Putting Cloud security in perspective

The move towards Cloud Computing will be seen as one of the defining trends of 2010. There is growing acceptance that the Cloud delivery model offers real business benefits, however perceived security concerns threaten the general uptake of the Cloud Computing model. Many take the view that the Cloud Model is somehow inherently less secure than more traditional IT delivery models. This paper examines how organisations can take advantage of Cloud-based services while managing risk responsibly.

First it is imperative to define what we mean by Cloud Computing, as the term remains somewhat nebulous. Some argue that it is re-badged utility computing, some that it is more a natural evolution of traditional outsourcing models, and others that it is simply a return to the mainframe model. For the purposes of common understanding in the rapidly evolving world of Cloud Computing, we will take the widely adopted definition of Cloud put forward by NIST, which suggests that Cloud Computing has:

Five 'Essential Characteristics':

- On-demand self-service
- Broad network access
- Resource pooling (i.e. some form of multi-tenancy)
- Rapid elasticity
- Measured service (use-based charges)

Three 'Service Models':

- Cloud Software-as-a-Service (SaaS)
- Cloud Platform-as-a-Service (PaaS)
- Cloud Infrastructure-as-a-Service (IaaS)

Four 'Deployment Models':

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

Risks associated with Cloud Computing

There are undoubtedly risks associated with the use of Cloud-based services, just as there are risks associated with other delivery models. The most talked about risks with Cloud Computing lie in four areas: compliance; multi-tenancy; lock-in; and availability.

Compliance

This embraces two areas: legislative and regulatory compliance, such as data protection legislation including the UK Data Protection Act 1998; and other compliance requirements, such as those associated with the Payment Card Industry Data Security Standard (PCI-DSS). Organisations are also concerned about the security of their data when hosted in foreign nations. This has called into question the ability of certain host governments to access their data, which might be done, as an example, under the Patriot Act in the United States. This latter concern is equally applicable to more standard models, a point illustrated by the US government's seizure of the Belgium-based SWIFT organisation's European payments data, which had been mirrored to a US-based operating centre.

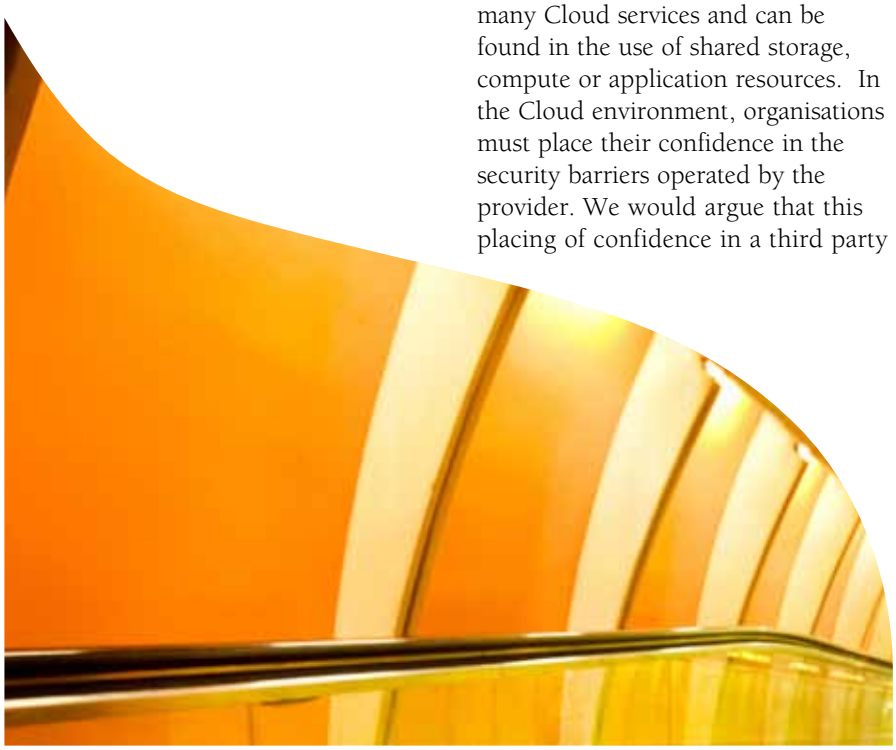
However the difficulties of complying with data protection legislation in the Cloud environment are often overplayed. For example, the Safe Harbour Agreement between the U.S.

