Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2005 Proceedings | Australasian (ACIS)

December 2005

Securing Small Business - The Role of Information Technology Policy

Lynn Batten
Deakin University

Tanya Castleman
Deakin University

Securing Small Business – The role of information technology policy

Lynn M. Batten and Tanya Castleman
Deakin University
Victoria, Australia
lmbatten@deakin.edu.au tanyac@deakin.edu.au

Abstract

As small and medium enterprises develop their capacity to trade electronically, they and their trading partners stand to gain considerable benefit from the resulting transaction efficiencies and business relationships. However, this raises the question of how well small business manages its IT security and the threats that security lapses may pose to the wider trading network. It is in the interest of all members of an electronic trading network, as well as governments, to assist smaller companies to secure their business data. This paper considers the relationship between IT security management and IT policy implementation among small businesses involved in business-to-business eCommerce. It reports the results of a survey of 240 Australian small and medium businesses operating in a cross-industry environment. The survey found a low level of strategic integration of eCommerce along with inadequate IT security among the respondents, despite the fact that 81% were doing business online and 97% identified their business data as confidential. Businesses which implemented satisfactory levels of security technologies were more likely than others to have an information technology policy within the organisation. The paper proposes a model that outlines the development of security governance and policy implementation for small and medium businesses.

Keywords
Information Security, IT policy, Small business, SME, eCommerce

INTRODUCTION

One of the benefits a small business may gain from internet commerce is an enhanced ability to sell to large organisations. The capacity to transact electronically gives these businesses access to a wider range of trading partners and business relationships. This appears to be a far more compelling reason for small business to trade electronically than improved transaction efficiency which is of more interest to large organisations. The mutual benefit of electronic transactions should ensure its swift and effective adoption and encouragement, but progress has been patchy and disappointing.

Governments and large organisations have made considerable efforts to encourage small and medium enterprises (SMEs) to engage in electronic trading (Levy and Powell, 2003; NOIE, 2000) which has contributed to the large numbers of SMEs which now use computers in the workplace for various administrative and business processes (Sensis, 2003). Despite these efforts, advocacy and offers of assistance (Coulthard, Castleman and Batten, 2004), SMEs have been slow to adopt electronic business-to-business trading at anything more than a superficial level (European Commission, 2002; Keeling, Vassilopoulou, McGoldrick and Macaulay, 2002; Levy and Powell, 2003; WITSA, 2000; Yellow Pages Business Survey, 2003). Few have taken a strategic approach to using online transactions and this problem is exacerbated when SMEs trade across industry sectors with different requirements for trading software. Without strong industry-based leadership, the smaller enterprises are more likely to make inappropriate decisions about information technology and to rely on in-house staff. The foregone business benefits, both to the SME and its larger trading partners, are a continuing cause for concern. In the move to a ubiquitous and seamless electronic transaction environment, SMEs remain the weak link in the chain.

A business moving to an electronic platform may do so in order to increase their availability to customers and facilitate the ordering and purchasing of products. Availability and proper functioning of the site is therefore important to the success of the business. However, problems caused by virus attacks can significantly interfere with availability, as pointed out in Maiwald (2001) and, over time, destroy the relationship between business partners. A less well recognised problem of SMEs' inadequate IT and electronic trading capability, is the information security risk it poses, not just to them but to their trading partners and the whole transaction network which is increasingly linked via the internet and other electronic or wireless connections. The risk to individual businesses from external threats (such as identity theft, theft of information, viruses, privacy breaches, etc.) is significant. Given the seriousness of these security threats, we need a better understanding of how SMEs approach information security and how they can be assisted to improve their security preparedness as an essential part of their development of effective electronic trading and eBusiness capability.

A survey of Australian SMEs, as presented in this paper, sheds light on a number of factors associated with the implementation of eBusiness, including their approach to security. The survey targeted SMEs which supplied business customers in a number of industry sectors and sought information about what transaction technologies they used, their business strategies and goals in general and their level of eBusiness readiness. Information security issues were included as part of the assessment. Like many small businesses in Australia and more widely, few of the participating firms saw electronic trading as a competitive advantage and did not approach it strategically. They tended to use various applications in response to the encouragement and demand from external quarters for online trading capability. Their approach to security typically followed the same pattern of ad hoc and imperfect provision for protecting their business. Yet the findings indicate relatively simple steps that can help address this deficiency. In this paper we outline the main eCommerce security issues for SMEs, report the results of our survey relating to security and propose a model of security adoption for SMEs. The proposed model may help us understand how these firms can develop more robust security applications and what techniques government and industry leaders might find effective for encouraging this development.

