

## BUYER BE AWARE

*“There is one simple but golden tenet: security in the cloud is exactly the same as security in a physical shared environment and should be approached and treated in exactly the same way.”*

*Questions to ask your cloud provider:*

- *How resilient is the data centre?*
- *Is the data replicated elsewhere?*
- *If so where and with what levels of resiliency?*
- *Are specified security levels maintained along the way?*
- *Are procedures logged and are they auditable on demand?*
- *Is provision made to test both the resilience of the system and the recovery of?*

**For all the talk of *cloud computing* – and there has been a lot – a number of concerns persist in the minds of executives considering adoption of this technology concept. At or near the top of the list of concerns is the question of information or data security. This paper sets out to investigate some of the issues raised by the question of the security of cloud computing, and to provide practical guidelines to help enterprises to settle on a sustainable position on the cloud computing model.**

The concept has many definitions, but most agree that cloud computing provides an environment for the scalable processing and storage of data and for the elastic management of and access to that environment, employing Internet and Virtualisation technologies. Both technologies are central to the concept of cloud computing and allow applications and data to be provided, according to demand, from a pool of hardware and software resources. Importantly, there is often no point-to-point connection between the user and the computing infrastructure. Data and applications are not held on any single PC or server or network; they are held on a conglomeration of computing resources.

So, what's new? There is an argument that says cloud computing differs little from bureau computing on mainframes of 30 years ago. And it's true that cloud computing does have features similar to mainframe computing. But just because they are similar does not mean that they are the same.

For example, one of cloud computing's great strengths is its heterogeneity – its basis in open systems, albeit ones that talk the same language (of TCP/IP, the family of Internet communication protocols). In contrast, the mainframes of the bygone era were proprietary to a single company – IBM. Moreover, mainframes were centralised resources, with virtual machines (VMs) deployed on that central hardware. Cloud computing is de-centralised, with VMs distributed in a variety of ways – some to aggregate disparate hardware, others (harking back to the mainframes of old) co-residing on single hardware boxes.

These are important distinctions, because they underpin the very trust models of each mode of computing. Mainframe computing has been more trusted (not, please note, necessarily 'trustworthy') because users knew where their data was – i.e. on the centralised hardware in one central location.

**By contrast** – and indeed as a reason for this White Paper – **cloud computing has been less trusted at least partially because users:**

- a do not necessarily know where their data is, and**
- b cannot be confident that similar rigour has been applied to the security of ALL of the multiple systems and networks aggregated into what they view as, *their* cloud.**

Furthermore, there continue to be well-publicised instances of people and businesses not being able to access their data for hours on end due to a system failure somewhere within the cloud.

What is also different is that the cloud is more universal, provides for a truly international (if not global) environment, and operates at phenomenal speed.

Consumer perceptions of cloud computing have been formed by people's experience of high profile and innovative companies like Amazon, Microsoft, Yahoo and Google, the latter with its Google Mail and Google Docs offerings, allowing the cloud concept to gain global recognition.

---

### **Irresistible proposition**

And for many businesses the financial proposition seems practical and irresistible: 'Hey, buy this and you'll decimate your computing costs. Don't worry; we'll look after everything for you.' For many new, small and medium-sized businesses, this model is little short of a godsend, particularly in the current economic climate, and the assurances of care may seem adequate. As a consequence, there are a growing number of companies offering 'cloud services' to cater for this sector of the market. Alas, it is not quite that straightforward if you take a little time to look under the bonnet – and any business looking for a cloud solution would be well advised to do so.

---

### **Data is either secure or it isn't**

The lower costs of outsourced cloud services, and the flexibility and speed of deployment that they offer, are all highly desirable to most organisations. However, a common concern remains amongst large enterprises about relinquishing control of data to cloud providers.

To an extent, this concern is well-founded: the sheer speed of acceptance of the cloud concept means that the regulatory environment and any framework of industry best practice standards, for example, are lagging behind the market and consensus is still some way off.

It is true that many technology hosting businesses are equipped to provide basic cloud services, but it is necessary for users or customers to be satisfied that the host can protect the confidentiality, integrity and availability of data with measures and controls that are extensive, efficient and sophisticated. Not all are equipped to do so.

It is an accepted wisdom that some of the financial savings made by the shift to the cloud should be invested by customers in building the required controls into their cloud environment to enable the analysis of risk, privacy and security on an ongoing basis.

