UKCeB

Cloud Computing

An Internet of Possibilities

October 2010

Table of Contents

Introduction

This white paper supports efforts by the Security and Public Key Infrastructure (PKI) ID Management working group of the UK Council for Electronic Business (UKCeB) Security to develop a position paper on the subject of security issues related to cloud computing. The paper presents an overview of cloud computing concepts, defines areas of risk, presents guidelines for considering risk during an evaluation of the technology for implementation, and documents references and material recommended for further review.

UKCeB would like to thank its members for feedback and contributions towards producing this paper. Special thanks go to Boeing for the lion's share of resource and technical expertise in producing a paper that we hope will prove informative and valuable to the UKCeB membership.

What Is Cloud Computing?

The term cloud computing refers to a group of technologies and approaches for managing those technologies. Some of these technologies and approaches have been around for a long time, whereas other, more recently developed aspects help to solidify these technologies, with the goal of creating a truly commodity-based computing model.

Cloud computing delivers shared resources (e.g., software applications, development platforms, and infrastructure resources) to computers and other devices by means of a network of which the Internet, private WAN, or trusted community network may be implementations. The service offers broad network access and pooling of resources. It can be measured and be able to rapidly expand or contract to fit customer requirements without capital costs. Cloud computing is usually sold as a commodity service where 'one size fits all'.

An important consideration in any cloud delivery is the type of service that is made available for consumption. These services range from simple computing and storage to more elaborate business services involving human interaction. Typically, such services (referred to 'as a service') are thought to fall into three main categories, as discussed in table 1.

Table 1. Cloud Utility Models

Type	Description	Public Cloud Examples	Private Cloud Examples
Infrastructure as a Service (IaaS)	Provides the basic elements of computing, such as servers, storage, networking, and operating systems, enabling users to construct computing environments without building or owning the infrastructure themselves.	Amazon EC2™ IBM Smart Business Storage Cloud Terramark vCloud™ Express and Enterprise Cloud™	Virtual machine with an operating system Virtual storage
Platform as a Service (PaaS)	Adds to the infrastructure a richer software environment with a variety of built-in capabilities and tools such as database, transaction management, middleware platforms, and development tools.	Amazon EC2™ Microsoft Windows® Azure™ IBM Smart Business Development and Test Cloud	Virtual appliances such as – • VMs with preconfigured development environment • Middleware stacks
Software as a Service (SaaS)	Delivers complete application systems over the Internet using an on-demand billing system.	salesforce.com® IBM LotusLive™ Microsoft CRM®	SAP® Sapphire®

Note: In the defence community, typically the term delivery model refers to the way in which the service is delivered to the end user (e.g., public cloud, private cloud, and hybrid), and XaaS is referred to as the service type. This allows specifications of XaaS offerings agnostic of the delivery model.

The Virtualised Infrastructure Oasis

Virtualisation is one of the foundational cloud computing technologies. Generally speaking, x86/x64 virtualisation makes IaaS possible by delivering the four primary hardware computing resources (i.e., CPU, memory, disk stor-0 age, and network) virtually. In fact, the buzz leading to the coining of 'cloud' is analogous because this abstraction coincides with the commonly recognised design element of a cloud icon to represent an arbitrary network. The user doesn't necessarily care about the details of how the bits get from point A to point B as long as the method is secure and timely.

Virtualised hardware is realised through the introduction of a software component known as a virtual machine monitor (VMM) or hypervisor, which provides a layer of abstraction between the physical hardware resources and the virtualised (i.e., guest) operating systems that consume those resources. Quite a few VMMs exist, both as open source as well as proprietary implementations. They typically fall into one of the following two categories. Type 1 hypervisors, also referred to as 'bare metal' hypervisors, run on top of and have direct access to the host system's hardware, whereas Type 2 hypervisors are part of a 'classical' operating system and provide a layer of abstraction for the guest virtual machines (VM), wherein system calls are interpreted through this host operating system. In addition to these types of VMMs, different techniques also exist for implementing virtualisation on top of the hypervisor. Implementations that do not modify or alter the guest operating system are known as full virtualisation, whereas another technique, known as paravirtualisation, aims to improve performance and gain efficiency by having the VMM interpret the guest's intent through a software interface and make the calls to the actual hardware on behalf of the guest VM.

No two VMM architectures or implementations are necessarily the same. Some may offer more security while sacrificing performance or flexibility while others may focus on usability and portability. For example, a cloud service provider (CSP) may modify a VMM to suit security or functionality requirements without being able to assess the positive or negative effect that these customizations have on the overall security posture of the architecture. In light of this, customers should realise that there is an implicit trust in the VMM to provide security assurance that one environment is safe from another. Customers should properly evaluate and discuss in detail the CSPs offerings related to their virtualisation infrastructure. Customers should also request any certifications or accreditations the CSP or virtualisation technology vendor may have received, such as Common Criteria Assurance Levels certification (http://www.commoncriteriaportal.org).

