“The Cloud” – your business in their hands?

Cloud Computing is all the talk at the moment. What is it, what are the upsides and downsides? How much are you in control of your own destiny when you use it?

This brief guide aims to answer several key questions about cloud computing:

- What is it?
- Benefits
- Downsides
- Who really is in control?
- How best to use the cloud?

What is it?

Most of you will probably have heard the expression “Cloud Computing” over the last few months, after a lot of hype from Google and others.

Well, it is nothing new, just an old idea (“Software As A Service”) delivered in a slightly different way than in the past.

What it means is that software applications you use on your computer, for example word-processing or email, are provided remotely by someone over the internet - an Application Service Provider. In other words, they are “hosted “ elsewhere. In order to be able to use these services, you have to be connected to the internet. If you prefer, you might call Cloud applications Online Services and a common example would be webmail provided by your ISP.

(If you are part of a large firm, then you may have your own, private “Cloud” services, which are hosted elsewhere in your company and delivered to you either over the internet or private lines. Most of this guide does not apply to that situation.)

Benefits

The key benefits of cloud computing can be summarised as follows:

Low cost of entry. Minimal investment is required in time or money to get started with cloud applications. (Generally limited) versions of some applications are free. You usually do not need to buy a high-spec computer to use online services. Access to sophisticated systems for a small number of users is relatively cheap.

No need to install upgrades or fixes. The service provider worries about all that stuff

No worries about backup. The service provider does that (you hope!). And you are also protected against a disaster with your own computer. But you need to check that the service provider holds multiple versions of backup, so you can go back in time to older versions of your data if you have to.

Flexibility. The facility to use more or less service capacity in line with your own demand. "Pay for what you use".

Access anywhere. A key plus point is that you can access your work wherever you can get an internet connection, without having to give external access to your own system or carry the data with you.

Mobile devices. If you don't have the in-house resources to host your own online services, then the cloud is the answer. Most mobile devices have insufficient resources to run applications locally.

Downsides

Access. Possibly being unable to access your data, for a variety of reasons. Most business can live with short interruptions to their computer services, how short a time depends on the business and the type of computer system. In a cloud-based system with current technologies it is all but inevitable that access to the system will be lost from time to time. Most outages last only an hour or two, but a loss of service for several days does happen from time to time. So, one key question is - How long can you afford to be without access to your system?

Security. Reputable providers make considerable efforts to protect your data. However, the hacking community spends its life trying to overcome such challenges, and from time to time succeeds. Once your data is up there on the web, someone may find an unauthorised way to access it. If Google or others are to be used as a repository for important data, how long before users need to treat such accounts as they would a bank account, and perhaps need PinSentry or similar to access them?

Performance. You are dependent on the speed of internet connection and the host provider's servers for how fast your application runs. Be aware that print traffic can be very bandwidth-hungry and can therefore drag down the performance of your remote link.

Forced upgrades. Many a user of application software over the years has decided to wait a while before adopting a new software release. Letting others sort out the bugs first, etc. With a hosted service you may not have that option – the service provider may upgrade the software and that's it – whether you like it or not.

Data Protection. It is your responsibility to ensure that your data that is subject to data protection laws, both EEC and UK, is kept securely in accordance with the various requirements. You will have to seek the necessary assurances from the service provider, as well as keeping your own access codes secure.

Terms & Conditions and Limitations of Liability. Service providers will have their own Ts & Cs and Limitations of Liability in respect of the service they provide you and the security of your data. You will need to satisfy yourself that you are happy with these, and that Service Level Agreements meet the needs of your business.

Application licensing. If you run an application that is server-licensed (some ERP software falls in this category), it may not be straightforward to transfer the hosting of that server to a remote and independent service provider. You are likely to have to negotiate this with the software vendor, and possibly pay for license extension to cover the new situation.

Loss of control. You are not wholly in charge of your own destiny. See below.

Who really is in control?

Your Application Service provider. Decides what services to offer, when to upgrade (or discontinue) them, how much server resource to allocate, how to back up your data, and how to keep it secure from unauthorised access.

Your Internet Service Provider. Decides the quality and speed of your connection.

The Internet Backbone providers. Provide the capacity for internet traffic worldwide, and hence determine the speed at which the whole thing works.

Your Telecoms Provider. Provides the means for an internet connection.

The Government. Applicable if you live or work in China, Burma or other countries where the regime in power is sensitive to criticism, and may choose to block service providers from time to time.

The Utilities – who periodically dig up the road and disrupt your telecoms connection.

Chinese, Russian and other hackers. Who from time to time may seek to sabotage the internet or selected providers by hacking or denial-of-service attacks. A recent example is the so-called Anonymous group who attacked the web-sites of several major companies following the Wikileaks affair. They succeeded in disrupting Mastercard payments for a day or so. Your service provider might get caught up in secondary action of this type through no fault of their own.

Everybody who uses the internet worldwide. Anything that results in coordinated action by millions of web users, maliciously intended or otherwise, has the ability to crash service providers' servers or clog the internet with traffic. The death of a pop star, outbreak of war, or a natural catastrophe can all generate huge amounts of internet traffic as people seek more details of the event.

How best to use the Cloud?

1. Think carefully about your business requirements – particularly for business continuity and security. Can you

afford for your system to be unavailable? For how long? Are you prepared to entrust possibly sensitive data to an internet-based service where it could be hacked, corrupted or even sold on?

2. Choose your service provider with great care and diligence. There will be all the difference in the world between a reputable, conscientious provider and others who are less so. As in most things, if you go for a cheap service you will lose out somewhere or other.

3. Are the service provider's Terms & Conditions, Limitations of Liability and Service Level Agreements acceptable to you, and are you satisfied you can comply with any data protection requirements that may apply?

4. Do you have a need to share data with others outside your company? This may be important for collaborative working with distant suppliers or customers, and cloud computing is ideal for this.

5. Get the best of both worlds if you can. If it is possible to get an application that can be used both locally and over the internet, you will have something that will work anywhere, anytime. You will not be left stranded if you cannot access the online service for a while.

6. Synchronisation is the key. If you can, choose a service that allows you to synchronise your data held online with a copy on your own local systems. That way, at least you have your data, and if the worst comes to the worst you will probably be able to find another way to open and use the files.

7. Critically sensitive or valuable data. You may decide never to entrust data in these categories to an external provider.

8. Consider getting an alternative means of connecting to the internet, in case your normal service is disrupted. Eg a 3G mobile service dongle.

If you have any questions arising from this paper, or to discuss the computer systems for your business, please contact:

Jim Symington
Chiltern Business Computing Ltd
Tel: **0845 521 1555**
Mob: **07813 080053**
Email: **Jim@ChilternBusinessComputing.co.uk**
Web: **www.chilternbusinesscomputing.co.uk**