Wigley & Company

BARRISTERS and SOLICITORS

CORPORATE GOVERNANCE AND IT

May 2004

Presentation to:

The New Zealand Computer Society Inc.

Technology Law Society of
New Zealand Incorporated

P O Box 10842 • 11-17 Bolton Street • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833

also at Auckland Ph. + 64 (9) 307 5957 • www.wigleylaw.com

IT, IP, information in company databases, and availability of computer systems, are increasingly becoming more central and critical to business. That trend, and an increased focus on corporate governance, leads to greater concern about risk for companies, senior management and directors.

In this first part of the paper we will overview the risks, the legal issues, and the guidelines recently produced by the Securities Commission and the Institute of Directors (IOD). We will deal with risks faced by companies, their directors and senior managers, and then turn to benchmarks such as the new guidelines. The IOD Guidelines are useful in addressing issues such as:

- whether or not a Board should have a separate IT committee; and
- the status of the CIO within the organisation (eg: should the CIO report to the CEO via the CFO?).

In the second part of the paper, Jenny Mortimer deals with governance issues from a management perspective

JENNY MORTIMER is an executive with 25 years comprehensive experience in Information Systems Management including CIO at TelstraClear and Acting CTO at the Ministry of Economic Development. She is now at Datacom.

While she has a strong technical background, this has been augmented by business experience in new business start ups and mergers, product development, business development, account management, and back office management.

INDEX

CORPORATE GOVERNANCE AND IT: The Legal Aspects

1 Executive Summary

1.1 IT, IP, information in company databases, and availability of computer systems, are increasingly becoming more central and critical to business. That trend, and an increased focus on corporate governance, leads to greater concern about risk for companies, senior management and directors.

1.2 In this first part of the paper we will overview the risks, the legal issues, and the guidelines recently produced by the Securities Commission and the Institute of Directors (IOD). We will deal with risks faced by companies, their directors and senior managers, and then turn to benchmarks such as the new guidelines. The IOD Guidelines are useful in addressing issues such as:

1.2.1 whether or not a Board should have a separate IT committee; and

1.2.2 the status of the CIO within the organisation (eg: should the CIO report to the CEO via the CFO?).

1.3 In the second part of the paper, Jenny Mortimer will deal with governance issues from a management perspective.

2 Legal Risk the Company Faces

2.1 Of course companies face numerous potential liabilities to third parties (such as customers, people whose information is being held by the company etc) if their IT systems become unavailable or there is a security breach. As well as substantial dollar risk (such as legal liability to third parties, lost business profit, reduced share prices, etc) there is reputational risk. Examples include:

2.1.1 failure of IT systems may mean the organisation can't meet its contractual commitments to customers;

2.1.2 security breaches may mean that private information is lost (leading to a claim under the Privacy Act or under judge-made law);

2.1.3 inadequate security and anti-virus systems may lead to liability to third parties if, for example, a virus gets passed on to third parties when good systems would have stopped that.[1]

[1] This is a developing area of the law. The degree to which a company would be liable may depend upon how close the relationship is between the third party and the company. However there is well established precedent for such liability (eg: a piggery was found to be liable when it passed on a virus to other piggeries, because of its

3 Potential Liability of Directors

3.1 All directors owe duties to their company to exercise the care, diligence and skill that a reasonable director would exercise in the same circumstances. That duty takes into account matters such as the nature of the company, the nature of the decision, the position of the director and the nature of the responsibilities undertaken by him or her.[2] If the director fails in that duty, he or she can be sued by the company or its liquidator.[3]

3.2 The Companies Act recognises that company business can be complex and no director can be expected to know everything. That applies especially to complex areas such as IT. So a director is entitled to rely on reports and statements etc provided by employees, professional advisors, other directors and Board committees (assuming there is no adverse indication that he or she should not be relying upon them).[4]

3.3 In practice of course Board members will be heavily reliant upon company staff and specialists. So in terms of corporate governance, they will be particularly concerned about having systems and processes in place, coupled with sufficiently capable and experienced staff.

4 Potential Liability of Senior Managers

4.1 In theory, senior managers can be liable to third parties in relation to their negligence. However, typically, the ability to sue senior managers is relatively limited. In practice it is rare for them to be sued personally anyway.

5 Benchmarks

5.1 Of course, part of doing business is taking risk. No IT system can be perfect and risk free. Obviously the more critical the system is, the more focus there should be on ensuring its availability and security. A risk analysis involving considerations of cost and benefit is appropriate. If a director fails to get sufficient reassurance, he or she may be liable (and of course the company itself may be liable to others such as customers and third parties).

5.2 There are industry standard benchmarks such as the security standard, AS/NZS 17799. There are broader expectations on companies, most recently reflected in the April 2004 Security Commission's *Handbook for Directors, Executives, and Advisors: Corporate Governance in New Zealand Principles and Guidelines* (http://www.sec-com.govt.nz/publications/documents/governance-principles/handbook.shtml). These Guidelines identify, at a high level,

---

inadequate sanitation. That precedent readily applies to companies which cause another to be infected with a computer virus because its systems were inadequate).