The promise of reduced costs can be dazzling. Cheap x86/x64 hardware and virtualisation of this hardware make massive scale-out and elasticity possible. Through the use of virtualisation technologies, CSPs can take advantage of the powerful hardware they have provisioned to offer separate, dedicated environments for their customers while benefitting from the economies of scale. In turn, customers of CSPs pay only for the resources they consume and the actual time that those resources are used. For example, multiple systems can be deployed easily within a CSP for, say, a research project with a finite lifespan. Once research activities are completed, those systems can be decommissioned instantly, and the resources can be reallocated to the next user. The customer for those systems pays only while the resources are being consumed, providing a more granular cost accounting model to meet the business requirements and costs associated with those specific requirements.

Delivering the Cloud

The shared resources in a CSP may be set up in a number of ways:

Public cloud. Resources are dynamically provisioned on a fine-grained, self-service basis over the Internet by using Web applications and Web services from an offsite third-party provider who shares resources and bills on a fine-grained utility (pay-per-use) and elastic scaling computing basis.

Community cloud. Organizations with similar requirements share infrastructure so as to realise some of the benefits of cloud computing. With the costs shared amongst fewer users than with a more general public cloud, this option is more expensive, but it may offer a higher level of privacy, security, and policy compliance.

Private cloud. A company builds an internal cloud on their own networks, typically behind the corporate firewall or other company-managed policy enforcement point (PEP), such as a private collaborative network.

Hybrid cloud. Commonly depicted as an extension (i.e., bursting) of a company's private cloud into an external public cloud, this method enables the company to consume additional resources as needed.

Compounded cloud. This deployment model is an alternative hybrid model, but it is likely to be confined in a public cloud domain. A compounded cloud consists of layers of CSPs (e.g., SaaS) residing within a separate IaaS provider's cloud. One important consideration in this situation is that the company using an SaaS application likely has an agreement with the SaaS provider and not directly with the IaaS provider who hosts the SaaS application.

Figure 1 describes some of the differences between the public and private delivery models.

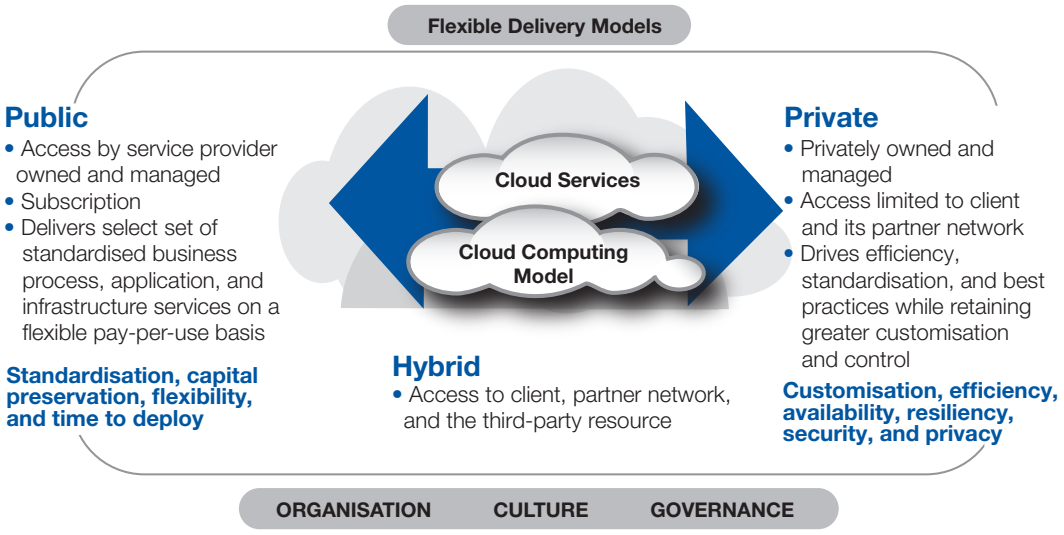

Figure 1. Public and Private Delivery Models

Design Guide

This section discusses security issues inherent in the cloud environment. These issues are followed by evaluation guidelines to consider before implementing a cloud solution.

Infrastructure as a Service

As the name implies, IaaS is a means of provisioning an infrastructure of computing resources and network in a co-located, multi-tenant environment. Various CSPs offer some subtle and some not-so-subtle differences in the ways in which they provide that infrastructure. Virtualisation technology plays a key role in IaaS offerings and may be deployed by using proprietary, open-source, or modified open-source technologies. Potential customers should evaluate IaaS services with an eye to compatibility issues that may occur should the need arise to migrate to a different CSP.

IaaS is offered as a common component-based subscription service in which services are typically accessed from the public Internet in several ways:

- A Web browser portal.
- CSP.
- Direct connection to an exposed system through a given service interface (e.g., Secure Shell (SSH), Secure Sockets Layer (SSL) Remote Desktop Protocol (RDP)).

