

# An Investigation of E-Procurements Risks

Ben Galloway - Researcher  
Rodger Jamieson - Director<sup>1</sup>

SEAR: Security, E-Business, Assurance Research Group  
School of Information Systems Technology and Management  
University of New South Wales  
e-mail: r.jamieson@unsw.edu.au

## Abstract

*"...e-Commerce is like marriage; both have to get some benefit out of it to work..." Consultant*

*The aim of this paper is to present an interpretation of the risk issues currently concerning e-Procurement. In seeking to explore a developing area of theory, the current perception of practitioners has been investigated and reconciled with existing related literature. This was approached through in-depth interviews with a variety of stakeholders in organisations that have embarked upon e-Procurement. After developing a literature-based taxonomy, current perceptions and practices were reviewed and refined, providing a foundation for the further development of a system for classification of key risks in e-Procurement, and a guide towards identification of risks and best practice.*

## Keywords

E-procurement, risks, security and controls, risk management, EDI

## AN INTRODUCTION TO UNDERSTANDING RISKS IN THE CONTEXT OF B2B E-PROCUREMENT

*'The global nature of e-commerce, the varying legal systems involved and the speed with which the innovations and technology are brought to the market, further complicates the challenges facing the organisation today.'* (Howard 2001)

Risk is an important component of e-commerce, with wide-ranging repercussions to information, linked systems and even an organisation's reputation. Interestingly it is usually Information Technology departments who are held responsible for the identification and monitoring of IT risks (Howard 2001). However, what is troubling is that an estimated 75% of organisations do not have formal processes to handle their e-Commerce risks (Howard 2001).

Since the Internet began to grow in popularity a range of papers and articles have been published outlining the potential risks inherent in this new medium of exchange (McNamee et al, 2001; Howard 2001; Freeman 2000; Lichtenstein 1998, Baird et al. 1999, 2002, Lek et al, 2001). While a diversity of papers and articles covering the topic of e-Commerce risks exist, there is very little reputable research that has investigated the area in any depth.

A summary of commonly stated e-commerce risks that may be applicable to this study are as follows:

Risk		(Source)
<b>Security Risks</b>		
Security Risk:	Compromise through potential weaknesses in the system.	(McNamee et al, 2001)
Availability:	The need for services to be 'on' all the time	(Freeman, 2000)
Authentication:	Masquerading identity or repudiation of message	(Rebstock et al, 2002)
Liability:	Through employment or legal contractual	(Howard, 2001)

<sup>1</sup> SAFE: Security, Assurance, Fraud-prevention for E-business Research Program at the Securities Industries Research Centre of Asia-Pacific

	obligations	
Computer fraud:	Internal abuse and misuse	(Howard, 2001).
Breach by external party:	External attack by various parties, whether corporate espionage or terrorists	(Howard, 2001; Mehta, 2001)
Virus affecting the system:	Email viruses such as NIMDA or Melissa which have capability of crippling systems.	(Mehta, 2001)
Denial of Service:	Flooding a computer's internet connection with requests to disrupt traffic flow	(Mehta, 2001; Wright, 2001; Lichtenstein, 1998)
Intellectual property:	Misappropriation or release of intellectual property	(Howard, 2001)
<b>Software Risks</b>		
Switching Cost	Control of spending to specific suppliers as part of e-Commerce	(PWC, 2002)
<b>Project Risks</b>		
Competitive information:	Risk to customer and supplier data, as well as other commercially sensitive information	(Freeman, 2000)
Lack of required skills	Staff not being properly equipped with the correct skill set.	(Shah, 2000)
Wrong technology choice	Investing in the wrong technology, this may lead to greater costs than initially projected, or being stuck with a vendor.	(Stevens, 2002)
Complexity:	Increasing complexity of organisations, systems and models	(Wright, 2001)
Reputation risk:	The risk of damaging goodwill or brand equity as a result of e-commerce mishap	(McNamee et al, 2001)
Customer expectation risk:	The threat of failing to meet partner expectations	(McNamee et al, 2001).
<b>Environmental Risks</b>		
Natural hazard		(Mehta, 2001)
Changing technology:	Rate of change of technology progressing ahead of the ability to secure it	(Wright, 2001)
Maverick Spend/Compliance	Procurement risk, describing employee's expenditure via non-preferred suppliers, resulting in a blow-out in costs.	(Lee, 2001)

