Multi-Tenancy Security Risks

Customer Expectations for Leading Cloud Service Providers
– An Architectural Approach

Paul G Dorey
Summer 2014

Contents

Introduction

A common question in almost every business and IT function is whether the offerings of cloud service providers (CSPs) are more or less secure than information technology (IT) services that are delivered through internal, on-premise implementations. This is not unlike the very first reactions of IT functions in the 1990's when the idea of using outsourced services was first mooted. Since then we have come to accept that using service providers and outsourcers is a normal way of conducting business, and very few organisations – if any – stand entirely alone.

Cloud services is in many ways an evolution of outsourcing and by analogy many companies are treating the risks and means of control as just another outsourcing exercise. Yet this approach may be flawed, because true CSPs aspire to offer services to many customers that are delivered from a shared platform. The relationship is not 1:1. The 'multi-tenant' nature of the cloud therefore raises many different questions and concerns, especially when it comes to security.

The purpose of this white paper is to explore the risks that concern security practitioners and the security controls that cloud service providers are deploying to address them, particularly in the context of multi-tenancy. The findings are the result of the analysis of views gained from a series of workshops and roundtables held with security practitioners from companies drawn across a range of industry sectors. This has been combined with insights provided by advisory firm consultants with client experience with both cloud service providers and their customers. The end result, according to both the author (Dorey) and many other security practitioners (Forrester), is that multi-tenant cloud systems can be at least as secure as important types of on-premise system and may in some cases be even more secure.

> "Despite resource sharing, multitenancy will often improve security. Most current enterprise security models are perimeter- based, making you vulnerable to inside attacks. Multitenant services secure all assets at all times, since those within the main perimeter are all different clients. Leveraging a mix of dedicated resources and metadata map architectures, these services can deliver stronger security."
>
> *Understanding Cloud's Multitenancy, Forrester, March 2012*

Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST)

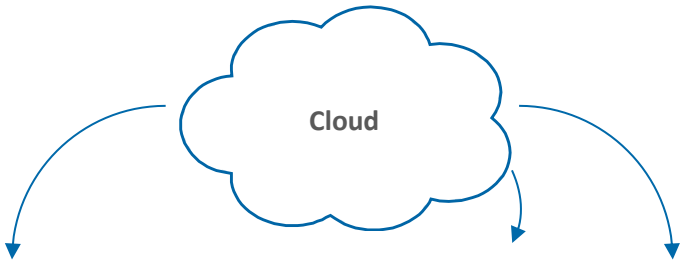
Forward-thinking businesses are benefitting from the cloud computing model which helps them transfer capital costs to operational costs, expedite the release of products and services, raise quality, and lower the cost of software and application acquisition.

CSPs offer their services according to a number of fundamental models: Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), and Software-as-a service (SaaS); where IaaS is the most basic and each higher model abstracts from the details of the lower models. This paper provides definitions and examples of cloud services utilizing these service models (figure 1).

Multi-tenancy is one of the cornerstones of the most important cloud computing offerings. The concept was pioneered by SaaS vendors and then spread across other key segments of the cloud marketplace, now taking the form of both PaaS and IaaS services. Multi-tenancy is explained in more detail below and is the primary focus of this paper.

Not surprisingly, perceived challenges relating to security and privacy continue to rank highly on the list of concerns for IT and business executives (Ponemon, Security of Cloud Computing Users Study). However, data gathered from an International survey conducted in 2013 (KPMG) indicates that organizations are becoming more confident in the security of cloud providers.

Figure 1: Cloud service models



	Software-as-a-Service (SaaS)	Platform-as-a-Service (PaaS)	Infrastructure-as-a-Service (IaaS)
Definitions	As-a-service delivery of applications targeted at private users (e.g., social networking, microblogging) and business users (e.g., ERP, CRM)	As-a-service delivery of tools for development, testing, deployment, hosting and application maintenance	As-a-service delivery of virtual CPUs, disk space, and database services
Key services	Salesforce.com Google Apps NetSuite Workday	Force.com Caspio Google Apps Engine Microsoft Azure	Rightscale Amazon Web Services Eucalyptus Gogrid

Defining Multi-Tenancy

When a user accesses data by using a multitenant SaaS application, the application instance to which the user connects is one which can also accommodate other users from dozens, or even hundreds, of other companies'. This is achieved without the users being aware of the other organisations.

