December 2003

The Board View of Electronic Business Risk

Ernest Jordan
Macquarie Graduate School of Management, Macqurie University

David Musson
Macquarie Graduate School of Management, Macqurie University

16th Bled eCommerce Conference

eTransformation

Bled, Slovenia, June 9 – 11, 2003

The Board View of Electronic Business Risk

Ernest Jordan, David Musson

Macquarie Graduate School of Management, Macquarie University, Australia
Ernest.Jordan@bigpond.com, DavidMusson@optusnet.com.au

Abstract

The selection and implementation of electronic business initiatives pose challenges to technologists and business unit managers, however this study focuses on the issues that impact corporate board members. They have special responsibilities to monitor the risks faced by the organisation. We outline some of the risks posed by electronic business and discuss the various approaches proposed to deal with them. This paper reports on a study that tests the adequacy of existing Australian standards among other management tools. The development and implementation of a survey of board members is described. The focus is on the perceptions of risks by board members, together with their views on procedures and responsibilities for such risks. Findings suggest three distinct approaches used by boards that are expressed in terms of Australian sporting metaphors.

1. Introduction

Electronic commerce[1] applications, especially business-to-business, generate risk across a broad spectrum, including business continuity, information security, fraud and a range of operational risks. Furthermore, the risks associated with electronic commerce are complex and interdependent. Although casual readers of press reports may form the opinion that the extent of electronic commerce use in Australia is small, IDC reported that, in 2001, Australian business-to-business electronic commerce transactions amounted to $11.9 billion. They also predict that this figure will rise at a rapid rate, reaching $168 billion in 2006.

> *The effectiveness of a board is dependent to a substantial extent on the form, timing and quality of the information which it receives (Hampel, 1998, 23)*

The management of risk is an important part of corporate governance. Boards of publicly listed companies and public corporations are expected to exert their duty of care to

[1] While the title and current usage supports the term 'electronic business', throughout this paper we shall use the term 'electronic commerce' as this was the term used in our interviews and survey.

monitor the risks that the organisation is taking. An early initiative in this area came from the UK, where the Cadbury Report noted that corporate governance assumed:

> "*The adoption by a company's board of a risk-based approach to establishing a sound system of internal control and reviewing its effectiveness. This should be incorporated by the company within its normal management and governance processes*". (Cadbury, 1992)

In Australia, the Australian Stock Exchange (ASX) Listing Rule 4.10 says that the board of each listed company should include, in its Annual Report:

> *"The [board's] approach to identifying areas of significant business risk, and to putting arrangements in place to manage them"*. (ASX, 2001)

The Parliament of Australia, Parliamentary Library Research Paper 18 (Cobb, 1998) highlighted Australia's vulnerability to high technology risks, particularly to our trade infrastructure and computerised systems. It proposed that a National Infrastructure Protection Agency should be established to include (*inter alia*) a warning centre responsible for monitoring the operation of the infrastructure and detecting irregularities. This is not unique to Australia.

Well-managed electronic commerce systems will be a cornerstone of significant economic development in Australia. This situation is mirrored in all developed economies. The appropriate selection, development, implementation, use and monitoring of such applications is a demanding challenge. There are many factors that threaten, creating a 'risk environment'. This research focuses on the board's view of these risks. What do they think they are?

Within this context, there is growing pressure around the world for higher standards of corporate governance to be required. The Hampel Report (1998) from the UK establishes principles that can reasonably be expected to emerge in Australia and around the world. Boards of publicly listed companies and public corporations are expected to exert their duty of care to monitor the risks that the organisation is taking. Yet the risks are increasing - a double-edged sword.

Aims

Our research program aims to test and enhance existing theories of information security management and risk management so that they can be used to monitor the risks of electronic commerce systems to meet the elaborated needs of corporate boards. This study investigates the approaches currently used by company boards.

Security is the persistent challenge impeding electronic commerce system proliferation. Our overall aim is to build upon and enhance existing theories of communicating risk to corporate boards, faced with this challenge. Specifically we will assess risk management and information security management practices that are utilised in providing information to board members and in communicating the board's directives to the organisation.

Major impediments to the rapid uptake of electronic commerce systems are the perceived risks (Ernst & Young, 2000). With increasing pressure on boards to take responsibility for risk undertaken by their organisations, it is critical to supply them with rigorous, tested, reliable information about the risks that these systems generate. This research seeks to investigate the board members' understanding and perceptions of risk in electronic commerce.

