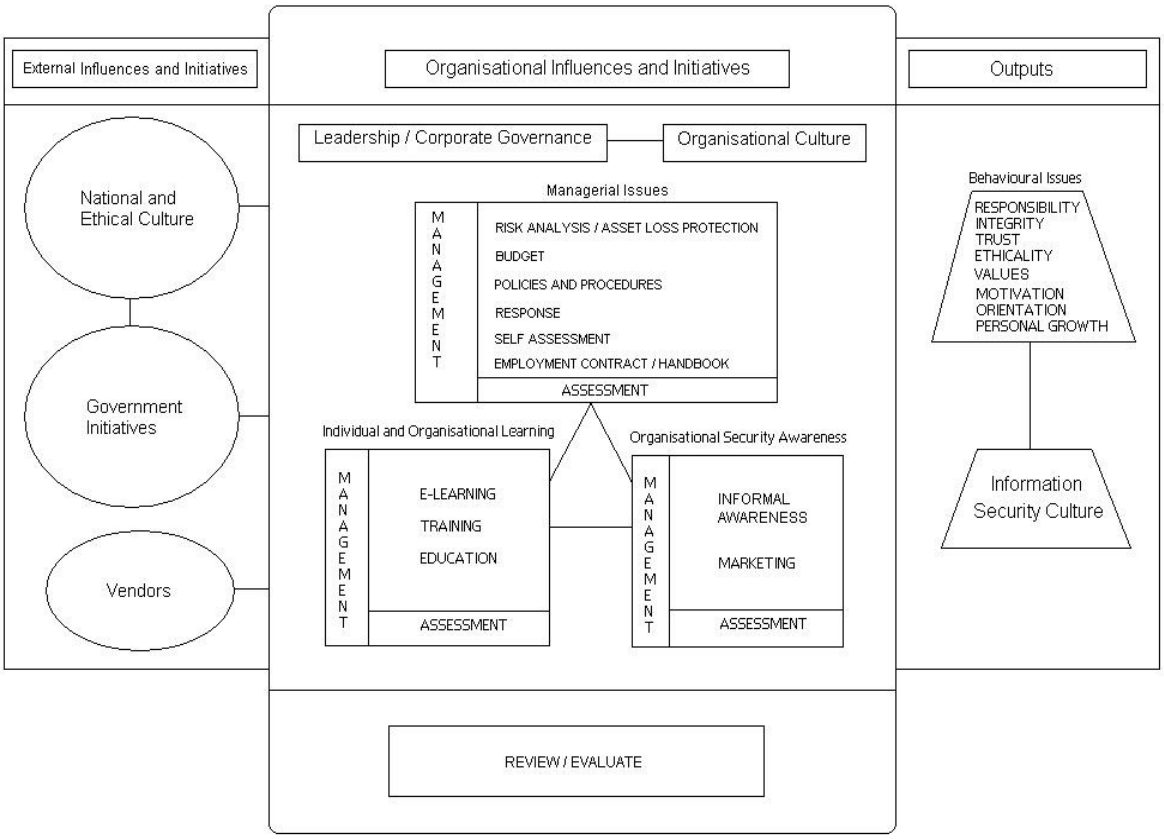

Figure 1: Framework for Enabling an Effective Information Security Culture for Australian SMEs

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

Leadership/Corporate Governance

> "It [information security management] has to start from management." [Owner, ServIT]

When an SME owner demonstrates leadership by organising information security measures, and acts as a role model in information security by adhering to information security policy and procedures, employees will follow:

> "Management must set a standard for the other employees. " [ConsultEng employee]

SME owners should be proactive by educating themselves about information security and developing information systems governance structures.

Organisational culture

The local organisational culture will affect the SME information security culture. For example, an open culture supports an informal *ad hoc* approach to information security. In contrast, an organisational culture which is security conscious supports a formal, systematic approach to information security.

Managerial

Various managerial approaches can support the development of information security culture. First, information security policies and procedures can have a significant impact on employee security-oriented behavior, particularly if well-structured, easy to read, and focused on key points:

> "The really important thing to do is establish at the beginning of their employment the policies, the rules. Inform them (employees) of our procedures and policies through their induction."
> [Owner, ConsultEng]

Marketing of the policy through awareness activities and other marketing activities helps to communicate and "sell" formal policies and procedures. Setting penalties for breaching policy influences the deterrent value of policies.

Second, when SMEs perform a risk analysis linked to asset loss protection, they are likely to discover important evidence of the need for expenditure on information security measures:

> "I think a lot of them [SME owners] would be surprised if they found out what the risks really were." [IT Consultant]

Third, an adequate budget should be allocated to information security management, particularly in SMEs where proper resource provision may easily be overlooked. The budget was considered by participants to be the most important influence on SME information security culture.