The mechanisms for Multi-tenancy can be established in different ways depending upon the particular service of the Cloud Service Provider (CSP). Almost every definition of cloud, amongst the numerous definitions that exist, includes the ability to isolate cloud subscriber- specific traffic, data, and configuration of resources using the same software and interfaces. For example, in the case of SaaS, multi-tenancy is almost always achieved via a database configuration, with isolation provided at the application layer. This form of multi-tenancy is the most mature model of isolation and the best understood.

In 2008, Gartner performed an analysis of the reference models for multi-tenancy which has gained widespread acceptance (Gartner). Figure 2 illustrates the Gartner multi-tenancy models, which are each based on a different approach to sharing the computing resources that underlie the application. The three technology layers are system infrastructure (may be IaaS), application infrastructure (may be PaaS) and application code (may be SaaS).

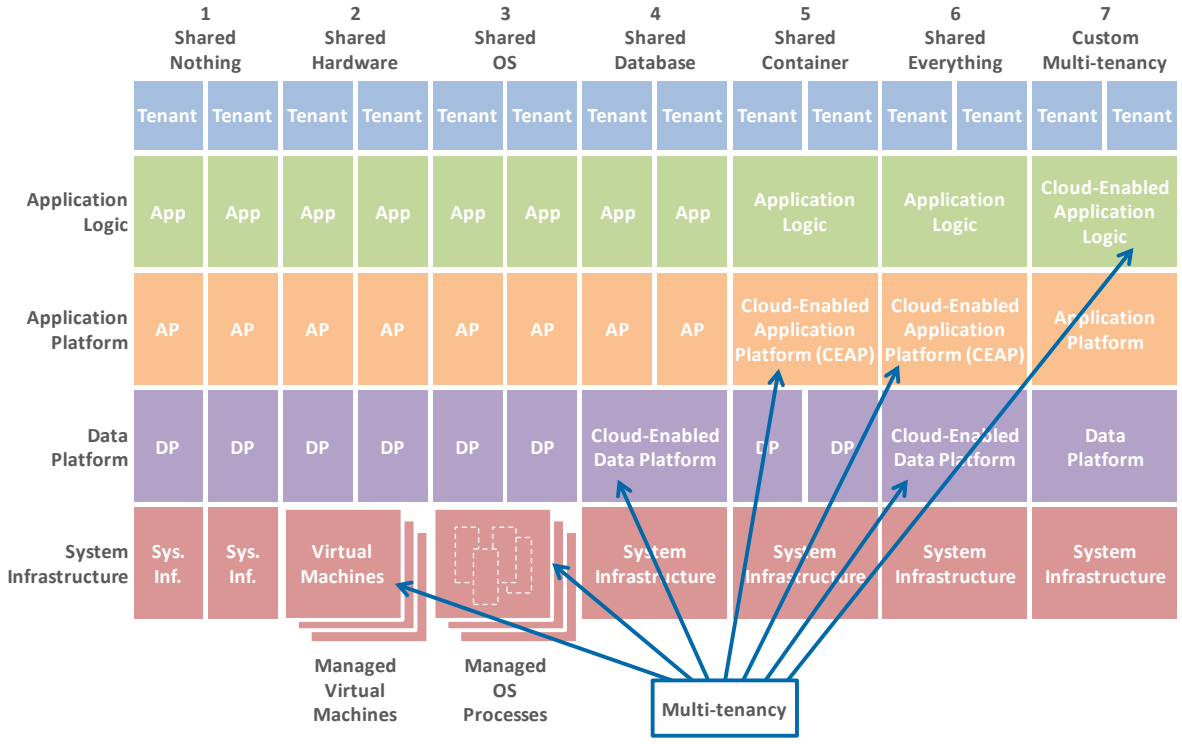


Figure 2. Gartner Reference Architecture for Multi-tenancy (Gartner)

The models show how multi-tenancy can be accomplished in different ways depending on the type of cloud service and technology offered by the CSP. One CSP may be multi-tenant at the hardware level in that its cloud subscribers may share a physical machine while another is multi-tenant at the database level such that its cloud subscribers share a database. Therefore, there is no standard

means to providing cloud computing services with the multi-tenancy model, and each distinctive cloud design has its own unique characteristics.

However, no matter which implementation is used, the vast majority of multi-tenancy security risks are common across all of the implementation models. Cloud subscribers should question/evaluate their CSPs on their specific implementation and the practices they use to mitigate security risks. They can then gauge the effectiveness of the CSP practices based on the implementation of their multi-tenancy model. To be business-relevant, such an evaluation should not stand in isolation, for as cloud subscribers move toward the cloud, they should also measure the risks to their existing internal, on-premise systems.

