

ASX 200 Roundtable
Summary paper 2011

Cloud computing as a transformational technology



Sponsored by



Cloud computing as a transformational technology

The Australian Institute of Company Directors hosted a series of roundtable events in October 2011 sponsored by CSC, at which Professor Craig Mudge FTSE led discussions on disruptive technology, cloud computing, the major barriers to cloud adoption and how companies can mitigate risk and similarly, become more agile, accelerate innovation and be cost effective to stay competitive.

The Australian Institute of Company Directors appreciates the participation of ASX 200 directors in these roundtables. This paper provides a summary of key themes from the roundtable discussions. The ideas presented in this paper are not necessarily the views of CSC or the Australian Institute of Company Directors and may not reflect the consensus view of roundtable participants.

Cloud computing

Cloud computing is a way in which a company or government can obtain its information technology (IT) infrastructure (computer servers, storage, networks, and applications) as a service, obtaining those resources as a utility, just as we acquire electricity and water at home. A matching business model, pay-per-use, means that entities can replace CAPEX with OPEX. Self service and payment by credit card further simplify ease of use and cost.

The US National Institute of Standards and Technology (NIST), identifies four types of cloud services:

1. Public cloud
2. Private cloud
3. Community cloud
4. Hybrid

Public cloud computing is when computer and storage resources are housed in massive data centres and offered over the Internet to all. The major providers of public clouds are Amazon Web Service, Google, and Microsoft Azure, with centres of massive scale networked across the globe.

With many tens of thousands of computer servers in a data centre, economies of scale can yield factor-of-five savings. This is achieved by automating operations and sharing the hefty burden of

cooling, physical security, and power backup.

A Private cloud delivers IT services to a single enterprise shared across multiple lines of business, and is protected by being within the corporate firewalls. An example is CSC's BizCloud – a private cloud delivered as a service.

A Community Cloud services the needs of multiple enterprises that share common IT services. For example CSC's CloudCompute, an invitation only offering for like-minded security-conscious businesses that require enterprise-class IT services with service levels, disaster recovery, warranties, service management and support.

A hybrid approach allows a company to split between a public cloud service and in-house infrastructure. In that case a company gets some of the cost benefits of scale but peace of mind from keeping its most sensitive data on its own premises.

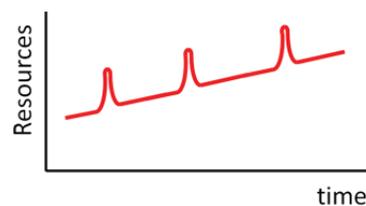
The "cloud"

The term "the cloud" is used to refer to the location of information stored with a cloud service provider and accessed via a web browser to be shared (business documents and photos), copied for backup (against losing a phone or deleting information on a laptop), or as part of an ecommerce distribution system (for example, eBooks and music).

“A Community Cloud services the needs of multiple enterprises that share common IT services.”

Utility computing

An elastic resource gives an economical way of coping with the variable nature of most demands for IT resources.



At the roundtables, we discussed two cases that showed the elasticity of pooled resources: the Victorian bushfires and a web-based start-up who was suddenly noticed on Facebook. A massive increase in traffic came from unforeseen circumstances and the entities involved, the Victorian

A massive increase in traffic came from unforeseen circumstances and the entities involved did not have to buy or configure a single new server.

Country Fire Authority and Animoto, did not have to buy or configure a single new server. Capacity was naturally added by Google and Amazon from their elastic resources. Then, just as importantly, scaled back down when the excess demand ceased several days later.

The drivers

The factors that enable cloud computing, namely, the Web, high speed broadband and high function commodity chips, have also given rise to contemporary business drivers, including, mobility, big data, and the need to improve productivity.

In some industries, customers demand mobile access and this allows transaction records to be created providing valuable data (items purchased, location of transaction, customer preferences,) which can be mined¹.