Fourth, the presence of procedures for responding to information security incidents will help emphasise the importance of information security. Fifth, SMEs will be helped by regularly assessing information security management. For example, managers could engage with online communities of practice to benchmark their efforts against those of other SME's. 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:

> "As new employees come in [to work for the company] you can … sort of say, 'It's part of your [employment] contract - and, by the way, it's part of your induction program - to spend a day with the IT administrator, or whoever it is, to learn about the way we do IT things [including information security] here." [IT consultant]

However security obligations in an employment contract should be introduced carefully to SME employees to avoid conveying lack of trust.

The above managerial processes should be regularly reviewed for effectiveness.

Individual and Organisational Learning

E-learning, training and education are potentially valuable initiatives for developing information security culture for SMEs.

> "If you don't teach me [information security policy and practices] and I do something wrong, then I'll just turn around and say, 'Ohhhh, hold on a second!' I'll just handball the blame!" [ConsultEng employee]

Knowledge sharing, cooperation and collaboration at individual and organisational levels help employees learn about information security. Learning processes should be reviewed regularly.

Organisational Security Awareness

Internal marketing of information security – including informal awareness measures that support the formal awareness provided internally and externally – is important for communicating important information risks, policy and procedures. Brown bag lunches and wall posters are examples of informal awareness activities. Awareness processes should be reviewed regularly.

Review/Evaluate

Focus group participants stressed that SMEs should regularly review and evaluate the information security enculturation measures, seeking continuous improvement.

Behavioural

> "I would put trust very high on the list. Our people have access to practically all client information. ... So if [SME owners] don't trust them, we're lost." [IT consultant]

Participants agreed that there were certain desirable personal qualities which would positively influence information security behaviour, including responsibility, integrity, trustworthiness, and ethicality. However, some participants suggested that such personal qualities would be difficult to change:

> "I see that [ethics] as a core value that comes from childhood. Ethics, values, trust and integrity - they're all core values that are very, very difficult to change." [IT consultant]

Participants agreed, however, that a range of external and internal initiatives can develop such qualities. External agencies include government and IT vendors which should recognise the role of national and societal/ethical culture. Developing intrinsic motivation is also important as is orienting employees towards the organisation's goals and supporting employees' personal growth. All these serve to encourage employees to support and protect information resources.

KEY CHALLENGES FOR ENABLING SME INFORMATION SECURITY CULTURE

The study identified six important challenges for Australian SMEs attempting to facilitate the development of an information security culture. The challenges are discussed below together with suggested practical solutions and avenues for future research.

First, Australian SME owners lack an understanding of the importance of information security to their business strategy success. As a result, SME owners are more likely to adopt a *reactive*, rather than *proactive*, stance toward information security. One possible solution to this problem, suggested by IT consultants in the study, is to persuade SME owners to undertake a formal scenario-based process for risk analysis/information asset protection. Leveraging external scenarios for this purpose may be helpful as SMEs lack the expertise to perform an information security risk analysis. A 'what if' template for information security risk analysis, based on scenarios, was proposed by one of the focus groups. Unlike traditional risk analysis, the template would focus on the actual consequence of the risk itself. Table 1 illustrates the template with an example. The first column in the template describes a possible information security risk scenario - for example, 'What if I lost my sales data for three days?' The second column identifies the business impact and the third column rates the priority or significance of the risk scenario. With such a template, SME owners will be able to identify their main information assets, the importance of protecting them, and implement appropriate measures.

Information Security Risk Scenario	**Business Impact**	**Priority**
What if I lost my sales data for 3 days?	$100,000	High

Table 1 An example of a risk-analysis/asset-loss protection scenario

Second, the study suggests that the inadequacy of SME budgets for information security may be due to a genuine lack of security and risk awareness by SME owners who are often preoccupied with other tasks, most notably the everyday running of their businesses. Participants in our study believed that the results of a risk assessment would bring the need for information security expenditure to the attention of SME owners. Apart from the scenario analysis approach proposed above, participants suggested there is a need for special standards for SME risk assessment, noting that current risk assessment standards may be too technical for SMEs. Barlette and Fomin have made a similar observation (Barlette and Fomin 2008). Beachboard, Cole, Mellor and Hernandez (2008) proposed a risk analysis process that may suit SMEs. Future research may help to identify other potentially valuable approaches.

