Institutionalising Information Security Culture in Australian SMEs: Framework and Key Issues

S. Dojkovski, S. Lichtenstein and M.J. Warren

School of Information Systems,
Deakin University, Australia.

sneza.dojkovski@deakin.edu.au; sharman.lichtenstein@deakin.edu.au;
matthew.warren@deakin.edu.au

Abstract

Many companies would prefer employees to follow information security practices naturally rather than by management directives and enforcement. The paper reports some of the main findings from a large interpretive research project involving a literature review, three case studies and two focus groups, conducted in Australia. Findings include a framework for fostering information security culture in Australian SMEs and a discussion of key issues. The paper highlights the criticality of both the SME owner role and the national context in fostering information security culture in SMEs. Implications for theory and practice are discussed.

Keywords

Information security culture, small and medium-size enterprises.

1. Introduction

One of the most important areas for information security management is employee misuse and abuse of information assets, also known as the "insider threat" (Furnell et al., 2000). According to recent reports, employee misuse and abuse of internet services comprise 20 - 50 per cent of internet incidents (AusCERT, 2006; CSI/FBI, 2006). Whether employees are inclined to behave securely in their use of company information systems can be viewed socio-culturally. The socio-technical perspective may best reflect employee behaviour with information security technologies. This new approach to managing the insider threat is the institutionalisation of information security practices as an *information security culture.* The potential effectiveness of adopting a socio-cultural approach is highlighted by recent findings from Galletta and Polak (2003) that peer and supervisory culture may strongly influence internal internet abuse.

However currently there is very little guidance available for small and medium size enterprises (SMEs) in the development of an information security culture and the issues to be faced along the way. SMEs typically have different managerial concerns to large enterprises - for example, they may possess fewer resources and may lack internal information technology expertise. In addition, existing conceptual frameworks for the development of information security culture are mainly aimed at large organisations. Often, such frameworks centre only on managerial directives such as policies and procedures to perform the task of enculturation. New conceptual frameworks are needed that integrate the complexities of behaviour modification and cultural change with managerial directives, and that accommodate the special characteristics of SMEs operating in a unique national context such as Australia – the context for this research. Such frameworks should be based not only on existing theory but on the real world experiences of SMEs and the IT professionals who provide them with services.

This paper reports some of the main findings from a recent research project that explored this topic. The project involved a literature review, three case studies and two focus groups. Early results from the project were reported in Dojkovski et al., (2005, 2006). This paper provides the final framework, and presents a discussion of key issues of interest arising from the study.

The rest of the paper is structured as follows. Following this section, the paper provides a theoretical background for the research. It then overviews the research design for the study. A section then provides a conceptual framework for developing and maintaining information security culture in SMEs, developed from the study. Next, key findings are discussed, and finally, conclusions are drawn.

2. Theoretical Review

This section synthesises representative contemporary literature on information security culture and reviews the unique challenges of SMEs concerning information security culture.

2.1 Information Security Culture

As mentioned earlier, recent research aims to better manage the insider threat by developing an information security culture (OECD, 2002). 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 (for example Lichtenstein and Swatman, 2001). However, such frameworks may be better suited to medium and large size organisations due to their significant infrastructure, stability and resources requirements. In recent years, dedicated frameworks for information security culture have been developed, as reviewed below.

Several frameworks have focused on organisational culture and the measurement of information security culture. Schlienger & Teufel (2000; 2003) describe a framework concentrating on a socio-cultural approach that is based on trust and partnership, accompanied by appropriate security technologies and employee security awareness.

To address weaknesses in information security, Siponen (2000) constructs a conceptual foundation for organisational security awareness based on prescriptive persuasion based on behavioural principles. The model consists of motivation principles, theory of planned behaviour and a technological acceptance model.

Also addressing awareness, Von Solms discussed the stages of information security awareness maturity (von Solms, 2000) culminating in an institutional stage, which involves cultivating an information security culture through standardisation, certification and paying attention to the human aspect of information security. An emphasis is placed on the continuous measurement of information security for proper management.

