This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30008160

Reproduced with the kind permissions of the copyright owner.

Copyright : 2007, ECIW
Developing Information Security Culture in Small and Medium Size Enterprises: Australian Case Studies

Sneza Dojkovski, Sharman Lichtenstein and Matthew Warren
School of Information Systems, Deakin University, Australia
sneza.dojkovski@deakin.edu.au
sharman.lichtenstein@deakin.edu.au
matthew.warren@deakin.edu.au

Abstract: Ideally, information security practices in Small and Medium Size Enterprises (SMEs) should be non-intrusive and intuitive to employees. Previous research has largely overlooked the development of an information security culture for SMEs, and the potential influence of the national context in which the companies operate. This paper provides insights on the key issues involved in developing an information security culture in Australian SMEs from case studies of three Australian SMEs. The paper provides understandings of business owner and employee viewpoints on the issues, and suggests that the main challenges in developing such a culture relate to business owner awareness and countering the Australian laissez-faire attitude of employees. Implications for practice and theory are discussed.

Keywords: Information security culture; small and medium size enterprises; information security management.

1. Introduction

An organisation’s employees are regularly reported as significant contributors to information security risk (Besnard & Arief, 2004). In recent surveys, employee misuse and abuse of internet services totalled twenty - fifty per cent of internet-based incidents (AusCERT, 2006; AusCERT, 2005; CSI/FBI, 2006; ISBS, 2006). Ideally, employees would naturally adhere to existing information security policy, processes and procedures (Dhillon, 2001; Galletta & Polak, 2003). However, while some progress has been made toward the enculturation of information security, greater efforts are required (Ernst & Young, 2006).

To date, several approaches have been proposed, based on multi-faceted management strategies of policy, awareness, training and education (Furnell et al., 2000; Lichtenstein & Swatman, 2001; Schlienger & Teufel, 2003a, 2003b). However, as managerial initiatives on their own are insufficient to influence employee behaviour (Rosanas & Velilla, 2005), new conceptual frameworks are sought. In particular, and of interest to this research, small and medium sized enterprises (SMEs) globally are aware of their weak information security capability (Taylor & Murphy, 2004). However, existing conceptual frameworks for developing information security culture are largely based on considerations for large organisations rather than catering to the special characteristics and information security needs of SMEs. Further, the influence of regional culture has been largely ignored by existing conceptual frameworks. This paper explores key issues that may be encountered in the development of an information security culture in Australian SMEs and reports relevant findings from three Australian case studies, extending earlier work reported in (Dojkovski et al., 2005; 2006).

The rest of the paper is divided into four sections. Section one reviews previous published research on information security culture, and information security in SMEs. It also reviews a framework developed in earlier stages of the project (Dojkovski et al., 2006). In the second section, we review the research design for the study, focusing on the conduct of the case studies reported in this paper. The case study findings are then provided, and finally, conclusions are drawn.

2. Theoretical foundations and framework

This section synthesises representative contemporary literature on information security culture, and information security in SMEs. To conclude the section, we describe a socio-cultural framework (Dojkovski et al., 2006) for developing and maintaining information security culture in SMEs in the national context.
2.1 Information security culture – A review of current frameworks

Information security culture portrays the security-oriented employee behaviour accepted and encouraged by an organisation where employees understand their share of responsibility for information security, support the security technologies already implemented and are conscious of the security consequences their actions might render (Martins & Eloff, 2002). Information security culture should support all security activities such that they become a natural aspect of the daily activities of employees (Martins & Eloff, 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 (e.g. Lichtenstein & Swatman, 2001). However, such frameworks may be better suited to medium and large size organisations due to their significant infrastructure, available budgets, stability, and resource requirements. In recent years, dedicated frameworks for information security culture have emerged, as reviewed next.