Evaluating the Multi-Tenancy Risk Profile

Confidentiality, Integrity and Availability (CIA), is a widely used framework for the evaluation of information systems security as part of business impact assessment (BIA). However, because shared services are fundamental to the public cloud, a view of how multi-tenancy architecture is implemented is also a key factor. Cloud subscribers looking at their multi-tenancy risks are therefore likely to perform their initial evaluation of the CSP risks and capabilities against the CIA model but could go further to use a specific architectural lens to test for a robust foundation in delivering a secure multi-tenant system. Similarly, detailed reviews performed based on assessment and compliance standards such as FISMA, ISO, and SOC can provide details around effectiveness of controls implemented by the CSP, but do not all take an architectural view. It is this often missing element of architecture that has therefore become the focus of this paper.

The following table describes the security objectives and impacts based on the CIA model and architectural considerations:

Key Risk Areas	Security Objective	Cloud Subscriber Impact
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Architecture	Providing an architecture that is robustly designed to meet the business objectives of cloud subscribers while maintaining operational excellence and meet the security objectives (C,I,A) noted above.	Cloud subscribers rely on the features and fixes that are added by the CSP. The CSP multi- tenant architecture supports security features that protect the isolation, confidentiality, and availability needs of the cloud subscriber.

Table 1: Security Objectives and Impacts

This paper aims to describe specific questions cloud subscribers should be asking CSPs related to multi-tenancy security risks that arise from this more architectural view. There may also be some unique risks in the specific architecture and service model of the CSP but the coverage of those types of CSP-specific risks is outside of the scope of this, more general, paper.

Customer Concerns over Multi-Tenancy

Before looking into the specifics of multi-tenancy risks, it is helpful to first examine some high-level requirements that cloud subscribers are using to evaluate CSP multi-tenancy maturity:

- From an architectural perspective:
  - How does the CSP achieve multi-tenancy for cloud services?
  - For virtualization security, how are virtual machines deployed and secured?
  - Is the CSP likely to roll-out a feature that is contrary to our wishes?
- From a confidentiality perspective:
  - Will CSP personnel have access to look at and steal our data?
  - Can other tenants look into and steal our data?
  - Will the sensitive data stored on a cloud remain confidential from third parties?
- From an integrity perspective:
  - How do I know that the CSP is doing the computations correctly?
  - How do I ensure that the CSP really stored my data without tampering with it?
  - How does the CSP monitor and conduct repairs of services/resources?
  - How quickly can the CSP roll out new security features throughout the pool of tenants?
- From an availability perspective:
  - Will critical systems go down, if the CSP is attacked in a Denial of Service attack?
  - Will my data be replicated without my authorization - prompting privacy issues?
  - What happens if the CSP goes out of business?
  - How quickly can the CSP recover in the event of a disaster?
  - How quickly can my data be restored in the event of a data loss event?

This is elaborated in more detail in the following table:

Table 2 takes the previous evaluation topics and highlights the core security risks for the multi-tenancy model. These are the questions more advanced cloud subscribers are asking their CSPs.

Key Risk Areas	Customer Requirements and Concerns
Multi-Tenant Architecture	• Which multi-tenancy implementation model is the CSP using? • How does the CSP manage individual tenants in the multi-tenant environment? To: – Provide 24/7 availability to support potential global user base? – Adopt new versions without disrupting the continuous operations of tenants, and preserve user customizations? – Scale up or down on demand? – Allow individual rollback and restore for each tenant? – Not allow a 'noisy neighbour' tenant to affect the performance of other tenants, or increase their costs? – Be accessible from various locations, devices, and software architectures to meet potential global demand? – Offer tenant-aware self-service? • What, exactly, is virtualized, if anything? Data centre, servers, OSs, storage, databases network, middleware, application, etc.? • What techniques are used for virtualization - is it a tool like a VM tool with a hypervisor, or is it a custom-built user separation layer? Further: – Can one determine where in the cloud infrastructure an instance is located? – Can one easily determine if two instances are co-resident on the same physical machine? – Can an adversary launch instances that will be co-resident with other user instances? – Can an adversary exploit cross-VM information leakage once co-resident? • What features does the CSP implement in their multi-tenant world that makes it appear like a single tenant world from the Internet (SSO, IP range restrictions, etc.)? • Does the CSP provide guidance and recommendation on what cloud subscribers should use? • Does the CSP have a robust process to handle user provisioning vulnerabilities? How are user sessions managed in the multi-tenancy model? How are credentials managed and stored? • Does the CSP provide strong access and identity management, i.e., multi-factor authentication for key systems and data access points? • Does the CSP have the capability to provide independent audit trail at various layers? • Does the CSP have the ability to allocate resources to tenants dynamically, as needed and based on policy? • Does the CSP have the ability to provide horizontal scalability to support real-time addition/removal of tenant resources, tenants or users without interruptions to the running environment?