2. Theoretical Frameworks

There have been many approaches to risk management within organisations, coming from such perspectives as audit and control, financial management, insurance, operational continuity, crisis and emergency management, and from the professional practice of 'risk managers'. An even wider view (Pricewaterhouse Coopers, 1999) included entrepreneurial risk within a framework for developing a risk map for an organisation. Increasing concern that boards should monitor and take responsibility for risk management has been shown in Hampel (1998), whose report has been adopted by UK listed companies. In Australia, the Australian Stock Exchange (ASX) now requires listed companies to include a "Statement of Corporate Governance Practices" in their annual report and also to identify areas of significant business risk and arrangements used to manage those risks (ASX, 2001).

In 1995 Standards Australia (in cooperation with Standards New Zealand) issued a risk management standard, now revised as Australian Standard AS4360: 1999 (Standards Australia, 1999), that describes a generic approach to risk management, that is being considered for adoption as a world standard by the International Organization for Standardization (Pricewaterhouse Coopers, 1999).

Computerised systems have been the subject of AS4444:1996 (revised 1999), *Information Security Management*, which has been widely accepted in the IT industry (Standards Australia, 1996). It modifies previous UK standards and is consistent with the new ISO17799 standard. This standard is not prescriptive, rather presenting good practices that are to be encouraged to enhance information security. It does not include performance measures or summative indicators.

There has been substantial professional practice in the area of risk management, one that has not been accompanied by rigorous theories. This divergent status of practice and theory is also to be found in the board of directors' formal role in monitoring risk within the organisation, although this is a much newer concern. Thus the two key perspectives on risk that will be used in the research will be those of standards and governance. These are not sufficiently rigorously developed as theories for research purposes, but can be used in a Grounded Theory approach as guidelines and indicators.

3. Research Methods

3.1 Research Questions and Hypotheses

This research project is driven by two key questions:

- Are official standards in risk management and information security management sufficient for assessing risks of electronic commerce systems and informing board members?
- Are Boards of Directors satisfied with information and advice they receive, in carrying out their duties of risk monitoring or governance?

3.2 Methodology – Phase One

In this phase a study of board members of organisations was conducted, examining their perceptions of board and management actions concerning electronic commerce projects. The interviews were content analysed to test the adequacy of existing theories and to extend them in necessary areas.

A random sample of companies was selected from the Australian Who's Who of Company Directors. This was restricted to companies ranked in the Business Review Weekly top 1000 organisations in Australia. From the randomly selected companies, each director was reviewed. Those with two or more such directorships were included into the mailing list. The random sample was such that a mailing list of 50 individuals was created. Personalised letters were sent to these individuals requesting their participation in the study. Ethics clearance was obtained from the researchers' university.

The approach taken was one of Grounded Theory (Glaser and Strauss, 1967) and a short semi-structured interview framework was constructed. Grounded Theory seeks to uncover the reality of the research subjects and aims principally at theory building rather than theory testing. Items included were:

a) What boards are you a member of? What is your role in these boards?

b) How much do you know about electronic commerce? What do you see as its risks and rewards? Threats and opportunities?

c) Have you had any involvement in electronic commerce projects? As a board member / otherwise? What were your experiences?

d) How are electronic commerce ventures reviewed in your boards? Do the boards have risk assessment routines for these ventures?

An initial target of eight such directors was extended as the range of issues raised in the early interviews was wider than had been anticipated. If the issues of Standards was not raised by the subjects, it was introduced at the end by the interviewer. Eventually 13 directors took part in the study with collective representation on more than sixty different boards.

In most of the interviews, two researchers were present. The proceedings were tape recorded and transcribed later. Content analysis was performed using categories raised by the subjects.

3.3 Methodology – Phase Two

From the interview transcripts, critical issues, events and approaches were identified that distinguished between the respondents. These issues were then framed as questions in a pilot instrument. The pilot questionnaire was tested with directors in a face-to-face situation so that they could identify problematic, vague or confusing questions. These were revised and the pilot testing continued. For the last four reviews only minor changes were required. An outline of the final questionnaire is shown in the Appendix.