*Table 1: e-Commerce risks from literature*

Mainstream information system risk literature identifies a wide-range of risks. As e-procurement is another form of information system, and the literature outlines general risks, many of these are also expected to be relevant in the e-Commerce and particularly e-Procurement context – refer Table 1.

E-procurement risk is therefore a set of risks that apply specifically in the context of e-procurement systems. These risks may have their genesis in e-commerce, information systems and process, however the set of risks also exhibits characteristics and emphasis different to previous forms of system implementation, such as compliance and relationship-based risks.

From review of the literature it may be concluded that management of risk should be an important facet of e-Commerce, however, little is understood about the actual environment of e-Procurement or its unique aspects. While current papers indicate that industry in general approaches risk from a risk management perspective, actual choice of frameworks used by industry to identify and address risks have not been confirmed in practice. It is expected that the Australian Standard for risk management (AS/NZS4360:1999) will be used as the standard framework, however there is little indication that this is the case.

A variety of issues are therefore not sufficiently addressed by current literature. Of these the most important to this study are:

- Understanding of the key risks involved in business-to-business e-procurement, and how these may differ from other forms of information systems.
- Understanding of the different perceptions of stakeholders towards risk.
- The way awareness and approach to risk (through established standards and methodologies) have been affected by e-Commerce.

This paper will endeavour to address these issues to better understand risk in the context of e-Procurement.

## DEVELOPMENT OF A RISK TAXONOMY FOR E-PROCUREMENT

### A Theoretical Framework for e-Procurement Risk

A hypothetical taxonomy of e-Procurement risks was constructed. The three dimensions of software risk, as adapted from Sherer (1995), were adapted to provide a basic structure for this model. The technical dimension was used to describe risks that are of a technology orientated description, concerned with development or the actual transaction mechanism between partners. Business ('Organisational' in Sherer's work) was used to describe risks that occur from internal pressures and concerns, including strategic and processual elements. External (previously environmental) refers to risks that occur from forces outside of the immediate business organisation. This includes risks from the Internet and business partners.

Risks were adapted from discussion and lists developed in the risk portions of the literature review. Additional literature influences from Smith & Staples (2001), Sherer (1995), Baird, Jamieson & Cerpa (2002), Schmidt (2001) and Stevens (2002) have assisted in influencing the development of this taxonomy.

### e-Procurement and Risk

As the area of business-to-business e-commerce (and particularly e-Procurement) is a relatively recent development, with limited existing literature (particularly in the selected niche of risk and security in e-Procurement) this research seeks to derive theory. It may be argued that relevant theory may be drawn from similar technologies – including the dearth of research being produced with regard to business-to-consumer e-Commerce (Cobb 1998, Rose et al 1999), the existing procurement structure of EDI (Joseph & Engle 1996, Ratnasingham 1997), and standard security and risk frameworks (AS/NZS4360:1999, AS/NZS 7799:2003). Direct application of existing theory does not hold, however. Particularly given the new environment of the Internet, the different relations and interactions being exhibited in this new medium, the broader access and scale of technologies involved, the manner in which e-Procurement extends existing business process, the size and volume of transactions and relatively wide-spread uptake of the technology.

It is therefore felt that too many assumptions are being made to directly apply existing structures. While it is possible some, if not all, existing theory may be applied, it is more likely that e-procurement, as a developing form of system implementation, will carry new concerns, new risks, and therefore new structures.