Key Risk Areas	Customer Requirements and Concerns
Confidentiality	• How is the isolation and separation implemented for the following: – Isolation of tenant data? – Isolation of the tenant workspace (memory)? – Isolation of tenant execution characteristics (performance and availability)? – Tenant-aware security, monitoring, logging, management, reporting, and self-service administration? – Isolation of tenant customizations and extensions to business logic? – Continuous, tenant-aware version control? – Tenant-aware error tracking and recovery? – Tracking and recording of resources use per tenant? • What additional technical controls are in place to keep the data segregated? What happens when/if something goes wrong? • Does the CSP provide protection from guest-hopping attacks, whereby attackers can access data on other virtual machines or within shared databases? Does the CSP provide strong network traffic encryption techniques, i.e., Transport Layer Security (TLS)/ Secure Socket Layer (SSL) for cloud subscriber access? • How do CSP operators/support staff manage the system and what exposure do they have to cloud subscriber data? How many will have access? – How identifiable is the data CSP operators are exposed to while managing the systems? – What precautions are taken in selecting, training and managing the CSP operators? – Does the CSP restrict operator access to cloud subscriber data unless approved by the cloud subscriber for troubleshooting purpose? How identifiable is the data they are exposed to while managing the systems? – Does the CSP provide annual training to operators on secure data handling practices? – Segregation of duties and access linkage to role (e.g. support tickets)? • Does the CSP provide capability for federated single sign-on to and from applications? • Does the CSP provide detailed technical data on data handling and transfer between federated clouds? • Does the CSP implement isolation in networking virtual layers alongside network intrusion prevention and data loss detection capabilities? • How does the CSP know that a breach has occurred? • How does the CSP notify cloud subscribers when a breach occurs? • Who is responsible for managing the breach notification process (and costs associated with the process)?

Key Risk Areas	Customer Requirements and Concerns
Integrity	• Does the CSP provide robust patch, change and vulnerability management processes for the hypervisor, underlying virtual machines and infrastructure vulnerabilities? • Does the CSP provide protection for Application Programming Interfaces (API) keys? • How are user sessions set up/torn down and otherwise managed for the CSP's multi-tenant model? Where are the credentials kept, and how are they stored? • Does the CSP provide protection from side channel attacks to protect crypto mechanisms and private keys? • Does the CSP operate the service based on least privilege, providing only information that is essential yet still giving a tenant enough information that can be used for useful debugging? • What features does the CSP implement that makes it appear like a single tenant world from the Internet (SSO, IP range restrictions, etc.)? Which features does the CSP recommend that cloud subscribers use? • Does the CSP limit attack surface for co-residence checks to restrict neighbour virtual machine enumeration? • Does the CSP build security checks into fabric layer to scan prebuilt virtual machines/virtual appliances containing malicious code? • Does the CSP provide options for cloud subscriber configuration of virtual firewalls or networking? • Does the CSP provide logging and monitoring capabilities for investigation? Does CSP provide automated alerting in the case of suspicious activity?
Availability	• Does the CSP limit data replication in the cloud? How data is replicated, how are back-ups stored? • Does the CSP commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their cloud subscribers? How are they secured? • How is data replication for disaster recovery or other failures one in the CSP model of multi-tenancy? • How long would it take for a complete restoration?

Table 2: Core Security Risks for Multi-Tenancy

Some surveys in the past have reported that CSPs are abdicating security to be entirely the responsibility of the customer (Ponemon, Security of Cloud Computing Providers Study). But this view is not shared by the customers surveyed for this paper. In their view an effective CSP must go beyond their own business risks and aim to understand the risks to their customers and thus create the controls required to properly mitigate those risks. In fact, customers report that leading CSPs are following best practices to mitigate the risks highlighted above. This includes a robust process to secure information systems which includes: clearly understanding core security requirements for cloud subscribers, building a secure technical architecture, segregating user privileges, and properly identifying and handling sensitive data. The next section of this paper explores the risk mitigations followed by leading CSPs to mitigate the concerns that have been highlighted so far.

