masonadvisory

WHITE PAPER

May 2016

SECURING THE CLOUD

Considering a new model for managing risk

Organisations moving to cloud-based services need to rethink their security model. The good news is that – if approached and managed correctly – it is possible to migrate to the cloud and gain its benefits without increasing risk.

Introduction

The flexibility of cloud can bring significant and measurable benefits to an organisation's IT services. The ability to scale on demand, access resilient infrastructure, and reduce capital costs can provide a compelling argument to adopt cloud services. Software as a service (SaaS) in particular can allow companies to deploy new functionality quickly using subscription-based models, thereby lowering the cost and increasing the speed of deployment. Research published by the Cloud Industry Forum shows the overall cloud adoption rate in the UK stands at 84%, with 78% of cloud users having adopted two or more cloud services.[1] But, although cloud services can reduce the cost and complexity of managing IT infrastructure, they also introduce a new set of information security considerations.

At their core, cloud service platforms are no different from any other IT infrastructure. They can suffer from the same security flaws, but arguably they carry more risk. There are issues around aggregated data from multiple customers sharing the same platform, creating an attractive target for attackers. Cloud systems can also create easier access to services and data – including from personal devices. And users installing cloud clients on company machines can create additional attack vectors, as many clients include features that allow extensive – and potentially misunderstood – levels of remote access.[2]

All of which can be managed, as long as organisations adopting cloud services consider security as part of their requirements from the outset.

This white paper explains how the move to the cloud can be at odds with traditional forms of information security management. It then goes on to look at the key questions that IT teams need to ask when sourcing cloud-based products, covering data classification; identity and access management; encryption; shared vulnerabilities; and incident response.

Moving away from direct ownership of data

The ISO 27001 standard defines three core pillars or characteristics of information security management:

- **confidentiality** – how access to information is controlled and limited
- **integrity** – how information can be assured as accurate and unaltered
- **availability** – how information can be accessed reliably by authorised parties.

In the direct ownership model for IT infrastructure, it can be fairly straightforward to assess system security against these characteristics. Ownership of the infrastructure can ensure an organisation understands the design and implementation of its IT services at a granular level, making it easier to gather the necessary data for risk assessments. It also requires the organisation to own the whole of the IT security strategy,

[1] http://www.cloudindustryforum.org/content/uk-cloud-adoption-rate-climbs-84-finds-new-research-cloud-industry-forum

[2] Microsoft OneDrive provides an in-built option to allow files to be retrieved remotely from a computer's local storage or network drives to which it's connected.

Types of cloud service provision

Similar security risks exist, regardless of which model is in use, although they manifest themselves in different ways.

Public

More correctly described as a public multi-tenant cloud. This is the most well-known type of cloud service. Multiple customers share the same underlying infrastructure, operated by a service provider, using a subscription or 'pay-as-you-go' model and scaling their service usage based on demand.

Private

Offers a flexible cloud infrastructure that is solely used by a single customer. This type is most often used by very large organisations that require the flexibility and scalability of cloud services without the requirement to share resources with other customers. Users must be able to absorb significant additional costs.

Hybrid

As the name suggests, this is a combination of connected private and public cloud services that allow organisations to benefit from the best of both models.

including designing controls and mitigating risks to protect the infrastructure.

Conversely, when using cloud services, the infrastructure becomes a black box which is owned and operated by the cloud provider. Although this also moves accountability for infrastructure security to the cloud provider, it's vital to understand that this represents only one area of information security. Using cloud services means that corporate data will be managed by a third-party provider, while the ownership of, and accountability and legal liability for, the security of that data remains with the organisation itself.

This shared ownership of risk requires a different approach to assessing security using the ISO 27001 characteristics described earlier.

Five questions to ask when planning cloud services

When considering this different approach, businesses should look at five questions that underpin security requirements in the cloud.

- What data will be migrated to and created in the cloud, and what risks are associated with it? (How do you *classify your data*?)
- Who can access what data, and under what conditions? (What's your approach to *identity and access management* (IAM)?)
- How will data be protected during transfer to, and storage in, the cloud ? (How will you implement and manage *encryption*?)
- What risks does the 'multi-tenant' nature of cloud services pose? (How do you *mitigate shared vulnerabilities*?)
- What needs to be done in the event of an incident or security breach that may affect the data? (What's your plan for *incident response*?)