Third, an important 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 while the three case study companies found them unnecessary. However, participants in both focus groups were emphatic that formal policies are essential. Persuading SMEs to undertake a risk analysis process may help motivate policy creation. Further assistance for SMEs could be provided by researching the special information security policy needs of SMEs. A related requirement is the provision of appropriate informal awareness activities to make the policies, procedures and responsibilities known and understood by employees.

Fourth, the study found that cooperation, collaboration, sharing of knowledge and electronic learning for Australian SME employees may be valuable activities. Currently an online community (StaySmartOnline 2010) aims to support Australian SME employees in understanding and addressing information security issues. It is still too early to assess the success of this community.

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

Finally, for Australia the study highlights the key challenge of overcoming the Australian laissez-fair risk posture toward information security concerns.

CONCLUSION

This paper has addressed a gap in the information security literature by developing an integrative framework of key influences for developing an effective information security culture in SMEs in a national context (Figure 1). Six key challenges for supporting Australian SMEs in their efforts to develop an information security culture were identified and discussed. The paper also generated theoretical insights which, while they cannot be generalised to other national or international contexts, contribute to existing limited theory in this fledgling research area.

The findings have broken new ground theoretically by highlighting the important facilitative role of SME business owner support. The findings suggest several new ways to develop such support for Australian SME owners:

- external provision of information technology and information security education and awareness for Australian SME owners;
- external initiatives such as the development of scenario-based risk analysis approaches that appeal to owner interest in information asset risk impacts and serve to highlight the importance and relevance of information security measures;
- development of special information security risk assessment standards for SMEs;
- external provision of benchmarking services to Australian SMEs.

The findings suggest that Australian SME owners lack an understanding of the strategic value of IT to their business. A UK study (O'Halloran 2003) found similarly that UK SMEs do not understand how IT can add business value. Security technologies are currently 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.

SMEs must be persuaded of the need to invest in information security and this study suggests that government (federal and state) agencies and IT security vendors can play key roles. The findings provide guidance to managers and external agencies (governments and vendors) by proposing new initiatives. We note that the current efforts represented by the online StaySmartOnline (2010) small business forum have had limited success to date and suggest that the application of theory on successful online communities may lead to greater participation rates and effectiveness. Researchers have also highlighted Web 2.0 tools as useful enablers of e-learning (Wang 2009) and this may also be a useful direction to pursue for future information security e-learning initiatives.

Finally, the findings have highlighted the challenges of an oft-touted Australian posture to information security, reflected by the well-known Australian catchcry, "She'll be right, mate." This challenge requires further exploration in the Australian SME setting.

The findings in this paper have several important limitations:

- The study is interpretive with findings based on two focus groups of Australian SMEs and three case studies of Australian small businesses. Regional (rather than urban) areas are well-represented by study participants. 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. The study should therefore be replicated in another country. It would also be useful to conduct additional interpretive studies in Australia to explore the framework and challenges.
- The framework lacks specific elements exclusive to SMEs. However we suspect that some of the elements are more strongly influential in SMEs, such as national culture. Future research can explore this avenue.
- The framework lacks detailed processual guidelines to support its application. Future research might develop such a process.
- 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 participants for future 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 we suggest is 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 require external support in order to develop the necessary proactivity to promote and support an information security culture.

REFERENCES

Albrechtsen, E. and Hovden, J. 2009. "The information security digital divide between information security managers and users", *Computers & Security* (28:6), pp 476-490.

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

Barlett, Y. and Fomin, V.V. 2008. "Exploring the Suitability of IS Security Management Standards for SMEs", in *Proceedings of 2008 Hawaii International Conference on System Sciences,* Hawaii, USA.

Beachboard . J., Cole, A., Mellor, M. and Hernandez , S. 2008. "Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda Setting Knowledge Free", *Journal of Issues in Informing Science and Information Technology* (5).

Besnard, D. and Arief, B. 2004. "Computer Security Impaired by Legitimate Users", *Computers & Security* (23:1), pp 253-264.

BIS (2008) 2008 *Information Security Breaches*, Department of Business, Innovation and Skills, UK.

Chia, P.A., Maynard, S.B. and Ruighaver, A.B. 2002. "Exploring Organisational Security Culture: Developing A Comprehensive Research Model", *Proceedings of IS ONE World Conference*, Las Vegas, USA.

D'Arcy , J., Hovav, A. and Galletta, D.F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", *Information Systems Research* (20:1), pp 79-98.

D'Arcy, J., and Greene, G. 2009. "The Multifaceted Nature of Security Culture and Its Influence on EndUser Behavior", *Proceedings of IFIP TC 8 International Workshop on Information Systems Security Research*, Cape Town, South Africa.