SMEs, eCOMMERCE AND SECURITY

While electronic commerce, and specifically purchasing tools, are intended to facilitate business, save costs, reduce order cycle time and enhance partnerships, there are many implementation barriers facing small firms. A comparative analysis of small and large American firms by Min and Galle (2001: 92) indicates that 'in contrast to large firms, small firms do not necessarily value EC-based purchasing as a way of reducing paperwork, but as a way of building a long-term partnership with their trading partners.' They go on to explain that their 'finding suggests that the use of EC-based purchasing among small firms is more limited to basic purchasing transactions such as purchase orders and shipment tracing where EC is proven to be successful.' Indeed, these results are confirmed in the Australian setting where SMEs engaging in electronic commerce tend not to integrate their electronic trading strategies with the business strategies of the organization (Ratnasingam et al, 2002; Coulthard et al, 2004).

Building relationships with trading partners involves trust in both the partner and the technology used by the partner. Seven types of technology trust are identified by Wagner et al. (2003). These are transaction confidentiality, integrity, authentication, non-repudiation, access control, availability and best business practice. The paper goes on to develop a statistically significant relationship, based on an international sample of 2500 organizations, between technology trust and trading partner trust, between technology trust and the perceived benefits to the business, and between technology trust and eCommerce performance. Thus, for the long-term partnership-building priority of small businesses, the establishment of technology trust is seen to be an implied priority. The point of view of large U.S. firms in this regard is described in Min and Galle (1999: 917), as follows '…the buying firm's number of employees, annual purchase volume and size of supplier bases influences its requirements for EC trading capability as an integral part of supplier selection attributes… It is interesting to note that the smaller the firm's supplier base, the greater the chance the buying firm would mandate the EC trading capability as an important part of supplier selection…'

Thus, for smaller organizations working in a narrow supply chain setting, the pressures to participate extensively in eCommerce-type activities would appear to be greater than for those supplying to a wider area. The technology requirements in this case, would be quite specifically related to the principal organizations involved in the supply chain, and one could argue that this makes decisions easier for all such connected businesses. On the other hand, it would be more difficult for SMEs outside of narrow supply chain structures to determine a basis of eCommerce technology on which to build their business as their partners would tend to have a wide variety of eCommerce mechanisms in place. This would, in turn, make it more difficult to establish the kinds of trust relationships with trading partners that small businesses believe to be of benefit.

While specialized e-payment technologies are available for use by businesses, small and large, the use of the Internet itself for simpler purposes, such as e-mail and searching for information has major drawbacks. The Internet was not designed for business purposes and is in many ways not suitable for it. The security risks associated with Internet use have been identified by several authors including Maiwald (2001) and Easttom (2005). These include theft of sensitive data from systems with inadequate security, inability to properly authenticate initiators of online business transactions, viruses which slow or shut down the network leaving the computer attacked inoperable, unauthorized access to computer data which can then be deleted or altered. Both authors argue that an effective Internet usage policy can go a long way to avoiding many of the problems identified in Internet usage for business purposes.

An independent study by the World Information Technology and Services Alliance (WITSA, 2000) indicates that the major concerns of organizations (small, medium and large enterprises are included) who wish to engage in global eCommerce are:

- *Payment*: security of payments affected by new technologies.
- *Security*: fear that technology infrastructure is not robust enough to prevent attacks.
- *Privacy*: uncertainty about how well information privacy and data integrity is protected.
- *Authentication*: uncertainty about the identity of communicating parties.
- *Compliance*: few established regulations governing commercial behaviour.
- *Risk*: companies uncertain of business risks of deploying electronic commerce.
- *Standards*: lack of universally accepted standards.
- *Liability*: lack of established methods of recourse.

Where, then, does an SME turn for assistance in determining how to secure electronic commerce transactions? Governments world-wide have developed websites containing information about the methods available; some have added information about best practice standards and the liabilities and legal requirements of electronic trading. In general terms, a small business which classifies its business data as low risk needs to implement only basic security mechanisms; a medium business for which data is classified as high risk needs to take all components of the WITSA report seriously, and implement fairly sophisticated security technologies. In all cases, education of personnel about in-house security management is an important component of the implementation of electronic commerce (Batten and Wasif, 2003).