Some CSPs also provide services that, in effect, extend a corporate intranet into their cloud IaaS in what is usually referred to as a virtual private cloud. These deployments are generally implemented through the use of a secure LAN-to-LAN tunnel, such as an IPSec router-to-router connection. The intent is to realise some of the benefits of elastically expanding intranet resources as needed while retaining some of the added security of limiting access into the Internet CSP's environment.

Factors such as flexibility and low cost create a yearning by large and small companies toward IaaS virtualisation, in which a quickly established, fast, and scalable purchased service is free of the costs associated with establishing, staffing, and maintaining an in-house infrastructure.

Platform as a Service

PaaS provides a cloud-based development platform which customers can use to develop SaaS-based applications. PaaS tends to offer a bit more flexibility for implementing security into the design of the application than, say, SaaS, but the interfaces should be well understood, providing a means for strong authentication and encryption, where required. Additionally, with PaaS as well as SaaS (and even, in some respects, IaaS), lock-in may be a risk because the customer is building applications with the cloud provider's tools and storing the data in their cloud. Should the company go out of business or increase their costs, it may not be easy to make a transition to another provider.

Software as a Service

It is imperative that the architecture be understood, especially in the ways that the capabilities align to a given set of requirements. For example, field- and record-level encryption may be offered, but not necessarily for all of the fields or records that a given customer requires. SaaS does not offer much flexibility, but rather, what you see is what you get.

Unknown Risks

Cloud computing is complex, encompassing many aspects of information technology. From a security point of view, the combination of complexity with a young market adds considerable risk. Because of the uncertainty involved in cloud computing implementation, customers and suppliers are both trying to reduce their risks. From the perspective of liability, early adopters have not yet established the middle ground. Contractual language, too, must be well vetted to ensure a thorough understanding by all parties of responsibilities and damages.

Security models for cloud computing are immature. Although we expect common accepted practices and standards to emerge, it hasn't happened yet. Early wholesale adopters of cloud computing are putting their company's intellectual property and financial assets on the line when they reach out to enjoy the immediate gains promised by cloud computing. We can count on early adopters to drive out concrete answers to questions about risk, liability, and true costs. In time, those companies will have valuable insights about short-term gain versus long-term loss to share. But the question a company needs to ask is: do you want to be one of them? Companies looking into cloud computing must realise that this is an analysis, not of a single technology or service, but of an entire analysis of IT and a new and somewhat debatable architectural approach for the consumption of these technologies and services. Also, while there are commonalities of the many cloud service offerings, no two are identical, so each case must be scrutinised separately.

In situations in which unknown factors cause risk, a policy of starting slowly is beneficial. For example, by starting with an internal cloud, a business can realise some of the benefits of cloud computing, such as rapid, self-provisioning, and pay-per-use IT cost accounting. Along with these near-term business benefits, this approach allows an IT team to become more familiar with cloud technology, continually increasing efficiencies in a secure manner while allowing the external CSPs, and the industry in general, to mature its model.

As soon as this strong internal foundation has been established and the external approach and technology service offerings have matured, an even more robust and cost-efficient approach can be realised through either a completely external service offering for a given collaborative project or a hybrid model that allows for an elastic bursting and withdrawal of computing resources in an external cloud.

Risks Related to Isolation

Because cloud computing involves users from different trust domains drawing on shared resources, the issue of multi-tenancy generally is at the heart of most defence-related cloud efforts. The basic approach in the market today is based on colouring (also called tagging or labeling) and enforcement of isolation between domains (also called zones) of different colours. This isolation can be implemented at various layers. Table 2 shows options for isolation at the server, network, and storage layers.

Table 2. Isolation Layers

Type	Option	Examples
Server	Hypervisor	z/VM LPAR pHype Xen VMware ESX
	Hypervisor-level security services	
Network	Security zones	
	Trusted virtual domains	Provisioning
	VLAN	IEEE 802.1Q
	Trusted and secure virtual private networks (VPN)	
	Encryption of data in transit	SSL/TLS SSH IPSec
Storage	Label-based access control (LBAC)	
	Storage zoning	Virtual storage area network (VSAN)
	Logical unit (LUN) masking	
	Encryption of data at rest and key management	Backups Maintenance
	Clean-up	Caches Files Disks Backups
	Fully homomorphic encryption	

Confidentiality and Integrity

Because CSPs maintain the security controls, your company will find it difficult at best to have complete assurance that all attack vectors have been mitigated. Customers must trust their CSPs, relying on the service contract to establish restitution in the case of data loss.

