Data security: the biggest concern for corporate counsel

By **Michael Wigley, principal, Wigley + Company**

An annual survey of US public company directors and General Counsels this year, for the first time, put data security at the top of the list of their concerns. That's ahead of long-standing priority concerns around operational risk and company risk (*Legal Risks on the Radar*, The Corporate Board Member/FTI Consulting, Inc, 2012 Law and the Boardroom Study). In this article, we overview the issues for corporate counsel based on our experiences. Then, we provide a straightforward legal benchmark along with a checklist of action points for lawyers.

We'll focus too on reassuring the CEO and the board. The same US survey shows that directors' perceptions of their organisation's ability to deal with data security breaches are higher than the reality. In the jostle for focus in busy workdays, data security may need higher priority at management and board level.

New Zealand's public sector lawyers won't be surprised at the US GCs and directors prioritising data security, given the avalanche of audit and remedial work triggered by the ACC and MSD debacles. But private sector corporate counsel face similar issues, as the poster-child disaster case of US retail business TJX shows (see below).

Just leave data security to the IT team?

No (see the governance issues that occurred in the TJX hacking case). Additionally, from our experience in dealing with numerous IT projects and issues, the IT people may cut corners on data security, based on a 'Pike River' type of approach. It's the organisation overall that drives that outcome. Take a project to roll out a new IT platform. Generally, the project team have a strong focus – encouraged by the organisation – on the here and now: to finish the project on time and on budget. Data security is a future issue by and large, not a 'now' issue. It is seen, wrongly, as a cost item without profit, not as a cost that generates profit or avoids loss. TJX dramatically illustrates the error of that view. Plus, the new service is different and fun: data security is dull. Experts point that out as a reason for the problems too.

We see this playing out time and again, but with notable exceptions. While the lawyers will be heavily dependent on the IT people, it is worth reality checking what is happening.

People and plans

A big chunk of managing data security is managing the people aspect. Two of the currently hot data security topics illustrate this:

- **Cloud computing:** Sending sensitive information offshore to be held in the 'cloud' by third parties sounds risky. And there are risks which the lawyers should carefully assess. But the critical thing is to compare those risks with the status quo, and not with perfect data security. I go into detail on this in my article "The case against cloud computing... revisited" (*CIO*, 17 August 2009, see: http://tinyurl.com/d68266k). That status quo is the office-based computer system where human error happens. That is relatively frequent compared with cloud computing. It may well be more risky than sending data into the cloud. Cloud computing is an example of the point that a balanced review of data security choices is important.
- **Bring your own devices (BYOD):** Staff plugging USB data sticks and iPads onto company networks is a CIO's nightmare. There are some smart technical solutions such as encryption, but the big issue is the human factor, such as leaving the iPad on the bus.

These examples show the need to ensure the people issues are well controlled and managed through: internal education programmes; acceptable use policies that don't just fester in Eastlight folders; comprehensive plans and governance models; and so on.

If the lawyers are not seeing signs of such material, well developed and usable, that's a big warning sign.

Likewise as to the plan for the crisis where there is a data breach. It's a teamwork thing. For example, the first day of the MSD crisis is a textbook example of what not to do, as we outline in a recent article on our website, "MSD Kiosk debacle – learnings" (1 October 2012, see: http://tinyurl.com/cbpvupn): great communications should be a key part of the plan and part of the team approach. The legal and data security treatment must mesh with communications. MSD ended up scoring an own goal. Expect a significant data security breach to happen sooner or later; for example, hacking is building all the time

TJX retail chain hacked

TJX is a listed US company operating chains of retail stores. In 2007, there was a Data Security 101 error: two stores in the chain didn't have encrypted WiFi connections – the sort of connections often used in home and business environments. And it's said there were attacks – just like for MSD – via in-store job application kiosks. The hackers were able to get deep within TJX's systems.

The impact?

- Hackers got 46 million records including customers' credit card, driver licence, and social security data (great for identity fraud);
- TJX's costs, for remedial work, litigation, etcetera, were estimated at up to NZ$1.2 billion;
- Share prices plummeted with major reputational damage and multiple law suits.

The easy entry to the system was only part of the problem. The hacking went on, undetected, for 18 months. TJX didn't have the appropriate internal access controls and audit functions. Plus, confidential data was stored in the wrong part of the system so it was easier to access.

This highlights that an important feature of data security is a layered protection: if one layer fails (eg the firewall is penetrated), other layers are there to resist the breach.

It took TJX years to unravel the mess. Five years on, TJX is coming right in the market. It could have gone under, some experts say.

Could it happen in New Zealand?

New Zealand cases in which we've been involved show that the TJX problem is not exceptional. For example, a well-known New Zealand large business had a mission-critical system for operating its core business. The system had to be highly reliable and secure, or the client's business would fail, causing mayhem for its customers.

The CIO got external consultants to penetration test the system (nice words for legitimate hacking). The testers got in within hours. The CIO raised this with the CEO. The CEO said not to raise it more widely including with the board… True story.

This is telling as to the need for strong governance relationships for data security. Poor governance is regarded as one of the main reasons for IT failures generally. There are intertwined responsibilities between the CIO, the GC, the CEO, the Board, and others, with clear allocation of ownership in the governance structure. No one person can cover the space. The lawyer should work in with the CIO's team and vice versa. All of this is motherhood and apple pie, but it is so frequently breached in the IT space that it is repeated.

and heading in the direction of sophisticated crime gangs.