STUDY METHOD

The study on which this paper is based explored eCommerce readiness and use by SMEs trading in a cross-industry environment. The sample for the survey was developed in three stages. The researchers compiled a list of businesses by amalgamating the supplier lists of nine large corporations and government departments representing six different industry sectors. An initial telephone survey was carried out in April-May of 2003 to determine the characteristics of supplier businesses using eCommerce, their perceived benefits of conducting transactions using a common platform (Batten, Castleman, Chan, Coulthard, Savage and Wilkins, 2004). A response rate of 48.8% yielded 2,495 responses. The industry sectors in which the participating businesses traded included retail, government, healthcare, mining and communication services, but many suppliers also had buyers in a variety of other industries. Thus, the participants were trading in a network setting rather than simply being part of narrow supply chains. The survey highlighted business transactions (purchasing and payment) rather than more sophisticated eCommerce applications since these lower level transactions are universally relevant to all businesses. Questions related to methods of conducting business (mail, phone, fax, e-mail, EDI, Web services), electronic bill payments and the extent of electronic trading with suppliers, buyers, government and banks. All respondents were asked whether they would be willing to participate in a further study and, if they agreed, were placed on a second list.

A second survey seeking further information about business goals, business strategies and B-2-B eCommerce behaviour was conducted in September 2003 to develop a broader picture of how they positioned their businesses. An email inviting participation was sent to approximately 1600 companies, of which two hundred and forty (240) completed this second survey. The web-based questionnaire was more extensive than the earlier phone survey and explored strategic issues. It asked companies about factors that might afford them a competitive advantage with a series of questions designed to provide a deeper understanding of their business goals. In addition to questions which explored problems resulting from trading across multiple industry sectors or dealing with multiple electronic business formats, they were questioned about the company's security practices.

While the response rate on the second questionnaire is much lower than the first, reflecting the web-based rather than telephone format, and cannot be taken as representative of all Australian SMEs, the number of respondents is substantial. Respondents were distributed throughout Australia in both regional and metropolitan areas. The analysis was able to match data from the first survey (focusing on eCommerce involvement) with data from the second survey (highlighting strategic and security issues). The size of the sample allowed statistical analysis and identification of relationships within the data.

A significant component of the survey (6 questions out of 22) was directed at security issues and in this paper we present for the first time the results of responses to the relevant survey questions. The relevant survey questions are as follows:

1. Excluding personnel data, how important is it to you to keep your business data confidential?
   Very important ☐ Somewhat important ☐ Not really important ☐

2. Which of the following security methods do you use:

back-up	☐	authentication	☐
virus protection	☐	encryption	☐
firewall	☐	audit	☐

3. Do you believe that your business has adequate computer security?
   Yes ☐ No ☐ Unsure ☐

4. Does your business have a formal policy for the use of computers at work?
   Yes ☐ No ☐ Unsure ☐

5. From which of the following sources does your company obtain its IT expertise?

Specialist in-house IT staff	☐
Non-specialist in-house IT staff	☐
External IT providers	☐
Other sources	☐

6. What percentage of your transactions with each of the following organisations do you conduct electronically?

	None	Up to 1/3	1/3 to 2/3	Over 2/3
Buyers / customers	☐	☐	☐	☐
Suppliers	☐	☐	☐	☐
Government	☐	☐	☐	☐
Banks	☐	☐	☐	☐

RESULTS

Under-resourced SMEs can be expected to respond with hesitation when making the decision to enter the electronic trading arena. Thus, we anticipated that a large number of organizations completing our survey might well continue to rely on tried and true methods of contacting clients, such as mail and phone. Indeed, as part of the survey, companies were asked about methods of conducting business (post, phone, fax, e-mail, EDI, Web services) and whether they made bill payments electronically. (About 30% of firms responding to the first survey relied solely on post, phone and fax for their business transactions.) They were asked about the importance of keeping their business data confidential, which methods of securing their computer systems were in place, whether they felt they had adequate computer security, from which sources they obtained IT expertise, and whether the company had a computer use policy. The six major areas included in the security methods list were: Audit systems, Authentication systems, Backup, Encryption, Firewalls and Virus protection systems. These choices are based on established knowledge about computer security needs of small and medium Australian business (Batten and Wasif, 2003).

IT security measures in SMEs

Of the 240 respondents to the survey, 230 were willing to answer the six questions relating to securing technology use. Almost all respondents were aware that their business data is a major asset and that loss of confidential information would have negative consequences. The great majority reported that it was important for their business to retain the confidentiality of their business information; 83% believe it is ‘very important’ and 14% believe it is ‘somewhat important’.