Several frameworks have focused on organisational culture and the measurement of information security culture. Such efforts include frameworks based on: trust and partnership (Schlienger & Teufel, 2000, 2003a); shared values (Helokunnas & livonen, 2003); stages of information security awareness maturity (von Solms, 2000); individual, group and organisational levels of information security enculturation (Martins and Eloff, 2002); human actions that influence the confidentiality, integrity and availability of information systems (Stanton et al., 2004); organisational behaviour and how employees are influenced (Vroom and von Solms, 2004); conceptual checklist of information security culture consisting of a compilation of information security and organisation culture concepts (Zakaria and Gani, 2003); prescriptive persuasion based on behavioural principles (Siponen, 2000); security awareness, training and education (Furnell and Clarke, 2005); outcomes-based education (Van Niekerk and von Solms, 2003); and dimensions for measuring the effectiveness of information security culture (Chia et al., 2002).

The abovementioned frameworks offer valuable contributions, however they do not take into consideration the national and cultural perspective that differentiates Australian SMEs from larger organisations globally, and they portray a fragmented, inconclusive field. Clearly, more work is needed, particularly for the overlooked SME sector.

2.2 Information security in SMEs

An increasing reliance on information technology has seen SMEs become increasingly dependant on technology and thus vulnerable to information security risks (Dimopoulos et al., 2004). According to the socio-cultural approach introduced earlier, enhancing the information security of SMEs requires changes in the behaviour and attitude of those people managing the organisation and employed within it, who are responsible daily for managing and using information systems. This requirement proves challenging as SMEs generally have a weak understanding of information security, security technologies and control measures, and do not conduct risk assessments or develop security policies (Dimopoulos et al., 2004; Gupta & Hammond, 2005; Helokunnas & livonen, 2003).

Furnell et al (2000) suggest that information security issues and responsibilities should be highlighted and reinforced in various ways in an organisation - for example, by formal coordination by an administrator, coupled with awareness and training strategies. Whilst such initiatives may be practical in larger organisations where financial resources and information security expertise are often available, in SMEs, the lack of resources and knowledge as well as their perception of information security as unimportant, may hinder this possibility (Furnell et al., 2000). Indeed, recent surveys have found that SME owners are not supportive of information security (Johnson and Koch, 2006) and that most SMEs spend a significantly low proportion of their information technology budget on information security technology (ZDNet, 2004).

Current surveys of SMEs in the developed world reveal very little enculturation of information security, suggesting the need for greater research attention in order to identify the issues involved. This paper explores the key challenges in fostering an information security culture in SMEs using
three case studies of Australian SMEs. A socio-cultural framework for this purpose is described next (developed in Dojkovski et al., 2006).

2.3 Socio-cultural framework for developing information security culture for SMEs

In figure 1 we provide a framework for developing information security culture in SMEs, based on a synthesis of (Detert et al., 2002; Dhillon & Backhouse, 2000; Furnell and Clarke, 2005; Helokunnas & Kuusisto, 2003; Martins & Eloff, 2002; OECD, 2002; Reich & Scheuermann, 2002; Rosanas & Velilla, 2005; Schlienger & Teufel, 2003a; Siponen, 2000; Van Niekerk & Von Solms, 2003) and an earlier exploratory focus group (as explained in Section 3, and reported in Dojkovski et al., 2006). The framework is briefly described next.

2.3.1 Managerial issues

Policies and Procedures; Information security policies and procedures are important as guidance for acceptable employee information security behaviour.

Benchmarking; Benchmarking provides an opportunity for an SME to compare the company’s information security with other similar organisations and recognise that it may need to do more in terms of information security management.

Risk analysis; By conducting an information security risk analysis, a company will become aware of the need to implement appropriate risk management measures.

Budget; An adequate information security budget is needed in SMEs where resource provision may otherwise easily be overlooked. This budget will enable cultural initiatives such as training to be adequately resourced.

Management; As managers are responsible for information security and are also role models for employees, they should model excellent information security behaviour.

Response; Responding quickly and satisfactorily to new information security issues will be beneficial in stressing the importance of information security to employees.

Training; Training provides skills to employees regarding how information security protection can be achieved.

Education; Education of employees provides a deeper understanding of why information security protection is required.

Awareness; An awareness of information security enables recognition of what needs to be protected.

Change management; Following a formal change management approach may help SMEs develop an information security culture.

