December 2002

Management Issues for Medium-sized Organisations in Outsourcing E-security

Malcolm Bertoni
University of Tasmania

Paul Turner
University of Tasmania

Management Issues for Medium-sized Organisations in Outsourcing E-Security

Malcolm Bertoni and Paul Turner

School of Information Systems
University of Tasmania
Hobart, Australia
Malcolm.Bertoni@utas.edu.au

Abstract

The advent of outsourcing in e-Security raises a series of management issues in the selection, implementation and evaluation of available solutions. More broadly, the growth of electronic commerce has increased business awareness of the need to respond to e-Security and other related issues. To date, there has been a lack of Australian research in this area and limited evidence suggesting that Australian medium-sized organisations are coherently managing the challenges faced.

This paper examines key management issues facing medium sized organisations in e-Security, explores different outsourcing models and provides a generic four-step approach to assist them in making strategic security decisions.

Keywords

e-Security, outsourcing, medium-sized organisations, strategic management issues

INTRODUCTION

The increasing importance of electronic commerce (EC) has heightened business awareness of issues relating to e-Security including privacy, trust and the integrity of on-line communications. Until recently the high cost of advanced e-Security solutions remained the preserve of large organisations. Advanced e-Security solutions being the full suite of applications, tools and techniques including monitoring, audit trails and timely reporting that protect organisations from internal or external attack, misuse and abuse of the Internet However, security solution providers have now started to proffer an outsourced approach that has brought these solutions within the financial reach of many medium sized organisations. This availability raises numerous management issues – the most obvious being: do we need these advanced e-Security solutions for our business? Significantly, while much of the previous research on the management of e-Security has focused on technology, it has recently been shown that the human aspects of e-Security solutions are as, if not more important in the implementation of effective e-Business security (Lichtenstein and Swatman, 2001). This raises management challenges for organisations looking to employ third parties to assist them in implementing e-Security.

While predictably security solution providers continue to promote the critical need for their services, much EC appears to continue apace without them. For most medium sized organisations this is both confusing and frustrating. At the same time the incidence of e-Security breaches and illegal or inappropriate online behaviours continues to rise (Broucek and Turner, 2002). The latest Computer Security Institute (CSI) figures illustrate Internet breaches and attacks have risen from being 38% of all attacks in 1996 to 74% in 2001 (Power, 2002). In Australia the trend is similar with 78% of attacks via the Internet or Remote Access (AusCERT, 2002), most commonly in the form of viruses, Trojan horses and worms. An example, highlighting the risks organisations face is the Klez E email worm that is programmed to delete and overwrite Word, Excel, video, image, and Internet files on the sixth day of every other month. The latest version of this worm has been traced to a source in Southeast Asia. Although to date this worm has only had a limited impact in Australia, the increasing threat of attacks from the Asia-Pacific in particular, strengthens the case for Australian organisations to address e-Security as a key management issue.

What are the management issues that should be considered in selecting, implementing and evaluating the security solutions available? How should these organisations assess and evaluate: the advantages/disadvantages of particular types of e-Security; the impacts of the introduction of e-Security into their organisation; and, the on-going and second order costs that may be associated with these decisions? What criteria should these organisations use to make decisions about how much or how little to outsource and to whom?

One conventional approach to these e-Security issues is the conduct of a basic risk assessment and analysis. This would address three basic questions on requirements to ensure a viable e-Security system (What are the assets that need protection?, What are the risks to these assets?, What level of resourcing is the organisation willing to expend on adequately protecting these assets?). This would be followed by an analysis of how the different answers to this assessment link to the different levels of security threat identified. At the broadest level, it is clear that the threat posed by e-Security breaches is growing with more frequent and more sophisticated attacks occurring. In bald figures over 85% of large corporations and government agencies in the USA reported electronic security breaches in the 12 months up to the end of 2001(Internet Security Systems, 2001). It is also evident that IT security is a substantial and rapidly growing global business. According to the International Data Centre group (IDC), global information technology security services will reach US$21 billion by 2005, up from US$6.7 billion in 2000 (IDC, 2001). More significantly, while small to medium sized enterprises (SMEs) remain the smallest commercial sector of the IT security market, IDC estimates that they will shortly constitute the fastest growing group of customers for information security services. IDC also forecast that the need for Managed Services Providers (MSPs) will continue to grow at an annual rate of 28% (IDC, 2001). Managed Service Providers (or ASPs – Application Service Providers) being businesses offering applications, services and the supporting infrastructure usually on the basis of monthly service charges. Within the MSP space specialised security MSPs are commonly known as MSSPs, (Managed Security Service Providers). From all these figures the consistent picture presented is that there is continued significant growth in e-Business and that e-Security is becoming increasingly important to businesses and end-customers alike worldwide.