Most CSPs encrypt data in transit, offering SSL Transport Layer Security (TLS) or virtual private network (VPN) LAN-to-LAN capabilities. Encrypting data at rest is more challenging but generally achievable. It must be understood whether data encryption is being offered according to the customer's requirements. One area that poses a challenge for confidentiality and integrity is encryption of the data while in compute (i.e., during processing). This aspect exemplifies the 'implied trust' of the virtualisation layer (VMM/hypervisor), as this challenge will likely remain for quite some time.

Ensuring the protection of all encryption keys and maintaining control of those keys is ideal, especially when looking into a storage-type offering. Consider pushing for mutual authentication for SSL/TLS and Extended Validation Certificates to provide additional mitigations. This approach is also appropriate for signed API calls and the keys providing the security, whether IaaS, PaaS, or SaaS. Unfortunately, this option may not be offered because the business model for CSPs tends to cater to multiple customers using a shared, co-tenant, co-mingled infrastructure, again, relying on economies of scale.

Today, the vast majority of authentication to a CSP is by means of weak security mechanisms such as static user ID and passwords. Accounts are provisioned and access to specified resources is granted through the use of a customer administrator account. In general, users connect to the CSP Web portal and log in using their user ID and password credentials. A better approach would be through a combination of strong multi-factor authentication (e.g., secure token or smart card), a Web single sign-on solution, and Security Assertion Markup Language (SAML) assertions. Some CSPs (mostly in the PaaS and SaaS environments) support single sign-on solutions such as SAML. OpenID, however, is more prevalent, but the consensus seems to be that this technology is not really intended for an enterprise at this time. Some CSPs have realised this and are beginning to offer an additional layer of authentication security by combining the user ID and password approach with a security token (generated by using a one-time key fob), but the customer must usually request this separately from CSPs that provide this capability.

Legal Challenges

In the vast majority of use cases for IaaS, PaaS, or SaaS, customers must understand that they are, in effect, handing over the control of the controls to a third party and that some trust is required. In situations like this, customers generally look to a legally binding contract to provide the mitigation, but it should be well understood that, in this situation, the contract does not come into effect until after a breach takes place (e.g., data is lost, stolen, seized, or corrupted, or an extended outage has taken place). A contract provides no mitigation whatsoever, but it does offer a means of recouping financial losses. Even that can be less than desired. For example, a startup company may sign a contract agreeing to legal and fiscal responsibility, but if the value of the data is greater than the worth of the startup company, then the compensation may be insufficient on a number of levels.

Trust is a key factor with a third party as is always the case during collaborations. For example, we trust that the individuals with whom we hold a nondisclosure agreement or proprietary information agreement will not anonymously post our discussion to a Web site or betray our trust in any other way. We trust that CSPs protect our data; however, in most cases, customers do not research the protections that the CSP provides. To get an idea of a CSP's security controls and their effectiveness, you can request that the CSP provide you any audit reports (e.g., SAS 70 Type 2). The following Physical Security section describes this concept in more detail.

Jurisdiction, Regulation, and Investigation

A number of legal issues relate to cloud computing technology. Some affect jurisdiction. On the one hand, data may be susceptible to search and seizure based on the laws of the hosting country where the data resides (e.g., the U.S. Patriot Act). On the other hand, the co-location and co-mingling of data may make it practically impossible to identify the exact location of data and, therefore, may not meet some regulatory requirements. There is an implicit trust with the underlying architecture and technologies, such as the database controls for the PaaS and SaaS environments and the virtualisation layer for the IaaS environment. It is difficult to prove that security controls are sufficient, especially when no two deployments are the same. Because of this, it is unreasonable to assess them all with much assurance. Investigations may be difficult. It is unlikely that any full penetration testing will be allowed. Because of this, CSP customers must ensure that their contractual agreements allow for an appropriate sharing of audit information and system logs in addition to a collaborative approach to investigations and incident response. Companies may find it difficult to receive the kind of support required to perform a thorough investigation, including the degree to which log files and other records can be provided and scrubbed of data unrelated to the company that performs the investigation. Also, somewhat obvious, assurance must be offered that a customer's data has been scrubbed when another customer requires an investigation.

Physical Security

Physical security should be well vetted for a third-party data center, but it is still important to ensure that appropriate security controls are in place to protect the life cycle of the data. These areas include proper control and handling of tape backups while in transport, and offsite storage. Elements to query CSPs relate to encryption of data on tapes, reuse of tapes, and processes for destroying tapes and other long-term storage devices. Additionally, data centers should have appropriate security controls for physical access which includes customer isolated caged areas or rooms within shared data centers that mitigate not only door access into the area, but also above ceiling and below floor mitigations.

Depending on the requirements, it may be appropriate to rely on a third-party assessment report such as SAS 70 Type 2, but the criteria used for the SAS 70 Type 2 should also be requested to clearly understand the controls that are measured. Because a large percentage of CSPs host their environments at known third-party data centers, there may already be a strong precedence that a SAS 70 Type 2 report and criteria would help to validate as to the security posture of the data center; however, if the CSP provides no information, then a site assessment may be more appropriate. Some CSPs may be willing under these circumstances to negotiate a physical site assessment.

