BUDDLE FINDLAY

Supplier failure and the cloud

Amy Ryburn

12 April 2016

The move to cloud computing continues to grow exponentially as organisations and individuals seek to take advantage of the many benefits offered such as capex savings, improved elasticity and scalability and geographic flexibility. Nevertheless potential customers of cloud services are often rightly concerned about the impact of shifting their data to applications or infrastructure which they don't own and over which they have no physical day-to-day control.

These concerns lead to a significant focus during the procurement process on issues relating to:

- Data security - How secure is the service? What obligations does the supplier have to keep the customer's data safe? What are the remedies if data is unsecure?
- Resiliency - How can the supplier guarantee continued service if there is a problem? What business continuity/DR arrangements are in place?

These are worthwhile issues to focus on but contractual obligations to keep data safe and ensure the service is resilient are not necessarily all that helpful if the supplier has gone under or for some other reason simply can't provide the service; consider the takedown of Megaupload where many legitimate users of the service have never recovered their files. In addition, many service providers will seek to exclude any liability for loss of data in their service terms which means that even if there is money available, customers may not be contractually entitled to recover the financial losses they suffer if their data is lost.

Of course security and resiliency issues are not only relevant to the cloud (indeed the security of cloud services may well be better than most organisations could deliver on their own local systems) and supplier failure is not a risk which applies only to cloud services. If a software licensor goes under it can cause considerable disruption to customers who rely on the licensor for ongoing support. However, it's one thing not to have support of a system – quite another not to have any access to data which that system processes.

To date, many customers seem to have chosen to keep their most critical and sensitive data out of the cloud (or at least avoided offshoring it to other jurisdictions). Alternatively, some take the view that there is some safety in numbers. If a cloud service is multi-tenanted and a supplier will affect an entire customer base, chances are there will be a number of people with an interest in keeping a supplier propped up and ensuring service continuity until data can be extracted.

Some trends are emerging which seek to tackle the risk of supplier failure for cloud services in a different way. These include:

- **Insurance**: There are a growing range of insurance policies available which may compensate a customer for income lost from a cloud outage or failure. This option won't of course recover lost data but it can help to address the pain and provide access to experts (eg PR, forensics and legal) in the event of a cyber attack. Cyber insurance is a fast growing niche market and it may be worth customers investigating whether insurance is available at a price that is acceptable. There is also a growing insurance market overseas for cloud service providers. If insurance is available to a provider they may be willing to take on a greater level of liability in their customer terms;
- **Cloud-to-cloud backup**: Even if a cloud provider offers back-up of data as part of its offering, that won't necessarily help if the supplier itself fails (and not simply its service). Some providers offer hybrid solutions where some data is held on a local server controlled by the customer. However, having to take a locally stored back-up of data held in the cloud can reduce the benefits a customer expects to gain from a move to the cloud. Cloud-to-cloud services are emerging which give businesses the ability to create cloud-based backups of SaaS data which are held by a third party provider. The copies stored by providers of these services include metadata and audit logs and can apparently be searched for quick and granular restores.
- **SaaS or cloud escrow**: Traditional escrow arrangements don't work for the cloud. There is no point in receiving source code if you don't hold the object code, don't have people familiar with the system and potentially don't have any infrastructure on which to run the relevant software. Many global escrow providers, such as NCC and Iron Mountain, have begun to provide service continuity options where the escrow agent will step in and host SaaS software to ensure service continuity if the service provider is insolvent (either from an alternative data centre or the existing data centre if this is possible).

It is clear that the market is starting to respond to customers' need for reassurance about potential failures of cloud providers.

However, the landscape is evolving constantly and quite what will become standard practice in New Zealand (and how these practices will be reflected in contractual terms) remains to be seen.

This article was written by Amy Ryburn, partner in our TMT team, for the IITP Techblog (12 April 2016). The original article can be found here.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659