In response to questions about how they secured their business data, 85% use back-up methods, 83% employ virus protection and 78% use both back-up and virus protection together. A substantially lower proportion (53%) use firewalls. In contrast, encryption and authentication were not widely used. Only 17% of businesses surveyed used authentication techniques and 16% used encryption techniques to secure their business data. The use of computer audit was even lower at 3%. It is unclear to what extent this indicates lack of awareness, a high level of trust or lack of resources and know-how.

Of particular interest is the total number of security mechanisms employed. Note that these security methods tend to be cumulative – that is, an organisation will not purchase encryption technologies without having first implemented virus-protection and data backup plans. And an investment in encryption and authentication signals extended use of the Internet for transaction purposes and a firewall is necessarily a component of protecting such transactions.

Figure 1 below indicates the percentage in our sample using each of the six security techniques identified.

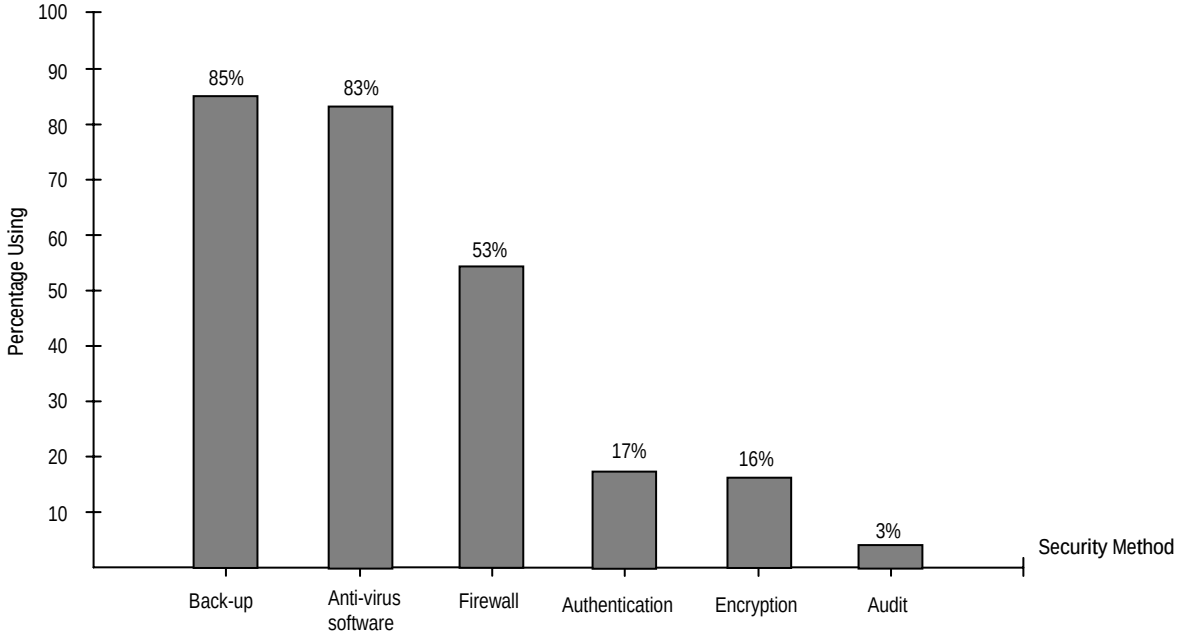

Figure 1: Percentage use of security methods

We asked the respondents if their businesses had a formal policy for the use of computers at work. Almost half of the respondents, forty-seven percent (47%), had developed such a policy. This variable appears to be significantly related to security activities.

Figure 2 below, demonstrates very clearly the inverse relationship between the number of methods used and the existence of a security policy. As the percentages in the above graph drop steeply as the number of methods increases, those in the graph below increase sharply.

