

opinion piece

dimension
data 

Securing the Cloud with Confidence



Contents

Introduction	01
Don't outsource what you don't understand	01
Steps towards control	02
Due diligence	02
E-discovery	02
Standards	03
Privacy	03
Business continuity	03
Application development	03
Identity	03
Virtualisation	03
Practice first	03

Today, it's widely accepted that cloud computing promises a number of opportunities for efficiencies and cost savings. By tapping into the cloud you can swiftly access business applications and enhance your infrastructure resources, at a reasonable cost. According to a 2010 IDG survey of 100 security executives around the world, upwards of 30% of large businesses have some enterprise applications in the cloud. More than a third of businesses have increased their use of cloud computing in the past two years.

Also interesting – and somewhat alarming – is the fact that two-thirds of the organisations surveyed do not have a security strategy for cloud computing.

Security in the cloud is actually more complex than traditional IT infrastructure and consumption models. Until now, most organisations have kept their hardware and software resources firmly under their own control. Even if they outsourced some or all data centre functions, their resources were located in a data centre and someone was being paid to keep a watchful eye over them. In the cloud, you are not in control of where your data resides, how it is processed, how it is destroyed, or who has access to it. When you move to the cloud, your data could conceivably be sitting on the same server as your competitor's. Rather than having direct or even indirect control over your data, you are essentially at the mercy of your provider.

Adding to the complexity is the fact that even though you are not in control of the technology in the cloud or the management of that technology, the onus for mitigation of risk still rests firmly on your shoulders.

Don't outsource what you don't understand

In order to move forward on your journey to the cloud with confidence, you need to ensure that you have a thorough understanding of your own security requirements upfront. This will allow you to select the provider whose environment best supports your needs.

This means undertaking a thorough assessment of your organisation's inherent risk, painting a scenario based on the required organisational changes as well as your appetite for managing additional risk in return for tangible business benefits – and using this information to determine whether your internal security environment passes muster.

Performing such an assessment will provide you with clarity as to what security your vendor will need to have in place in order to keep your data safe. Then it's a question of mapping your security needs to vendor capabilities.

Organisations' responsibility for security doesn't end here, however. There are currently no specific cloud computing standards. The Cloud Security Alliance, whose aim is

“to promote the use of best practices for providing security assurance within Cloud computing, and provide education on the uses of cloud computing to help secure all other forms of computing”,

has made some strides in documenting the issues and some solutions. That said, the lack of universally-accepted standards means that organisations cannot look to an industry body to regulate cloud security.

This means you'll need to do your own policing vendors' security environments.

Your checklist

The fact that there are no fewer than fifteen disciplines, in three overarching groups, that need to be addressed, means that gauging vendors' security capabilities is no mean feat.

The first grouping covers **governance, risk, and compliance** and includes legal and e-discovery, compliance and audit, business continuity and disaster recovery, and incident response, notification, and remediation.

The second addresses **architecture and operations** and incorporates security architecture, information lifecycle management, portability and interoperability, data centre operations, storage, and virtualisation.

Group three addresses **identity and access management** through key management and encryption, and application security.

According to an IDG survey of **100 security executives around the world**, upwards of **30% of large businesses** have some enterprise applications in the cloud. More than **a third of businesses have increased their use of cloud computing in the past two years.**

Most organisations struggle to acquire and retain the broad skills required to deal with these issues inside their own organisations, let alone at an external provider location. In addition, each of the areas is influenced by the characteristics that differentiate cloud computing from traditional computing models. These include abstraction of infrastructure, resource democratisation, services oriented architecture, elasticity/dynamism of resources, and a utility model of consumption and allocation.

The situation is complicated still further by the fact that the cloud offers three different service delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) – as well as four types of deployment and consumption: Private, public, managed, and hybrid.

It is critical to be aware of the trade-offs between extensibility (openness) and security responsibility within the three service delivery models.