In another framework, Chia and colleagues (2002) argue that an information security culture has not yet been clearly defined. They identified the following important dimensions for measuring the effectiveness of information security culture: a belief in the importance of information security; balancing of long- and short term goals, policies, procedures and processes; continuous improvement; cooperation and collaboration; attention to objectives; and audit compliance. However, this list was recently criticised by Helokunnas and Kuusisto (2003) for de-emphasising the human aspects of information security.

A structured framework for information security culture was developed by Martins and Eloff (2002). Their framework is comprised of individual, group and organisational levels of information security enculturation. Issues that promote adequate information security culture were identified in each group. The effect of change agents on these issues will transform the organisational culture to an effective information security culture.

Helokunnas & Iivonen (2003) provide a framework based on shared values. The research looked at the values that a group of Finnish SMEs in the Tampere Region held in relation to security and developed a security framework based upon their beliefs and values.

Van Niekerk and von Solms (2003) examine the role that education plays in the establishment of information security culture. Their approach centres on the concept of an outcomes-based education forming the basis of cultural change, and they show how such an approach can play a positive role in creating a culture of information security.

A conceptual checklist of information security culture consisting of a compilation of information security and organisation culture concepts was proposed by Zakaria and Gani (2003). The model consists of three levels with analytical dimensions such as

surface manifestations (artefacts, ceremonial, course, hero, language, motto, myth, norm, physical layout, rite, ritual, slogan, story and symbol), values (confidentiality, integrity, availability, authentication non-repudiation and legitimate use of information) and basic assumptions (mission and strategy, goals, means, measurement and remedial strategies) relevant to information security identified for each level.

A socio-technical perspective was proposed by (Stanton et al., 2004). In their framework they focus on the human actions that influence the confidentiality, integrity and availability of information systems. They suggest that security-oriented end-user behaviours are derived from a combination of relevant situational and personal factors and improving information security culture is done by examining the motivational antecedents of employees, such as situational and personal factors combined with a variety of interventions.

A framework based on informal methods was proposed by Vroom and von Solms, (2004) whereby the behaviour and culture of an organisation at all levels is examined in an informal fashion. They suggest that studying organisational behaviour and how employees are influenced would prove useful in improving the security culture of an organisation. They suggest behaviour be separated into three groups of: the individual, the group and the formal organisation. Each level needs to be examined simultaneously with how it impacts the culture of the organisation.

A framework based on personnel capabilities was proposed by Furnell and Clarke (2005) who suggest security awareness, training and education as important elements in establishing an information security culture. Management addressing the security risks and what awareness, training and education could do to combat these risks. They also suggest that a 'one size fits all' approach will not work, and that a company must determine which approaches will work in a given context.

While the above frameworks are clearly valuable, they portray a fragmented theoretical field and lack integration across the different areas of focus. Further, they do not address the unique challenges faced by SMEs operating in a national context.

2.2 Information Security Culture and SMEs

SMEs suffer special disadvantages compared with large organisations in pursuing an information security culture. First, SMEs generally possess a weak understanding of information security, security technologies and control measures (Dimopoulos et al., 2004). Second, they lack the funds, time and specialised knowledge needed to coordinate information security or offer effective information security awareness, training and education (Furnell et al., 2000; Dimopoulos et al., 2004). Third, SMEs are unlikely to have yet reached the stage of policy, procedure and responsibility definition (Helokunnas & Iivonen, 2003) let alone addressed the cultural issues. Fourth, they are susceptible to peculiar national influences such as the collapse of Australian information security coordination programs for businesses arising from the recent demise of the National Organisation for the Information Economy (NOIE)

(Warren, 2003). Fifth, recent studies highlight various SME concerns regarding the difficulties of developing an information security culture (Taylor & Murphy, 2004).

3. Research Design

This section overviews the conduct of the research study, which was an interpretivist study. A literature review was first conducted and an initial conceptual framework for fostering information security culture in Australian SMEs developed as a result (Dojkovski et al., 2005). The review also helped to develop questions for an exploratory focus group ("Focus group 1") held in November 2005 with four participants (representatives of SME IT service providers in the Geelong region of Australia). A focus group transcript analysis resulted in a revised conceptual model (Dojkovski et al., 2006).

