



Cloud Computing Security Considerations

Roger Halbheer, Chief Security Advisor, Public Sector, EMEA

Doug Cavit, Principal Security Strategist Lead, Trustworthy Computing, USA

January 2010

Introduction

This paper provides a high-level discussion of the fundamental challenges and benefits of cloud computing security, and raises some of the questions that cloud service providers and organisations using cloud services need to consider when evaluating a new move, or expansion of existing services, to the cloud. This document presumes that the reader is familiar with the core concepts of cloud computing and basic principles of cloud security. It is not the goal of this paper to provide all the answers to the questions of security in the cloud or to provide an exhaustive framework for cloud security.

Key Security Considerations

As with any other technological shift or change, security benefits and risks need to be addressed before the full benefits of cloud computing can be realised. Considerations such as compliance and risk management; identity and access management; service integrity; endpoint integrity; and information protection should all be explored when evaluating, implementing, managing, and maintaining cloud computing solutions.

- *Compliance and Risk Management:* Organisations shifting part of their business to the cloud are still responsible for compliance, risk, and security management.
- *Identity and Access Management:* Identities may come from different providers, and providers must be able to federate from on-premise to the cloud, as well as to enable collaboration across organisation and country borders.
- *Service Integrity:* Cloud-based services should be engineered and operated with security in mind, and the operational processes should be integrated into the organisation's security management.
- *Endpoint Integrity:* As cloud-based services originate--and are then consumed--on-premise, the security, compliance, and integrity of the endpoint have to be part of any security consideration.
- *Information Protection:* Cloud services require reliable processes for protecting information before, during, and after the transaction.

While they bring many potential benefits, services provided through cloud computing may also create new concerns, some of which are not yet fully understood. Adopting a cloud service may also require IT organisations to adapt to data management no longer under their direct control. This is especially true in a "hybrid model" in which some processes remain on-premise and some are in the cloud, requiring new and extended security processes that encompass multiple providers to achieve comprehensive protection of information. Risk management and security management remain the responsibility of any organisation, but should be extended to include the cloud provider(s).

Clear strategies related to these five considerations¹, as well as a strong service-level framework, will help to ensure that implemented services deliver cloud computing functionality that meets security requirements and business expectations.

¹ These are just some of the question areas which must be considered. Further details and advice on cloud computing in general can be found in the papers from The Cloud Security Alliance and ENISA.

Compliance and Risk Management

In an on-premise computing system, organisations have primary control over how the environment is built and run. In an “off-premise” cloud (provided by a facility not run or managed by the organisation), responsibility is delegated to the cloud provider. This can cause new and unique challenges, such as delegating parts of the organisation’s fundamental compliance and risk management processes and entrusting them to a cloud provider.

*Compliance requirements can be fulfilled by a **skilled internal team** and a certain level of **process transparency** by the cloud provider(s).*

By no means does this delegation of responsibility discharge IT organisations from managing risk and compliance. In fact, cloud services providers often exclude compliance responsibility in their agreements. Organisations continue to be responsible

for proving policy compliance through their own business processes.

Working with different cloud providers to integrate and/or distribute risk and compliance management controls requires some level of transparency into the provider’s operations. Striking the right balance between transparency and the provider’s confidentiality presents a challenge. Yet, transparency is essential for building trust with service providers while maximising an organisation’s ability to meet its obligations. The customer requires enough process transparency to make informed risk decisions—which will vary depending on the sensitivity of the data to be protected—while allowing the provider to protect its proprietary systems and processes.

Once visibility into the cloud provider’s controls is achieved, the organisation’s internal team can integrate these controls into their own risk and compliance management and security management environment. Given its invaluable expertise and unique understanding of the organisation’s compliance needs, this team should typically be included in the contract negotiations with any cloud service provider(s).

During planning, organisations should consider additional forward-looking logistical questions, such as: Does the organisation retain the option of returning part or all of the service back to on-premise management in the future, or move all or part of the service to a different cloud service provider? What are the associated costs of such a change? How does the organisation ensure that all the data (including backups) previously stored on the provider’s premises are permanently deleted? How can access to data be gained if there is a dispute with the cloud provider?

Identity and Access Management

Cloud-based services require secure cross-domain collaboration, with protections against the misuse of the identities of people and devices. Any system for identity and access control, especially for

*Any digital identity system for the cloud has to be **interoperable** across different organisations and cloud providers and based on strong processes.*

higher value assets, should be based on an identity framework that uses in-person proofing, or a similarly strong process, and robust cryptographic credentials. These credentials help enable a “claims-based” access control system, which authenticates the claims made by any entity in the system. The strength of that authentication system should be reasonably balanced with the need to protect the privacy of the users of the system. To

help achieve this balance, the system should allow strong claims to be transmitted and verified without revealing more information than is necessary for any given transaction or connection within the service.

