Wigley & Company

BARRISTERS and SOLICITORS

Corporate and Public Sector Governance: Who Carries the Can for ICT, Electronic Information and IP?

November 2007

IT and telecommunications (ICT), ICT security, electronic information and IP (which is frequently held on IT systems), are major features of company and public sector affairs and risk. Failure can be catastrophic.

Recent developments confirm that legal responsibility goes all the way to the top.

IT systems, security, information held electronically, and intellectual property, are an ever expanding factor in public sector and commercial enterprises. They can make up a high proportion of the value and risk of the organisation. Intellectual property alone could be worth more in the balance sheet than bricks and mortar assets. Collectively they can have a high impact on delivering value.

If things go wrong, outcomes are potentially severe. On the flipside, getting it right leads to better organisational performance.

Certain types of large scale IT implementations are notorious for failure.

While there are reputational and performance issues and risks, there are also legal issues.

Where does the legal responsibility lie?

Right at the top in the public and private sectors

We'll deal first with the private sector.

TJX: A nightmare

There's a great example from what's happened in the last few months to Fortune 500 company, TJX. This is one of the largest retail chains in the world (an upsized version of NZ's Postie Plus group of retail outlets). The sort of problem encountered by TJX almost certainly will happen to NZ organisations, whether public or private sector.
It's just an example of many other potential problems such as loss of crucial IP, internal failure of computer systems so that business performance erodes, loss of key data, and so on. Those things happen more often than is known: problems may get out only in TJX-type situations.

TJX had a security breach which saw consumer information from an estimated 46 million debit and credit cards walk out the door.[1] It's not clear where the breach was, although it might have been via a single wireless connection in one of the many retail outlets.

TJX has been lucky and things have gone better than expected. Following considerable adverse press, in the end the hit on their bottom line and their reputation is relatively manageable.

However early on, there was talk that TJX would go under because of what appears to be relatively straightforward security breaches.

Significantly from a governance perspective, major shareholders in TJX looked at suing the directors for failing to meet their obligations to ensure systems were in place to meet security needs.

If this could happen, TJX itself might have been able to sue the directors as well.

New Zealand Company Boards' legal risk

[1] For more details, see *The Meaning of TJX's $168 Million Data Breach Cost* http://www.eweek.com/print_article2/0,1217,a=213421,00.asp.

In the private sector, this could happen here as well. Board members could end up being sued for failing to ensure that adequate systems are in place to deal with ICT, IT security, electronic information and IP.

Of course, the role of governance (the board) remains limited: management have key responsibilities.

All directors owe duties to their company to exercise the care, diligence and skill that a reasonable director would exercise in the same circumstances.[2]

A commonly used source as to what is expected of directors is the Institute of Directors' Best Practice Guidelines. One of the most relevant Guidelines has been the Institute of Directors' 2003 Guidelines: *Information Technology and the Board: Best Practice for New Zealand.*

Those Guidelines are reflected in the Institute's September 2007 comprehensive update: *Principles of Best Practice for New Zealand Directors: The Four Pillars of Effective Board Governance.*

The *Four Pillars* paper has some useful ideas on how boards should handle these issues. A number of questions and issues for management are framed. While many companies use their audit committee to overview these ICT types of risks, the Institute suggests that "*companies which have a critical reliance on IT may do well to establish separate IT governance committees."*

While boards need to juggle their priorities, what company now doesn't have *"critical reliance on IT"* and related areas?

Public sector

Some public sector organisations have governance issues that overlap with the private sector: obvious examples are SOE and many Crown Entities.

In the public sector, these assets and risks are of such magnitude that responsibility ends up at the top (for example, with the chief executive of a public sector agency where there is not a structure similar to a Board).

That the responsibility is at the top, legally, is demonstrated by the likely responsibilities as to electronic and other records under the Public Records Act. Record-keeping is integrally tied up with all aspects in this paper (ICT, security, electronic information and IP).

Archives New Zealand, on 3 November 2007, released an exposure draft on the creation and maintenance of full and accurate records in the public sector (including central government, local government and their trading enterprises, SOEs and Crown Entities).[3]

As the proposed Standard notes:

> The administrative head of the organisation is ultimately responsible for recordkeeping and compliance with the requirements of the Public Records Act.[4]

The standard will be implemented under statute. So, legal responsibility ultimately lies at the top.

Conclusion

Boards and chief executives (or their equivalent) can't treat ICT, ICT security, electronic information and IP as a matter only for others. Of course they must delegate. But these are key risks and need to be well up on the agenda.

The legal issues are only part of the story. The benefits (delivering value) and the risks are now so pervasive in organisations that responsibility lies at the top, whatever the legal position might be.

[2] Section 137 Companies Act 1993.

[3] http://www.archives.govt.nz/continuum/documents/Create%20and%20Maintain%20Exposure%20Draft.pdf.

[4] Page 14.

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.