Department of Commerce and the European Union exists to enable the personal data of EU citizens to be exported to US organisations that abide by it. There are other suitable mechanisms for enabling the export of personal data overseas, such as through the use of Binding Corporate Rules (BCRs) or by incorporating the model contractual clauses issued by the European Commission. These model clauses ensure compliance with EU requirements relating to data export (Principle 8 of the UK Data Protection Act 1998). Although such mechanisms are available to control and enable suitably secure data export, legal advice should be sought to ensure that these standard mechanisms are sufficient for individual organisations.

It is important to note that compliance can also be a problematic area with traditional delivery models. It is the responsibility of the end user organisation to operate within the applicable compliance environment irrespective of the delivery model. In short, the ultimate responsibility for compliance cannot be outsourced.

Multi-tenancy

Multi-tenancy is a core component of many Cloud services and can be found in the use of shared storage, compute or application resources. In the Cloud environment, organisations must place their confidence in the security barriers operated by the provider. We would argue that this placing of confidence in a third party differs very little from when organisations place their trust in third parties for service delivery, or data hosting.



The primary difference between the Cloud environment and more traditional outsourcing is the extent to which resources are shared. Whereas in a traditional outsourced environment services will typically run on dedicated hardware, conversely in a Cloud environment services will typically run on a shared physical infrastructure. Clearly this sharing represents a level of increased risk, however we believe it is a risk that can be reduced, through tailored security monitoring, and through appropriate use of cryptographic technologies within a comprehensive security architecture.

As with any business decision, the benefits of flexibility and value need to be weighed against the disbenefit of this elevated security risk. Often the former will outweigh the latter, although the risk management function of the business (and not IT) must ultimately adjudicate in each case.

Lock-in

Once an organisation has built a service in the Cloud, how straightforward is it for them to move to a different supplier? At present, not at all straightforward, particularly for those implementing PaaS. If you consider a SaaS model, then the data must be exported from the provider and transformed into a format compatible with the new target environment. For transport between SaaS providers this may be relatively straightforward as most providers support the export of data in .csv format. However the data elements within these exports may still require some transformation if they are to support a different target data model.

Similarly, if an organisation has built or purchased a service hosted on a PaaS Cloud then the data must, again, be exported. However the organisation now also needs to consider how to

migrate the code itself from one PaaS to another (or to an on-premise alternative).This is unlikely to be a trivial undertaking.

At the IaaS level, migration is likely to be more straightforward, provided that operating system images are not saved in proprietary formats that preclude them running on similar hypervisor environments elsewhere. But once again, data must be exported from the provider, which may be time-consuming or even unrealistic if the data generated and stored on the Cloud platform is significant. Of course, if an organisation is planning to bring a service on-premise from a Cloud based provider then it must ensure that it has all of the appropriate resources available to host the service.

However all the above has to be seen in perspective. That perspective is given by the significant business pain of migrating services in the on-premise world. An analogy exists here with the early days of the electricity market in the UK, when it was very difficult to switch between different electricity providers. Increased competition and the emergence of common procedures and technologies mean that today it could scarcely be more straightforward.

Similarly, in the future, an emergence of common methodologies and competition in the Cloud Computing market is likely to force the process of switching providers to become simpler. Work is underway on many different standards in the Cloud space, via the Open Group, the DMTF and other initiatives, which will help to promote standardisation and encourage the development of a flexible and dynamic market. Organisations such as Capgemini can help to integrate and manage Cloud offerings from numerous different providers to present a unified service to their customers.

Availability

Critics of Cloud provision ask organisations to consider what would happen were they to move e-mail and personal productivity services to the Cloud. They might do so, for example, through an implementation of GoogleApps or the Microsoft Business Productivity On-line Suite. Attention is then drawn to the damage that would be caused by the loss of their connection to the Cloud or by an outage in the Cloud service itself.

Again, this needs to be put in proper perspective. If an organisation has already outsourced its back-office functions to a more traditional outsourcer then they face these risks now. Moreover, the Cloud service is likely to offer more resilience at a much more competitive price than most outsourcers, due to the more distributed nature of the offering.