E-SECURITY AND OUTSOURCING

In this context, the major difficulties facing senior managers and IT security managers are the issues of what and how much e-Security they should have, should they outsource it and if so from whom? Clearly there are numerous permutations, combinations, add-ons and extra services that can be outsourced (Martensson, 2001). This compounds the difficulty for firms trying to determine what the best security choice is for their particular e-Commerce ventures. Indeed, anecdotal evidence suggests that very often decisions by medium sized organisations on e-Security are made on the basis of an executive or senior manager having simply read or heard about a particular product or service, rather than on the basis of a structured analysis of options. This exploratory paper identifies a range of key management issues regarding e-Security, attempts to explore outsourcing models and provides an initial generic four step approach to assist medium sized organisations in making strategic decisions about e-Security in the Australian context. Before moving forward it is important to define outsourcing. Following Lacity and Willcocks (1998), outsourcing involves placing in the hands of a third party the management of IT/IS assets, resources and/ or activities for a required result (Martensson, 2001).

While conventionally small and medium sized organisations (SMEs) are grouped together, the specific focus of this ‘research in progress’ is on medium sized organisations. This focus is purely practical and based partly on the fact that MSSPs solutions are still relatively expensive for most small business and partly because explicit management practices, policies and strategies are more common in medium sized organisations. As the figures below illustrate it is also evident that medium sized organisations are among the fastest growing sector of EC. Following the Australian Bureau of Statistics (ABS) definition medium sized organisation consist of between 20 and 199 people (ABS, 1997). Unfortunately because most ABS statistics group SMEs together it is difficult to quantify exactly the number of medium-sized organisations. However, as Table 1 illustrates there are some

comparative figures available examining the use of the Internet for marketing, selling and purchasing (i.e. e-Business). These figures illustrate that during the 96/97 and 97/98 periods medium sized organisations exhibited the fastest growth rates in EC (ABS, 1999)

	Marketing %	Selling %	Purchasing %
Small business			
1996/97	4	1	1
9997/98	8	3	6
Medium business			
1996/97	16	4	1
9997/98	30	12	15
Large business			
1996/97	36	2	3
9997/98	54	13	16

Table 1: Use of the Internet by Business size group

Strong network security has become increasingly recognised as an essential part of a firm's strategic approach to EC (Lichtenstein and Swatman, 2001). While multi-national corporations, government departments and financial institutions may have the resources for adequate in-house security (Pappalardo, 1999) it is only recently that outsourced e-Security solutions have brought good e-Security within the financial reach of Australian medium sized firms. Looking at the US experience many organisations of equivalent size have already begun to take the opportunity provided by these solution providers. It can only be anticipated that this trend will be replicated in Australia amongst medium sized organisations. While MSPs and MSSPs currently offer a variety of services from network monitoring to forensic analysis, vulnerability assessment and network architecture and design (Powers, 2000; Papparlado, 1999), it is evident that their use raises numerous issues for the organisation deploying their services. Aside from cost, there are numerous other issues including fro example, the selection of the provider (due to the potential for variability in the nature and quality of services provided), and the definition and use of service level agreements (SLAs). Previous research has identified and explored the reasons that organisations decide to outsource. Among these reasons financial, business, tactical and political factors have been noted as important (Lacity and Hirscheim, 1995). Subsequent research has illustrated that cost savings are often not realised and expectations versus actual benefits vary widely (Lacity and Hirscheim, 1993; Lacity and Willcocks, 1998). While cost remains a factor, the range of specialised security outsourcers and security offerings continues to expand and has further complexified the management issues facing firms trying to decide on a suitable solution. This variety of outsourced security services also has other important implications in Australia, where the B2B e-Commerce is the back-bone of most EC ventures. (Booz-Allen and Hamilton, 2001). In this context, e-Security emerges as an element that needs to be considered in the broader context of a firms broader strategic planning. The next section briefly reviews current IS thinking in this area.