A database of the sponsor's clients was provided for the questionnaire test phase. For each client, the chairman of the board was identified as the target for the survey. Three copies of the questionnaire were sent to each chairman with the request that it be distributed to board members. The objective was to obtain triangulation within each board. To deal with the issue of privacy, a fax-back form was included that allowed the participant to request removal from the database.

4. Analysis

4.1 Phase One - Interviews

The Australian Standard AS 4360 (1999) for risk management presents the model shown in Figure 1, below. The first phase "Establish the context" contains a first step "Establish the strategic context" that includes many issues identified by board members:

> Define the relationship between an organisation and its environment
>
> Identify the organisation's strengths, weaknesses, opportunities and threats (SWOT analysis)
>
> Context includes financial, operational, competitive, political, social, client, cultural and legal aspects.
>
> Identify internal and external stakeholders, consider their objectives and establish communication policies with these parties. AS4360 (1999) page 9.

However, board members gave significant regard to shareholders above other stakeholders and were more concerned about threats than the other SWOT components. In many cases it was pointed out that some electronic commerce opportunities were also threats, timing being critical.

Board members also emphasised their role to review and approve management decisions, rather than initiating activities. Thus the role of the board towards electronic commerce projects generally was to give management proposals the strongest review and criticism.

Executive board members, such as CEOs or Managing Directors, perceived themselves as the channel for the flow of information, issues, priorities and understanding between the board and other management. Thus the active role in the above items: define, identify, etc, was felt by them.

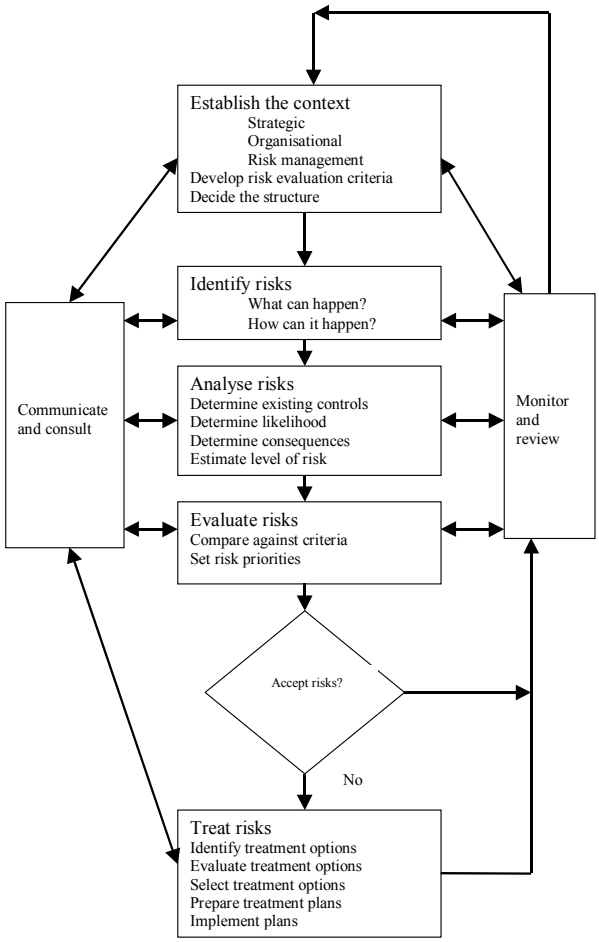

Figure 1: *The Risk Management Process (Standards Australia, 1999) p.11*

However, the evaluation of risks was frequently mentioned as an item for which board members were responsible. Appropriate corporate governance in Australia requires board members to be aware of all risks that the business is undertaking. This is clearly interpreted to require their assessment of risk. On the other hand, board members uniformly did not expect to participate in the 'risk treatment' phase.

Thus the AS4360 Risk Management reference was insufficient as an instrument in reviewing board roles. It is also lacking in specifics about IT projects generally. Board members discussed issues of development risk, implementation risk, partner risk, technology risk and product risk. Operational risks are covered in the Information Security Management standard (AS4444) but as the standard is aimed substantially at existing systems, development and implementation issues are not covered. The relationship of IT continuity to business continuity is also important (Musson and Jordan, 2000; Hecht, 2002) and needs to be included.