Next, three in-depth interpretivist case studies explored the key issues and framework in greater detail. Three SMEs from technical industries in regional Geelong, Australia, were studied. Seven semi-structured one hour interviews were conducted with a total of seven participants in 2006. Interview questions were drawn from literature and participants were also asked about each element of the conceptual framework. Case study findings were used to further refine the framework.

To validate this framework, a final validation focus group with four participants was conducted. Three participants were from technically-oriented SMEs in the Geelong region and one was a national expert in IT security. The focus group validated each element of the framework and suggested several final enhancements resulting in a final version of the framework, described next. A transcript analysis also revealed other important findings, some of which will be reported later in this paper.

4. Conceptual Framework for Fostering Information Security Culture for SMEs

Figure 1 provides an issue-based conceptual framework for developing information security culture in SMEs in a national context, derived from the study. The framework is divided into three groups of elements: Organisational, External and Outputs. It is overviewed below and, due to paper size constraints, will be discussed in more detail in future publications.

4.1 Organisational Elements

Leadership/Corporate Governance: Corporate governance is concerned with managing the business operation of an organisation and administering the optimal utilisation of its resources. IT security governance is a subset of corporate governance and can be extended to address the issues and implications to business of security responsibilities.

Organisational Culture: Organisations already have their own values and cultures established. By working together, the interaction of these values and cultures can promote effective information security in organisations.

Managerial: There are many managerial activities and initiatives that might attempt to develop information security culture in SMEs.

- Risk Analysis/Asset Loss Protection: An asset loss protection process provides an approach to risk analysis that may motivate SME owners to focus on information security management and issues.
- Budget: A budget is needed for information security, especially in SMEs where resourcing may easily be overlooked. This will enable cultural initiatives such as training to be resourced.
- Policies and Procedures: information security policies and procedures are required to direct required and acceptable employee information security behaviour.
- Response: Procedures to respond quickly and satisfactorily to new information security issues (for example breaches) as they arise will also be beneficial in stressing the importance of information security to employees.
- Self Assessment: Every element of the management program should be regularly self-assessed seeking continuous improvement.
- Employment Contract/Handbook. During the induction of new employees it is important to use an employment contract or company handbook outlining what management regards as important information security information, policies and procedures and place restrictions and/or offer incentives.
- Management: As managers are responsible for information security and are role models for employees, they must model excellent information security behaviour.
- Assessment: Periodic assessment of each managerial element allows for continuous improvement.

Individual and Organisational Learning: For smaller organisations, a process of organisational learning from individual to an organisational level is needed. In SMEs there is likely to be a variation in, e-learning, training and education needs for individual employees.

Organisational Security Awareness: Informal awareness activities such as brown bag lunches are needed Marketing of these activities is needed.