Privileged Identities

Within the defence community, next to multi-tenancy the issue of privileged identities is a top security concern. Given that cloud administrators require privileged (i.e., root) access to cloud and client resources, any reasonable policy demands strong accountability for administrator actions. However, the volume of managed systems grows almost exponentially in a cloud environment, and typical polices do not scale when they require distinct identities for each environment. This issue affects both policy and technology. Several possible approaches can address this issue: 'reverse single sign-on', a SME type of privileged identity management (PIM) system that manages all privileged accounts where the PIM does log on and log out. In this situation, the administrator never sees passwords. The administrator must also check out privileged accounts.

Opportunities to Simplify Security Controls and Defences

Table 3 demonstrates some ways that cloud computing offers benefits not possible in other environments.

Table 3. Benefits

Aspect	Cloud-Enabled Controls	Benefit
People and identity	Defined set of cloud interfaces Centralised repository of identity and access control policies	Reduced risk of user access to unrelated resources
Information and data	Computing services running in isolated domains as defined in service catalogues Default encryption of data in motion and at rest Virtualised storage providing better inventory, control, tracking of master data	Improved accountability Reduced risk of data leakage and loss Reduced attack surface and threat window Less likelihood that an attack would propagate
Process and application	Autonomous security policies and procedures Personnel and tools with specialised knowledge of the cloud ecosystem SLA-backed availability and confidentiality	Improved protection of assets Increased accountability of business and IT users
Network server and endpoint	Automated provisioning and reclamation of hardened runtime images Dynamic allocation of pooled resources to mission-oriented ensembles	Reduced attack surface Improved forensics with ensemble snapshots
Physical infrastructure	Closer coupling of systems to manage physical and logical identity and access	Improved ability to enforce access policy and manage compliance

Additional Considerations

A Bigger Target Is Easier to Hit

A single CSP location is likely to house data for multiple companies (e.g., government agencies, defense contractors, and other high-value corporations). This target-rich environment makes the opportunity much more tempting. In security circles, it's well understood that there is no perfect security and that, given enough time and resources, anything can be exploited. By sharing an environment, even with security segregation, the target becomes much more interesting to those willing to attack.

The Neighbour Next Door

Multi-tenancy should be a concern for any company considering using a CSP. Again, this relates to the issue of trust: in particular, trust that the security controls are sufficient. It's a very real possibility that your cloud neighbour could be a group such as the Russian Business Network (RBN), which uses stolen credit cards to purchase the resources and are, in effect, untraceable.

Proprietary and Open Standards

Open standards may help, but they do not guarantee that your exit strategy will not prove difficult and costly to execute. Just as important is understanding the CSP's architecture to ensure that their environment, whether using proprietary or open source software, has been created in such a way that migration to another provider is not cost prohibitive or impossible; otherwise, a company runs the risk that their data could be lost entirely. Each SaaS company is likely to develop its own schemas regardless of the technology used to implement them. For example, if a CSP goes bankrupt, the customer may (if they're fortunate) receive a character-delimited file containing their data, but they will then have to find a company that can either import this file and build a schema to support it or build it themselves.

Information Security Checklist

Based on the issues inherent in cloud computing, consider these questions as you explore the idea of adopting cloud technology.

Information Security

- How does the data get to and from the cloud service?
- How is it protected while there?
- How is access authenticated?
- How are access decisions made?
- How is access audited?
- What separation exists between customers at the application, operating system, and disk level?

Interoperability

- How do I collaborate with partners who use different CPSs?
- Who owns the intellectual property developed in a cloud service?
- Most providers will return your data, but are you prepared to lose any investments in building applications or services in the cloud?
- If my company switches providers, would we be prepared to rebuild our IT environment from the ground up with an all-new infrastructure and data restored from backup tapes?

Short-Term Service Availability

- How does the contract guarantee uptime, and what protections are in place to prevent short-term outages caused by software or hardware failures or denial of service (DoS) attacks?
- Risks
  - Will my company become collateral damage from a DoS attack against others?
  - How does a short-term outage affect my application?
  - What happens to my customer base during an outage?
- What applications are suited for an IT model that
  - Communicates by using the public Internet?
  - Operates on data off site?
  - Is subject to instability?

Long-Term Service Availability

- How would my company address long-term outages that could include loss of data for months or years?
- Most cloud service providers co-mingle data from many customers on the same physical disks.
  - What happens when one of those disks is seized by law enforcement because of illegal activity on the part of another client?
- What happens when I build applications in the cloud and the CSP goes out of business or is bought by a company which shuts down or radically changes the service?