2.3.2 Behavioural issues

Management initiatives aim to develop desirable behavioural traits of responsibility, integrity, trust and ethicality. Other individual traits to cultivate are strong employee values, intrinsic motivation, an interest in the organisation (orientation) as well as the promotion of personal growth.

2.3.3 Individual and organisational learning

Individual learning of information security threats and their management, when shared with others in an organisation, will promote organisational learning. Thus organisational learning approaches may be useful to develop an information security culture.
2.3.4 e-Learning; cooperation, collaboration and knowledge sharing

Electronic learning (e-Learning) can enable collaboration and cooperation between employees across SMEs and the wider information security global community. Knowledge sharing at all levels is needed, including the sharing of values, experiences and emotions, particularly at the global level.

2.3.5 Ethical, national and organisational culture

National cultures may affect organisational information security culture and should be considered. Societal ethics may also have an impact on SME employees' approach to information security. Different nations may have their own values and cultures which will impact the development of information security culture.

Figure 1: Framework for developing information security culture in SMEs (Dojkovski et al., 2005; 2006).

3. Research design

The research project is multi-method, and commenced with a literature review and exploratory focus group, in which debate and prioritisation of issues took place between key stakeholders, thus enabling identification of the key issues and development of the framework in figure 1. The results of the focus group were reported in detail in Dojkovski et al. (2006). Three case studies of SMEs in a small Australian regional city, Geelong, near Melbourne (a large city in the south eastern state of Victoria) were then conducted, in 2006. Fictional company names are hereafter used. One company comprised engineering consultants 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 two employees ("ProviT"). The three firms were selected for three main reasons. First, as regional (rather than city-based) firms, the three companies represent the less advantaged companies of Australia. Second, the three firms believed they lacked effective information security cultures and were interested in exploring how it could be promoted. Third, as
technical firms, some employees possessed an understanding of information technologies, enabling more specific issues relating to information technologies to surface.

In each case study, ordinary employees, as well as business owners and managers, were interviewed. Interviews were semi-structured single interviews of around one and a half hour's duration. First, definitions of key terms were provided. Second, questions were posed, based on the preliminary framework (figure 1). Participants were asked to consider how each issue in the framework was present, or not present, in their firm, and how that issue might, or might not, contribute to intuitive information security practices. Background documents of organisational structure and information technology strategy were also collected, however no formal policy documents were available as none existed; Inductive qualitative content analysis techniques were employed for each case study in order to analyse the interview data. Coded categories were developed over iterative readings of the case interview transcripts, drawing on the framework (figure 1) 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.

4. Case study findings: Key issues

Table 1 summarises case findings regarding key issues in developing information security culture at the three companies for the issues shown in figure 1.

4.1 Policies and procedures

All three of the case companies identified that information security policies and procedures are an essential element of an effective information security culture. The owner of ProviT stated:

"Obviously you need policies. You have to enforce the policies." [Owner, ProviT]

However, only one company had an information security policy (and that was in draft form) while none had formal information security procedures. Many employees and owners also felt that such policies (which they had sighted elsewhere) were generally too long and often not easy to understand. Thus they expected that compliance with such policies would be difficult.

"We don't have one just because we're so small. Although now that you've mentioned it we could probably have one. They should be, I think, a lot simpler than they are." [Owner, ServiT]

The timing of policy introduction to an employee was also considered important. For example:

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

4.2 Benchmarking

It was noted by all of the case studies that benchmarking was a useful measure. However, SMEs would find it almost impossible as they do not have any knowledge as to how to go about benchmarking.