As a result of reviewing the literature, a number of research issues have arisen which can be summarised as follows:

*1. A lack of understanding of the key risks involved in business-to-business e-procurement, and how these differ from other forms of information systems.*

From review of the literature a noticeable gap was identified in the understanding of how risk functions in the context of e-Procurement. It was determined that e-Procurement as a unique form of information system, would be affected by different risks to traditional systems. The effect of linkages to external customers, relationships with partners, existing process and the changeable technological landscape of the Internet all influence the manner in which risk may be perceived and approached.

*2. A lack of understanding of the different perceptions of stakeholders in the business-to-business cycle – towards risk and security.*

While different roles in the e-Procurement cycle have been identified (buyers, suppliers, intermediaries), little research has investigated how these different roles, motivations and responsibilities affect traditional approaches to risk and security.

*3. The way awareness and approach to risk (through established standards and methodologies) have been affected by e-Commerce.*

Standard methodologies such as the Software Development Lifecycle (SLDC) and information risk assessments are designed for normal system environments. Existing literature does not address how these methodologies

have been affected by the different requirements of electronic commerce. Risk and security standards have in recent years been released by international standards groups. The level of awareness and adoption of these methodologies by industry continues to remain undefined, yet with the growth of e-commerce the importance of the enterprise view of security is continuing to grow in importance.

There is little to inform how classifications and methodologies defined in theory compare with practical requirements and usage. What methodologies are being used? Which risks are considered to be business critical? In this paper these research issues will be considered, using an exploratory descriptive approach.

## RESEARCH DESIGN

This section discusses the research methods employed in conducting this study and sets out the research questions posed as part of this research.

### Research Questions

The following questions were formulated to address the issues outlined above:

1. What are the perceived risks of business-to-business e-Procurement?  
This question addresses issues concerning perception and identification of risks. It also aids in refining and reviewing the hypothetical taxonomy, potentially identifying areas not covered by literature (or by exclusion not considered as important, or implicitly handled).
2. What is the perception of risk and security between stakeholder groups in the business-to-business cycle?  
The second question seeks to more closely understand the difference and similarities between stakeholder group's perceptions of e-Procurement (relating directly to the second, and in part the third, issues defined). These perceptions will in turn inform the approach toward risk and security.
3. What other issues are arising in e-Procurement?  
The question aims to capture other issues related to e-procurement risks.

### Research methodology

In conducting this research a retroductive strategy was chosen, using a constructionist epistemology and informed from an interpretivist theoretical perspective. The research is exploratory in nature, and is based on the view that meaning emerges from social engagements with the realities of the world (Crotty 1998). In conforming to the aims and structure of the retroductive strategy, a model (taxonomy) is developed and its existence established, using participants accounts to access rules and meanings (Blaikie 2000).

The collection of data in this study uses qualitative methods to assist in developing the postulated model. Literature is used in two ways – to answer the research questions posed, and as a means to assist in defining a 'hypothetical explanatory model' (in stating that the model is hypothetical, this does not mean that a hypothesis is proposed, but that the model has not been proven). The model will assist in refining the perceptions of practitioners towards defining a classification structure for risks within e-Procurement. The constructionist view of this strategy explains the explanatory mechanisms to consist of "the rules, plans, conventions, images, and so on that people use to guide their behaviour" (Harre' and Secord 1972, as cited by Blaikie 2000, page 111). That is, their perceptions.

Methods of data collection were chosen that would provide in-depth qualitative data. Semi-structured interviews and questionnaires are both common methods used in exploratory research, and were selected on their ability to elucidate participants' perceptions and interpretations.

The method of grounded theory was used in analysing data. Grounded theory is a qualitative research method used to develop theory from data that has been systematically gathered and analysed (Myers 2001). As retroduction commonly uses "creative imagination and analogy to work back from data to explanation" (Blaikie 2000 page), this approach seems apt, particularly as the methodology is "evolving towards a constructionist paradigm" (Myers 2001). Backhouse et al. (2001) have stated that in the area of security and risk there has been a distinct deficiency of interpretivist research (Backhouse et al, 2001), as most research in this area has reflected an overly technical focus, which fails to address security as a holistic, enterprise-wide concern. This research seeks to address this perceived deficit, examining concerns of stakeholders using an interpretivist approach.

