“The Cloud”

Before the cloud people would either have a room(s) with their computers in, or maybe a computer no one touched sitting under a desk. With the advent of the cloud another option exists.

What is the cloud? It’s a question that I have asked at a number of trade shows to the vendors there and even at shows with ‘cloud’ in the title. I get many different answers, normally it depends on what the vendor is selling, but it does show that ‘cloud’ is a term used to cover a multitude of sins and often abused by marketing types. In this article I will attempt a quick romp through the ‘cloud’.

To many people the cloud is ‘out there’ and they use it with things like Dropbox, Office 365 or Google Docs, these are examples of public cloud but that is only a type of cloud. Public cloud can be defined as running on shared infrastructure somewhere.There is also private cloud where everything is running on owned or dedicated equipment and you know where that equipment is (so called ‘on prem’). Here at Collegiate we use something called a hybrid cloud infrastructure, with workloads internally on our private cloud infrastructure running on our premises and publicly available external workloads in the public cloud, all talking to each other. However in this article I will talk about public cloud rather than private or hybrid.

We can divide public cloud into 3 main areas, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Infrastructure as a Service is the most basic and is like what used to be called Co-Location, you get a computer or more commonly a virtual machine that you install your operating system on and go from there and build up what you want to do as if it were a private server, with associated licensing and running costs just as if they were yours, but you can specify the hardware you want in terms of processor, RAM etc.

Platform as a Service is a level up from Infrastructure as a Service and is normally built on the Infrastructure as a Service platform and is a computing platform with an operating service, webserver, database and programming language built in. The actual computer or virtual machine is hidden from you; the main selling point at this level is that the platform can scale up or down to match your needs and wallet. The big players here are Microsoft with Azure, Amazon with AWS and Google with App Engine.

Finally you have Software as a Service which again is built on the proceeding layers and can be identified as the charging is normally done on a per user per month basis, Software as a Service is normally a specific application that is accessed via a web browser or app and example of this is SAP or Dropbox and sold as a subscription. Here you know nothing about the underlying structure or how it is built.

Having defined what a cloud platform is, it may be helpful to explain what cloud is not but is often thought to be. If you are using a file sync application like Dropbox or a cloud app the data is held by the provider not you, this is not a backup, this is the original version. The question is can you rely on the provider’s backup? We would suggest not as you have no idea if they may or may not work the cloud provider may go bust. Normally you would have a second copy of your data stored elsewhere to the first. The cloud is no different. The second back up could be stored locally or with another cloud provider. You will also have to test these backups regularly just as you do already, beware some cloud providers charge for this testing.

For those who have not read the bottom of this article, I am the main IT person here at Collegiate and I am saying this in the name of disclosure, because what I am about to say may sound self-serving but it is not. Using the cloud does not mean that you do not need a person who is 'doing IT'. The job is not the same when everything is on site and managed by the company. But you need someone who is going to check the cloud provider is doing what they say they are. These people additionally have to make sure that you have redundant links to connect to these providers and make sure that as you open up more to the Internet that you are still secure. Finally they need to secure the data when it is in the cloud with your provider.

The cloud is not necessarily going to save you money; you will have to do the sums. You may be able to move money from Capex to Opex but that isn't a real saving. You can buy a subscription for years and then cancel the subscription and have nothing to show for it, compare that to the people who have only just moved from Office 2003 and who got a decade out of a one off purchase. It is swings and roundabouts and is different for everyone; the watch word is to do your Total Cost of Ownership sums before leaping in.

The other thing to do before leaping is to ask up front and get signed agreements on how you get out of the cloud. Vendors have lovely tools to suck data into the cloud and into their systems, the systems to move the other way are the ones that you want to look at. If you cannot get your data out in a format that is useful then you are the one with the issue, so check this when signing up, and test it. During the honeymoon period at the start of the service is the time to test all this, not when you have fallen out and no one will help.

Finally you have the questions of trust, the law and regulation. If you have your data stored in the cloud do you trust that the firm you are dealing with have the skills and security to stop others or even their own staff poking through your data? Edward Snowden has shown that the security services seem to have huge appetite for any data they can get and that they are tapping into the less secure internal systems of the providers rather than hacking in from the front. How is your provider secured to stop this? Also where is the data stored? Has the provider got a US office which means the US government could demand your data is transferred to the US for them to have a look at? Does it matter to you? What data are you going to be placing in the cloud? How are you going to deal with a leak if this information gets into the public area? These are the same questions you should be asking whether the data is local or in the cloud, just because it's in the cloud doesn't mean these questions have gone away.

Even the biggest cloud providers have disappeared off the internet due to a failure, at the time of writing Sony is recovering from an outage that seems to have started from them forgetting to renew a domain name. You may think an SLA will cover you, but unless that payment covers your losses then you are the loser. If the penalties are enough, can the firm afford to pay out and still trade? Worse if your provider does fail, how do you get your data out? In the case of 2e2, customers were given 48 hours to pay between £4K and £40K to allow 2e2 computers to remain on whilst customer's data was reclaimed by those customers after the firm went bust.

The cloud may be good for specific workloads and for specific people, but the cloud isn't for everyone or for every job. Think carefully what you want from the cloud and why and then plan for the worst case, just as you would for on premise workloads. What cloud don't mean is that you can ignore the basics of IT any more than you can when the computer is on premise.

Questions to ask (boxout)

- If I keep my data in the cloud, do I back up locally?
- If I can't pay my bill for a month or so, do I lose my data?
- If I still have to buy computers, printers, firewalls, switches and routers -- and get a better, and probably redundant, Internet connection -- and retrain my workforce, where's the savings?
- Where's my data at, exactly, in case I need to go get it?
- How do I know I can trust the people that maintain the servers?
- If it's all encrypted, and no one can see it, what happens if they lose it? Can they find it again?

Michael Dear is the main IT guy for Collegiate Management Services and is celebrating his 15th year there this month.