STRATEGIC PLANNING FOR E-COMMERCE

There are numerous academic research papers on EC management strategies and the requirements for successful strategic EC. At the broadest level this paper argues that these strategic responses to the growth of e-Business can usefully be conceptualised from within theories on strategic planning. More specifically e-Security as a component of EC can be explored using these theories on strategic planning and they can be used to assist understanding of the methodology required to develop a generic model for making strategic decisions on outsourcing e-Security.

One recent approach is the SPECS (strategic planning for e-Commerce systems) model developed for SMEs (Hackney *et al.*, 2000; 2001). This affirms that managing EC strategies requires an integrated and multi-dimensional approach (Kumar and Crook, 1999). In examining SPECS a question arises as to whether it is significantly different from

conventional Strategic Information Systems Planning (SISP)? Hackney *et al*. (2000) argue that SPECS is far more complicated than SISP and requires an integrated, multi-dimensional approach across the e-Business. They suggest a comprehensive approach to SPECS involves e-Market Analysis, e-Chain Analysis and e-Alliance Analysis. While it is acknowledged that much research into small business has noted the lack of explicit strategic planning for EC (Bode and Burn, 2001), this is not the case with most medium sized organisations. Furthermore, even in the case of small business, considerable work has subsequently been done examining their approach to EC, highlighting that many adopt a strategic focus; see for example (Poon and Swatman, 1997; Cragg, 1998; Chau and Turner, 2001). Turning to examine SISP, Marshall and McKay (1999) suggest that it involves planning to achieve the optimal impact for IS/ IT and that this is an evolutionary process. Historically, this has progressed from the data processing (DP) era starting in the 1960s to the management information systems (MIS) era of the 1970s. Both these eras were internally focused. The 1980s and 1990s saw the advent of the strategic IS systems (SIS) era as organisations geared up to improve their competitive position and to form alliances and partnerships with business partners and customers (i.e. an external focus) SISP can be viewed as using IT as a key for enabling competitive advantage (Ward and Griffith, 1996; Kearns, 2000). There is now the understanding that SISP cannot be undertaken in one part of an organisation without other areas being affected (Moore, 1996 in Tapscott *et al*., 1998; McBride, 1998). This recognition of the need for a dynamic approach to SISP suggests that the implementation of SPECS should be no different.

Falconer and Hodgett (1997) in their Australian survey, found that many large organisations failed to identify their information requirements and that this also the case for Australian SMEs. These results corroborated previous research that had illustrated that information systems issues were one of the most difficult areas for managers to address (Pervan, 1994). Combined these insights suggest significant ramifications for understanding the relationship between SISP and SPECS. This is particularly the case as organisational boundaries blur and business process concepts change. It now seems appropriate to regard SISP as something being implemented across organisations; ie both internal and external to an organisation. This is usually undertaken for reasons of efficiency, (i.e. cost), effectiveness (i.e. expertise) and competitive advantage (i.e. marketing strategy).

Whether e-Commerce strategic planning is an e-Commerce term for SISP or a subset of SISP is a moot point. What can however be agreed upon is that e-Commerce security can be viewed as a subset of either of these strategies. This then implies that the security aspect of e-Commerce has to be planned just as carefully as any IT/IS strategic plan.

STRATEGIC MANAGEMENT ISSUES IN E-SECURITY

In seeking to implement e-Security, medium sized organisations face numerous challenges including cost, expertise, strategic management and practical implementation. Previous research has examined various aspects of these challenges, for example, Wood (1988) has stressed the importance of management endorsing security planning; Cole (1990) has examined the technical security problems and issues with distributed systems, and Lock *et al*. (1992) have identified security concerns in networked environments. More recently, a substantial literature on the e-Security issues has emerged, for example, Lichtenstein and Swatman, (2001), Bernstein, *et al*. (1996), Pethia *et al*. (2000). Generally these e-Security risks include denial of service, malicious code, flawed software, hacking, fraud, spoofing, information theft (interception) and non-authorised use of Internet services.