Interview transcripts were loaded as text documents into a qualitative data analysis suite – NUD\*IST Vivo (NVivo). This approach is somewhat similar to Pandit (1996), who utilised grounded theory in conjunction with 'computerised databases' and a 'qualitative data analysis software package to aid in the process of grounded theory'.

## Research Participants

Research participants for this study have all had experience in the implementation or operation of procurement systems in Australia. Industry backgrounds range from Information Technology to Finance to Manufacturing to Retail organisations. Business roles were predominantly management or business owners of systems, but also included analyst level members and security managers.

A concern with this research was that the complete e-Procurement cycle of buyer, supplier, consultant and intermediary be covered. These stakeholders play different parts in the e-Procurement process, and as such hold different priorities and responsibilities. While the majority of participants were in management roles related to e-Commerce and e-Procurement, previous experience of participants included information technology/technical backgrounds, security, project management and finance/business.

Representatives from each of the five stakeholder groups were represented in the study. This included an academic expert in e-Procurement who was used in the initial (investigatory) stages of the research. Participant organisations ranged quite dramatically in system maturity, with one organisation still using an intranet-based system. While the study is primarily concerned with e-Procurement systems (i.e., over the Internet), this organisation was included to contrast against more developed systems.

## RESEARCH FINDINGS

### Major Risks Arising...

Unfortunately, a justifiable method for ranking risks or selecting a 'Top 3' was not entirely practical due to the manner of data gathering selected. Nonetheless, the risks that received the most emphasis from participants were:

1. Change Management
2. Partner Relationship Risk (and trust issues)
3. Switching cost

Change related risks, and risks affecting buyer/supplier relationships were of particular concern to participants. Most participants suggested change management and process risks explicitly. These risks were perceived to be important to use and acceptance of technology within the organisation. Switching cost and availability/reliability of connection were two other risks that received regular attention. Specific controls for switching cost and availability/reliability of connection were not readily suggested beyond rigorous selection processes.

The main risks identified by participants were:

- Availability - Availability refers to services/connectivity being available at all times. Most participants raised this as loss of transaction flow could also affect other systems, such as inventory, in the event of a failure. This was particularly important for high volume, low item cost orders and perishables.

*"There is a risk with any trading relationship, traditional or electronic, that any interruption to service or product supply across supply chains will have an adverse affect on the involved parties to conduct business."* (Supplier 1a)

Not all participants agreed however. With non-business critical items delay was considered an inconvenience rather than a key risk.

- Strategic risk - Strategic alignment of e-Procurement initiatives was indicated to be an important risk. Without proper management backing a system could suffer and even fail. Without communication within the company projects may be overlooked or replicated.

*"...think about how many of these projects start from an IT department, talking to an IT department and ends up affecting the way the businesses interacts. You know it is critical. That this is not something that is done in isolation. It's got to be a business process. It's got to be driven by the business."* (Supplier 2)

- Compliance - Compliance risk is concerned with ensuring that the system is used to channel spend in specific areas. This was often cited as one of the key reasons for e-Procurement implementation.
- Switching Cost - Switching cost can take two avenues, through indirect costs to business and as a direct expenditure on a new system. An indirect cost to the business may be activities such as retraining and usability:

*"Switching costs for them (Buyer Firm), to go to another stationery provider is very hard, because the staff would have to learn new passwords, new menus, new lists would have to be built, and (Supplier Firm) is very clever, because they have locked in that customer, using technology as a mechanism. So price now becomes a secondary consideration (to) probably convenience." (Intermediary)*

Switching cost as a direct expenditure can be expenses incurred on a new system, hardware and personnel.

