Michael Wigley

Security in the cloud

WHEN EVALUATING CLOUD computing, organisations are of course concerned about security issues. Information is hosted elsewhere, often offshore. Legal aspects are important for wider security considerations, although reputational risk of a security breach can be more significant.

The risk of security/privacy breach may be lower overall with cloud computing than applies in the status quo (for example on-site processing of data).

In assessing whether to move to cloud computing, it is important to compare with the benefits and risks of the status quo. I outlined this in my earlier column *CIO* article, *The Case against Cloud Computing... revisited* (See CIO August 2009 and http://tinyurl.com/yafjay2), picking up on the same theme in Bernard Golden's excellent *CIO* article, *The Case against Cloud Computing* (see http://tinyurl.com/nqoedl).

Privacy and security risks?

It's not just about privacy legislation. People often discuss cloud computing as though the considerations stop and start with privacy legislation.

There is general law that applies too, such as the law in relation to negligence, contract, confidentiality and so on.

However, following the principles in the Privacy Act will often lead to compliance with other legal obligations as well.

Privacy Act

For cloud computing, the key obligation is in Information Privacy Principle 5 in the Privacy Act. This requires:

- The New Zealand organisation to protect information with such security safeguards as are reasonable in the circumstances;
- If it is necessary to give information to a third party (for example a cloud computing service provider), that New Zealand organisation must do everything reasonable in its power is done to prevent unauthorised use or disclosure.

For cloud computing, several conclusions flow from this:

- 100 percent security protection is not required. What is called for is protection of information by such safeguards as are "reasonable in the circumstances to take".
- Robust industry practice, codes, and so on, are likely to be relevant in determining the appropriate approach.
- If the organisation (for example the New Zealand-based company using cloud computing services) gives information to a cloud computing provider, that organisation must "ensure ... that everything reasonably within [its] power ... is done to prevent unauthorised use or unauthorised disclosure of the information". This obligation applies whether the cloud computing provider is based in New Zealand or offshore.
- That obligation also means that the New Zealand-based organisation often won't be able to rely solely on, for example, a supply contract under which the provider takes responsibility. This assumes that the provider does take responsibility. At present, many cloud computing providers do the opposite. So, further due diligence, systems, monitoring, and so on are likely to be required on the part of the New Zealand organisation in order to be Privacy Act-compliant.

Offshore considerations

Because the New Zealand organisation retains responsibilities, it should assess whether a particular service provider should be permitted to have the information in particular countries, some of which may have a weak privacy regime. It is one thing to send the data to Australia or Europe (each with a robust privacy regime). It is another to send it to a country without such law and practice.

The EU provides useful guidance on the adequacy of protection of data in other countries (see http://tinyurl.com/2w47yu).

Increasingly, cloud computing customers can require providers to limit the transmission of their information to certain countries.

For example, it could be limited to Australia, to New Zealand itself, or even, in the case of government, limited to public sector networks and servers (the so called G-cloud).

Reducing risk

The way contracts are framed can of course impose greater risk (for example, a contract term ensuring that all data will remain secure is risky for an organisation).

Of course, just as the cloud computing provider will seek to limit its risk in its contract with the New Zealand organisation, so can the latter seek to do so with its customers.

This may be achievable where the New Zealand organisation's customers are businesses. It is more difficult where the information is personal information and the customers are individuals.

Standard form contracts from cloud computing providers currently tend to eliminate liability to a large degree. Increasingly over time, larger users of cloud computing services, in particular, may be able to negotiate more favourable terms.

The public sector

The public sector has additional considerations such as the Public Records Act and the Official Information Act, as well as certain security requirements specific to Government.

When assessing the benefits and risks of cloud computing, the comparison should be with the real world (the status quo) not perfection.■

Michael Wigley is the Principal of Wigley & Company, a law firm specialising in ICT. He can be reached at michael.wigley@wigleylaw.com