However, the temptation to over-complicate a cloud's architecture, simply because of perceived security risks, should be resisted: a fine line has to be drawn between practicality and security.

Any enterprise looking for a cloud solution must therefore fully appreciate precisely what it needs and expects from a cloud and then satisfy itself with the provider's capability to fulfil those requirements through a thorough evaluation – and might even want to consider third party audits.

It must examine the viability of the vendor's business; the expertise it applies to providing individual solutions and its track record of managing the availability and security of data. It must also look for accountability, and ask what resources are in place to enforce service level agreements. The provider must also be conversant with customer-domain-specific regulatory requirements governing the whereabouts of data.

---

## Public or private?

The cloud does not impose a 'one size fits all' environment: different types of data require different levels of security and availability. The first step is to decide which tasks should be assigned to the cloud. Business Impact Analysis and Risk Assessment activities can help to identify which type of environment is most suitable for any particular function.

**There are broadly two types of cloud, public and private, and it's important to understand the pros and cons of each.**

A **public cloud** presents multiple customers with servers, storage and connectivity in a shared operating environment in which resources are dynamically allocated according to levels of demand. It enables the deployment of an entire IT infrastructure without the capital costs associated with 'owned' systems and offers pay-as-you-go usage and elastic capacity. However, customers may, in some instances, find the choice of applications they are able to run limited by the supplier's chosen infrastructure.

In a public cloud, access is usually through standard, in other words shared, Internet connections and all management of the environment is in the hands of the service provider. Today, a simple guideline is that if information is sensitive or mission critical, then it probably doesn't belong in a public cloud. Yet in the very near future, as technology and software evolve, this is destined to change.

In a **private cloud** all resources in the operating environment are dedicated to one business alone. With private leased line access, as opposed to public Internet connections, data never shares space with data from any other business. In the right hands, a private cloud is a highly controlled and customisable environment: elasticity, software and security, for example, are configured to meet the customer's precise requirements. Whatever software and applications a business currently uses can be simply deployed on the system: there's no need to re-engineer an existing business computing model to fit a private cloud. A private cloud is comparable to tried and tested hosting models already offered by leading information availability providers.

According to need, the provider and/or the customer can be granted access to security and management controls. Predictably, private, dedicated systems tend to cost more, but can offer an extremely resilient and bespoke environment.

Some providers offer either public or private cloud systems. Others, most likely to be established businesses with greater expertise and more advanced technology, can provide both, and even offer interaction between public and private environments without compromising security. For example, this interoperability allows users to run applications in-house, to modify and store data that lives in the cloud and vice-versa.

Many IT specialists agree that this 'hybrid' model is the real future of cloud computing. Any business seeking a service provider might be inclined to seek one that can manage the whole, not just the parts.

## Security – what to bear in mind

Prior to any move to the cloud, it's simple common sense and good practice to ensure that the necessary security procedures, standards, guidelines and processes are already in place at home to ensure the technical security of data.

Typically, people look at security in terms of breaches and access etc, but when the goals for security are confidentiality, integrity and availability of data there are broader issues to be addressed. It's time to ask some tough questions:

### Supplier transparency

The supplier of cloud solutions must be willing to offer transparency, not only about its people, premises, processes and equipment, but also on its business viability. You need to be sure that the company is going to be around for a while:

- **Is the business in good financial shape?**
- **What experience does it have in data management, storage and availability?**
- **What investments has it made that enable it to deliver the services you require?**
- **Does the provider subcontract any of its operations? If so, how does this affect you?**

### Security of resource

One of the real benefits of the cloud is its elasticity: when demand is high, data and systems need to be ready and available. What would happen if each customer sharing your cloud ran its end of month reports at the same time? To what extent can the supplier guarantee adherence to service level agreements?

It is also important to bear in mind that when people share resources in a cloud a 'new' environment is created. Ensuring the security of this space means that systems need to be built and organised so that applications tidy up after themselves and don't leave clusters of data where they have no right to be. This requires a constant line audit of information on the system: you need to know where data is – and where it isn't.

### Jurisdiction

To the vast majority of users of widely available and free cloud email services, for example, there is no real need, or desire, to know where their messages are stored, or the routes they take to their destinations.