- Change Management and Personnel –

*"More noticeable is the level of cultural and organisational change required to support electronic trading. If those responsible for managing the operational processes of transaction handling, especially in order processing, do not have an understanding of why electronic trading is required, why it is a business imperative... And how their roles will change as a result, the risk is that any attempt to implement electronic trading will fail due to a lack of organisational support." (Buyer 1)*

*"...a big culture shift for everyone. What we're asking people to add another thing onto their job description. And we are asking a lot of non-technical people to add it to their job description. Umm, you know, there are people on the factory floor who use the system. The sales people who use the system, as well as IT people who use the system. So a very broad range, so that culture shift was fairly difficult." (Buyer 3)*

*"You come across customers who have worked by phone and fax for the last 25 years. Now you're going - 'Hey, there's the Internet. It's so much better, and you should do this.' And their impression is 'When I send a fax it takes 10 seconds from the fax machine to the other fax'. But they forget that they might have spent half an hour reading through the catalogue, getting a price list, all these other things. They just think 'Oh the fax is really fast'. And trying to convince them that entering an Internet password and logging in is actually faster and more efficient. So it's really change management processes that will put more trust in electronic ordering, for older people who might not be so PC literature." (Supplier 3)*

- Process Risk - *"To be able to procure... two key things - our processes change, changes to the way relationships are handled. Because you are fundamentally shaking up the way they have done business before, and changing the way they are doing transactions..." (Buyer 2)*
- Partner Relationship Risk - Risk to business partner relationships and business partner trust was another concern. Changes resulting from automation and loss of contact/communication with partner organisations were cited as having the potential to affect responsiveness.
- User abuse - User abuse was suggested as a potential risk, but was easily mitigated through purchasing controls and authorisation limits. While a popular risk, it was not considered overly important.

## TOWARD A TAXONOMY

Categories were established to assist in separation and identification, using grounded theory to draw out the main themes. Categories were added during sorting, based on the source of the risk. Alternatively, classification could have been based upon the effect such a risk would have on an organisation. This was not seen to be practical however, as risks often have a variety of different (and sometimes unquantifiable) effects.

From analysis, risks have been categorised into Development, Transaction, Management, Financial, Legal, Process, Internet, External, Partner Relations. These groups are similar to the categorization of risk presented by Smith & Staples (2001), and somewhat similar to some of the risk groupings used within the Delphi risk study (Schmidt et al, 2001).

Categorisations are based upon how risks originate (to the best of understanding). These categories are intended to act more as a guide to understanding and to provide structure, rather than deliver a prescriptive approach. System environments are not static, but consist of many forces and actors. As a result risks are not always as clear-cut, or as easy to categorise, as may be suggested by these frameworks.

From the risks identified in this study, through literature and review of practitioners, some interesting observations may be made. A surprising number of risks were not identified by the initial literature review, and a number of risks were not identified by participants. This would seem to indicate that more research is required in the area to better understand this gap. Risks that were identified as being particular to e-Procurement were

predominantly related to switching costs and partner concerns, although significant emphasis was placed by participants upon process and change management.

The majority of risks that were identified were relatively balanced between categories, with no predominance of technological or processual risks. Certainly risks that were considered to be more serious were those affecting the organization as a whole.

From the risks identified, the majority can be applied to information systems in general, however e-Procurement does have its own subset of particular concerns. This would seem to suggest that while the core elements of e-Procurement risk can be perceived as being the same to other information systems, these other externally and internally directed risks require a different approach.

The revised taxonomy in Figure 2 categorises risks that were identified through literature review and verified by participants in questionnaires and interviews. Risks have been categorized to three levels, starting at a broad conceptual level of risk (Development, Business, External) and further categorizing to risk groupings, and specific risks.