The remainder of this paper takes each question in turn, and identifies the key issues that need to be addressed.

Data classification

Information is the life blood of any organisation. Protecting data is not only about maintaining business effectiveness and competitive advantage. It can also be a legal obligation with significant penalties attached. Knowing the value, risks, and legal obligations associated with different data, and the impact if it is compromised, is essential to creating a cloud security strategy. The first step to reaching this understanding is the creation of a data classification process.

An effective data classification system should be easily understandable, consistent and directly relevant to an organisation's day-to-day activities. Onerous or complex systems should be avoided as they often produce confusion and are used inconsistently. Instead a simple tiered confidentiality model can be used.

Figure 1: Example of classifications within a simple tiered model for confidentiality

Classification	Description
Highly confidential	Must not be shared beyond named individuals or is legally protected, e.g. employees' personal information
Confidential	Could affect the operation of the business if publicly disclosed, e.g. contract terms or competitive processes
Internal	Can be freely shared internally, but could create risks if disclosed externally, e.g. sales performance data.
Public	Can be freely shared outside the organisation, e.g. press releases

Once the *confidentiality* tier of data has been defined, a business impact analysis of the *availability* requirements can then be performed. As cloud-based data is no longer physically and locally accessible to the organisation, it's essential to understand the cost of downtime should access to the service become unavailable (for example, due to a network outage, service failure or malicious attack).

Again the availability requirements can be broken down into a simple tiered model.

- **Critical**. This is data that is essential to the operation of the business, and must be accessible more than 99.99% of the time (equating to approximately 52 minutes of unavailability per year), for example the customer-facing presence for an online retailer.

- **Important**. This is data that is essential to the operation of the business, but where limited loss of service can be accommodated, with accessibility of more than 99.9% of the time (equating to approximately nine hours of unavailability per year), for example email systems.

- **Standard**. This is data that supports internal processes where loss of service can be accommodated and worked around, for example automated reporting systems.

By categorising information using confidentiality and availability tiers, an organisation can quickly identify what data merits additional control and protection, allowing a decision tree to be created for data that is used or stored in the cloud. This type of data classification also supports a number of other key cloud adoption activities, including the proper selection of tiered storage models, setting of service level agreements (SLAs), and disaster recovery planning.

Using cloud services means that corporate data will be managed by a third-party provider

When classifying data, it is important to consider the holistic context of the information, as innocuous stand-alone data can become sensitive when combined with other sources. For example, a database containing a list of employee salaries linked only to a reference number may be considered confidential when viewed in isolation. However, if a second database exists that links those reference numbers to employees' names and addresses, the aggregated data becomes highly confidential. A case of the whole picture being more than the sum of its parts.

Data classification can also help to address regulatory compliance or contractual issues with cloud adoption. Many countries, especially in Western Europe and North America, place legal restrictions on the movement of some types of data outside of their borders.[3] This creates an interesting challenge when moving to the cloud, as many cloud providers offer data storage services that cross national boundaries in a way that may not be fully transparent. In many cases this type of distributed storage is a positive feature, improving availability, resiliency and speed of access across regions. But, if data stored in a cloud service has a regulatory restriction on cross-border transfer, this feature can become a legal liability if not managed correctly. Other contractual agreements, such as codes of connection and non-disclosure agreements may also include requirements regarding classification and use of cloud storage. Users of cloud services may need to make alternative arrangements for special projects (for example, those involving security, defence and criminal justice organisations or critical national infrastructure[4]).

Clearly marking this type of data during the classification process is essential, and in these cases the decision tree for cloud data storage becomes a critical tool to ensure information is properly protected.

Identity and access management

As well as classifying data, managing its integrity is of paramount importance. Strong identity and access management (IAM), ensuring that only authorised users have access to appropriate data at the right times, is a cornerstone of data security and compliance. Broadly, there are two approaches to identity management in the cloud, as outlined below.

Individual identities per service. In the early days of cloud services, users were required to register separate accounts for each cloud platform they accessed. This approach created 'credential soup': a user would need

[3] Global storage of data by foreign-domiciled companies can also create challenges. The US Patriot Act is a well-known example, requiring US companies to surrender data to the US authorities, regardless of what country it is stored in.