In a cloud, data can be moved through data centres in different international locations in response to varying levels of demand. Data located in any country may be governed by the laws of that country and there are sophisticated regulatory demands on businesses to ensure the security of the information they hold and generate. These laws are complex and can vary between international borders – for example, between the US and the EU. Within the US, laws can even vary from state to state.

Furthermore, organisations have legal obligations to preserve data and ensure that it is available for any legal proceedings – called electronic discovery – even if the customer is not in direct possession or control of that data.

Therefore, cloud customers must seek contractual assurance regarding the geographical storage and transit of their cloud-based data, to ensure compliance with existing as well as the inevitable introduction of new laws governing international data traffic flows. Jurisdiction is a complex and constantly evolving issue, but any data hosting business worth its salt will already be adhering to best practice guidelines and be prepared to offer competent advice on any relevant developments.

### The physical security of data

Business continuity and disaster recovery services are a fundamental requirement for most enterprises, simply to protect the viability of the business and to comply with legal requirements. The cloud makes this no different.

SunGard Availability Services, for example, has built its success in the business continuity and disaster recovery sector over four decades, and operates four purpose-built data centres across the UK and 34 worldwide. Each is linked to the others by multiple secure and fast links. Its enterprise class private cloud services can be spread across multiple data centres for double or even triple resilience.

Ask to see where your data is kept, and many providers will show you a humming suite of hardware and be unable to detail precisely where yours resides. SunGard can point you at individual servers: it builds and configures each individual component of a cloud for every customer and assigns discrete management teams for each solution.

### Portability and life management of data

Just as there are many new companies offering cloud services, others are discovering some harsh realities: newspaper reports of providers completely losing data and/or going out of business are not infrequent. Besides, somewhere along the line there may be sound motives that incline you to switch providers. These factors raise several issues:

- **Loss of data** – In the correct environment with sufficient resilience built into the system, this simply should not occur. The provision of such resilience has a cost that not all cloud providers can afford to offer.
- **Bankruptcy or takeover** – Customers should make efforts to ensure that they are able to get hold of their data physically on demand, ensuring that copies of backups are moved out of the cloud on a regular basis. Many cloud providers are unable to offer these services.
- **Move to another provider** – It is wise to ensure that data isn't held in a proprietary format and is readily transferable to other systems as required. The format of information entrusted to a provider should be agreed and be documented in the contract.
- **Destruction of data** – In addition, the destruction of information is more difficult to guarantee in a shared environment. Encryption, and the provision of different encryption keys for each customer in a public cloud may go some way to mitigate this, but not all cloud providers can offer this.

Companies seeking cloud services should consider best-of-breed providers – those that can offer a full range of resilience options and who have existing capabilities to migrate data from another provider, should the need arise.

---

### Logs and audits

During the consultation period with any company offering cloud services, customers should be able to dictate how customised their security is at a granular level. They must also decide the stringency of their ability to audit technology and security processes and to ensure that the correct level of reporting techniques are built into the product they buy. Many global businesses will require access to architecture, logs and most importantly, people – 24/7, for example.

The ability to deliver this level of configurability and accountability is not easy to achieve, and is still largely the preserve of specialised companies that continue to make the necessary investments in resources and expertise to stay ahead of the game.

The encryption of data is also a significant factor of security whether it's at rest in a data centre or in-flight. In the unlikely event of a breach, sound encryption practices will ensure data remains confidential. The customer must agree its encryption requirements with the cloud provider and establish a verifiable key management process.

## Conclusion

Cloud computing is gaining credence because it can deliver tangible operating and economic efficiencies. The 'we'll take care of everything for you' sales pitch from a growing number of suppliers is all very well, but common sense, good business practice and indeed the law dictate that the owners of data are responsible for it.

It is therefore essential that enterprises seeking the benefits of cloud computing ensure that their cloud providers can deliver the levels of security and control that they need and should expect.

- Make sure your own data centre is secure, with the necessary levels of security in place
- Use risk assessment and business impact analysis to decide which functions are appropriate for the cloud. It's imperative, and cheaper, to consider all of your requirements and options before progressing with cloud computing plans
- It's worth repeating that 'the cloud' is not a one-size-fits-all solution. Ask to look at the menu.

**A cloud provider must be able to deliver the security, availability, audit and reporting configurations you require.**