The framework adopted by Pricewaterhouse Coopers (1999) is particularly strong in referring to partner risk, entrepreneurial risk and corporate governance issues of risk. Risk of disintermediation is one risk that was frequently cited.

Thus to develop an instrument to study risk associated with electronic commerce, it was necessary to integrate factors from many domains. Furthermore, demographic characteristics of board members, such as age, IT 'comfort', perceived specialist role on the board, and previous experience may have very significant impacts on the processes and methods used.

4.2 Phase Two - Survey

From the interviews, a questionnaire was produced and piloted with five further directors. The tested 28-question questionnaire was then sent to a sample of 151 company chairmen. Of these 151, there were two duplicate entries, reducing the sample to 149. Nineteen recipients declined to take part and a further fourteen envelopes were returned, giving an effective base of 116 companies. Eighteen completed questionnaires were returned from a total of fifteen companies. This response rate, whilst not overwhelming, is satisfactory for our purpose[2], especially as the questionnaire analysis supported the collective judgement of the eighteen directors previously interviewed.

The impact of electronic commerce

The interviews showed that electronic commerce had affected business strategies and was seen as a source of risk. The questionnaire responses confirmed these impressions. Most respondents were already experienced in electronic commerce, with over 80% having engaged in it for more than two years. 83% had had to change their business strategies to take account of electronic commerce and 88% thought that further electronic commerce driven changes to strategy would be needed in the future.

Clearly, electronic commerce has been and continues to be a significant strategic issue. In terms of risk, 67% believed that electronic commerce had exposed their organisations to new risks and 89% thought that electronic commerce would expose them to further risks in the future. In terms of the sources of risk, all respondents agreed that these risks included a dependence on IT, threats from hackers or electronic intruders and an increasing need for new IT skills. 90% saw an increase in the risk of fraud or corruption and 93% saw risks caused by possible exposure of confidential information. These are extreme figures; we suggest that no other environmental factor has loomed so large in recent corporate history.

Electronic commerce is seen as having profound effects on the industry attractiveness in which organisations trade. As a result of electronic commerce,

- Over 90% saw rivalry between industry participants increasing.
- Over 80% saw the bargaining power of customers or buyers increasing.
- 60% of respondents thought that electronic commerce would permit new entrants into their area of business, sharpening competition.
- 50% saw the potential for substitutes for their products or services increasing, and
- 40% saw electronic commerce as increasing the bargaining power of suppliers.

Collectively, these figures suggest a serious lessening in industry attractiveness, especially in the financial services industry, the largest group of respondents.

In terms of external effects, over 80% of respondents saw electronic commerce increasing sales channel conflict. The key internal effects of electronic commerce were given as:

- 93% saw risks arising from staff being unable to adjust to or accept electronic commerce, and
- 85% saw electronic commerce resulting in an increase in reliance on key staff.

[2] The main purpose of this phase of the research was to develop and test the survey instrument. A national or international survey is needed for more substantial conclusions.

Thus the external turbulence is matched by internal uncertainty.

Who is responsible to the board for determining electronic commerce risks?

With such profound changes in their operating environments, this responsibility sits at a high level in most organisations. Generally, a board member is responsible. In over 65% of cases it is the CEO and in another 6% of cases, it is the Audit Committee chairman.

Responsibility for putting risk procedures in place

A key responsibility in risk governance is putting risk procedures in place and ensuring that they work. This study reports highly divergent practices, not generally satisfactory. Who is responsible? Half thought that the CEO was responsible for putting risk management processes in place, 17% thought that it was the job of other management and another 22% saw it as an audit committee or board responsibility.

Are the procedures in place?

This area revealed the greatest discriminators between organisations. Given that almost all boards knew that electronic commerce had exposed their organisations to new risks, it might be expected that the internal control systems had been amended to take account of these risks. Here the responses showed three distinct groups, each about one third of responses. We can characterise these groups as:

- The "surfers"; who responded to new threats with new initiatives.
  These had new formal procedures in place, but mostly these new procedures had been in place for less than one year (although the average period that these organisations had been engaged in electronic commerce was between two and five years).
- The "batsmen": who believed their practised skills would carry them through.
  These expected that the existing procedures would cope with the new risks. Of course, this attitude may be reasonable or foolhardy, but our survey could not detect this.
- The "lawn bowler": who saw the threats but were unable to respond.
  These said that they knew that their organisations needed new procedures to cope with electronic commerce risks (and did not have them).