SaaS provides least extensibility and greatest security responsibility taken on by the cloud provider, with the organisation's security department losing control of:

- Physical and logical network barriers
- Endpoint restriction and management
- Non-password authentication
- Fine grained credential quality controls
- Password reset processes
- Real time anomaly detection
- Event logging

By contrast, IaaS offers the greatest extensibility, and the level of security responsibility taken on by the cloud provider is minimal. PaaS falls somewhere in between.

SaaS and PaaS providers all assert the robustness of their systems, often declaring that security in the cloud is tighter than in most organisations. But then again, every security system that has ever been breached was once thought infallible. For example, Google's Gmail service collapsed in Europe in February 2009. Recently, Amazons' EC2 service was the target of a zombie attack.

Steps towards control

Begin with the basics. Getting into technical detail too early will obscure the fundamental issues.

Due diligence

As an initial step, perform an extensive, in-depth due diligence exercise on the cloud provider you are considering. As is often the case with disruptive technologies, the law lags behind the technology development for cloud computing. Also, there's the question of jurisdiction. Data may be secure in one country but not in another. In many cases, users of cloud services don't know where their information resides.

Remember too that contracts are your key legal enforcement mechanism and must, therefore, be negotiable to reflect your specific needs, while still aligning to the dynamic nature of cloud computing. Contracts should include provision for both an expected and an unexpected termination of the relationship and for an orderly return or secure disposal of assets.

E-discovery

While cloud providers are custodians of primary data assets, their customers, who own the data assets, are legally responsible for preserving the data and making it available in legal proceedings (e-discovery). It is essential therefore, that organisations and their cloud providers have a clear and mutual understanding of their respective roles and responsibilities related to e-discovery, including activities such as litigation hold, discovery searches, and the provision of expert testimony.



Standards

Given the absence of security standards specific to the cloud, organisations should ensure that their providers comply with, at least, the SAS70 auditing standard and ISO27001, which is designed to provide the foundation for a third party audit and implements OECD principles governing security of information and network systems.

Be sure that you understand data locations – specifically, the copies of data that are made and how they are controlled. Importantly, maintain a right to audit on demand, as regulatory mandates and business needs can change rapidly.

Privacy

Your cloud provider should have a thorough understanding of the privacy restrictions inherent in the data entrusted to it. The possibility exists that the cloud provider may not be permitted to hold the data without very specific partner designations.

Business continuity

The technology architecture infrastructure of cloud providers in terms of business continuity and disaster recovery will naturally differ. Nevertheless, providers should be able to demonstrate comprehensive compartmentalisation of systems, networks, management, provisioning and personnel. And, of course, your own business continuity plans should take into account the impacts and limitations of cloud computing.

Application development

For application security, remember that IaaS, PaaS, and SaaS create differing trust boundaries for the software development lifecycle and they must be accounted for during the development, testing and production deployment of applications.

Identity

Key to managing identities when using the services of cloud providers is a robust, federated identity management architecture and strategy internal to your organisation. Insist that the vendor operates according to federation-enabling standards such as SAML, WS-Federation, and Liberty ID-FF. Consider implementing single sign-on for internal applications and then leveraging this architecture for cloud applications.

Virtualisation

Virtualisation does offer certain security advantages – such as creating isolated environments and better defined memory space – which can minimise application instability and simplify recovery. Nevertheless, organisations should augment virtualised operating systems with third party security technology to provide layered security controls and reduce dependency on the platform provider alone.

Practice first

Adopting a staggered approach is perhaps the most basic tenet of cloud security. Consider opting for a private cloud as a first step, virtualising your internal operations and using in-house and therefore already authorised personnel, to establish a working cloud methodology that can be extrapolated to a public cloud as your business needs – and your confidence – grows.

Your cloud provider should have a thorough understanding of the **privacy restrictions** inherent in the data entrusted to it. The possibility exists that the cloud provider may not be permitted to hold the data without very specific partner designations.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • GHANA • KENYA
MOROCCO • NAMIBIA • NIGERIA
SAUDI ARABIA • SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES