Red Circle Strategies

VOL 1. EP 3

In the olden days of traditional IT, organizations knew where their data resided and where it was replicated to. They could access their physical kit. Or at least send someone into the data centre to physically it … In the era of the cloud, how many organizations actually know where their data resides and where it replicates to?

Where does your data reside in the cloud?

This poses questions about which legal jurisdiction applies to the data, who has access to the data from a legal perspective and also what data protection laws come into effect.

Many organizations have a defined policy regarding access to data and their legal provisions and requirements that will apply to the data.

But do we always refer to the corporate position before entering into cloud service agreements?

Are the cloud architects helping the legal department understand what changes, and what needs to change? If not, why not

Is your data, and your customers information, replicating to a jurisdiction where it can be seized without you even knowing? Not sure…ummnnhh
This area is very interesting for a number of reasons.

If your organisation does not know the answer, it does ask another question. Has anyone here read the cloud contract / contracts? There should be some indication of where data will reside and in what jurisdictions somewhere in the cloud contract. If not, then ask the question to your cloud provider / cloud provider account manager.

My recommendation is to ask them regardless of having read the contract or not. See what they say – do they even know; use their answers (or lack of answers) to make informed decisions.

Another critical aspect of this is how you architect cloud services. In order to architect in level of geo-redundancy will you be replicating data into jurisdictions where your data, and your customers data, might be unsafe. Is this something your architects would even consider. Possibly not unless they have been given some guidance or governance policies around this highly sensitive area.

By the way, it is also a good idea to retain a level of cloud architecture in-house, who has oversight and final say on your cloud architectural designs. Outsourcing parts of this role is ok, but we recommend you do not outsource cloud architecture fully. The outsource model gets you so far, and too far gets you into trouble.

A simple exercise you can take is to ask around. Who knows where our organisation's data resides in the cloud? And perform this against all cloud services which you use including SaaS apps. Validate what you know and address what you don't know.

And this is before you ask the next question – is our data, and our customers data, safe? Followed by: How do we know?

Mark O'Loughlin

CEO

Red Circle
Strategies