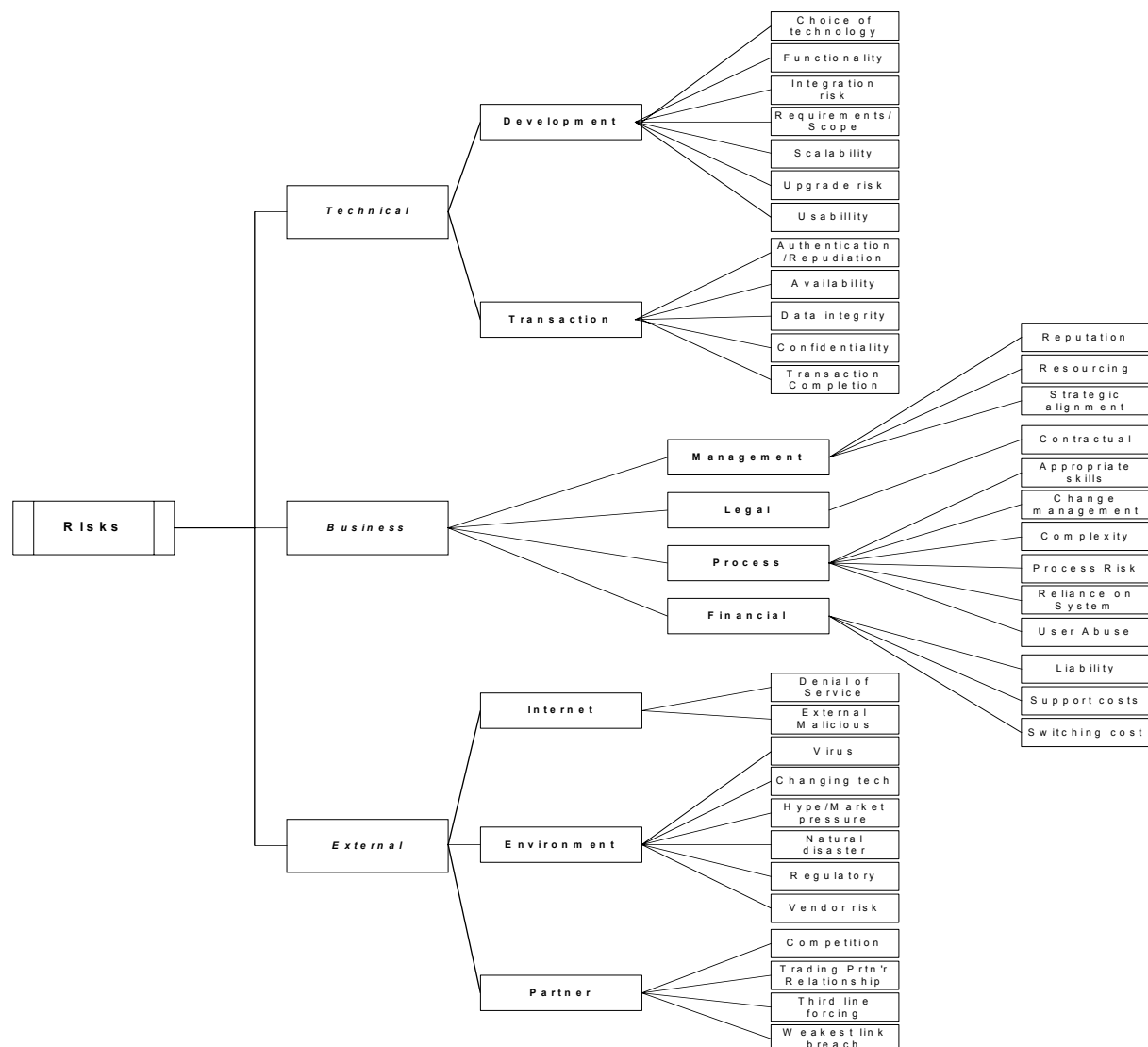


Figure 2: Taxonomy of e-Procurement Risks

## CONCLUSION

A taxonomy of risks in e-Procurement was constructed from literature in the area, and refined from data gathered from practitioners. This taxonomy was created to support the central research questions identified from the literature issues. These questions seek to develop an understanding of the perceptions and approach to risk and security in industry, as well as assist in understand the unique position of the Australian environment.

The taxonomy balances technical/transaction concerns with organisation/process risks. Participants provided a wide-variety of interpretations of risk, not confined it solely to security concerns.

The major risks perceived by participants were found to be:

- change management;
- partner relationship risk (and trust issues);
- switching cost;
- availability; and
- strategic risk.