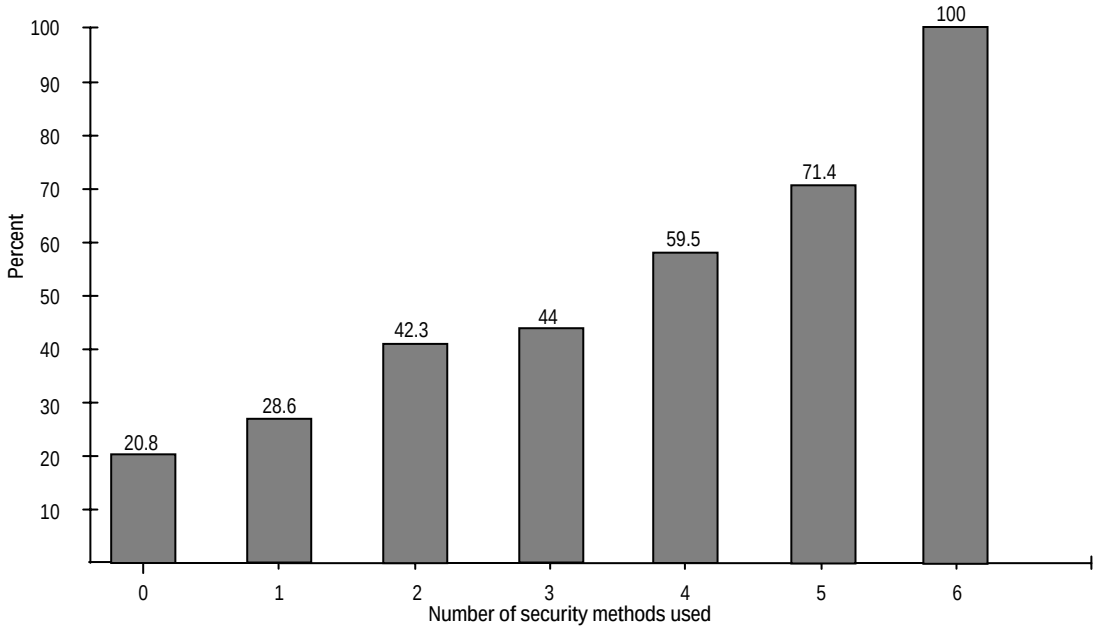

Figure 2: Proportion of firms with a security policy by number of security methods used

Perception of Business about IT Security

Respondents were asked to assess the adequacy of their security measures. While 97% of businesses responded saying that their data was somewhat to very confidential, only 57% reported that they have adequate security. This is an optimistic assessment. In fact, the average number of security methods used by respondents in our survey is 2.8. According to work of Batten and Wasif (2003), SMEs should employ at least five methods in order to secure their system if they are small businesses and at least six methods if they are medium businesses. Consequently, compared to recommended eBusiness security strategies presented in the above-mentioned paper, only seven businesses responding to our survey have introduced adequate security technologies into their business. Part of the reason could be the lack of technical skills since 33% reported that they had no technical skills related to electronic trading in-house and either do not engage in any such activities or outsource their IT requirements. Whatever the reason, this leaves the firm vulnerable in relation to risk assessment and implementation of security standards.

While businesses easily identify security issues as a serious obstacle to electronic trading, they are often willing to overlook the problems if the efficiencies produced by the implementation of electronic commerce technologies can be measured. In a survey of United States purchasing organizations, Min and Galle (1999: 919) conclude that 'even though the surveyed purchasing professionals cited EC (electronic commerce) network security as one of the most serious obstacles to successful implementation of cyber-purchasing, their security concern alone would not deter them from utilizing EC as an effective purchasing tool. That is to say, purchasing professionals generally seem to believe that the potential benefits of EC still outweigh its security risks.' Developing a policy for computer use may well have an independent effect on heightening awareness of security issues and taking steps to secure business data recognised as valuable.

Limitations of the Survey

While the majority of participants completed the survey on-line, a small group (33) specifically requested that they be allowed to print the surveys and submit by post. The existence of this latter group indicates the unwillingness of some organizations to participate in electronic activities. However, since all of our respondents from survey one who had agreed to participate further, whether or not they did so electronically, did indeed complete the second survey in some format, we did not feel that we had disadvantaged businesses not already committed to electronic business.

The set of questions targeting security was only part of a larger survey and consequently did not reach as deeply as possible into the security aspects of the business. As indicated below, further work can establish finer links between security issues and security policies.

PROPOSED MODEL OF SECURITY GOVERNANCE IN SMEs

Combining interpretation of the survey results and patterns identified in the literature on IT security management led us to propose a model describing typical stages in the development of security governance by an SME. The model outlines the necessary elements of a comprehensive approach to security and suggests the steps by which small businesses will tend to develop such an approach, helping to identify where and how they might be assisted in this.