Secure identity management is essential in any environment, but can become more complex in a cloud computing context. Cloud systems typically include multiple identity claims providers with separate processes that need to be understood and verified as trustworthy. Moving services to the cloud raises several questions: Who owns the identity? What controls surround identity and access management? Can the organisation change the claims provider? How does identity federation work with different providers? How is authentication and authorisation tied to identity? How can ad-hoc collaboration with people outside the organisation who work with different identity providers be established?

Any identity environment should be interoperable across applications that consume identity claims, and needs to enable the secure migration of data access controls to the cloud and back. This environment has to be manageable for the organisation as well as for an individual using cloud services.

Certifications and reputation systems for identity providers play a key role in helping each participant understand to which security level an identity provider can be trusted and held accountable. In this regard, a digital identity system with strong credential requirements that is able to validate users from both on-premise and cloud providers based on interoperable claims, could dramatically improve security and data integrity.

Service Integrity

Service integrity includes two components: 1) Service engineering and development; and 2) service delivery. Service engineering and development encompasses the way in which the provider incorporates security and privacy at all phases of development. Service delivery covers the way the service is operated to meet contractual levels of reliability and support.

Service Engineering and Development

Any organisation developing software should follow an engineering and development process to build security and privacy into its products. Engineering and development for cloud computing environments is no different in this regard, and requires a process that emphasises security and privacy as applications and software are built—whether by an organisation's development group, or by the cloud provider and/or third parties. While a cloud operator can bring the benefit of consolidated security expertise, it is also important to ensure that the provider's development and maintenance processes integrate security and privacy into each phase of development. Microsoft uses the Security Development Lifecycle for application development, and has extended the stages outlined below to development in a cloud computing environment.

*The provider should follow a **clear, defined, and provable process** to integrate security and privacy in the service from the beginning and for the whole lifecycle.*

- **Requirements.** The primary objective in this phase is to identify key security objectives and otherwise maximise software security while minimising disruption to customer usability, plans, and schedules.
- **Design.** Critical security steps in this phase include documenting the potential attack surface and conducting threat modelling.
- **Implementation.** During this phase, the development team must take steps to ensure that there are no known security vulnerabilities in the code by adhering to specific coding standards, and by applying analysis tools to the evolving software.
- **Verification.** During this phase, the team must ensure that the code meets the security and privacy tenets that were established in the previous phases. The team must also complete a public release privacy review.
- **Release.** A final security review happens during this phase. The review helps to determine whether the product is secure enough to ship by ensuring that the software complies with all standard security requirements and with any additional security requirements that are specific to the project.
- **Response.** After software has been released, there should be a security response group in the provider that identifies, monitors, resolves, and responds to security incidents and Microsoft software security vulnerabilities. The provider should also manage a company-wide security update release process and serve as the single point of coordination and communications.

When evaluating a cloud services provider, questions should be asked about the specifics of the provider's secure development process. The process should reflect each of these generic phases, as each area is critical to the overall secure development process. There should also be discussion about the on-going nature of this security process, including how often threat models are updated, how functional the security response group is, how the customer is informed about security updates, etc.

Service Delivery

If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed. These

The service delivery capabilities of the provider and the security management and auditing needs of the customer must be aligned.

include processes such as security monitoring, auditing, forensics, incident response, and business continuity. This collaboration must be covered during the initial cloud delivery setup between the customer and the cloud provider, taking both parties' needs into consideration. For certain applications or services, service security requirements are fairly simple and straightforward. Yet for other services (such as those involving high-value assets), more stringent requirements have to be considered and established, including physical security requirements, additional logging, deeper background checks for administrators, etc.

Any cloud service agreement should include a detailed plan for managing performance problems and conducting network and image forensics as needed, and should include specific response contacts and processes for restoration in the event of interruptions in service delivery. Finally, the agreement should define which security monitoring and auditing capabilities will be provided by the cloud services and at what price.

End Point Integrity

Discussions of cloud security frequently focus on the service itself, as well as the provider's security quality and practices. But failure to evaluate the entire service chain from beginning to end can introduce flaws in service design and delivery. Cloud services begin and end either within an organisation or at the personal computer or device of an individual using the service. In many cases when an organisation's security is compromised, the issues occur on individual workstations and not on the backend servers. To increase the trustworthiness of cloud computing end-to-end, the full spectrum of activity should be considered, to help protect users from threats including online identity theft, website cross-scripting attacks, phishing attacks, and malicious software downloads.