"(It) is a good idea, however will be difficult to do as SMEs don't know who or what they should be comparing against." [Owner, ServiT]

A possible challenge to benchmarking could be the concern that SMEs may be reluctant to divulge potentially damaging information regarding their organisation's information security. As one business owner generalised:

"We find that no one likes sharing their secrets between different organisations and that might hamper benchmarking." [Owner, ProviT]

A suggestion was made that the national government could assist SMEs by providing benchmarking information to them.
The 6th European Conference on Information Warfare and Security

Table 1: Case study findings for developing information security culture in Australian SMEs

<table>
<thead>
<tr>
<th>Managerial Issues</th>
<th>Summary of Case Findings</th>
<th>C</th>
<th>S</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies and Procedures</td>
<td>Policies and procedures are an essential element in developing information security culture however they need to be more employee-friendly.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benchmarking</td>
<td>Benchmarking is a useful measure, however SMEs would find it almost impossible as they don't have any knowledge in how to benchmark.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Risk analysis is an essential issue; however it presents a challenge as owners view their companies as too small to conduct a risk analysis.</td>
<td>✓</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Budget</td>
<td>Few Australian SMEs allocate a budget to information security as owners must first clearly see the risks involved before they acknowledge the need for a budget (and time) for information security.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Management initiatives help to shape employee information security behaviour. It is important that managers are proactive about security; however they do not always have the time to keep up to date with security knowledge.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response</td>
<td>Procedures to respond quickly to new security measures should be measured and swift. Response and management are important in permeating security throughout the organisation.</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Training and Education</td>
<td>Training and education may be conducted however on an informal basis. However they present a challenge as some SME owners believe that because of their small size, there is generally good communication in SMEs which eliminates the need for extensive training and education.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness</td>
<td>A lack of awareness is a contributing factor to many SME owners not having recognised the existence of an information security problem in their organisation. A government national campaign to raise awareness is needed.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td>A formal change management approach may be implemented if all other managerial measures have failed.</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavioural Issues</th>
<th>Summary of Case Findings</th>
<th>C</th>
<th>S</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behaviour</td>
<td>Employee behaviour can be changed however it is a difficult process. It very difficult to change a person’s sense of responsibility, trust, ethicality and personal growth. It is almost impossible to change a person’s sense of integrity, values, orientation and motivation.</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Individual and Organisational Learning, e-Learning</td>
<td>Learning is an integral issue however it would be difficult for SME owners to measure whether employees are gaining much knowledge from any form of learning if left to do it in their own time. Thus they should be followed up with group meetings/discussions.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical, National and Organisational Culture</td>
<td>There is a lack in government initiatives in helping SMEs with security risks and issues. A national government campaign to market security awareness is needed.</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Column 1 of the table identifies an issue. Column 2 summarises the findings for the issue. Columns 3, 4 and 5 show whether the issue was present as a factor in developing information security culture in each organisation (ConsultEng = C; ServIT = S; ProvIT = P). The findings are then elaborated and the voices of participants provided to add understanding to this interpretive research.

4.3 Risk analysis

In order for SME owners to acknowledge the risks, all of the case companies noted that a risk analysis was essential. However, convincing SME owners to conduct a risk analysis currently presents a challenge. ProvIT expressed the view that their organisation was too small to conduct a risk analysis:

"No, because I gather we're too small for it." [Owner, ProvIT]
Other reasons were presented, varying from inside knowledge of the organisation to accepting certain information security risks and the lack of awareness of security issues.

"I do think it's important to, yes, I haven't really done one because I set the business up and I know how it works." [Owner, ServiT]

"You hope it (information security risk) never occurs, but it could happen." [Owner, ConsultEng]

It was stressed that it is only when SME owners can see the threats and consequences that they will take action.

"I think that's also an awareness thing. They don't realize how important it is." [Owner, ServiT]

4.4 Budget

All companies considered that an adequate budget allocated to information security was important. For example, the owner of ProviT noted that:

"[a budget] must be one of the most important factors..." [Owner, ProviT]

However, according to the study informants, none of the case companies, and very few Australian SMEs in general, 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.

"[a budget is] probably the biggest obstacle. It is hard to get smaller companies to set a budget for information security." [Employee, ConsultEng]

4.5 Management

All of the case companies agreed that appropriate management initiatives can help shape employee information security behaviour. For example:

"[Management] is one of the more important factors. Management must set a standard for the other employees." [Employee, ConsultEng]

It is important that management be proactive about security, however SME owners noted that management might not have the time to keep up to date with security-oriented information.