Risk Mitigation Leading Practices

The experienced cloud subscribers stated that they look for a CSP with a track record of trust, strong balance sheet, innovation and a demonstrable long- term commitment to the market. Only then should the price, or value, of a service be considered. The security teams in these companies were developing policies and governance to ensure that security capability of the CSP was assessed as part of procurement. In their conduct of cloud security reviews advisory firms are finding that with few exceptions leading CSPs tend to have a very firm grasp on security (KPMG). These CSPs typically make significant investment in technology and capability to secure data centres infrastructures, and networks.

Currently, the onus usually falls on the company acquiring the service to conduct the security assessment, or commission these reviews and this can be time consuming for both provider and subscriber. The subject of assurance is therefore covered in more detail later in this paper.

The leading CSPs were reported to have a number of best practices which are described in Table 3.

Key Risk Areas	Risk Mitigation Leading Practices
Architecture	• Provide architectural assurances on how resource sharing is achieved while preserving tenant's trust in configuration, security, and isolation and compliance. For example: – Traffic isolation between the tenants – Confidentiality and protection of information – Tenant apps and data with built-in firewall and VPN capabilities – Enterprise directory services for security policies – Logging all traffic information on per-tenant basis. • Implement the CIA triad for tenant data, services, and applications across all layers of the data centre stack where multi-tenancy is used. • Implement strong security controls at the hypervisor layer (if using virtualization) to provide secure separation. • Define the architectural boundary for who's the insider? Where's the security boundary? Who can I trust? • Implement strong security controls for secure interfaces and APIs. • Solutions should support continuous verification and monitoring.

Key Risk Areas	Risk Mitigation Leading Practices
Confidentiality	• Data isolation - Common practice among CSPs is to encrypt data in transit at a minimum. There is a growing capability to encrypt data storage areas or sensitive fields. • Network isolation – In order to single out the physical machines running a cloud subscriber's VM, CSPs provide each VM with a "pseudo" randomly-allocated IP address that VMs use when communicating with each other, keeping the actual cloud-provider IP address allocations. – Different instances running on the same physical machine are isolated from each other via the hypervisor. – VLAN Segmentation reduces asset visibility and achieves tenant isolation – Software-based firewall is implemented that resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbours have no more access to that instance than any other host on the Internet. • Confidentiality and protection of tenant apps and data is achieved with built-in firewall and VPN. • IP address restriction is applied to limit to access from known IP address ranges. • Access control, including multifactor authentication. • Multi-tenant infrastructures and applications require transactions to authenticate each cloud subscriber on submission of a request. This process helps authenticate and authorize the types of transaction resources a user can access, thereby enforcing role-based access control for network, security, and administrator duties. • An opt-in feature by certain CSPs that adds additional layers of authentication for critical access points to the cloud environment. • Operator access to cloud subscriber data is limited to a group of cleared, audited personnel.
Integrity	• To reduce the likelihood of a side channel attack, obscure the activity of a program that writes and reads data from the memory. • Logging and monitoring to allow logging all traffic information on a per-tenant basis. • Health monitoring with near real-time health monitoring that is implemented at hypervisor level to examine the internal state of a running VM and perform continuous verification and monitoring and automated shutting down of any offending components. • Configure event alerts to notify operations and management personnel when early warning thresholds are crossed on key operational metrics.
Availability	• Perform near-real-time data replication, constantly maintains multiple healthy replicas of cloud subscriber data at primary and secondary location. • In case of failure, automated processes to move cloud subscriber data traffic away from the affected area. • Provide approximately 99.98 percent availability and durability of data.