Unfortunately, while the e-Security risks are well known there is little empirical research into the efficacy of different management approaches (including outsourcing) amongst medium sized organisations to meeting these e-Security challenges. As has been mentioned above, for medium sized organisations this is both frustrating and confusing. From a cursory examination of the Australian business landscape there are numerous approaches evident. These appear to vary depending on the type and structure of the organisation and on what e-Security outsource business models managers have considered. At the conceptual level these different approaches can be mapped into the Lacity and Willcocks framework that identifies: total outsourcing; selective outsourcing; and, total insourcing (Lacity and Willcocks, 1998). However, there is little practical advice for Australian medium sized

organisations on what to outsource and how this is best achieved. MSSP vendors clearly have a vested interest in desiring an organisation to outsource as much of their e-Security requirements as possible. The question has to be asked: how does a senior executive or manager make a strategic decision on e-Security?

OUTSOURCING: MODELS FOR THE DELIVERY OF E-SECURITY

There are many issues and benefits of outsourcing IT (and as part of that e-Security). The issues of costs can include strategic issues, cost issues, managerial issues, operational issues technical issues and contractual issues (Lacity and Willcocks, 1998). Against this must be weighed the benefits – whether perceived or real. These may include: costs reduction, improved quality of service, access to IT skills and resources, better management control, efficient cash flow control, a refocus on other aspects of the core business (Lacity and Willcocks, 1998; Lacity and Hirschheim, 1995). Although various authors (e.g. Putrus, 1992) have offered opinions on the outsourcing of IS, theoretical work on outsourcing in general, and IS in particular, is sparse. Few managers have a basis for evaluating outsourcing as a management tool (Jacobs, 1994), especially for determining how the outsourcing decision is to be guided (i.e. overall business strategy or by financial considerations) (Malhotra, 1995).

What has to be explicitly stated is that outsourcing has to be managed. There have to be phases in any management decisions, (i.e. planning, analysis, design, implementation and operation) for determining the outsourcing decision of any of the organisations IT functions. This also applies to having a similar structured approach for e-Security. While cost or lack of in-house expertise may be the determining factor for considering outsourcing, how it is implemented is critical. E-Security has to be managed as effectively as any other aspect of the organisation's management infrastructure. As Lacity and Hirschheim state IS should be included in the corporate strategy and planning (Lacity and Hirschheim, 1995). Therefore if IS should be a part of corporate strategy, why not SPECS and within that e-Security?

It is clear that managed e-Security is now becoming a part of the basic IT strategy for IT managers and administrators. If one requires specialist IT solutions experts, and it is more cost effective to get that expertise outsourced, then it makes good business sense to do so. The same goes for e-Security. A MSSP checklist matrix can be developed outlining the features offered or those required by the organisation. The four generic steps outlined below can assist managers in approaching the difficult question of e-Security and what and how to outsource. This developmental 4-step model is still in the process of refinement but it is anticipated that it will make a useful and practical contribution to this complex area. Baskerville (1993) and Lacity and Hirschheim (1995) have developed outsourcing methodologies that have evaluated the various outsourcing options and this work uses and attempts to further develop their valued and excellent work. In the section below, it assumed that the security requirements and threats (e.g. risk analysis, threat identification) have been identified, and that an organisation's management understand that e-Security is of importance to the organisation. It should be noted that these generic guidelines are attuned to the resource levels characteristic of Australian medium sized organisations.

FOUR GENERIC STEPS FOR STRATEGIC DECISIONS ON IMPLEMENTING E-SECURITY

Step one: Have a sourcing strategy: Determine how security is to be implemented.

The first step in the strategic decision process is to determine how security for the medium sized enterprise is to be implemented and the model to be chosen.

There are various models for the implementation of security by medium sized organisations, and these are:

- In-house
  Setting up and implementing one's own security.
- Outsourced

Especially for specialised applications such as e-Commerce, website hosting, VPN services, Firewalls, etc. from commercial e-Security vendors.