"You might find management may not have time, I feel. Most managers don't always keep up to date with issues such as [information] security." [Owner, ProviT]

4.6 Response

Employees noted that procedures to respond quickly to new information security measures should be precise and fast. As one employee put it, the response should be:

"Measured and swift." [Employee, ConsultEng]

As an issue, response is connected with management and all of the case companies stressed the importance of management in permeating security throughout the organisation.

4.7 Training and education

SME owners expressed the view that because of their small 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." [Owner, ServiT]

"We don’t really have a need for training our own people." [Owner, ProviT]

It was suggested by SME owners that training and education are measures more appropriate to larger sized organisations.
The 6th European Conference on Information Warfare and Security

"If I were to grow and take on quite a number of people, I'd be looking for a training course." [Owner, ServIT]

However, employees within the organisations thought that education and training should be essential for employees to know how to act and set boundaries

"A must for staff at all levels." [Employee, ConsultEng]

"Most important. Must train employees otherwise they won't know what to do. Must teach people how and why. Tell employees what can go wrong. And what can be done." [Employee, ConsultEng]

4.8 Awareness

A lack of awareness is a contributing factor to many 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. It was suggested that a national government campaign on raising SME awareness of information security is needed, with the use of brochures, websites, emails, TV advertising, and other initiatives.

4.9 Change management

ConsultEng noted that a formal change management approach might be implemented if all other measures have failed. The remaining case studies neglected to comment on this issue.

"Doesn't need to happen if all the above is done well." [Employee, ConsultEng]

4.10 Behaviour

SME owners noted that employee behaviour is very hard to change and thus it is better to hire the right person initially. ProviT expressed the view that employee behaviour can be changed using managerial measures i.e. policies, procedures, and training, however it is a difficult process.

"... obviously you’ve got the right steps here like policies, training which is probably a key factor to changing someone’s behaviour; the way they think, making them aware of issues...[but] you’re just going to be hoping. You’re saying these procedures and policies will obviously change the behaviour of the person; but you’re really never going to know." [Owner, ProviT]

4.11 Individual and organisational learning, e-Learning

Employees accepted learning as an integral issue for information security culture in SMEs.

"Important to feed into the organisational level." [Employee, ConsultEng]

However, SME owners noted that it would be difficult for SME owners to measure whether employees are gaining much knowledge from learning if they are left to do it in their own time. It was suggested that any form of learning should be followed up with group meetings/discussions.

"Yes it needs to be combined with the human touch, that's the only way you can really know; unless you test people afterwards, that's the only way you'll really know if they've listened." [Owner, ServIT]

SME owners also noted the lack of awareness of available learning packages for small organisations.

4.12 Ethical, national and organisational culture

The case studies were critical of the lack of Australian government (federal and state) initiatives in helping SMEs with security risks and issues.

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

Suggestions were made for the Australian federal government to market security awareness; including brochures containing a variety of case studies that would spark interest among SMEs; templates for risk analysis; and information security standards for SMEs.
5. Conclusion

The paper provides key findings (summarised in Table 1) from three interpretive case studies of Australian SMEs that explore issues relating to the development of an information security culture in the Australian context. Understandings and challenges that hinder the development of an information security culture in Australian SMEs were highlighted by the case study findings. The paper has highlighted that internally, SME owners have the greatest responsibility and role in ensuring a more security conscious organisation. An organisational security awareness program of informal activities to increase the awareness of SME employees is imperative. Greater external support for developing an information security culture in Australian SMEs is needed by the federal government. Although the study was conducted in the Australian setting and the framework cannot be generalised to an international context, the insights revealed are supported by several studies incorporating SMEs globally (AusCERT, 2006; Briney & Prince, 2002; ZDNet, 2004) and thus offer numerous insights into the challenges of establishing an information security culture in SMEs worldwide, and contribute to existing theory in this area. Future research will continue to explore and validate these findings in Australia and overseas.

References


The 6th European Conference on Information Warfare and Security


ZDNet Australia (2004) "SMEs reluctant to open wallets for IT security", ZDNet Australia, [online], 16 June 2004