*It is very important to **include the end point** in any security consideration for cloud-based services.*

Most enterprises today have internal risk management programs with mitigations to protect the end points and manage information security. The infrastructure is well understood and visible to all levels of the environment. However, in a cloud computing environment, security measures and approaches should be reviewed, as cloud services may have dependencies on more than one service provider where the same level of visibility may not be available.

It is very important to consider how different services are brought together and consumed across an entire organisation and the multiple end point systems that are in place. If end point security is shifted to the provider, this raises some important questions such as: How are security and compliance requirements enforced? How is data protected against misuse? Will the customer still have the ability to use encryption or a rights management mechanism to protect data loss or theft? Can the service be restricted to specific authorised endpoints or machines?

Information Protection

The sensitivity of the data involved in the operation of a service is a critical factor in determining whether the service can be managed by a service provider, and if so, which access controls can be utilised to ensure compliance obligations are met throughout the transaction. Implementing a sound data classification approach to identify the sets of data involved in the transaction and determine the control mechanisms that apply to each under specific circumstances can help organisations make these decisions. Organisations need to determine their level of comfort with data handling and information management, no matter where the data is stored or how it is transmitted. This basic guideline also applies to on-premise environments today.

***Implemented Data Classification** helps to decide which data is ready for the cloud, under which circumstances, and with which controls.*

Additionally, it is important to be aware of several challenges surfacing with the delivery of cloud services, including data sovereignty, access to information, and data partitioning and processing.

Over the years regulations have been developed for the protection of data. These regulations are tied to specific jurisdictions—the limits, or territory in which authority may be exercised. With the advent of cloud computing, data may be stored outside of the originating territory or in multiple territories or locations. Hosting of data outside the customer's jurisdiction or co-location of data can present information management and access issues associated with the question of whom, or what entity, has "sovereignty" over the data. Some new cloud services today are trying to address these challenges by allowing customers to specify where data is physically stored.

When the management and control of information moves from one party to another, organisations can lose the ability to protect, retrieve, or move information. It is therefore important to understand who controls the identity and authorisation system for access to information, where the back-up data is stored, whether encryption of data is supported, what cost is associated with the encryption solution (e.g. feature loss), and how access to data is granted and managed if there is a dispute with the service provider. For example, are there guarantees that the service provider will not retain any data if/when the service is cancelled?

Finally, if data is stored in a “public cloud,” it may possibly reside on infrastructures shared with other organisations. Strong data protection practices can still be followed to ensure data is partitioned and processed appropriately. It is important for organisations to understand who has access to their data and to consider whether that risk is acceptable before they allow their data to be processed in the cloud. They also need to understand the architecture of the cloud service provider and to gain assurances about how shared virtual machines are secured against various forms of potential attack from other virtual machines on the same physical hardware being used by malicious individuals.

In Closing

In order to fully realise the opportunities enabled by cloud computing, several specific security elements should be addressed: process, skills, technology, and controls. Organisations embracing the cloud should consider the following practical points:

- A well-functioning compliance program for identities, data, and devices is essential before adopting cloud services.
- Data classification is a key requirement for evaluating risk and making informed decisions on whether to use cloud computing or not. Low-risk data can be put into the cloud with less concern than high-impact data, which requires stronger security and privacy controls.
- The choice of deployment model (private, community, and public) must be based on data classification, security and privacy requirements, and business needs.
- Even when fully embracing cloud computing, an organisation still needs a strong internal team to manage the security and compliance requirements together with the cloud provider(s).
- Transparency, compliance controls, and auditability are key criteria in the evaluation of any cloud service provider.
- Organisations must implement a secure development lifecycle methodology for applications that are hosted in the cloud, and should evaluate the cloud provider’s compliance to a similar process.
- Stronger credentials should replace usernames and passwords as the foundation of the access management system.
- Consideration should be given to information lifecycle controls that would limit access to information to only authorised persons and timeframes no matter where the data originates.
- Access controls for data need to operate across organisational boundaries—among different departments, outside vendors, governments, and consumers. Federated access across these

boundaries must be obtainable even when a customer does not directly manage the identity and authentication.

Related Reading

- Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing:
<http://www.cloudsecurityalliance.org/csaguide.pdf>
- ENISA: Cloud Computing Information Assurance Framework:
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/>
- Securing Microsoft's Cloud Infrastructure
<http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf>
- Security Considerations for Client and Cloud Applications
<http://go.microsoft.com/?linkid=9704049>
- Security in the Business Productivity Online Suite from Microsoft Online Services
<http://go.microsoft.com/?linkid=9671260>