- Hybrid approach – selective outsourcing

  Purchase components, products and services, from commercial e-Security vendors, but also have in-house specialist and consultants. Possibly have control over certain processes and components. Often this is the preferred model.

Step Two: Evaluate: consider the advantages and disadvantages of outsourcing security

There are distinct advantages and disadvantages of outsourcing security and some of these are listed below.

Advantages:

- Flexibility – services can be purchased separately or as a package.
- Expertise in the required field.
- 24-hour 7-days a week, 365-days a year support and monitoring - offering immediate response.
- Consistent industry standards and best practices.
- Latest software releases, updates, testing and fine-tuning.
- Decreased implementation time – usually a matter of weeks, whereas an in-house security could take many months to implement and fine-tune. This can be a significant advantage for SMEs.
- Disaster recovery management and off-site back-up can be part of the outsourced contract.
- Management of inter and intra organisational e-Communication links.
- Costs can reduced with less administration staff and training.
- Costs can be spread out over a period, rather than a full one-off payment.

Disadvantages:

- Real or perceived risk of loss of control.
- Downtime can impact significantly if an outside provider fails to provide the necessary support.
- Smaller centres may not be able to get required support.
- E-Security providers need careful selection – ensure that they are the big names, with a reputable reputation.
- Loss of in-house technical skills and expertise.

(Bounds, 2001; Lacity and Hirschheim, 1995)

Step Three: Assessment Awareness: Awareness of the assessments and considerations

The third step for the manager is to be aware of some of the many important assessments and considerations that they need to confront having decided on the security model for their organisation:

- How is strategic security decisions made for the organisation? Is it a senior management/board decision, an IT manager decision or a committee decision? It is very easy to make the incorrect decision regarding security, especially if senior executives are not familiar with the security requirements for the company.
- An evaluation of outside providers needs to be undertaken. A selected list of outside providers could be compiled and benchmark criteria established. A scoping document would be required to determine the range of security solutions desired by the organisation. As well, an examination of what services and products are offered by the various companies would be required. Careful

attention is needed to determine exactly what is being purchased and what is in the service contract.

- Policies and guidelines that govern security should to be in place before implementation.
- What are the costs involved – this includes implementation costs and ongoing service costs. A costing analysis would be required to determine whether to stay in-house or to outsource.
- Will security intrude in the everyday running of the business, i.e. will it be unobtrusive and seamless?
- Services (and prices) can vary a great deal from vendor to vendor, and this makes comparisons difficult.
- It is best to start small by outsourcing a few components of security, assess how it is working and then add more services at a later date, ie use an incremental process. However, a decision still has to be made as to what components are outsourced and what are kept in-house.
- How are standards maintained? What benchmark does one use? How often does this require reviews and revision?
- What is type of company for which the security is required? Banks and financial institutions, governments and specialised industries (e.g. defence industries) would probably need to retain control of all their e-Security. However, in the US, many banks such as Continental Bank have outsourced their entire information services (Huber, 1993), and the trend to outsource part or all IT activities seems to be accelerating rather than tapering off (O'Henry, 1996).
- What service/product is best for the company? There are site protection systems such as access control, asset protection and tracking, intrusion detection. Software applications such as password management, firewall controls, audit trails, virus detection, penetration tools and testing tools are now available and these are becoming more automated to take the load off the shoulders of the IT/Security manager.

(Bounds, 2001; Sandhya, 2001; Stross, 2001)

Step Four: Evaluation and Selection: Select a Managed Security Service Provider (MSSP)

Among the critical requirements necessary to evaluate and choose an MSP are:

- The company should have a solid history. A good reputation with a long history helps.
- A well-defined and detailed service level agreement (SLAs) that is clear, flexible and substantive. It is vital to leverage a binding contract as this is the mechanism that establishes the benchmarks and penalties.
- A decision has to be made between long-or short-term contracts. The marketplace is becoming more and more competitive and it could pay to go for a shorter-term contract. Contracts can very extremely complex and it often necessary and prudent to hire a legal specialist to negotiate the contract (Barthemely and Quelin, 2002).
- High availability security operation centres.
- Adequate staffing policies that is sufficient for a 24 x 7 x 365 basis.
- Comprehensive services. The company should offer a comprehensive suite of services that will meet evolving security needs.
- Global resources and infrastructure. Have worldwide coverage and resources.
- Sound business practices. Financially stable, good resources and a sustainable business.