Table 3: Multi-Tenancy Risk Mitigation Leading Practices

Sharing Responsibilities

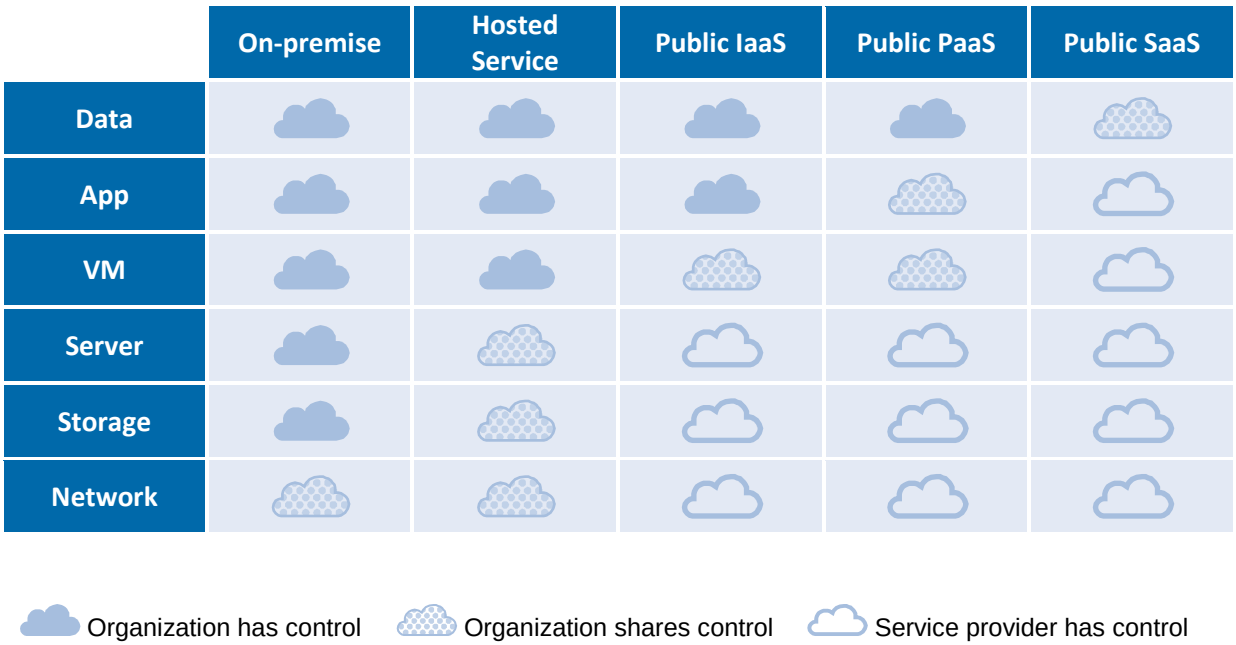
A mature approach to security recognises that the use of a service provider immediately introduces shared responsibilities and these should be clearly understood. The roles and responsibilities between the cloud subscriber and the CSP should be clearly defined and documented in any Service Level Agreements (SLAs) or other legal contract. What this means is that the cloud subscriber selection team will need to include representatives from outside the IT organization, such as legal, procurement, and compliance. Cloud subscribers, as a general rule, should also make sure that these other functions understand the cloud model and the potentially different considerations for shared responsibilities that should be identified.

In this sense, there is nothing different about security in cloud computing than any other service. As noted previously, responsibility for making the risk-based decisions about the system and the data it contains remain with the cloud subscriber. But multi-tenancy is not identical to a dedicated service as controls will be more standardised and the cloud subscriber should take efforts to understand how the service is implemented.

The shared, hybrid model places the onus on cloud subscribers to get answers to key questions regarding technical architecture and operations before signing a contract with the CSP. This architecture will form the basis for the specific security roles and responsibilities between the cloud subscriber and the provider and should thus be clearly defined and documented in the contract.

The leading CSPs should therefore have thorough documentation of the security features and options they make available to cloud subscribers. This should include where some cloud subscribers can opt to enable more restrictive security features than the defaults if they feel that additional protections are needed for the level of protection they require of their data.

Figure 3: Security Responsibility



As illustrated in Figure 3, the cloud subscriber's share of security responsibility and control is the greatest in the IaaS model. As we move up the stack from IaaS to SaaS, the cloud subscriber's share of security responsibility shrinks and the CSP's share of the responsibility grows. Thus:

- **IaaS:** The cloud subscriber has the greatest responsibilities for security. Due to extensibility, security is required across all layers of the implementation.
- **PaaS:** Responsibility will lie somewhere in the middle, with extensibility and security features that must be leveraged by the cloud subscriber.
- **SaaS:** The CSP assumes primary responsibilities for defining security controls and the cloud subscriber controls limited service settings.

Cloud subscribers will find some situations where it is relatively easy to determine responsibility between the CSP and the cloud subscriber. We can assume that the use of a CSP will move responsibility for the physical control of facilities, data centres, servers, and storage to the CSP. We also expect the CSP to implement isolation mechanisms and access control that protects one cloud subscriber's data from access by another and protect both from external attacks.