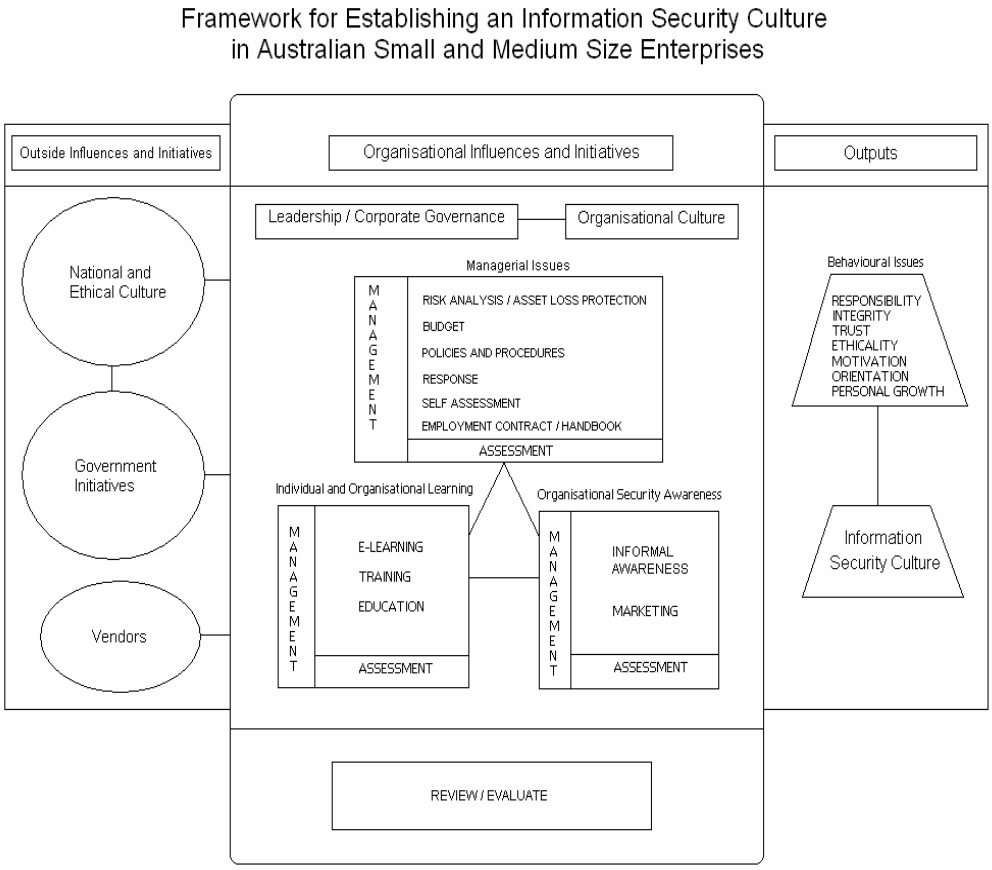

Figure 1: Conceptual framework for fostering information security culture in SMEs in a national context.

4.2 External Influences and Initiatives

National and Ethical Culture: Different nations may have their own values and cultures which will impact the development of culture and must be considered by government and IT vendors, as summarised below.

Government Initiatives: In the Australian context, the national government (federal and state) can provide benchmarking, tax break incentives for implementing security procedures and technologies, training and education programs and implementation information, among other initiatives.

IT *vendors* have an important role to play to raise information security awareness for SMEs.

4.3 Outputs

Behavioural Issues: External and internal measures should develop the behavioural traits (in employees) needed for an effective information security culture. These traits are identified below.

Responsibility refers to employees needing to understand rules and responsibilities. *Integrity* refers to an employee feeling part of the company and thus identifying with its norms and morals and handling information with due integrity. Employees and management must *trust* one another. Finally, employees should behave *ethically.*

Employee motivation, orientation and *personal growth* are also important to consider when developing organisational culture. Such behavioural issues will influence the effectiveness of information security culture in SMEs. When employees are motivated, aligned to the organisation's objectives, and learning and improving their skills and knowledge, the information security culture will be strengthened.

Review/Evaluate: SME's should periodically review their information security measures in order to use lessons learned to continuously improve the information security culture.

5. Discussion

This section summarises information security at the three case organisations (a greater description is not possible due to paper size constraints), followed by a discussion of a range of issues that arose throughout the project. As this is qualitative interpretivist research, the voices of participants are provided to better highlight the issues.

5.1 Case Study Analysis: Information Security Culture at Organisations A, B and C

Organisation A is a small company specialising in engineering consulting with fifteen employees. Organisation B is a small IT consultancy company with three employees. Organisation C is also a small IT consultancy with two employees. Thus, it would be expected that at least some of the employees would possess some technical skills and be able to follow information security practices.

However, of the organisations interviewed, only organisation A had an information security policy and procedures in the organisation, although only a few of the employees were aware of the policy and knew that it should be implemented. Information security was not a priority in any of the organisations and very little effort was put into managing and implementing it effectively. Management in all of the organisations was of the opinion that information security was not a priority. However there was still a high expectation from employees regarding information security behaviour. Both employees and management were uncertain whether the level of security in the organisation was adequate, and believed that information security was not yet enculturated in their firms.