Of the risks outlined above we consider only two to be significantly more applicable to Cloud Computing than traditional delivery models: those associated with multi-tenancy due to the new attack surface not present in single tenant models; and those associated with compliance particularly where compliance requirements mandate the use of physical audits or knowledge of the physical location of data assets.
In the main, though, organisations need to be far more clear-eyed about the risks associated with their current delivery model. Individual risks associated with outdated data centres or legacy applications have frequently been accepted over the lifetime of the existing service and no longer receive due consideration or re-evaluation in a wider context. Similarly, thought needs to be given to how data is managed, secured and transported within or between organisations; for example how much sensitive data is still being transported on unencrypted devices such as memory sticks?

On the other side of the coin, Cloud Computing can offer significant security benefits to an organisation. These include, inter alia, improved data centre security, increased resilience, reduced reliance on portable media, and greater concentration and retention of skilled security resource. Here, as elsewhere, those benefits need to be weighed in the balance.

Securing Cloud Computing

First things first: no matter what the delivery model, security is still security and the same principles apply. Although implemented security technologies and processes vary, the essential techniques of risk management, by which we mean threat modelling, risk assessment and assurance on risk mitigation measures, apply equally for a Cloud service model.

Many blue chip organisations have established security architectures, often tied into a wider enterprise architecture. Where possible, Cloud security should be managed within such existing frameworks, in a way that takes advantage of existing impact assessments and assurance requirement definitions. A proper level of integration will allow an organisation to protect assets in a consistent manner across all delivery models. Moreover, it removes the unfortunate tendency to apply stricter controls in the Cloud wholesale simply because of the model rather than any underlying increase in risk or threat.

Many organisations have established security architectures, but many more do not. What assistance is there for these organisations? On the positive side, security guidance is often available from the providers themselves and from independent forums like the Cloud Security Alliance and the Jericho Forum. Both of these have been working on the implications of security in Cloud-like environments for some time. Furthermore, organisations like Capgemini have experienced staff who can advise on the implementation of secure Cloud services, and indeed contribute to these Cloud Security fora.

Any organisation considering moving to a Cloud-based service must conduct a thorough, honest and pragmatic risk assessment. This must be based on the threats appropriate to the delivery model and the business impacts of vulnerabilities being exploited. Of course, such a risk assessment should take place for all new services, not merely those destined for the Cloud. Such risk assessments need to be owned by the business. It is the role of the risk management professional to identify and assess risk, it is for the business to decide whether that risk is acceptable.

Often, the business may decide to accept a security risk in exchange for increased business functionality – a perfectly rational decision provided it is based on a full understanding of the relevant information. Failure to involve the business in the process of risk assessment may lead to the increasingly common problem of shadow IT. This is the term for business units bypassing existing IT operations and adopting Cloud services directly. For only two things are typically necessary for Cloud Service adoption: an Internet connection and a credit card. If the IT or security departments are seen as inhibitors, business units can easily bypass those perceived to be blocking progress.

If a risk assessment has been conducted and risks are deemed acceptable to the business, subject to the implementation of appropriate technical controls and processes (Capgemini utilises a security controls checklist based on the Cloud Security Alliance guidance), then certain actions need to follow:

1. Consider any requirements sourced from existing security architectures where available. These requirements may dictate (for example) encryption requirements, evaluation levels for firewall technologies and service

level requirements for processes such as user management or incident response.

2. Take these requirements, or those sourced from a more specific exercise, and translate them into a form appropriate for the proposed Cloud service and deployment model, ensuring that accountabilities between the consumer and Cloud provider are clearly understood. Typically an end-user organisation will retain most security responsibility in an IaaS implementation where they are responsible for security from the operating system upwards. Conversely, in a SaaS environment the provider must shoulder most of the security burden as a consumer typically only has access to the application with no visibility of the underlying platform or infrastructure. The PaaS environment is the most complex to understand (for example, a customer coded application making use of Provider coded APIs) and so concomitantly the split of security responsibilities can also be complex.

3. Identify a Cloud provider most able to meet the identified profile for provider responsibilities. Providers may make many claims regarding the security of their services, and establishing credibility is key. Options include independent assurance (many Cloud providers are independently certified to standards such as ISO/IEC 27001 or have been subject to SAS70 Type 2 audits), or conducting your own security testing of the service (usually controlled under standard provider agreements dictating the scope of such exercises). For Capgemini's Cloud Service Solutions we have been able to obtain improved terms and conditions from our Cloud provider partners. These include improved rights of audit and provide evidence of the additional value and influence offered by service integrators.