Step 1: Securing the boundaries

The company recognises that doing business online involves risk and that security measures are necessary to protect the business from data loss, hacking and virus damage. Sources of information about the need for this level of security include the popular press, ISP providers and IT vendors. The solutions at this level are relatively easy for small businesses to enact and include the use of firewalls, backing up of data, the purchasing and updating of virus checkers, running anti-virus software frequently and educating employees about the dangers of virus-carrying email.

Step 2: Risk containment

The business recognises that it is exposed in a number of ways and that its security requires a systematic assessment of the risks and actions to address them. Firms that take this step typically deal with confidential data or data they identify as their business capital. They may also be motivated by their involvement in online trading (e.g., purchasing) or extranets which make the in-house business activities more vulnerable to security threats. Security measures include provision for authentication to provide selective access to company data and encryption to protect data in transit to clients from third party interference or spying.

Firms are motivated to move to containing risk if they value their data highly. In many cases they must meet the security requirements of trading partners. Relationships with trading partners are extremely important for smaller companies and the trust on which such relationships depend involve trusting technological systems as

well as personal trust. Risk containment measures are also more likely in companies with sophisticated IT operations or which have a separate IT unit in the firm. They are likely to be larger companies and employ solutions to security risks involving both technologies and management (protecting the firm from potential abuse by employees).

Step 3: Policy development

The business develops a framework and set of procedures for internal operations. This builds on its assessment of risk and seeks to extend that orientation to all members' actions. By setting up a security policy, a company is more likely to promulgate it and communicate its expectations, not leaving security matters as an unformulated intention. Even if a policy is not, in the first instance, complete, it concretises the issue and encourages increments in security measures. The significance of this stage is its incorporation of security into normal business rather than treating it in an ad hoc way. For instance, a standardized approach to the use of passwords with practical guidelines for maintaining their confidentiality would be a natural item for inclusion in the procedural component of a security policy.

Companies which match their security measures with external standards and frameworks have attuned their security awareness with the activities of the broader trading community. This will ensure that the policy is regularly reviewed and matched to independent standards and technology developments.

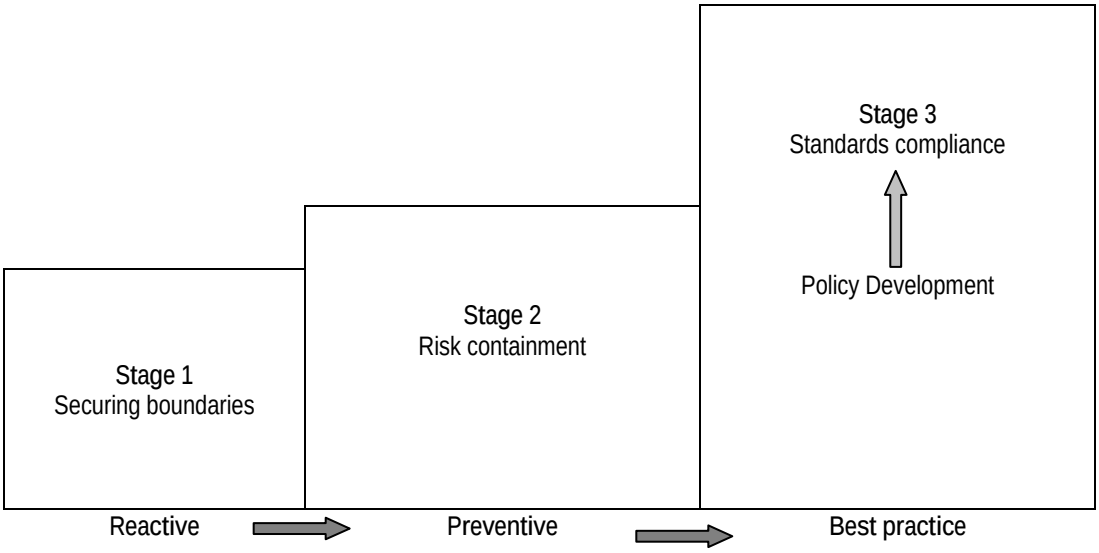

Figure 3: Model for the development of security governance

This model suggests that there are a number of stages which trace the path of SME's security governance development from a reactive approach to dealing with security threats through to a more planned and systematic approach to security issues which deals with general management as well as IT management issues. Stages 1 and 2 differentiate most smaller organisations from larger organisations (and even many larger organisations may have achieved only Stage 1 activities). The strategic shift from response towards systematic assessment is a major leap forward for a business. Not only does this transition recognise the link between security management and the placement of the business as a whole, but it can be a significant contributor to more proactive management of security along with relationship building.