In comparison to change related risks, and risks affecting buyers and suppliers, technical/technology risks were considered to be secondary risks. Organisational change was felt to affect acceptance and the realisation of potential benefits of e-Procurement, and was ranked very highly. Issues affecting partner relationships were also considered very high in importance, with the concept of trust and collaboration arising throughout.

**Contribution to Theory** - This exploratory study furthers our understanding of e-Procurement, and the issue of risk within e-Procurement. A taxonomy of risks is presented, developed from literature and validated by perceptions of practitioners in the field, providing a means of classification for risks. Additionally, verification of these risks indicates that EDI, e-commerce and e-Procurement share similar foundations. This study also extends the tradition of interpretivist work within risk and security domain, which has to date been traditionally a positivist technically-orientated area.

The taxonomy derived from this study may now be used in future research to verify these findings and investigate the area in greater depth. Practical application can be made by use of the taxonomy as a guide to identification and practice, broadening practitioners understanding of risk.

Finally, through drawing together literature and current practice, this study has built upon the existing body of knowledge. A new understanding of risks has been proposed, and a greater understanding of the real concerns of practitioners provided.

**For Practice** - This research also carries significance for identifying and approaching risk and security in e-Procurement practice. The study has identified major risks and concerns (as perceived by practitioners), as well as potential shortfalls and oversights. It provides a balanced view from a variety of e-Procurement stakeholders, enhancing understanding of risk and security in a new domain, and building a snapshot of current maturity and perception.

Being an exploratory study, more research will be required to validate and explore the area of risk in greater depth. The taxonomy and factors provided in this study are only representative of a very small sample, and are not intended to be readily generalise-able.

**Future research Directions** - Potential directions for research may lie in:

- prioritisation and quantification of risks, investigating risk likelihoods and impacts for practical application;
- further prioritisation and quantification of risks into likelihoods and impacts for practical application;
- expansion of investigation to be by industry, looking at particular stakeholder groups, or examining risks and success within e-Procurements; and,
- different approaches based upon e-Procurement system types, contrasting off-the-shelf commercial products against in-house development, or ASP-based web-browser models against java applications.

## Summary

While this study has provided an initial investigation into the area, there remains many questions to be answered, and a breadth of research issues which need resolution. This exploratory study is only the beginning to furthering our understanding of perceptions towards risk and security within B2B e-commerce in Australia. Initial perceptions have been presented, with a major focus on internal process concerns however, e-Procurement continues to mature, and as different approaches develop so too will perceptions.



It may also be pertinent to bear in mind that information technology has now become an intrinsic part of business. This idea has been illustrated throughout this study in participants expressing that their concerns are less about technology, and more about how technology affects the manner in which business is conducted.

By focusing research into understanding risks and perceptions, we will be able to shape awareness and improve effectiveness in providing a more secure business environment. Management needs to be aware of the threats posed in participating in these new environments and their responsibilities in participating. Today Business-to-Business e-commerce cannot be seen to be just another set of systems, e-commerce systems now encompass organisations, extending them beyond previous boundaries.