Dimopoulos, V., Furnell, S.M., Jennex, M. and Kritharas, I. 2004, "Approaches to IT Security in Small and Medium Enterprises", *Proceedings of the 2nd Australian Information Security Management Conference*, Perth, Australia.

Furnell, S.M., Gennatou, M. and Dowland, P.S. 2000. "Promoting Security Awareness and Training within Small Organisations", *Proceedings of the 1st Australian Information Security Management Workshop*, Geelong, Australia.

Furnell, S.M. and Clarke, N.L. 2005. "Organisational Security Culture: Embedding Security Awareness, Education and Training", *Proceedings of the 4th World Conference on Information Security Education,* Moscow, Russia.

Galletta, D.F. and Polak, P. 2003. "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace". *Proceedings of AIS SIG-HCI Workshop.* Seattle, USA.

Gerber, M. and von Solms, R. 2005. "Management of risk in the information age", *Computers & Security* (24:1), pp 16-30.

Gupta, A. and Hammond, R. 2005. "Information systems security issues and decisions for small businesses", *Information Management & Computer Security* (13:4), pp 297-310.

Helokunnas, T. and 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. and Kuusisto, R. 2003. "Information security culture in a value net" *Proceedings of the 2003 IEEE International Engineering Management Conference,* Albany, New York, USA.

Hofstede, G. 1991. "Cultural constraints in management theories", *The Executive* (7:1), pp 81-94.

Kraemer, S. and Carayon, P. 2007. "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists", *Applied Ergonomics* (38), pp 143-154.

Leary, J. and Berg, Z.L. 2007. "Challenges and Strategies for Sustaining e-Learning in Small Organizations", *Online Journal of Distance Learning Administration*, (X:III), Fall 2007. Retrieved 10th May, 2010, from http://www.westga.edu/~distance/ojdla/fall103/berge103.htm

Lee, Y. and Larson, K.R. 2009. "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems* (18), pp 177-187.

Martinez-Moyano, I.J., Rich, E., Contrad, S., Andersen, D.F. and Stewart, T.R. 2008. "A behavioral theory of insider-threat risks: A system dynamics approach", *ACM Transactions on Modeling and Computer Simulation* (18:2), Article 7.

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

Myyry, L., Siponen, M., Pahnila, S., Vertianen, T. and Vance, A. 2009. "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", *European Journal of Information Systems* (18), pp 126-139.

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

PWC (Price Waterhouse Coopers). 2008. "Safeguarding the New Currency of Business", Price Waterhouse Coopers.

Richardson, R. 2008. "CSI Computer Crime & Security Survey", Computer Security Institute, San Francisco.

Schlienger, T. and Teufel, S. 2003. "Information Security Culture - From Analysis to Change", *Proceedings of 3rd Annual Information Security South African Conference*. Johannesburg, South Africa.

StaySmartOnline 2010. "Small business e-security, Stay Smart Online, Australian Government", Retrieved 10th May, 2010, from http://www.staysmartonline.gov.au/small-business-security

Symantec. 2009. "2009 Global Small and Mid-sized Business (SMB) Security and Storage survey", Computerworld, Retrieved 12th May, 2010, from http://www.computerworld.com.au/article/302806/symantec_survey_reveals_more_than_half_small_midsized_businesses_australia_new_zealand_experience

Thomson, K., Von Solms, R. and Louw, L. 2006. "Cultivating an organizational information security culture", *Computers Fraud & Security* (10), pp 7-11.

Van Muijen, J.J. and Koopman, P.L. 1994. "The influence of national culture on organizational culture: A comparative study between 10 countries", *European Journal of Work and Organizational Psychology* (4:4), pp 367 – 380.

van Niekerk, JC and von Solms, R. 2003. "Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach", *Proceedings of 3rd Annual Information Security South African Conference*, Johannesburg, South Africa.

Vitell, S. J., Nwachukwu, S. L., and Barnes, J. H. 1993. "The effects of culture on ethical decision-making: An application of Hofstede's typology", *Journal of Business Ethics* (12), pp 753–760.

Walsham, G. 1995. "The Emergence of Interpretivism in IS Research", *Information Systems Research*, (6:4), pp. 376-394.

Wang, M. 2009. "Integrating organizational, social, and individual perspectives in Web 2.0-based workplace e-learning", *Information Systems Frontiers* (9:4), pp 343–358.

Warkentin, M., and Willison, R. 2009. "Behavioral and policy issues in information systems security: The insider threat", *European Journal of Information Systems* (18), pp 101-105.

COPYRIGHT