- Near the conclusion of the first contract, a report card summarising the vendor's performance could be completed. This could be used as a guide to evaluate the vendor and for the renewal of their contract.

(Internet Security Systems, 2001; Ambrosia, 2001; Lacity and Willcocks, 1998)

Figure 1 indicates the various permutations for insourcing or outsourcing that organisations could have when making the e-Security decision. As can be seen this can vary from in-house, to outsourcing all or selected components, via single or multiple vendors.

The framework presented here does not pretend to be the complete answer to the difficult issue of what and how to outsource when implementing an e-Security. What it is attempting to do is provide a checklist for managers to assist them in making these decisions. The model is still in its infancy and will require further modification.

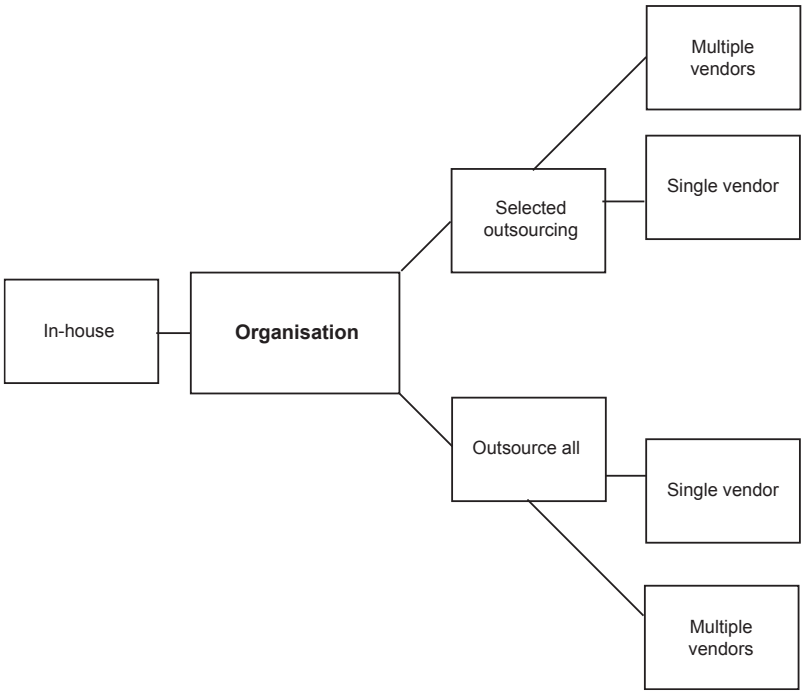

Figure 1: Indicating the various alternatives for e-Security implementation

CONCLUSION

This paper provides an initial attempt at developing a generic 4 step conceptual model for assisting managers in medium-sized organisations to make decisions about outsourcing e-Security. As data collection with these organisations continues it is anticipated that the model will be refined further to generate a checklist for their e-Security requirements. It is also anticipated that this research will be able to make a theoretical contribution to IS work in the area by advancing conceptual approaches to both strategic planning and IT outsourcing practices.

As EC continues to evolve it can be anticipated e-Security and outsourcing will grow in importance as strategic issues facing organisations. Enhanced management of the organisation's security will become increasingly critical as the volume and sophistication of attacks grows. Significantly, technology is not the issue – the challenge is to use the technology to enable e-Security solutions that are easy to understand and use and that remain transparent to the end-user. Whether outsourced or in-house, e-Security should be approached from a managerial aspect and this requires a good management policy that has to be in place prior to implementation. As this 'research in progress' paper has shown decisions around outsourcing and e-Security are highly complex that have to be addressed in a structured and comprehensive manner. In this regard, it is very important that the information systems discipline continues to develop conceptual and practical approaches that will assist organisations to handle these challenges.

REFERENCES

Ambrosia, Johanna, (2001) Outsourcing security a good plan, but be careful out there. EBusiness News, 14 September, 2000. URL: http://www.techtarget.com/. Accessed 22 March, 2002.