Available measures

Organisations must also consider how to fulfil their responsibilities while ensuring that providers operate as advertised. Fortunately, the wider IT market has long recognised the need to implement services securely in the Cloud. Many Cloud vendors now offer optional services to improve the security of their standard offers. A good example being Amazon Web Services, who offer of a Virtual Private Cloud service. This attempts to mitigate some of the risks of multi-tenancy by offering security separation through cryptographic means. Should an organisation wish to implement further separation between their data/service and the Cloud provider using software produced independently of the Cloud provider, then similar functionality is also available from CohesiveFT via their VPNCubed product. Amazon also offers host-based firewalls that are used to control communications with customer containers. Similarly Salesforce.com allows customers to control which IP addresses have access to their service.

Crucially, though, organisations are not limited to the controls provided by Cloud vendors. The growing popularity of federated identity management allows organisations to manage the access rights of their users in the Cloud from within their own organisational boundary. The use of standards-based identity management and federation technologies also promotes transparency and interoperability between different Cloud providers and on-premise systems.

Technologies such as those from PingIdentity help to make access to Cloud-based services seamless, as well as secure, enabling a more user-friendly experience for both end-users and user administrators. For those organisations that require two factor authentication, CRYPTOCard offer a managed authentication service that enables secure token-based authentication to be implemented quickly, securely and cost-effectively. It is important to note,

here, that in almost all environments people, and their access to systems and data, represent the weakest spot in a security solution.
This is particularly true in Cloud environments where access typically comes via the Web browser. Here social engineering attacks can be extremely serious, using techniques such as phishing or brute force guessing to obtain user passwords, or more direct unauthorised access via cross-site scripting. As an example, corporate information relating to Twitter was recently exposed after an attacker compromised an email account belonging to a Twitter employee. This account also provided access to the employee's Google Docs and Google Apps from where the confidential information was obtained. The use of a strong two-factor authentication mechanism would have frustrated this attack.

Security monitoring must also be considered, and becomes even more vital when services and data are hosted outside organisational boundaries or distributed across multiple Cloud providers. There it becomes a critical control to maintain visibility of service levels and security. Many technical controls are available to implement such protective monitoring, some Cloud-specific (e.g. CatBird), some more generic and some of a contractual and procedural nature. The most appropriate tools will depend upon the service and deployment models in question.

While this paper does not attempt to provide an exhaustive assessment of the security mechanisms for every Cloud Computing service and scenario, it does show that solutions are available to mitigate the most common security risks in a pragmatic and sensible manner.

Conclusion

Assessing the security of the Cloud Service model cannot sensibly be done in isolation. Instead it must be considered in its proper context – namely in comparison with the inherent risks in more traditional models. Adoption of Cloud Computing is not a risk-free exercise, but nor is adoption of a more traditional model.

While the Cloud has unique challenges, those challenges do not mean it is inherently insecure. Indeed, alternative IT delivery models have unique challenges of their own. Moreover their challenges, such as maintenance of aging data centres, retention of qualified staff, and lack of IT flexibility or wasteful use of resources, might easily be seen as more significant.

Therefore, as a rule, security concerns should not be a block to the adoption of Cloud Computing. There *may* be data or services that are not appropriate to place on a multi-tenant Cloud service, which is perfectly understandable due to specific compliance requirements or its extremely high value to the business. Organisations need to be sensible, business-focused and pragmatic about Cloud-sourcing. Decisions should be arrived at through an understanding of business risk that looks honestly at the associated risk within more traditional delivery models. Frank appraisal, not instinctive fear, should inform those decisions.

About Capgemini

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies. Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™. The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients. Present in more than 30 countries, Capgemini reported 2009 global revenues of EUR 8.4 billion and employs 90,000 people worldwide.

More information is available at
www.capgemini.com
www.capgemini.com/immediate

Rightshore® is a trademark belonging to Capgemini

Lee Newcombe Ph.D.
Security Consultant
lee.newcombe@capgemini.com

Capgemini
11, Rue de Tilsitt
75017 Paris
France
Phone +33 (0) 1 47 54 50 00
Fax +33 (0) 1 42 27 32 11

Copyright © 2010 Capgemini. All rights reserved.