Another driver was the introduction of smart phones which raised the expectations for easy-to-use technology². These drivers demand a flexibility which is uncustomary for in-house IT services, where legacy systems are often difficult to repurpose to meet new demands.

¹ Bloomberg Business Week, in September 2011 cited five companies, from retail banks to retailers, who are using Hadoop, the new enabled-by-the-cloud, data-mining software, instead of the traditional Teradata approach.

² Apple's App Store delivers software that is easy to find and updated and serviced with minimal requirements.

“Cloud computing, where infrastructure is offered as a utility, with pay-per-use, is disruptive.”

A disruptive technology and disruptive innovation

A disruptive technology is one that helps create a new value network in one’s business, alters the market served by the existing approach, and eventually displaces it. Cloud computing is disrupting today’s IT services model.

Examples of past disruptive technologies are ink-jet printing over laser printing, steel mini-mills over integrated mills, and recently eBooks over paper books.

Cloud computing, where infrastructure is offered as a utility, with pay-per-use, is disruptive. Furthermore, everything as a service: the infrastructure running your applications or the service provider offering applications as a service (eg search and customer relationship management) is also challenging.

Security and privacy

The major barriers to the adoption of cloud computing are concerns about security and privacy. Security has always been an important concern for information managers, and the protection of personal, scientific, commercial and intellectual property information must be assured by cloud service providers.

A “one size fits all” approach to providing the latest in security, privacy and trust technologies is neither appropriate nor even possible. For example, Australians may be willing to have personal information stored in Facebook’s cloud in the USA. Yet these same users will cite the multi-tenancy (shared resources) of warehouse size data centres as a reason not to store their business data with a cloud provider.

Some government regulations forbid the storage of customer data overseas, which is a barrier since none of the three major public cloud service providers have onshore facilities. However, HP has recently completed a data centre on a 13.4 ha site at Eastern Creek to the West of Sydney³. Telstra, Fujitsu, Optus and CSC have also expanded existing local data centre facilities in Australia to provide cloud services. The Australian facilities do not yet have the scale of the big three public clouds, but are configured to meet the needs of Australian enterprise clients.

Tension between the IT department and management

Some IT departments, by keeping their sacred cows, are holding back a company’s ability to sense and respond to changes in the business environment.

³ The design is being completed in stages, with just the first cell of five completed to date. This staging matches growth in demand, but, more importantly, allows the steady improvement in cooling technology to be incorporated as it becomes available. This is an example of the cost benefit of outsourcing one’s infrastructure to a specialist.

“...the IT department turned off a company’s Blackberry network when an innovative application from the marketing department was trialled.”

Companies need greater agility to respond to the ever-changing environment with such challenges as:

- Customer demands for increased access to information.
- The shifting dynamic of interaction with customers and suppliers through social media.
- The blurring between employees business, personal and entertainment information.

If the Chief Marketing Officer (CMO) or the Chief Innovation Officer have investment proposals better aligned with the company’s strategic needs, then consider giving the IT budget to them.

Roundtable participants were able to produce experiences similar to a recent US case where the IT department turned off a company’s Blackberry network when an innovative application from the marketing department was trialled.

Of course, to forward-thinking CIOs and IT departments, a transformational technology like ICT infrastructure as a service, is something they recognise as giving them greater scope and opportunity. These are the IT departments who will sense

business opportunities and respond to achieve better alignment between IT and the business.

Security is everyone’s business

Just as each of us takes responsibility for physical security, by fitting locks, engaging security monitoring services, and following processes, so should information security be everybody’s business – directors, the CEO, and all employees. We all need to be engaged in conversations about, and reviews of, information security, especially as attacks are getting better.

A checklist of best practice security measures for review should include:

1. Certifications
2. Physical security
3. Secure services
4. Data privacy via encryption
5. Backups
6. Constant monitoring
7. External review
8. Compare with Google, Amazon, Azure

Have your information security staff, and those responsible for risk management, compare line-by-line, your security practices with those of Google,

“Service Level Agreements (SLA) coupled with adequate backup and recovery processes are essential.”

