

technology viewpoints

May 2009

ABOUT THIS DOCUMENT

This issue of CGI's Technology Viewpoints takes a look at the topic of information security within a cloud computing environment.

This document is a complementary transcript to a podcast on the topic with Andy Pridham, the director responsible for CGI's National Capital Region's information security practice and a Certified Information Systems Security Professional (CISSP).

In the midst of all the cloud hype, the podcast identifies some of the risks inherent to the use of cloud computing and presents strategies for managing those risks.

Information Security within a Cloud Computing Environment

Let's start with the basics. What is cloud computing? What are some of its advantages and where does security play a role?

Cloud computing at its simplest means computing using networks outside of your control and without knowledge of the resources employed. It is reliant on, and synonymous with, the use of the Internet and incorporates resource virtualization technologies and software as a service [SaaS].

These technologies have been proven to reduce cost by making more effective use of physical space, bandwidth and software licenses through the sharing of these resources. This requires flexibility with respect to where data might physically reside at a given moment so as to maximize use of the resources within the pool. We long ago learned the benefits of server-based applications and storage, as opposed to multiple discrete desktops. This is an extension of that, outside of the organization.

The proven ability of cloud computing to reduce costs for an organization has resulted in a rapid uptake of this approach. But concerns over security have been a major hindrance to more rapid growth. There may be situations where all aspects of cloud computing cannot be embraced due to security concerns; nevertheless, there are approaches that can be taken to reduce the risk to a level that might be acceptable to an organization.

Let's talk more about these concerns and approaches. Can you cite some of the security pitfalls and safeguards our clients should consider when moving to a cloud computing environment?

Lack of control and absence of knowledge, which are fundamental to cloud computing, run counter to the fundamental requirements for security. Therein lies the rub; as you add control and insist on knowledge, you negate advantages. It comes down to risk management—balancing the benefits against the potential for harm.

There are five major areas where attention is due. Satisfying concerns in those areas will go a long way in reducing the risks inherent in cloud computing.

Before I discuss these areas, it's important to note that most of what I will discuss is not unique to cloud computing; the areas I'll discuss are common to other forms of outsourcing and other similar situations where an organization entrusts its assets to an outside provider. The difference with cloud computing is that by definition there are fewer controls on how and where data will be stored, processed and transmitted.

The questions to which answers are required include: Is my data going to be adequately protected? Will the arrangement meet my legal requirements?

First, clients should think about compliance.

Much about an organization is said by the certifications they possess, such as ISO 27002, SAS70 for the organization, CISSP for their employees, and, for example, common criteria for the security products they use. The cloud computing provider should have internationally recognized standards for which they are audited on a regular basis by certified auditing firms. Ask these questions: What certifications does the vendor maintain? Do they undergo regular audits?

Further to that—and this is not specific to security, but does affect how it is done—it is important to understand how mature the organization is by looking at their processes and determining how viable they are. How long have they been in business? Who are their clients? How much work have they booked? Publicly traded firms are required to disclose this kind of information and to attest to its accuracy.

Finally, there may be regulatory requirements related to security that must be met. If some cannot be met, it can be a showstopper unless approved workarounds can be produced. Be aware that all of this applies equally to any sub-provider that may be engaged by your cloud provider.

Several of the next points I'll discuss will be addressed within compliance programs, but it is nevertheless prudent to explore them further to ensure that not just the letter of the law is met.

Next, examine the location of the data.

Can clients specify where the data will be/will not be located? I'm speaking here to the countries and jurisdictions where it will be stored and processed. There are countries where local laws and/or governmental practices might not provide the confidentiality clients expect. Clients should ask these questions: What degree of data segregation can be expected? Will data reside on the same server as data from a competitor or a suspected hostile country? Do regulatory and legal requirements even permit storage and processing of certain parts of data within that country?

Herein lie some of the dilemmas caused by security requirements. A compromise solution is what's called a private cloud where a client can specify where and how some or all of the data will be stored; however, in that case, clients must accept reduced benefits from the virtualization of server space.

Third, look at access control.

If a client's data is sensitive and if it falls into the wrong hands, great harm could occur. Only those authorized and with a need to access it should be provided that ability. Find out if the data will be encrypted and, if so, how the keys will be managed. Determine how else access will be controlled. When the contract ends, how will clients be assured that all of their data artifacts will be deleted?

Clients need to accept that some system administrators will have a legitimate need to access their data. It's important that cloud providers are competent, but their intimate access to your data also provides an opportunity for malicious acts. The client has already determined their levels of competence; they should also determine the provider's level of trustworthiness. What is the policy on background checks for system administrators? What controls are placed on them? What degree of auditing occurs? Is there accountability?

FIVE AREAS FOR SECURITY ATTENTION

There are five major areas where attention is due. Satisfying concerns in those areas goes a long way in reducing the risks inherent in cloud computing.

1. Verify the certifications and regulatory compliance standards of the cloud provider
2. Examine where your data will be located from jurisdictional, legal and competitive perspectives.
3. Look at access controls and auditing processes
4. Examine the cloud provider's backup and recovery processes and systems
5. Determine the adequacy of incident reporting and response

Next, examine the cloud provider's backup and recovery processes and systems.

Availability of data is critical, and like all outsourcing arrangements, is an aspect that requires careful consideration. It is one of the few objective measures that will be negotiated in service level agreements and will be a major factor in what is paid for that service. Here are a few questions that clients should ask of their cloud providers:

- How robust is their system?
- How does their architecture provide redundancy?
- Where are their back-up sites and how do they conform to the previous points just discussed, such as compliance?
- How do they manage outages?
- What are their practices and track record?
- How well equipped are they to monitor, detect and respond to attacks?

This leads us to the final point: incident reporting and response.

It's surprising how many otherwise mature organizations lack an effective incident reporting system. If a process has been prescribed, it is often not effectively communicated. If communicated, it is sometimes not exercised so that when something bad happens, the response is ad-hoc, as if it is the first time it has happened. This can lead to serious loss and extended periods of downtime.

What is their incident reporting and response process? How capable are they of investigating incidents? What are the circumstances when outside agencies might be involved, such as local law enforcement? What is their policy on informing the client of an attack or even a possible attack?

Before we close, can you provide some final thoughts on the topic of ensuring security within a cloud computing environment?

There is always risk. It exists no matter what measures you take, how much you spend, and who is entrusted with your assets. Clients should understand the value of their data to the organization and their legal and regulatory requirements and take appropriate measures. Like with outsourcers, assume nothing and be thorough in choosing and monitoring a cloud provider.

With respect to security, the dilemma with cloud computing is that its greatest advantages pose some of the greatest threats. Due diligence in assessing a potential service provider and a balanced set of restrictions can still provide an opportunity to exploit the advantages of cloud computing within an acceptable level of protection for clients' data.

COMPANY PROFILE

At CGI, we're in the business of satisfying clients. For 30 years, we've operated upon the principles of sharing in our clients' challenges and delivering quality services to address them. As a leading IT and business process services provider, CGI has approximately 25,000 professionals operating in 100+ offices worldwide, giving us the competitive advantage of close proximity to our clients.

Through these offices, CGI offers local partnerships and a balanced blend of global delivery options—including onshore, nearshore and offshore expertise—to ensure clients receive the combination of value and expertise they require.

CGI defines success by exceeding expectations and helping clients achieve superior performance.