The broader findings from the overall project involving two focus groups and three case studies are now examined

5.2 Information Security Awareness, Budget and Risk analysis in Australian SMEs

According to focus group (1 and 2) participants, information security risks for Australian SMEs have increased as a result of greater internet access however the level of information security awareness in SMEs has not kept apace and remains low. A lack of awareness is a contributing factor to many Australian SME owners not having recognised the existence of an information security problem in their organisation, and thus their unwillingness to allocate a budget to this area. For example, one case study participant noted:

Employees and management don't have an awareness of security issues and the consequences of such issues. [SME owner, Organisation B]

According to focus group participants, very few Australian SMEs allocate a budget to information security. This was thought to be because SME owners must first clearly see the risks involved before they would acknowledge the need for a budget (and time) for information security.

…[budget is] probably the biggest obstacle. [It is] hard to get smaller companies to set a budget for information security. [SME owner, Organisation A]

In order for SME owners to acknowledge the risks, focus group participants argued that a risk analysis was essential. However, convincing SME owners to conduct a risk analysis currently presents a challenge. According to IT consultants in the initial exploratory focus group (focus group 1), clients do not trust IT vendors and consultants and do not wish to pay for a risk analysis which they feel is aimed at selling them IT security products. Organisations B and C expressed the view that their companies were too small to conduct a risk analysis. Participants in the validation focus group (focus group 2) suggested that the Australian government provide sample security risk scenarios derived from sources such as the SANS Institute in the US. Such scenarios would emphasise asset loss protection in order to attract the interest of SMEs. As one participant conceptualised it:

So federal government does their thing - you know, handing out templates - and then you have the state government … roll it out to businesses who are [just] commencing (starting up). [SME Owner, Focus Group 2]

Further to the issue of awareness, it was noted in one of the focus groups that as SMEs generally do not have an IT department, they do not have internal knowledge of security issues and risks, unlike large organisations with dedicated in-house staff and budgets allocated to IT security. It was thought to follow on that SME owners would have the belief that information security is only a significant concern for large businesses.

Three case study participants also suggested that another challenge to being security conscious in SMEs was because management was preoccupied with the running of

day-to-day business operations and was only reactive concerning security matters. For example, in one case organisation it was remarked that:

It is very hard to raise awareness as owners are generally too busy with other business issues to worry about security. [SME owner, Organisation B]

It was also suggested by focus group participants that IT vendors can play a key role in raising security awareness within SMEs. However it was noted that before they can provide information security information, they must (somehow) prove themselves trustworthy as SMEs can feel they are being marketed IT security technologies. In the past, IT vendors had issued numerous security warnings of viruses and other risks that never eventuated. As one participant recalled:

… there was a lot of hoo-ha (fuss) about the Year 2000 bug and, you know, we all sat down expecting our whole computer society to crash - and it didn't! [SME owner, Focus group 1]

5.3 Behavioural Issues

Commenting on the behavioural issues, participants in the focus groups and case studies supported the need for such behavioural traits in employees. They believed it would be very difficult to change a person's sense of responsibility, trust, ethicality and personal growth and that it is almost impossible to change a person's sense of integrity, values, orientation and motivation. For example:

I see that 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. Almost impossible! [SME owner, Focus group 1]

It was also noted that workers often refuse to be held responsible for information security breaches and that personal behaviour is not easily changed by a policy document. It was suggested that it was better to hire the "right" person than to attempt to shape a worker into the "right" person.

5.4 Management Initiatives

Participants agreed that appropriate management initiatives can help shape employee information security behaviour. They suggested that policies and procedures should be marketed to employees with the timing and manner of such marketing deemed important. Many participants felt that policies were generally too long and often not easy to understand. Thus, employees find it difficult to follow them.

Don't make policies very long. Make them well structured and easy to read.
[SME owner, Organisation A]

It was also noted that SMEs do not understand the concept of benchmarking and why it would be considered important. They have no knowledge in how to benchmark against other organisations. They felt that this was an area in which the national

government should assist SMEs by providing more information on how to go about benchmarking and the benefits of such action.

[benchmarking] is a good idea however it will be difficult to do as SMEs don't know who or what they should be comparing against [SME owner, Organisation B]

Focus group participants also suggested that information security awareness could be integrated with the employee induction process so that employees understand, from the very beginning, the importance of information security to the organisation. However, it was pointed out by some that SMEs are often informally organised and so may lack a formal induction process. Focus group participants noted that this could be remedied by including the security induction within the employment contract/company handbook. Participants also mentioned the importance of explaining the business ramifications of information security breaches to employees – for example, by mentioning the potential disclosure of corporate strategic information. Showing the employees "What's in it for me?" in such meaningful ways would help "sell" the policy.