Amazon, and Microsoft who publish theirs quite openly and clearly⁴.

Adoption in government

The Government’s uptake of cloud in Australia has been slow. Governments in other countries are moving quickly to ensure the rapid adoption of cloud computing. In the US, President Obama promoted cloud computing for government services early in his administration; the first version of

the Data.gov web site went live in May 2009. Later, an “Apps for Democracy” competition challenged government staff to create cloud computing applications that would improve government service delivery. Business can do the same.

Business continuity, security and service agreements

Given the diversity of the businesses represented in our four roundtables, it is not surprising that the top priorities varied. For some, security of customer’s data was top of mind, for mining companies the risk of IT infrastructure going down and halting production was the top concern, and for some, the opportunity for productivity improvements was of most interest. Some felt that security is not the major question, expecting that accepted solutions “... will fall into place” but that the ambiguity allowed by APRA and the Privacy Commission is a bigger impediment to progress.

Service Level Agreements (SLA) coupled with adequate backup and recovery processes are essential. Good SLAs can be performance monitoring tools, not just references supporting a finger-pointing exercise⁵.

A checklist of best practice security measures for review should include:

1. Certifications
2. Physical security
3. Secure services
4. Data privacy via encryption
5. Backups
6. Constant monitoring
7. External review
8. Compare with Google, Amazon, Azure

⁴ Please refer to <http://aws.amazon.com/security/>; [Google.com Security Whitepaper \(Google Apps Messaging and Collaboration Products\)](#); [Windows Azure Security Overview](#)

⁵ For example, an SLA requiring the customer to be notified if a sub-contractor is engaged for data storage, allows one to monitor compliance of data staying in the home jurisdiction.

Where to go for more information:

Mudge, J. C. Cloud computing: Opportunities and challenges for Australia ATSE, J Craig Mudge, Principal Author. Report of a Study by the Australian Academy of Technological Sciences and Engineering (ATSE), ISBN 978 1 921388 15 6

Available at www.atse.org.au/resource-centre/ATSE-Reports/

www.pacific-challenge.com

www.cloudinnovation.com.au

McAfee, Andrew. What every CEO needs to know about the cloud. Harvard Business Review, November 2011

Issues raised by an engaged group

Many issues were raised in our roundtable discussions. The rules defining when customer data can be stored overseas are governed by the Australian Prudential Regulation Authority (APRA) and the Australian Privacy Commissioner, but their ambiguity has led to much frustration. Other questions raised and discussed at the four roundtables include the following:

- Who owns the data?
- What happens if the service provider goes bust?
- Is a private cloud more expensive than public?
- Do companies monitor hacking attempts? And if so, is the legal system up with the new technology?
- How advanced is Australia in comparison to the US?
- What is the take-up of this new technology globally?

Disclaimer © Copyright in this material (Material) is strictly reserved. Any disputes arising out of the Material are subject to the laws of the state of New South Wales, Australia. No part of the Material covered by copyright should be copied or reproduced in any form or by any means without the written permission of the Australian Institute of Company Directors. The Australian Institute of Company Directors endeavours to contact copyright holders and request permission to reproduce all copyright Material. Where the Australian Institute of Company Directors has been unable to trace or contact copyright holders, if notified, the Australian Institute of Company Directors will ensure full acknowledgment of the use of copyright Material.

The Material has been prepared for information purposes only and is not intended to embody any professional or legal standard. The Material does not constitute legal, accounting or other professional advice. While all reasonable care has been taken in its preparation, neither the Australian Institute of Company Directors nor any contributor makes any express or implied representations or warranties as to the completeness, currency, reliability or accuracy of the Material. The Material should not be used or relied upon as a substitute for professional advice or as a basis for formulating business decisions. To the extent permitted by law, both the Australian Institute of Company Directors and all contributors exclude all liability for any loss or damage arising out of the Material.

© 2011 Australian Institute of Company Directors