[2] Section 137 Companies Act 1993.

[3] Sometimes there can be liability to other parties too, although that liability is generally narrow.

[4] Section 138 Companies Act 1993.

corporate governance principles such as the need for the Board to regularly verify that the company has appropriate processes that identify and manage potential risks (including IT and technological risk).[5]

5.3 There are also useful draft guidelines produced by Standards Australia (see http://www.standards.com.au/PDFTemp/FreeDownload/DR%2004198%20Corporate%20governance%20of%20information%20and%20communication%20technology.pdf) and a wealth of material on the IT Governance Institute website (www.itgi.org).

5.4 Compliance with standards and principles such as this will not only reduce legal liability but facilitate a pragmatic approach which reduces company, director and senior management risk overall. Particularly relevant to IT are the IOD's Best Practice Guidelines issued in December 2003.

6 Institute of Directors Guidelines: *Information Technology and the Board: Best Practice for New Zealand Directors*

6.1 These December 2003 Guidelines are available from the Institute of Directors (www.iod.org.nz). In this paper we will summarise some of the key features. The Guidelines set out issues much more extensively. They contain useful checklists suitable for use by Boards, senior managers including CIOs, etc.

7 Should there be a Board Committee Specifically for IT?

7.1 Directors of course delegate specific tasks to Board committees. Historically, the IT function has often been reviewed by the audit committee of the Board. However, the IOD Guidelines recommend that, where there is critical reliance on IT, a separate IT committee might be set up. Anyway a special committee for a large IP project could be established. An example of the latter is a large-scale ERP implementation, a substantial outsourcing project, a big refresh of existing technology etc. Such projects are inherently risky on a large scale.

7.2 The IT committee of the Board (or whatever committee is looking after IT) will check to make sure that IT delivers value and minimises risks, that the IT function is aligned with the overall strategies and planning of the company, and that IT staff are of appropriate quality and experience. In view of its complex and specialist nature, the Guidelines suggest the committee can get help if appropriate.

8 Where Should the CIO fit in the Management Structure?

8.1 The CIO should be linked directly to the highest executive levels. Historically, CIOs often report to the CFO, who in turn reports to the chief executive. The Guidelines question whether this is appropriate in all cases. It could lead to undue focus on financial applications to the exclusion of other IT and strategic

[5] Principle No. 6 at page 19 of the Handbook.

issues. Increasingly, given its importance and significance, consideration should be given to having the CIO as a direct report to the chief executive.

9 Availability of the IT System

9.1 Our experience is that senior managers and Boards do not always have sufficient regard to the importance of ensuring continuous availability of critical systems. Extended outages have such a large ability to create problems for a company that this should be a key concern, and this is identified in the Guidelines.

10 Infringement of Intellectual Property Rights

10.1 The risk of companies and individual staff members misusing copyright and software etc means that there should be some focus in this area as well.

11 Conclusion

11.1 The duties and potential liabilities on companies and directors reflect commercial practicalities as do the benchmarks and guidelines referred to above. Companies are increasingly dependent on their IT, intellectual property and information. So there needs to be increased focus in this area.

BOARD / IT STEERING COMMITTEE / CIO BEST PRACTICES: Jenny Mortimer

12 The following notes cover a number of proposed best IT practices for any person or group overseeing IT, including public sector.

13 Strategy and Planning

13.1 IT Strategy and planning should, of course, reflect and support the organisation's business strategies and constraints.

13.2 In addition, IT Strategy and planning should encompass architectural direction, and changes to meet these business strategies and constraints (technology refreshment).

13.3 For planning purposes, all IT projects should be grouped together, business unit - driven IT projects as well as IT infrastructure projects, to ensure that major interdependencies are planned for.

13.4 The plans should show, at a high level, proposed projects, including estimated costs and timeframes.

13.5 I prefer plans to cover the next 3 years, with the latest year being the most detailed and concrete.

13.6 Each year, in the organisation's budget / planning phase, re-prioritisation can be made in light of business needs, risks, and budget available.

13.7 It is also good practice to review plans and budgets historically, to judge not only how well the IT department achieves against plan, but also how well the department plans and budgets.

14 Technology Trends

14.1 Organisations need some kind of capability for reviewing technology trends.

14.2 This capability may be provided by internal staff with that specific responsibility, and/or through contracting in expert external resources, and/or through attendance by IT managers at seminars and reading of relevant journals.

14.3 Plans should include a description of existing technology and issues, and a description of proposed future technology and expected benefits.

14.4 Plans should include comments on current technology trends, and what the IT department proposes to do about these.

14.5 These should be revised annually as part of the IT plan, or more frequently if resourcing allows.

14.6 The Board/Steering Committee should ask what the IT department is doing about specific technology trends (eg: thin clients, EBusiness, Blackberries).