For a crisis, it's of course useful to have strong backup of data. Backups, all too frequently, don't work when needed. We saw that happen with a big New Zealand organisation where a number of its backup tapes didn't contain what was assumed to be there. Then, during the crisis, elementary human error wiped tapes with real information. This is not an isolated instance.

Legal obligations – a simple benchmark

Within the variety and complexity of legal causes of action and facts, we suggest a simple test to apply.

Each situation can have unique features, such as specific legislation. That needs to be checked. We'll cover contract duties below. Otherwise, generally, using one of the 12 Information Privacy Principles in the *Privacy Act* 1993 – IPP5 – is a good benchmark for New Zealand-based legal obligations and often overseas obligations too. Apply the IPP5 test and risk overall is minimised.

IPP5 (Storage and security of personal information) states:

> "An agency that holds personal information shall ensure–
>
> (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against–
>
> (i) loss; and
>
> (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
>
> (iii) other misuse; and
>
> (b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information."

Summarising:

- The required security safeguards are what is reasonable in the circumstances to take (that overlaps with the test for the tort of negligence).
- All organisations must manage information at differing levels. My hospital's standard of care must be much higher as to my lab test results, than it is for my inpatient order from the breakfast menu. So, data security requirements are fact-specific.
- If the organisation gives the information to a third party – for example, an IT supplier managing its computer systems – the organisation's responsibility doesn't end there. The organisation must still do "everything reasonably within [its] power … to prevent unauthorised use or unauthorised disclosure". Again, there's an overlap with the negligence test.
- There's no 100 per cent obligation in all cases: the requirements are expressed in terms of what is reasonable in the circumstances. In fact, 100 per cent security is rarely achievable. Additionally, highly robust security can lead to impracticalities in delivering services. If I have a heart attack in Invercargill, and my medical records are in Auckland, I want the clinicians in Invercargill to have rapid access to my records. But that involves a level of security risk. The trade-off is appropriate even though the information is highly personal. So it is in other situations too.
- IPP5 compliance is likely to be measured by reference to good industry practice. IT Departments have source materials and there are useful sources such as the UK's Information Commissioner's Office. At a basic entry-level, IT security standard NZS17799 represents good industry practice. But, like IPP5, it is just a framework.

IPP5 is a valuable benchmark because it has overlaps with common law and equitable causes of action. For example, a claim in tort for inadequate security might be brought in negligence (and perhaps there can be a claim for the emerging tort of invasion/breach of privacy). The equitable duty as to confidential information may kick in as well.

While IPP5 is not an analogue for these causes of action, applying the IPP5 approach will broadly reduce risk overall, including non-legal risks such as reputational.

In terms of financial liability risk, the *Privacy Act* risk, in fact, will often be a much lower legal risk than the common law causes of action – although other risks such as reputational remain high. That's because the Act applies only to information about people and not corporates. Often the big ticket risks are around breach of security as to another corporate's information. So, the common law claims are important.

Contract

From what's above, promising 100 per cent security in a contract with a customer raises the bar beyond the IPP5 level. In contracts and website material as to the organisation's customers, look to diluting the commitment and/or having adequate limitation of liability. (For consumer contracts, there will be issues under the *Consumer Guarantees Act* 1993, plus, as is likely, the new and major obligations to be added to the *Fair Trading Act* 1986, outlined by us in our article "Tight controls for standard form consumer contracts – likely NZ law change", November 2012, see: http://tinyurl.com/d4box27.)

For suppliers dealing with the organisation's information, ideally there is back-to-back protection, but that would be unusual. The organisation needs to take all reasonable steps as to information given to those suppliers, as IPP5(b) points out. That can include doing due diligence on new ICT suppliers and having appropriate service and contract arrangements. Just having flash contract terms may not be enough, but it's a great start if achievable. On contracting with cloud computing providers, we provide some pointers in our 1 October article "Cloud computing Ts and Cs – News from Europe", see: http://tinyurl.com/cuqpbf6).

What should the lawyer do?

We have put together a high-level checklist (see below) to help lawyers review and report on the adequacy of the organisation's data security, based on the background outlined above. Most steps involve review of material and information provided by others. Otherwise, the task would be overwhelming.

It's hard to fit this into already busy workdays, competing with other priorities, but data security is a core issue for all organisations.

Checklist – legal review of data security

- Comprehensive review done of categories of information held, risks and their management, systems, etcetera?
- Legal requirements – including legislation and international issues – factored into that review?
- Comprehensive and workable plan and governance structure, reviewed and updated regularly (including to deal with changing security threats)?
- Plans contain a layered approach to security, combining a number of tools and techniques?
- Governance structure includes the board and the relevant board committee? Does a higher level employee 'own' data security as a significant part of their job?
- Reality check whether there are sufficient time, resources, and expertise put into data security, given the 'Pike River' factor? Don't assume this will automatically happen.
- Workable plan for when problems arise, such as hacking, loss of data, disaster recovery? This includes the communications plan.
- Audit and other testing – such as penetration testing – in place?
- Staff-related material such as acceptable use policies, education, etcetera, actually usable and used? There are legal issues here such as employment law and also incorporation of obligations in contracts (often the latter fails).
- Review contracts with suppliers and customers. Review websites and other sales/marketing collateral for unsustainable commitments.