Australian Bureau of Statistics. 1999. Small and Medium Enterprises. Publication number 8141.0 Friday September 10, 1999. Canberra.

Australian Computer Emergency Response (2002) (AusCERT), Deloitte Touche Tohmatsu and The NSW Police.

Barthemely, J and Quelin, B. V. 2002. Competence, Specificity and Outsourcing: Impact on the complexity of the Contract. Academy of Management Conference. 23

Baskerville, R. 1993. Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computmg Surveys, Vol 25, No 4, December 1993. Proceedings, 375-414.

Bernstein, T., Bhimani, A. B., Schultz, E. and Siegel, C. A. (1996) Internet Security for Business, John Wiley & Sons.

Bode, Shirley and Burn, Janice, (2001) Who Wags the "E"tail? Strategic Planning for E-business in SMEs. Seventh Americas Conference on Information Systems. Boston, Massachusetts, USA. August 3-5, 2001. Proceedings, 964-970.

Booz-Allen and Hamilton, (2001) Is B2C doomed in Australia? Nua International Surveys. 8 February, 2001. URL: http://www.nua.com/surveys/. Accessed 22 February, 2002.

Bounds, Gene, (2001), Managing Outsourced E-business Initiatives. Ecomworld, 8 February, 2001. URL: http://www.ecomworld.com/global/includes/content/print.cfm?contentID=505. Accessed 15 March, 2002.

Broucek, V. and Turner, P. (2002) Bridging the Divide: Raising Awareness of Forensic Issues amongst Systems Administrators (2001) Proceedings of 3rd International SANE Conference, 27-31 May, 2002 Maastricht, the Netherlands.

Chau, S. and Turner, P. (2001) A Four Phase Model of EC Business Transformation amongst Small to Medium Sized Enterprises: Preliminary Findings from 34 Australian Case Studies, Proceedings of the Australasian Conference on Information Systems, Sourthern Cross University, NSW, December 5-7, 2001.

Cole, R. (1990) A Model for Security in distributed Systems. Computers & Security (9:4), 1990. 319-330.

Cragg, P. B. (1998) Clarifying Internet Strategy in Small Firms. Proceedings of the Australian Conference on Information Systems, Sydney, Australia. 29 September- 2 October, 1998.

Falconer, D. J. and Hodgett, R. A. 1997. Strategic Information Systems Planning, an Australian Experience. Proceedings of the Americas Conference on Information Systems, 15-17 August, 1997. Indianapolis, USA. 837-839.

Hackney, Ray, Burn, Janice and Dhillon, Gurpreet, (2000) SPECS: a new approach to strategic planning for e-commerce systems. Association for Information Systems (AIS) Americas Conference on Information Systems. Long Beach, California, USA. Aug 10-13, 2000. Proceedings, 843-847.

Hackney, Raymond A. and Burn, Janice, M. (2001) SPECS: Strategic Planning for E-Commerce Systems – Towards an E-Customer Focus. Seventh Americas Conference on Information Systems. Boston, Massachusetts, USA. August 3-5, 2001. Proceedings, 845-850.

Huber, R.L. (1993, January/February). How Continental Bank Outsourced Its "Crown Jewels". Harvard Business Review, 121-129.

IDC Research, (2001) Information security market growing. Nua Internet Surveys, 24 September, 2001. URL: http://www.nua.com/surveys/. Accessed March 17, 2002.

Internet Security Systems, (2001) How to select a Managed Security Provider: A Comprehensive Guide and Checklist for Networked Enterprises. 9

Jacobs, R.A. (1994), The Invisible Workforce: How to Align Contract and Temporary Workers with Core Organization Goals. National Productivity Review, (Spring), 169-183.

Kearns, G. S. 2000. Top Management Support of SISP: Creating Competitive Advantage With Information Technology. America Conference on Information Systems. Long Beach, California, USA. August 10-13. Proceedings, 1153-1157.

Kumar, R. L. and Crook, C. W. A. (1999) Multi-disciplinary Framework for the Management of Interorganisational Systems. The Data Base for Advances in Information Systems, Winter, Vol. 30 (1).