Policy Issues

- How do you enforce your corporate security policy in the cloud?
  - Incident visibility, governance, audit ability, forensics, and investigation.
  - Inbound-outbound perimeter services to support managing clouds.
  - Proxy perimeter connections and TCP forwards.
- Who runs the cloud?
  - Are background checks performed and adhered to?
  - Is support for the cloud outsourced? If so, by whom, and do they perform background checks?
- What happens if there is a change of third parties?
- Who has access to your data in the cloud?
  - Disgruntled employees?
  - Social engineering and (corporate) espionage?
  - Foreign nationals?
- Co-mingled data and environments
  - How does the CSP prevent data leakage (e.g., when consumer X wants to audit their environment, what prevents a compromise of consumer Y's data)?
- Access provisioning
  - Cloud administrators, image and service administrators, image and service consumers (local administrators).
- Lock-in resulting from proprietary cloud deployments (e.g., in situations in which it may not be possible to move an SaaS application developed using a proprietary PaaS to another CSP provider).
- Data disposal and long-term data archival
  - Are disks destroyed or made unreadable?
  - Is the data guaranteed to be available years down the road?

Worldwide Privacy Issues

Consistent application of data privacy laws would go a long way toward driving important and needed technology solutions; however, in this area we see significant variation. To the extent that your company supports global customers, your legal department must be alert to the wide variety of data privacy issues. On the other hand, if you use a CSP, you may also need to understand how international data privacy laws could affect your data. Figure 2 shows a worldwide map that demonstrates the kind of variation that exists.

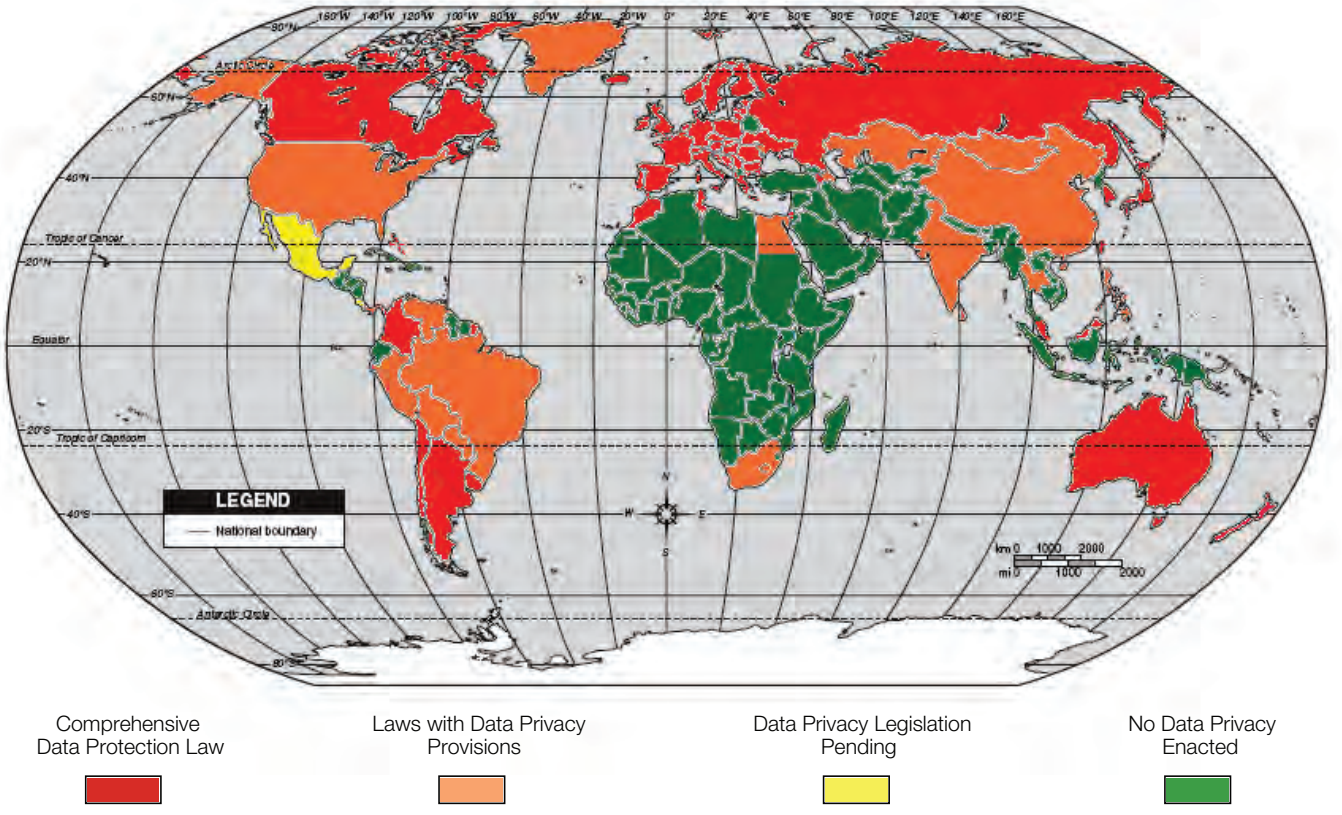

Figure 2. International Privacy Overview

Stability

Figure 3 evaluates the state of the art for cloud computing based on a large, complex company's business requirements.