After employment, a build up to presenting policies could encourage employees to attend and become involved. Brown bag lunches were suggested as an example of an informal enjoyable environment in which to present and discuss security policies.

5.5 Individual and Organisational Learning

Participants noted that because of their size, there is generally good communication in SMEs which eliminates the need for extensive training and education.

You don't need a lot of education and training in a small business. Because it's a very closed environment there's a lot of communication, and once people know what they're meant to be doing they'll continue to do it and especially if they see everyone else doing it.
[SME owner, Organisation B]

It would be difficult for SME owners to measure whether employees are gaining much knowledge from any form of learning if they are left to do it in their own time or if they were to implement a learning program. They were unaware of any available programs for small organisations.

…at the moment, if I wanted to conduct training I would make up my own course because I'm not aware of any courses for employees except for large organisations.
[SME owner, Organisation B]

The question of whether SME owners would permit employees the time to engage in e-learning and online communities was raised by focus group participants:

Perhaps the smaller places wouldn't be able to afford the time for their employees to be able to become involved in that? And I wonder if the employees would take the

time on their own clock to become part of those sorts of experiences and those sorts of communities?
[SME owner, Focus group 1]

It was also mentioned that some types of employees may not be interested in such activities:
Some people go to work so they can show up at 8:45am and leave at 4:35pm, and earn their wage. And those people perhaps may not take as much out of it [e-learning] as somebody who's really interested in furthering their career. [SME owner, Focus group 1]

It was suggested that learning may be better accepted by employees if offered by an independent neutral business body such as a regional Chamber of Commerce, or academia, rather than an IT professional firm:

If it's a governing body or a body that's respected within the context of a society, where there's a means of interacting and benchmarking because you meet many peer businesses, then that's good for enculturation at the owner/manager level. [SME owner, Focus group 1]

5.6 Australian Governmental and Cultural Context

It was noted in the Australian SMEs interviewed that they often have a relaxed, unconcerned approach to security issues. Participants also criticised the lack of government initiatives in helping SMEs with security risks and issues. Suggestions were made by participants for a government (either Federal or State) marketing campaign raising security awareness; a brochure that includes a variety of case studies that would spark interest among SMEs; templates for risk analysis; and information security standards for SMEs.

In addition, it was agreed that different countries exhibit unique values and cultures. According to many participants, the Australian culture can be characterised by the catchcry "She'll be right, mate!" and, as such, is a barrier to information security culture development in Australian SMEs.

Well, you look at national culture and what to change, well, when it comes to computer security, the old Aussie saying of "She'll be right, mate!" [characterises the culture].
[SME owner, Focus group 1]

6. Conclusion

This paper has provided a theoretical perspective on information security culture and has presented an issue-based socio-cultural framework for developing and maintaining information security culture in Australian SMEs (figure 1). The paper also provided key findings from three interpretive case studies of Australian SMEs

and two focus groups that explored the framework in the Australian context. Key issues hindering the development of an information security culture in Australian SMEs were highlighted by the case study and focus group findings.

The framework has highlighted that internally, SME owners have the greatest responsibility and role in ensuring a more security conscious organisation. They should perform an information asset protection process (that is, risk analysis) that helps them to identify the need for a range of measures including policies and procedures (supported by enabling technologies). However the effectiveness of these measures relies on an organisational security awareness program of informal activities to increase the awareness of SME employees. Awareness, training and education form the backbone of organisational initiatives to influence employee security behaviour.

Australian SMEs should also be given greater external support for developing an information security culture by federal and state governments. Many initiatives were proposed in this study, including a national SME information security awareness campaign, benchmarking of information security culture in Australian SMEs, a brochure, tax incentives, formal training and education programs, and opportunities for business collaboration.

In conclusion, this research has highlighted the criticality of a proactive SME owner role and the need to consider the national context in order to institutionalise information security culture in SMEs in a national setting.