Lacity, M. C. and Hirschheim R. 1995. Beyond The Information Systems Outsourcing Bandwagon. John Wiley and Sons, England. 237

Lacity, M. C. and Hirschheim, R. 1993. The Information Systems Outsourcing Bandwagon. Sloan Management Review, Fall, 35, 1. 73-86.

Lacity, M. C., Willcocks, L. P. (1998) An empirical Investigation of Information Technology Sourcing Practices: Lessons from experience, MIS Quarterly, September 363-408.

Lichtenstein, S. and Swatman, P. M. C. 2001. Effective Management and Policy in E-Business Security. June 25-26, Bled, Slovenia. Proceedings of the 14th BLED conference on Electronic Commerce, 750-764.

Lock, K. D., Carr, Houston H. and Warkentin, M. E. (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, June 1992. 173-186.

Malhotra, Yogesh. (1995) An Empirical Analysis of the Determinants of Information Systems Productivity and the Role of Outsourcing Policy. BRINT Research Institute. URL: http://brint.com/. Accessed 14 May, 2002.

Marshall, Peter and McKay, Judy. (1999) Strategic Information Systems Planning in the Virtual Organisation. Association for Information Systems (AIS) Americas Conference on Information Systems. Milwaukee, WI, USA, Aug 13-15, 1999. Proceedings, 124-126.

Martensson, A. (2001) On Selective IT Sourcing: Choices in Application Development, Seventh Americas Conference on Information Systems, Boston, Massachusetts, USA. August 3-5, 2001 Proceedings, 1861-1866.

McBride, Neil. 1998. Towards a Dynamic Theory of Strategic Information Systems Planning. De Montford University, Leicester, UK. Proceedings of the 3rd UKAIS Conference, Lincoln University, April, 1998. Proceedings, 218-230.

O'Henry, S. 1996. Outsourcing is Hotter than Ever, ABA Banking Journal (88:5, May), 1996, 44-54.

Pappalardo, Denise, (1999) Securing E-commerce Web Sites. NetWorldFusion, 12 July, 1999. URL: http://www.nwfusion.com/newsletters/isp/0712isp1.html. Accessed 22 March 2002.

Pervan, G. P. 1994. Information Systems Management: An Australian View of the Key Issues. Australian Journal of Information Systems, 1, 2, 1994, 32-39.

Pethia, R., Paller, A. and Spafford, G. (2000) Consensus Roadmap for Defeating Distributed Denial of Service Attacks, Global Institute Analysis Center, SANS Institute, U.S.A., http://www.sans.org/ddos_roadmap.htm. Accessed September 13, 2002.

Poon, S and Swatman, P. (1997) Small business use of the Internet: Findings from Australian case studies, Proceedings of PAWEC Conference.

Power, P. (2002) CSI/FBI 2001 Computer Crime and Security Survey. 2002. Computer Security Issues and Trends. Computer Security Institute and Federal Bureau of Investigation. 24

Powers, Kathleen, (2000) Managed Service Providers: A new for IT security. Serverworld, May, 2000. URL: http://www.serverworldmagazine.com/compaqent/2000/05/msp.shtml. Accessed 16 February, 2002.

Putrus, R.S. (1992), Outsourcing Analysis and Justification Using AHP, Information Strategy: The Executive's Journal, (Fall), (9:1) 31-36.

Sandhya, S. M. (2001) Network sentinels: outsourcing the security. EBiz Channel. 13 July, 2001. URL: http://www.ciol.com/content/services/ebiz/. Accessed 17 March, 2002.

Stross, Kenner, (2001) Managed PKI for B2B Computing. MessageQ, 26 March, 2001. URL: http://www.messageq.com/security/stross_1.html

Tapscott, D., Lowy, A. & Ticoll, D. (Eds.). (1998) Blueprint to the Digital Economy: Wealth Creation in the Era of E-Business. McGraw-Hill. NY USA. 384

Ward J. and Griffiths P. (1996) Strategic Planning for Information Systems. John Wiley and Sons, 2nd edition, Chichester, USA, 606

Wood, C. C. (1988) A context for information Systems Security Planning. Computers and Security (7:5) 1988. 455-465.

COPYRIGHT