Thus the third stage identifies the development and articulation of security policy. This goes beyond anticipating and managing security risk. It sets out a series of protocols and procedures which shape the behaviour of all members of the organisation, providing an educative intervention as well as directing behaviour. It then moves on to link security policy to international benchmarks, ensuring a best practice approach to security management. This can be a strategic advantage for an SME seeking to trade electronically with larger organisations that have a high level of vulnerability and demand top level security among their trading partners. Although benchmarking security policy and practice against international standards is onerous, it can help a small firm demonstrate exemplary management and it can achieve the goal of cementing trading relationships.

POLICY DEVELOPMENT

As businesses grow and information technology becomes a critical part of the business environment, the governance of IT becomes increasingly important. Usually operations matters are left to management while the board of directors is not concerned about its relevance to overall business strategy (Gertz, Guldentops and Strous, 2001). According to Pollard (2003), the responsibility of policy development lies with either the program manager or the information security manager. As these positions require high level management support, the lack of such support will result in failure to produce an effective information technology policy. In order to minimize this failure, the appointment of a senior management 'champion' who has sign-off authority on policy decisions is highly recommended. Credibility of such a person's authority is enhanced if she or he has appropriate credentials.

Australian businesses have various standards and frameworks available to assist them in securing their businesses from external and internal threats. The Australian standard AS/NZS 7799.2:2003 for information security management contains a clear definition of a comprehensive Information Security Management System and a description of the activities required to implement it (Keeling et al, 2000). This standard is also supported by the worldwide standard ISO 17799:2001.

Several frameworks for the integration of good technology and security management implementation now exist. COBIT, or Control Objectives for Information and related Technology, is an example of a world-class framework which was published by the Information Systems Audit and Control Foundation in 1996, followed by second and third editions. COBIT is designed to provide comprehensive guidance to management and business process owners (Guldentops, 2002).

According to a study by PriceWaterhouseCoopers (Hoekstra and Conradie, 2004) COBIT's real strength lies in its analysis of information technology controls and its quality assurance metrics, while ISO 17799 contributes a strong commercial security dimension aligned to international standards.

Table 1 below indicates the key components of a policy, along with the procedural components. Assessments of the business vulnerabilities as well as legal obligations are critical components of the document. An indication of where responsibilities lie within the organization must be detailed for effective implementation.

Items in a policy document	
Information	Definition of information security. Statement of intention supporting the goals and principles of information security. Managing of security incidents
External Regulations	Explanation of applicable proprietary principles, standards and compliance regulations. Risk assessment and liabilities. Confidentiality and privacy requirements.
Education	User training.
Policy Assessment	Maintenance of the policy document. Assessment of the effectiveness of the policy. Assessment of the applicability of the policy over time.
Items in a procedure document	
Task Allocation	Allocation of responsibilities for every aspect of implementation. Nomination of the policy owner. Assurance of continuous services. Assurance of systems security. Delineation of authorization, authentication and access control. Profile establishment for authentication and authorization. Incident handling, reporting and follow up. Virus prevention and detection. Firewalls. Establishment of a centralized security administration.
Applications for Inclusion	Virus prevention and detection. Firewalls. Cryptographic key management. Tools for monitoring compliance, intrusion testing and reporting.

Table 1: Items in policy and procedure documents

CONCLUSIONS AND FUTURE WORK

Small businesses have struggled to adopt basic electronic transaction methods, especially when they trade in multiple industry sectors with many other enterprises. Without the more extensive resources available to large companies, smaller businesses may be obliged to rely on inexpert in-house staff for IT decisions and may invest in inappropriate or inadequate proprietary transaction software, leading to serious risk to the individual business from external threats. This also involves a threat to the business' trading partners and to the whole transaction network, increasingly linked via the internet and other electronic or wireless connections.

Major involvement of SMEs in Internet, mobile or wireless transactions will have major implications for the nation's economic safety and well-being. Consequently, large organizations for which SMEs form a large part of their client base need to be aware of the transaction methods used by them, as these methods may directly impact on their own reliability and security.