	Capability maturity	Information risk	Relative effectiveness of technical controls	Relative effectiveness of contract controls	Inter-operability risk	Difficulty of enterprise integration
Services	Mature	Immature	Immature	Mature	Mature	Mature
Application	Stable	Immature	Stable	Mature	Immature	Immature
Development	Stable	Stable	Stable	Stable	Immature	Stable
Platform	Stable	Immature	Stable	Stable	Stable	Stable
Storage	Mature	Stable	Mature	Mature	Mature	Stable
Hosting	Mature	Mature	Mature	Mature	Mature	Mature

Mature Stable Immature

Figure 3. The State of the Art for Cloud Computing

Guidelines

If you are considering cloud computing, ask these questions about information security (figure 4):

Figure 4. Information Security Issues

Guidelines (continued)

As you consider service interoperability, ask these questions (figure 5):

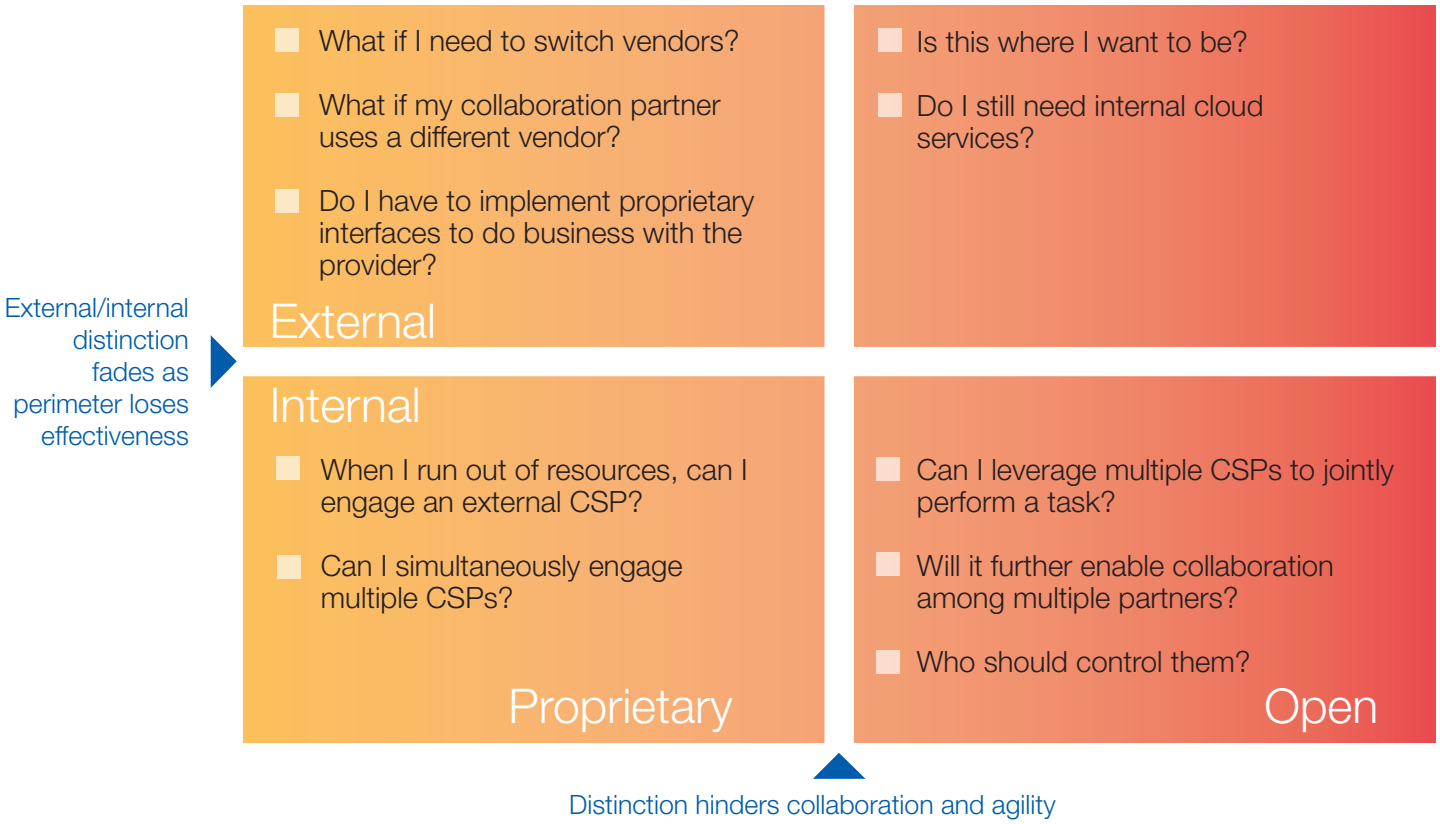

Figure 5. Service Interoperability

Recommendations

Cloud computing is at the height of its popularity as an exciting but untested environment which promises low costs, increased flexibility, and improved productivity. That said, your company should explore the technology before implementing it completely.

