



DOES THE BOARD CARRY THE CAN FOR ICT?

by Michael Wigley

INFORMATION and communications technology (ICT) is an ever-increasing feature of corporate value and risk. Failure can be catastrophic, such as in the case of a serious security breach or an internal network failure. Recent developments confirm that legal responsibility for managing ICT risk goes all the way to the top.

ICT doesn't always get enough attention from boards, yet it can make up a high proportion of the value and risk of the organisation. It involves wide-ranging issues including information stored and used electronically, through to intellectual property (which is often located on computers).

Certain types of large-scale IT implementations are notorious for failure, particularly company-wide projects. Hershey's Chocolate almost went under for example when one project melted. Locally, INCIS has its private sector equivalents: they just don't get the same press. These large projects call for heightened board focus.

WHERE DOES THE LEGAL RESPONSIBILITY LIE? RIGHT AT THE TOP, WITH THE BOARD

TJX: There's a great example in what happened to Fortune 500 company, TJX. One of the largest retail chains in the world: it had an electronic security breach. Consumer information from an estimated 46 million debit and credit cards walked out the door. 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.

Early on, there was talk the company would go under because of these security breaches. In the end, it has been lucky and things have gone better than expected.

Significantly, from a governance perspective, major TJX shareholders and lenders looked at suing the directors for failing to meet their obligations to ensure adequate IT security systems were in place. TJX itself might have been able to sue the directors as well.

This could happen in New Zealand as well. Board members could end up being sued for failing to ensure that adequate systems are in place to deal with ICT failures.

All directors owe legal duties to their company to exercise the care, diligence and skill that a reasonable director would exercise in the same circumstances. Directors are more likely to breach duties such as this if they don't endeavour to apply best practice

approaches in respect of ICT governance. Of course, the role of the board is limited and needs to mesh with the key responsibilities of management.

GUIDANCE

A commonly used source for what is expected of directors is the Institute of Directors' Best Practice Guidelines. Directors ignore such guidelines at their legal peril. The IOD included updated best practice IT expectations in its comprehensive update in September 2007: *The Four Pillars of Effective Board Governance*.

These new guidelines are essential reading for company directors that want to meet legal and other board commitments and have some very

useful ideas on how boards should handle ICT challenges. Among other useful sources is IT Governance Institute material (www.itgi.org) and the COBIT guidelines it co-sponsors.

“Board members could end up being sued for failing to ensure that adequate systems are in place.”

A SEPARATE ICT BOARD COMMITTEE AND BOARD/ MANAGEMENT RELATIONSHIP FOR ICT?

Many companies use their audit committee to overview ICT of risks. However, *Four Pillars* 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?

International ICT governance expert Basie von Solms notes a trend toward the IT security risk specialist having a direct reporting line to a board committee, similar to the auditors' direct channel. He also sees a trend to at least one director having strong ICT skills (although the board can bring in skills, such as tapping into external expertise).

CONCLUSION

The benefits and the risks associated with ICT are now so pervasive in organisations that responsibility lies at the top, whatever the legal position might be. Boards and senior management can't treat ICT risk as a matter only for others. ICT risk needs to be well up on the agenda. ●

Michael Wigley is the principal of law firm Wigley and Company.