However, there are situations that are not as straightforward in determining roles and responsibilities. For example, how will network connectivity with the CSP be established? How will identity and access management be addressed? How will authorized users be identified, have their privileges managed, and ultimately be de-provisioned? How about data encryption and key management – who will control or hold the keys? Who is responsible for host intrusion detection and response? How will monitoring and log management be performed? What level of VM security or application security is the responsibility of the CSP versus the cloud subscriber? The CSP should as a minimum be able to answer these questions and in some cases offer the cloud subscriber choices.

So while the fundamentals of good security are unchanged in the cloud model, leading CSPs are making sure that the hybrid technical architecture and sharing of operational responsibilities is well documented and understood in their implementation approach. Cloud subscribers must also be rigorous in clearly understanding the CSP's service offering and in defining where responsibilities lie. They must then ensure that contracts and SLAs reflect, clarify and enforce that shared responsibility.

Unfortunately (in the context of a more utility or multi-tenancy market) the subscriber surveys in this study showed that there was little or no standardisation in how CSPs were approached by their potential customers to gather information. Almost every subscribing company had their own questionnaires and processes, with some limited take-up of Standardized Information Gathering (SIG) (Santa Fe). Standards like the Cloud Controls Matrix (CSA) were used to contribute to some company questionnaires but there was considerable variation in the eventual result.

Contracting & Assurance

Once the CSP has been chosen based on their capabilities, the subscribing company generally moves on to the contracting stage. Previous experiences in outsourcing contracts have shown examples of quite poorly thought-out or even missing security requirements. For example, the author has seen a quite common practice of security requirements being stated as "meeting the [customers] security policies as attached in the following appendix". These internal corporate policies will not have been

written with a service provider view in mind and so there is much interpretation and discarding of irrelevance required to work out what a supplier is required to do. A far better approach is for the contract to contain a clear definition of delivered security services and capabilities, as well as clarity of responsibilities as mentioned before.

Without exception, all of the cloud subscribers surveyed for this paper acknowledged that the larger and more capable CSPs do have significant security capabilities, in many cases being far greater than they themselves had in their own companies. The concern expressed was therefore not whether a CSP was capable of good security; it was whether the CSP would bring this capability to bear to adequately protect them as a subscriber. Clear contracts and SLAs certainly help in achieving this alignment, but there is something more fundamental at play here which is to do with loss of direct control and therefore the need for assurance and trust.

Assurance and Right of Audit – The most common form of assurance is checking that security processes are being followed and the standard outsourcing response is to require direct right of security audit. This requirement has produced challenges for outsourcers with the significant costs of queues of customer auditor visits and potential exposure of sensitive information from one client to another. The utility and multi-tenancy models of cloud computing just exacerbate this situation.

The outsourcing community have attempted to address this with the independent assurance reports available to all subscribers, originally SAS-70 but now superseded by SSAE16 (AICPA, SSAE16 Standards for Attestation Engagements No.16) - SOC2 (AICPA). These are relatively well received but still not universally accepted by all end user companies nor by their regulators. This must change with time, but needs more work to build confidence.

The Cloud Security Alliance is also aiming to address the assurance challenge with a 3 tier standardised model that starts with tiers one (self-assessment) through to three (continuous independent assessment) (CSA).

Trust and Through-life security - As recognised by the proposals for more real-time assessments, what subscribers are ideally looking for is greater transparency in what security is being provided by the CSP and how well it is actually performing for the subscriber. This more dynamic model is recognised by the CSA assurance work and also by the proposal to have standardised audit and security alerts that could feed a subscribers security operations centre. (CSA) Transparency is also starting to appear with 'Trust Centre' information sources in CSPs (Salesforce.com) (Microsoft)

The Emerging Ecosystem

Where security features are seen to be missing from CSPs, or subscribers are starting to lose their security situational awareness outside of their corporate network, then vendors have stepped in to fill the vacuum. This new ecosystem of service providers is one which the better CSPs are working with. Two of the main services are: Cloud assurance – where CSPs can be independently tested on a regular basis. Encryption – where sensitive data can be encrypted before reaching the CSP. Although more limited than the native encryption that can be provided by CSPs these services do provide a more integrated cross-provider capability for the subscriber. We can expect more developments.

Conclusion

While security-related concerns are still at the forefront for cloud subscribers considering cloud adoption, the real state of the industry is that organizations are quickly gaining more confidence in the security of CSPs and in adopting multitenant cloud services. In the experience of firms conducting cloud security reviews, with few exceptions, leading CSPs tend to have a very firm grasp on security. In most cases, these CSPs offer robust and resilient architectures, security measures, and controls that may even enhance some companies' security.