## REFERENCES

- Baird, A., & Jamieson, R (1999). Risk and Security Issues for Electronic Commerce Practice, Americas Conference on Information Systems 1999
- Baird, A., Jamieson, R., & Cerpa, N. (2002). Development of a Framework for Risks and Security in B2C E-Business, IFIP Conference on E-Commerce (I3E 2002). Lisbon, Portugal
- Backhouse, J., & Dhillon, G. (2001). Current direction in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11, 127-153
- Blaikie, N. (2000). *Designing Social Research*. Oxford: Polity Press, Blackwell Publishers Ltd, Oxford UK.
- Cobb, S. (1998). Security Issues in Internet Commerce. Version 2.0. NCSA White Paper on Internet Commerce (<http://www.secor-mea.com/Downloads/security%20issues%20in%20internet%20commerce.pdf>)
- Crotty, M. (1998). *The Foundations of Social Research*. Sydney: Allen & Unwin, St Leonards, Australia.
- Freemen, E. (2000). Risks: Operational Issues and Solutions in a Cyberage. *Risk Management*
- Howard, L. (2001). RMs Struggle with Technology Risks. *National Underwriter, Property & Casualty/Risk & Benefits Management*
- Joseph, G., & Engle, TJ . (1996). Controlling an EDI environment. *Journal of Systems Management*, 55, 42-49
- Lee, R (2001) Visibility and Invisibility in Networks of Procurement: An Examination of the Evolution in Control System Design In Response to Information Technology-based Organisational Change (unpublished thesis) UNSW, School of Accounting
- Lek, M., Anandarajah, B., Cerpa, N., & Jamieson, R. (2001). Data Mining Prototype for Detecting e-Commerce Fraud, ECIS 2001. Bled Slovenia
- Lichtenstein, S. (1998). Internet Risks for Companies. *Computers & Security*, 17(2), 143-150
- McNamee, D., & Chan, S. (2001). Understanding E-Commerce Risk. *Internal Auditor*
- Mehta, M., & George, B. (2001). Security in Today's E-World, Eighth Americas Conference on Information Systems. Dallas, USA
- Myers, M (2001). Qualitative Research in Information Systems. (ISWorld, <http://www.isworld.org/>). (<http://www.qual.auckland.ac.nz/>)
- Pandit, N. (1996). The Creation of Theory: A Recent Application of the Grounded Theory Method. *The Qualitative Report*, 2(4). (<http://www.nova.edu/ssss/QR/QR2-4/pandit.html>)
- PriceWaterhouseCoopers (2002). Information Security Breaches Survey 2002: UK Department of Trade and Industry. (<http://www.security-survey.gov.uk/>)
- Rao, V., Cerpa, N., & Jamieson, R. (2001). A Comparison on Online Electronic Commerce Assurance Service Providers in Australia, 14th Bled Electronic Commerce Conference: e-Everything: e-Commerce, e-Government, e-Household, e-Democracy. Bled, Slovenia
- Ratnasingham, P. (1997). EDI Security - Re-evaluation of Controls and its Implications on the Organizations. *Computers & Security*, 16(8), 650-656
- Rebstock, M., & Tafreschi, O. (2002). Secure Interactive Electronic Negotiations in Business-to-Business Marketplaces, ECIS 2002. Gdansk, Poland
- Rose G, Khoo H, Straub DW (1999) Current Technological Impediments to Business- to-Consumer Electronic Commerce, CAIS, Vol 1, Article 16, June 1999

- Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems*, 17(4), 5-36
- Shah, N., & Dawson, R. (2000). Management Issues Regarding E-Commerce and the Internet. ICMIT
- Sherer, S. (1995). The Three Dimensions of Software Risk: Technical, Organisational, and Environmental, 28th Hawaii International Conference on Systems Sciences (HICS'95). Hawaii, USA: IEEE Computer Society 1995
- Smith, H., McKeen, J., & Staples, D. (2001). Risk Management in Information Systems: Problems and Potential. *Communications of AIS*, 7(3)
- Standards Australia (1999). AS/NZS 4360:1999 : Risk management: Standards Australia. (<http://www.standards.com.au>)
- Standards Australia (2000). AS/NZS7799:2:2000 Information security management Part 2: Specification for information security management systems
- Standards, Australia (2003). AS/NZS ISO/IEC 7799:2003: Information technology - Code of practice for information security management: Standards Australia. (<http://www.standards.com.au>)
- Stevens, K. (2002). Preliminary Report on eBusiness Project Risk Think-Tank. Unpublished
- Wright, A. (2001). Controlling Risks of E-Commerce Content. *Computers & Security*, 20, 147-154

## **ACKNOWLEDGEMENTS**

The authors wish to acknowledge the assistance and cooperation of participants in this research project in helping identify key research issues in the e-procurement area.

## **COPYRIGHT**

Ben Galloway and Rodger Jamieson © 2003. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.