Strategy

One sensible strategy is to develop long-term intentions and short-term tactics to address grid, cloud, and utility computing efforts for delivering utility IT services to your company. Any IT solutions that use cloud services should be able to offer a fast start, optimised demand management, and guaranteed secure capabilities. The business value of cloud services, which is the primary driver for this new technology, must deliver concrete gains.

Tactics

These are examples of tactical plans that can be used to implement cloud computing:

- Determine foundational characteristics of cloud computing and its relationship to both your company's existing computing strategies and tactics.
- Inventory emergent cloud services from your company's IT strategic suppliers and map to application and infrastructure domains.
- Learn from initial pilots and prototypes of cloud and grid computing in limited environments.
- Develop the potential considerations, if any, of cloud services on the next-generation plans for your data centers.
- Evolve a preliminary cloud services roadmap by leveraging current initiatives on virtualisation, service orientation, and utility computing.

Use Cases

Table 4 describes specific use cases that your company can evaluate:

Table 4. Use Cases

For this model...	And this environment...	These use cases...
Information as a Service	External provider	• Virtual labs • Training • Backup and storage
	Internal (possible bursting external)	• Development and test environments • Partner collaboration • High-performance computing • Desktop virtualisation • Backup and storage
Platform as a Service/ Software as a Service	External provider	• Sales force • Metrics

Summary

By understanding the hype related to cloud computing, companies can protect their intellectual property and other valuable assets from the pitfalls that may lie ahead. An exploration of both internal and external clouds should start with virtualisation as an enabler, leveraging existing technology aggressively. It is possible to take a leadership role in terms of exploring the technology to identify solutions for your company and your customers while also carefully following security best practices.

Contributors

Federico Genoese-Zerbi
Vice President, IT Business Partners, The Boeing Company
Herbert W. Canfield
CISSP, Senior Manager, Federal Programs & Cyber Business Support, The Boeing Company
Jeffery P. Dion
Senior Analyst, Information Security (IS), The Boeing Company
Stephen Whitlock
Technical Fellow and IS Chief Strategist, CISSP, IS, The Boeing Company

Special thanks to Peter Jopling of IBM for his review and contributions to this document.

Reading List

Dan Blum, *Developing a Cloud Computing Security Strategy*, Burton Group, 2010 (client access only)

'Business case for Software as a Service', Intellect, October 2009
http://www.intellectuk.org/content/view/5534/84

John Byrne,'Jeff Bezos' Risky Bet', *Bloomberg Businessweek*, 13 November 2006
http://www.businessweek.com/magazine/content/06_46/b4009001.htm

Cloud Computing Initiative, Gartner, Inc.
http://www.gartner.com/technology/initiatives/cloud-computing.jsp

Steve Lohr, 'Google and I.B.M. Join in 'Cloud Computing' Research', *The New York Times*, 8 October 2007
http://www.nytimes.com/2007/10/08/technology/08cloud.html?_r=3&ex=1349496000&en=92627f0f65ea0d75&ei=5090&partner=rssuserland&emc=rss&oref=slogin

John Markoff,'Internet Critic Takes on Microsoft', *The New York Times*, 9 April 2001
http://www.nytimes.com/2001/04/09/technology/09HAIL.html?ex=1217563200&en=7c46bdefb6a8450a&ei=5070

Scott Morrison, 'Visualizing the Boundaries of Control in the Cloud', *Cloud Computing Journal*, 25 January 2010
http://cloudcomputing.sys-con.com/node/1206665

Amy Schurr, 'Keep an eye on cloud computing', *NetworkWorld*, 8 July 2008
http://ocw.mit.edu/courses/sloan-school-of-management/15-571-generating-business-value-from-information-technology-spring-2009/

Glossary

API	application programming interface
CRM	customer relationship management
CSP	cloud service provider
DoS	denial of service
IaaS	infrastructure as a service
IPSec	Internet Protocol Security
LAN	local arera network
LBAC	label-based access control
LUN	logical unit
PaaS	platform as a service
PEP	policy enforcement point
PIM	privileged identity management
PKI	Public Key Infrastructure
RBN	Russian Business Network
RDP	Remote Desktop Protocol
SaaS	software as a service
SAML	Security Assertion Markup Language
SAS	Service Auditing Standard
SLA	service-level agreement
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UKCeB	United Kingdom Council for Electronic Business
VLAN	virtual local area network
VM	virtual machine
VMM	virtual machine monitor
VPN	virtual private network
VSAN	virtual storage area network