References

AusCERT (2006) 2006 Australian Computer Crime and Security Survey, AusCERT, Retrieved 26 September, 2006, from: http://www.auscert.org.au/render.html?it=6311

Chia, PA, Maynard, SB & Ruighaver, AB 2002, "Exploring Organisational Security Culture: Developing A Comprehensive Research Model", Proceedings of IS ONE World Conference, Las Vegas, 2002.

CSI/FBI 2006, "2006 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, Retrieved 26 September 2006 from: https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27372&sessionid=1&key=42F39B89EE0B30BA951711A5E7A98EDD&partnerref=Netseminar&sourcepage=register

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

Dojkovski, S, Warren, M & Lichtenstein, S 2005, "Information Security Culture in Small and Medium Sized Enterprises: a Socio-cultural Framework", Proceedings of the 6th Australian Conference on Information Warfare and Security, 24-25 November 2005, Deakin University, Geelong, Australia

Dojkovski, S., Lichtenstein, S. & Warren, M.J, 2006 "Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises", in Proceedings of 5th European Conference on Information Warfare and Security, 1-2 June, 2006, National Defence College, Helsinki, Finland.

Furnell, SM & Clarke, NL 2005, "Organisational Security Culture: Embedding Security Awareness, Education and Training", Proceedings of the 4th World Conference on IS Education WISE 2005, 18-20 May, Moscow, Russia, 2005.

Furnell, SM, Gennatou, M & Dowland, PS 2000, "Promoting Security Awareness and Training within Small Organisations" Proceedings of the 1st Australian IS Management (AISM) Workshop, Geelong, Australia, 2000.

Galletta, DF & Polak, P 2003, "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace", Proceedings of the 2nd Annual Workshop on HCI Research in MIS, Seattle, WA, December 12-13, 2003

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. Available: http://www.ebrc.info/kuvat/helokunnas_iivonen.pdf

Lichtenstein, S & Swatman, PMC 2001, "Effective Management and Policy in e-Business Security", Proceedings of 14th Bled Electronic Commerce Conference, Bled, Slovenia, 2001.

Martins, A & Eloff, JHP 2002, "Assessing Information Security Culture", Proceedings of the 2nd Information Security for South Africa Conference (ISSA 2002), 10-12 July 2002, Gauteng. South Africa.

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

Schlienger, T & Teufel, S 2000, "Information Security Culture: The Socio-cultural Dimension in Information Security Management", Proceedings of the IFIP TC11 International Conference on Information Security (SEC 2002), Cairo, Egypt.

Schlienger, T & Teufel, S 2003, "Analysing Information Security Culture: Increasing Trust by an Appropriate Information Security Culture", Proceedings of 14th International Conference on Database and Expert Systems Applications (DEXA 2003), IEEE Computer Society.

Schultz, E 2005, "The Human Factor in Security", Computers & Security, vol. 24, no. 6, pp. 425-426.

Siponen, MT 2000, "A Conceptual Foundation for Organisational Information Security Awareness" Information Management & Computer Security, vol. 8, no. 1, 2000.

Stanton, JM, Jolton, J, Mastrangelo, PR & Stam, KR 2004, "Behavioural Information Security: Two End User Survey Studies of Motivation and Security Practices" Proceedings of the Americas Conference on Information Systems (AMCIS), 5-8 August 2004, New York, USA.

Taylor, M & Murphy, A 2004, "SMEs and eBusiness", Journal of Small Business and Enterprise Development, vol. 11, no. 3, pp 280-289, 2004.

Van Niekerk, JC & Von Solms, R 2003, "Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach", Proceedings of ISSA 2003, 3rd Annual IS South Africa Conference, Johannesburg, South Africa, 2003.

Von Solms, B 2000, "Information Security - The Third Wave?" Computers and Security, vol. 19, no. 7, pp 615- 620.

Vroom, C & Von Solms, R 2004, "Towards Information Security Behavioural Compliance", Computers & Security, vol. 23, no. 3, pp. 191-198.

Warren, MJ 2003, "Australia's Agenda for E-Security Education and Research", Proceedings of the TC11 / WG11.8 3rd 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", Proceedings of 2nd European Conference on Information Warfare and Security, 30 June -1 July 2003, Reading, UK.