15 Performance

15.1 Key Performance Measures should be established for all departments, including IT.

15.2 While it is most important to actually perform well, it is almost as important to be seen to perform well.

15.3 KPMs need to be monitored and reported against, probably monthly.

15.4 KPMs for an IT department could include eg:

15.4.1 System uptime (main systems), explanation of any outages

15.4.2 System performance (main systems)

15.4.3 Help desk (calls logged, calls fulfilled, average time to fulfill)

15.4.4 Changes made

15.4.5 Updates on main Projects

15.4.6 Capital and operating finances in accordance with budget and/or agreed change (monthly)

15.5 User surveys can be a useful tool to judge general satisfaction with IT delivery of services, and for eliciting suggestions for improvement.

15.6 One-off tasks can be monitored and updated eg quarterly.

15.7 KPMs should also be shown as trends, and if possible, measured against industry best practice.

15.8 The Board/ IT Steering committee should ask about significant variants on measures, significant outages, and significant project issues.

16 Personnel

16.1 Structure and staffing levels should be reviewed, but not changed too often. It is healthy to have some change, but unhealthy to have too much.

16.2 Staff should have personal KPMs agreed and reviewed as per HR policies. I prefer quarterly.

16.3 Outsourcing; Outsource KPMs should be set as part of the contract and should reflect what the organisation wants from its contract; eg agreed service levels, cost savings.

16.4 Outsource performance needs to be monitored regularly (monthly if for Projects, Operations and/or Help desk), and should be reviewed annually.

17 Governance

17.1 The IT reporting line can be quite different in different organisations. The variants I have experienced include:

17.1.1 to the CEO (the best in our opinion; the CIO is best placed to offer and execute visionary and effective use of technology to assist the business at the highest levels).

17.1.2 to the CFO (gives the CIO more power, but can often end up being a more control-oriented culture, with a focus on cost savings rather than quantum leap operational or marketing improvements).

17.1.3 Operations (ensures that IT is well utilised to support the organisations' operations, but can lose focus on innovative improvements).

17.1.4 Corporate Services (IT would be well-positioned to align with other support functions such as Finance & HR, but may then be seen as a corporate overhead).

17.1.5 With Strategy & Programme management (good support for IT for strategic innovation, but can lose the focus on day-to-day operations).

17.1.6 Chop IT up! (the worst in our opinion; as it loses the vision and power of the CIO to execute change in a cohesive way).

17.2 IT decision-making & IT budget management are often contentious issues. Too much control by IT can stifle change, and can cause projects to fail through non-support by the business. Too little control by IT can allow many competing and differing technologies and projects to proliferate, which are likely to be more costly.

17.3 I prefer business unit bidding for budget and prioritisation of projects, and strong ownership by the business of their IT projects and successful outcomes, but with 'the how' managed by IT (who should be the experts in 'the how' of technology).

17.4 Project management can be a mixture of business & IT management. Projects will only succeed if the business unit and IT are working in a healthy partnership.

17.5 The Board/ Steering Committee should become concerned about a key project's viability if there is conflict and finger-pointing amongst business units and IT.

18 Risk & Security

18.1 Responsibility for IT risk is often shared with a risk manager, often within Finance.

18.2 IT operational risks should be evaluated annually, firstly by internal managers, then by external experts, with additional reviews during periods of change.

18.3 For projects, risk reviews should be part of project lifecycles, resulting in a risk register for the project.

18.4 Security is becoming an increasing risk, as the online environment has created increasing opportunities for online disruption and fraud. Security will continue to need increased focus and effort.

18.5 Security policies need to be in place, well-communicated to staff, audited regularly, and updated regularly.

19 Personal Information Privacy

19.1 Personal Information policies need to cover both customer information policy, processes and database security, and staff information policy, processes and database security.

19.2 A hot topic, in the public sector particularly, is Email & internet access policy. There are no concrete rules for these. Organisations must have policies for these, which are communicated to all staff.

20 EBusiness

20.1 The opportunities that EBusiness can give an organisation to reduce its costs, improve its service, and increase its market presence, are major and should be regularly evaluated as part of the organisations strategy-setting.

20.2 Extra risks exist and extra security is required for EBusiness transactions. It is advisable to use experts and industry clearing systems to implement these for you, rather than home-grown solutions.

21 Availability

21.1 System availability & performance is of ever-increasing importance to virtually all organisations, and must be valued, managed, invested in, and monitored.

21.2 Good systems and processes, that are well managed, will generally run reliably.

21.3 There is a balancing act between the risk and impact of downtime, and the cost of additional redundancy.

21.4 Some functions require maximum redundancy (generally anything to do with people's lives, or with money). Others do not.

21.5 It is equally important that business continuity processes are in place, and have been documented, tested, and communicated.