



Michael Wigley

The case against cloud computing ... revisited

EARLY THIS YEAR, *CIO* online ran Bernard Golden's excellent article, "The case against cloud computing" (<http://tinyurl.com/nqoedl>). Having formulated key issues against cloud computing, he concluded that there are, usually, solutions.

Golden's five key issues all raise legal questions as well. So, is the case against cloud computing made out from a legal perspective?

His key issues are:

- Current enterprise apps can't be migrated conveniently
- Risk: legal, regulatory, and business
- Difficulty of managing cloud applications
- Lack of SLA
- Lack of cost advantage for cloud computing.

In summary, Bernard broadly concludes there are issues to face in cloud computing, but over time they are solvable. Additionally, it's important to compare risk and benefit in the existing WAN/LAN environment against what can happen with cloud computing. It's all too easy to overlook that the existing platforms have their problems.

As he says: "Given the very real pressures to examine cloud computing for reasons of IT agility and overall cost examination, resisting it by a bland contention that 'cloud comput-

ing is too risky; after all, what about X?' where X is some law or regulation the organisation operates under is probably not a good strategy."

From a legal perspective, moving to cloud computing is not plain sailing, but solutions will emerge over time.

For example:

- Enterprises risk getting locked into a proprietary approach on cloud computing platforms such as Salesforce. Traditional systems have developed to better enable transition from one platform to another. Cloud computing will need to develop to better accommodate this, to attract more customers. This in turn is helped by strong transition provisions in cloud computing agreements. This ability to transition will be a significant legal consideration, although it is still a pragmatic challenge on traditional systems.

- Security, confidentiality and privacy issues will be major concerns for the new platforms. But they are issues already for traditional platforms. It doesn't automatically follow that those systems are more secure than cloud computing. (For example there is the "people" element of maintaining security). However, to succeed, cloud computing will need to move toward offering high levels of security

reassurance, both in practice and in legal commitment.

- Confidentiality and security issues raise the international transfer of data. Depending on the country of source and the countries where data is stored and processed, enterprises will need to consider carefully how they ensure compliance in this area. Sometimes offshore law, such as EU Directives, may need to be considered. Reassurance may be needed that risk is not increased by data going through countries, which have low thresholds for privacy protection.

- One risk area that is increased is the prospect law enforcement agencies can "bug" internal traffic under internet surveillance legislation in various countries.

- Mission critical apps for enterprises may well require high QoS SLAs. Yet, some cloud computing providers are thin in this area. Enterprises need to assess this when deciding what to do. The level of SLAs should improve over time, particularly as large enterprises migrate to cloud computing.

In the early stages, expect "take it or leave it" standard, form contracts from cloud computing providers, which may be unsatisfactory. Over time, and as large enterprises buy into cloud computing, more

balanced terms, and one-off negotiated agreements (as with outsourcing) may become more prevalent.

Enterprises will need, when weighing up risk and benefit, to take into account the legal and regulatory risks and the ways in which this can be mitigated including by contract.

We may even see the public sector, with its critical concern about security of information, moving to these cloud computing platforms. The UK government signalled this in its landmark Digital Britain report last month, given the potential cost-savings. This highlights that cloud computing comes in different shapes and sizes, which enables risk to be minimised. Rather than using a "public" cloud, government may instead use a dedicated "G-cloud". ■

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

If there is a question you would like Michael to answer in relation to IT issues, please forward it to divina.paredes@ffxbusinessgroup.co.nz