The Australian sports metaphors are useful for explaining the results within the community, however for international audiences some explanation may help. Surfing is at its essence dynamic – unique responses may be created on the moment. Cricket batsmen develop a comprehensive set of skills that are designed to deal with any ball that can be delivered to them. Lawn (green) bowling is a dying sport but the participants are not making changes to appeal to a new audience.

To test the respondents' application of formal procedures in specific cases, we asked about a hypothetical risk to the organisation. Half said that it was the job of the line manager to detect this, but that no formal procedures existed to do so. In another 22% of cases, it was expected that audit processes would reveal the risks. In only 17% of cases would a procedure detect this risk.

Where the board or audit committee had been responsible for ensuring that risk procedures were in place, they were in place. Where management had been responsible, they were in place in 78% of cases. Where the CEO had been responsible, the procedures were in place in only 37% of cases. This suggests poor monitoring of the CEO in this respect, by the board

Who in management is responsible for devising the risk management procedures?

Electronic commerce is a business tool implemented by information technology. Defences against the technical aspects, such as security against attack or data theft, are largely implemented by technical means not by written procedures. However, the majority of risks will arise from the business aspects of electronic commerce. It is surprising, then to find that, in 42% of cases, it is the task of the IT manager to devise the risk management procedures. In 25% of cases it is the task of the risk manager and in another 25% the task of the CEO. In only 8% of cases is it the job of a business manager.

It must be emphasised that the actual percentage responses given above are from a small data set from a population that overemphasises the financial services industry. However, many of the figures are so extreme that they cannot be overlooked.

5. Conclusion

The foregoing results show that boards do not appear to carry out their corporate governance duties, at least in respect of electronic commerce risk. Despite agreeing that electronic commerce presented new threats to their organisations, boards have not changed their internal control systems to cope with these risks. Moreover, there were diverging views on whose task it was to ensure that the necessary control system changes were made.

The interviews threw some light on possible reasons for this disregard. Selections include:

> *"Most of them are very content to delegate [risk] to management"*
>
> *"For traditional businesses… [who are] going to embark on an electronic commerce strategy, one of the bigger risks for them is to really understand…how do they make those decisions, there are no guidelines for it?"*
>
> Speaking of the Internet: "*[The CEO] put his hand up and said, you know, I'm sixty-one years of age and I don't have a clue and I probably don't want to have a clue"*
>
> *"I feel that around the board table, you have got certain age groups, the older the board the larger the trend is really there not to be any electronic commerce understanding and while it's seen as a shift in direction…, the average board… [doesn't] like change*"
>
> "*I think a preponderant number of directors in Australia [think] that [electronic commerce is] all too hard, and should be left to the next generation or to their children or therefore to management….most of them are very content to delegate it to management…having delegated it comfortably, whatever comes back to the board tends to be rubber stamped if it seems sensible, but there is no thorough analytical review in the way you would have in other areas where the directors know what is going on."*
>
> "*It's a management decision, management would report on initiatives such as that, outlining the advantages and the risks. So long as there is an awareness of it without the specific details, that's OK. There are risks associated with everything*"
>
> "*But I don't think that any of [my fellow directors] see [electronic commerce] as[a] risk…*"

The results of the survey indicate that electronic commerce risk is not taken seriously by all boards. It may be that CEOs have little insight into the risks posed by electronic commerce or that they have more pressing concerns. The quotations above suggest that serious issues of governance exist in Australian companies, at least in respect of electronic commerce.

The established literature such as Australian Standards for Risk Management and Information Security Management is clearly aimed at management, and a 'risk governance' perspective is taken by boards of directors. The research instrument examines the role of the board in monitoring the risk management processes that are used, rather than in examining the risk management processes themselves. A very significant proportion of boards are dealing with electronic commerce risks in new ways, ways that have not been used before. The responsibility of board members, to become informed of the relevant issues in electronic commerce, is an issue raised by many of the subjects.

Thus, the monitor and review component of the AS4360 model in Figure 1 is one that boards see as important for them, but **what** they are monitoring and reviewing differs somewhat from the other elements of the model. The research instrument will be valuable in revising risk management thinking, in particular giving risk management professionals better guidance into the requirements and expectations of their governing boards.

