5 Challenges to Cloud Computing Success

Cloud technology can benefit many firms and small businesses but making the move to the cloud is not without pitfalls.

In 2017, few businesses do not use cloud-based technology. It is easily acquired, usually simple to manage and its computing power readily scaled. Generally, it is also more reliable than most “roll-your-own” solutions.

For example, Amazon Web Services (AWS) provides on-demand cloud computing platforms to individuals, companies and governments. In 2016, it comprised more than 70 services including computing, storage, networking, database, analytics, applications, deployment, management, mobile, developer tools and measures for the so-called “Internet of Things”.

The resources can cost a fraction of traditional, non-cloud solutions, but don’t come problem-free.

Here are five challenges to consider before adopting cloud technology for your practice.

1. Find the right provider

A service provider’s technical capability and capacity to innovate can be just as important as price. The real issue is sustainability. Ask yourself: “Will they be there for as long as I need them?”
Cloud computing is a long-term commitment. A financially viable partner means it should be able to refine and develop the product so that in later years you are not left with “cloud envy” – a bit like investing in a laptop only to discover that it can’t be upgraded and will no longer properly function.

Assembling a portfolio of reputable cloud-based providers can dissipate risk. For example, you might use Xero or QuickBooks for accounting, AWS for client data analysis, and various Microsoft or alternate applications for email and file storage. If one falls over, all is not lost – or worse, compromised.

The key is to assess the reputation and sustainability of service providers before, rather than after, an event. Due diligence is about avoiding the traps of entering into agreements with “cheaper” providers that make promises, but fail to deliver.

Ensure you understand how a provider monitors its services and justifies reliability claims. Of course, no entity is infallible, but what contingency plans does it have should worse come to worst? All relationships need to be built on trust, but never forget that the trust of your own clients is also at stake.

2. Learn that passwords are paramount

There is little tolerance for error in the cloud. Diligent password management is vital, but in times gone by at least businesses had more control over the devices through which information could be accessed.

Without multi-factor authentication (MFA) – when a user is granted access only after successfully presenting several separate pieces of evidence – anyone who knows your passwords will be able to access
information you have in the cloud. All businesses need to ensure passwords are secure and changed regularly, especially when staff members leave and – whenever practically possible – that MFA is implemented.

Importantly, access rights associated with usernames and passwords should only be assigned to those who need them to conduct designated tasks.

3. Security and availability

Ironically, cloud-based services need to be both secure and accessible. This means installing anti-virus software, firewalls, applying relevant security precautions to operating systems and applications, encrypting files (where feasible) on a business’s network as well as in the cloud.

Clearly, time-effective access to information in the cloud requires a fast and reliable internet connection.

4. Data privacy

The Privacy Act 1988 (Cth) imposes data protection obligations on any entity which carries on a business with an annual turnover of more than $3 million or provides a health service.

Carefully managing personal or sensitive information is imperative. Personal information relates to “any information relating to an identified or identifiable individual” such as a TFN.

“Sensitive information” pertains to health, religious beliefs, sexual orientation, or political affiliations.

Australian Privacy Principle 8 requires that companies disclosing any such information to overseas entities ensure that it is not accessed by
non-compliant third parties. In practice, this means organisations must put in place contractual arrangements so that information is only accessed by third parties in accordance with relevant compliance obligations.

In a cloud context this creates difficulties, as information could be stored anywhere in the world. For example, Dropbox keeps files in US-based data centres.

If personal and/or sensitive information stored in the cloud is not shared with third parties, it is defined as being for “internal use” rather than “disclosure” – meaning there is no legal breach.

On the other hand, if a non-compliant third party gains access to the information, a “disclosure” is deemed to have occurred; a breach of the privacy principle.

All businesses must have a strategy to effectively manage and securely hold the data they collect, and if that fails, the new mandatory data breach notification means they better have a good incidence response plan. For more information, see “Changes to the Privacy Act”, below.

5. Locked in without a key

Entering a cloud computing arrangement is far easier than exiting it.

Vendor “lock-in” happens when changing providers is either prohibitively expensive or simply not possible.

It could be that the service is non-standard, and finding another provider non-viable. Without an alternative option, it’s hard to renegotiate with the existing one.

It comes down to buyer beware. Ensure the services you engage are standard, transferrable to other providers and above all, understand what
might be required if – for whatever reasons – you need to take everything back in-house.

(本文转载链接：https://www.intheblack.com/articles/2017/10/06/challenges-cloud-computer)