Results of our survey indicate that small and medium businesses implement insufficient security methods in their use of information technologies, while, for the most part, believing that their security is adequate. Our survey results also indicate that SMEs which do implement satisfactory levels of security technologies are more likely than others to have an information technology policy within the organization. It is not clear to us whether the introduction of security technologies generates the impetus for a company IT policy, or whether the existence of a policy results in the adoption of a high level of security implementation. This will be investigated in further studies at a deeper level to determine the impact of IT policy development on the raising of security awareness within the business and the applicability of the model we propose. However, it is quite possible that both of these scenarios apply.

Nevertheless, it seems very clear that in developing a policy around secure implementation of IT, a small or medium business will learn how to implement the security correctly and strategically. We therefore highly recommend the development of IT policies within organizations as a means of raising security awareness at management levels and we proposed a three-tier model for the development of security governance which includes the development of such policies.

REFERENCES

Batten, L.M., Castleman, T., Chan, C., Coulthard, D., Savage, R. Wilkins, L. (2004), 'Engaging Suppliers in Electronic Trading Across Industry Sectors', IFIPWG8.4 Working Conference, Salzburg, Austria, June, 182-199.

Batten, L. M, and Wasif S. A.(2003) 'e-Business Security Strategies for SMEs'. In *Proceedings of the International Telecommunications Society's Asia-Australasian Regional Conference*, Perth, Australia, Communication Economics and Electronic Markets Research Centre, III.1,1-19.

Coulthard, D., Castleman, T. and Batten, L.M., (2004) 'eCommerce strategy in a multi-sector trading environment – quandaries for SMEs.' Proceedings of BLED eCommerce Conference, 1-13.

Easttom, C. Network Defense and Countermeasures. Pearson 2005.

European Commission 'The Ebusiness Watch' (2002); http://www.ebusiness-watch.org/marketwatch/ accessed 5/12/ 03.

Gertz M., Guldentops E., & Strous L. (2001) 'Integrity, internal control and security in information systems: connecting governance and technology'. In *Integrity, Internal Control and Security in Information Systems* Proceedings IFIP, Brussels, Kluwer.

Guldentops, E. (2002) 'Governing information technology through COBIT' . In *Integrity, Internal Control and Security in Information Systems* Proceedings of IFIP Nov 2001, Brussels, Kluwer Press.

Hoekstra A., & Conradie N. 'CobiT, ITIL and ISO17799, How to use them in conjunction' PriceWaterHouse presentation [On-line. Last accessed: February 11, 2004]
http://www.itsmf.org.za/Presentations/CobiT%20ITIL%20and%20BS7799.pdf.

Keeling, K, Vassilopoulou, K, McGoldrick, P. and Macaulay, L. (2000) Market Realities and Innovation in Small to Medium Sized Enterprises: Facilitators and Barriers to the Use of Electronic Commerce, New Product Development and Innovation Management, March/April, 57-70.

Levy, M. and Powell, P. (2003) 'Exploring SME Internet Adoption: Towards a Contingent Model'. *Electronic Markets*; Jun2003, Vol. 13 Issue 2, 173.

Maiwald, E. Network Security – a Beginner's Guide. McGraw-Hill, 2001.

Min, H. and Galle, W.P. (1999) 'Electronic commerce usage in business-to-business purchasing'. International Journal of Operations and Production Management, Vol.19, no. 9, 909-921.

Min, H. and Galle, W.P. (2001) 'Electronic commerce-based purchasing: A survey on the perceptual differences between large and small organisations'. *International Journal of Logistics*, Vol. 4, No. 1, 79-95.

NOIE (National Office of the Information Economy). (2000) 'Taking the Plunge: Sink or Swim: Small Business Attitudes to Electronic Commerce'. *Dept of Communication, Information Technology and the Arts*, Canberra.

Pollard M. (2003) 'Developing an IS18, AS/NZS 7799.2 and ISO 17799 Complaint Information Security Management System'. *Whitepaper for Bridge Point Communication.*

Ratnasingam, P., Pavlou, P. and Tan, Y. (2002) 'The importance of technology trust for B2B electronic commerce'. Proceedings 15'th Bled Electronic Commerce Conference, Slovenia, 384-398.

Wagner, B. A., Fillis, I and Johansson, U. (2003) 'E-business and e-supply strategy in small and medium sized businesses (SMEs)', Supply Chain Management, 8(4), 343-354.

WITSA (2000): International survey of e-commerce 2000. (Electronic) Available at: http://www.witsa.org/papers/EComSurv.pdf , January 08, 2003.

Yellow Pages eBusiness Survey, '2003 Yellow Pages ® eBusiness Report'. Sensis, Melbourne, 2003.

COPYRIGHT