Cloud subscribers have found that the most mature CSP architecture currently exists in the multi-tenant cloud-based SaaS implementation. This is where cloud subscribers can expect that a single instance of an application is running on the hardware infrastructure, and that the single instance of the application virtually partitions a cloud subscriber's data and configuration information. This differs from a virtualized application where virtual machines are used to host isolated instances of an application on a shared server, each application instance serving a different cloud subscriber. Since it is very difficult to re-architect existing applications to be multi- tenant, most multi-tenant applications are designed from the ground up to be truly multi-tenant. Typically, there is only one 'production' version of the application running, and all cloud subscribers are benefiting from the features and fixes that are added to that application by the CSP. The CSP does not need to maintain support for multiple versions, nor rely on cloud subscribers to update to the latest versions, and can manage and monitor the security and usage of the overall system.

Some leading CSPs have built their applications completely multi-tenant from top to bottom, with a single, shared database as the foundation layer. These CSPs argue that the economies of operation and the rapid pace of collective innovation are so great that you can never achieve the same effect simply by implementing client-server virtualization and automation.

Throughout the industry, consultancies and advisory firms have noted that not all multi- tenant architecture deployments at CSPs are created equally (Ponemon, Security of Cloud Computing Providers Study). They vary in terms of their overall maturity and level of investment in technology, process, and controls to help ensure confidentiality, integrity, and availability of cloud subscriber data. Therefore, it is important for cloud subscribers to understand the risks associated with multi-tenancy and what any given CSP is doing to mitigate those risks. The risk areas and leading practices that are noted in this paper are a good starting point for these discussions and an architectural view is key.

The author believes that active discussion along these lines will go a long way to educate cloud subscribers and CSPs alike and address misunderstandings regarding the security capabilities of leading CSPs. Cloud subscribers who work with their CSPs to successfully address the questions noted in this paper can be confident that a well-designed, executed and operated multi-tenant cloud system will not increase their risks and may even reduce them.

> "Reviewing 12 months of operational data, including more than two billion events and over 60,000 security incidents, Alert Logic concluded that the cloud is inherently no less secure than the on-premise environment."
>
> *Alert Logic, "State of Cloud Security Report", Fall 2012* (Alert Logic)

Bibliography

AICPA. “Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) - AICPA Guide.” 2012.

—. “SSAE16 Standards for Attestation Engagements No.16.” 2010.

Alert Logic. “State of Cloud Security Report.” Autumn 2012.

CSA. *Cloud Audit*. n.d. https://cloudsecurityalliance.org/research/cloudaudit/. 27 June 2014.

—. “Cloud Controls Matrix V3.” 2013.

—. *Open Certification Framework*. n.d. https://cloudsecurityalliance.org/star/. 27 June 2014.

Dorey, PG & Leite, A. “Commentary:Cloud Computing - A security problem or solution?” *Information Security Technical Report* (2011): 89-96.

Forrester. “Understanding Cloud’s Multitenancy.” March 2012.

Gartner. “Gartner Reference Architecture for Multitenancy.” 2008, Updated 25th August, 2010.

KPMG. “The Cloud Takes Shape V4.” 2013.

Microsoft. *Azure Trust Center*. n.d. http://azure.microsoft.com/en-us/support/trust-center/. 27 June 2014.

NIST. “The NIST Definition of Cloud Computing SP800-145.” 2012.

Ponemon. “Security of Cloud Computing Providers Study.” April 2011.

—. “Security of Cloud Computing Users Study.” March 2013.

Salesforce.com. *Trust*. n.d. http://www.trust.salesforce.com/. 27 June 2014.

Santa Fe. *Shared Assessments*. n.d. sharedassessments.org/about/. 27 June 2014.

Acknowledgements

The author would like to thank Salesforce.com for supporting this work and the consultants and end user companies who shared their experiences and helped with some of the analysis in this paper. The views expressed remain those of the author.

About the Author

Prof. Paul Dorey PhD. CISM M.Inst.ISP is a Visiting Professor at Royal Holloway, University of London and Chairman Emeritus of the Institute of Information Security Professionals. He is a Director and Founder of CSO Confidential which supports public and private organisations in information security strategy development. His security career of over 25 years includes security and risk leadership roles at BP, Barclays Bank and Morgan Grenfell/Deutsche Bank. He can be contacted at: paul.dorey@csoconfidential.com