A more substantial population needs to be surveyed before authoritative conclusions can be drawn – this research indicates however, that such a survey is highly warranted.

This research was kindly funded by Gadens Lawyers and an earlier version of results published at the Australasian Conference on Information Systems.

References

ASX (2001) Guidance Note 9: Disclosure of Corporate Governance Practices: Listing Rule 4.10. Australian Stock Exchange, Sydney.

Cadbury, A. (1992). Cadbury Committee Report: Financial Aspects of Corporate Governance. Burgess Science Press, Basingstoke.

Cobb, A. (1998) *Thinking about the unthinkable: Australian vulnerabilities to high-tech risks*, Parliamentary Library Research Paper 18, Parliament of Australia, Canberra

Ernst & Young (2000) *An Australian View of Risk Management*, Ernst & Young, Sydney

Glaser, B.G. and Strauss, A.L. (1967) *The Discovery of Grounded Theory: Strategies for Qualitative Research,* Aldine, New York

Hampel (1998) *The Committee on Corporate Governance, Final Report*, Gee Publishing, London

Hecht, J. (2002) "Business continuity management", *Comms of the AIS*, Vol.8, 444-450.

Musson, D. and Jordan, E.(2000) *Managing for Failure*, Macquarie Research Limited, Sydney

Pricewaterhouse Coopers (1999) *Enhancing Shareholder Wealth by Better Managing Business Risk*, IFAC Study 9, International Federation of Accountants, New York

Standards Australia (1996) *Information security management,* AS/NZS 4444:1996, Sydney

Standards Australia (1999) *AS/NZS 4360:1999 Risk Management*, Standards Australia, Sydney

Appendix

electronic commerce corporate governance survey (questions only)

1. Years experience as a board member (any board).
2. Professional background
3. Age
4. What is the main activity of your organisation?
5. Is your company listed on a Stock Exchange?
6. Does your company have a controlling shareholder (for example, as a substantially owned subsidiary or through an individual or family significant controlling interest)?
7. Do you hold an executive board position in this organisation?
8. Have you been or are you currently a member of the board audit committee?
9. When asked to evaluate a new project proposed by management, how do you usually assess the risks to the organisation that could be posed by that project? Please √ the most significant answer for an electronic commerce project in the first column and for other projects in the second column.
10. If a serious risk to the organisation arose because of, say, the actions of a key supplier, how would you as a director of that organisation expect to become aware of that risk?
11. Is the process mentioned in your answer to question 10 formally documented?
12. Who is responsible for ensuring that the organisation has risk management procedures in place that cover the likely risks such as Occupational Health and Safety, environmental compliance, fraud and risk to the reputation of the organisation?
13. If an employee, operating within their delegated limits, took an action that could cause risk to the organisation (say a marketing person set up a Web site), how would that risk be discovered and assessed by the organisation?
14. The emergence of internet-based electronic commerce has required many organisations to significantly review or change their strategies. (Please circle answers that apply)
15. How long has your organisation been engaged in electronic commerce?
16. Do you believe electronic commerce has already exposed your organisation to new risks?
17. Do you believe that electronic commerce could expose your organisation to new risks in the future?
18. Has your organisation introduced new formal and written risk management procedures to cope with these electronic commerce risks?
19. How long ago were these procedures authorised?

20. Who was directly responsible for devising these procedures?

21. Who manages the electronic commerce projects in your organisation?

22. Who, in your organisation, is responsible to the Board for identifying and evaluating the significant electronic commerce risks faced by the organisation?

23. Is the person identified in question 22 a Board member?

24. Does this person report directly to a Board member?

25. Standards Australia has produced a standard for risk management (AS4360:1999).

    a) Were you aware of this?

    b) Would you expect your management to use it?

    c) Would you expect management to mention its use in their reports?

    d) Is it applicable to electronic commerce?

    e) Would you expect your Audit Committee to refer to it?

26. An electronic commerce project is proposed to your board, that involves the use of well-regarded, established technologies but which will lead to significant restructuring within the organisation or the redefinition of relationships with business partners. How would the board assure itself that such risks were properly assessed?

27. What is the effect of electronic commerce on your industry?

28. The following are generic risk categories that may be affected by electronic commerce projects. Please indicate those where you expect a change has occurred or will occur through electronic commerce by circling the appropriate words.