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf

to manage a number of different usernames and passwords, inevitably leading to the poor security practice of re-using the same details for multiple services. With a lack of central management, early corporate adopters of cloud services were left with little visibility and control over their data.

Federated identity management. Providers have realised that IAM services are a core requirement for corporate adoption of cloud services. Allowing companies to operate a single user directory for cloud authentication solves the conundrum of how to manage the provision and revocation of user access effectively, for example when an employee joins or leaves an organisation. By using federation through an identity provider to connect a cloud service to an organisation's internal user directory, such as Microsoft Active Directory, users only require one set of credentials to access both internal and cloud resources through single sign-on (SSO) capabilities. This in turn allows organisations to extend their internal access management processes out to the cloud automatically, and to audit the use of cloud services centrally. Many cloud service providers, such as Salesforce.com and Amazon, as well as third parties such as Okta , now offer comprehensive federated IAM and SSO services.

If the worst happens, being properly prepared to respond will save time and help reduce the impact of a security incident

Controlling the confidentiality and integrity of cloud data extends beyond identity management. Ensuring data is protected against compromise, alteration and unauthorised distribution requires more than monitoring and auditing of access. A key tool in the protection of data confidentiality is encryption.

Encryption

Encrypting data ensures that if the security of the cloud service is breached, stolen data is unreadable to the attacker. As a side benefit it also prevents the data from being accessed by the cloud service provider, who has *de facto* administrative access to customer data storage. This is good practice for maintaining data confidentiality regardless of whether data is stored in the cloud or on dedicated internal infrastructure.

However, before encrypted data can be used it must be decrypted, which requires the encryption keys to be stored in an accessible location. For this reason, encryption is not a panacea and the protection of encryption keys is of paramount importance. Keeping encryption keys as separate as possible from the data they protect is essential, although this is not always possible where automated systems such as online purchasing portals must encrypt and decrypt data on the fly.

For most organisations using cloud services to store 'data at rest', separation of keys and data can be achieved by encrypting data before it is sent to the cloud. The key benefit of encrypting data within the internal infrastructure, prior to transmission to, and storage by, the cloud service provider, is that the organisation retains control of the encryption keys. As well as ensuring the separation of data and decryption keys, this is also a core requirement of many information security regulations such as PCI-DSS.[5]

Encrypting data prior to storing it within the cloud also helps to protect against a further risk: shared vulnerabilities within a multi-tenant cloud infrastructure.

Mitigating shared vulnerabilities

Sharing resources is known as 'multi-tenancy', with cloud providers using logical, 'soft' controls to segment customer data. While this approach underpins the flexibility and cost effectiveness of cloud, it also means that if one customer of a cloud service – or a component of the cloud management platform – is compromised, other customers of the same service may be at risk. Without the physical separation provided by dedicated IT infrastructure, an attacker that breaches the security of one customer's cloud services may be able to extend the attack back into the cloud provider's infrastructure and into other customers' environments.

Although accountability for preventing these infrastructure attacks lies with the cloud provider, encryption can provide a powerful tool to protect an organisation's data. Even if an attacker is able to breach the cloud environment, encrypted

[5] The Payment Card Industry Data Security Standard (PCI-DSS) is a framework for developing robust payment card data security processes (https://www.pcisecuritystandards.org/security_standards/).

data and the security of the encryption keys will mitigate much of the risk and potential reputational damage.

However, in today's environment of complex systems and determined attackers, it is an unfortunate fact of life that security breaches can still occur despite the use of best-practice security methods. If the worst does happen, being properly prepared to respond will save valuable time and help reduce the impact of a security incident.

Incident response and governance

Keeping incident response policies updated to include cloud services is a critical security and service management activity. Not all security incidents are malicious breaches or attacks – they can include accidental disruption of service, loss of data integrity through database record corruption and so on. In the event of an incident or breach occurring – whether internally or within a cloud service – a clearly defined response process that documents the accountabilities for both the cloud provider and an organisation's internal staff is essential to handle incidents robustly and quickly.

Ideally the creation of an incident response policy would involve directly co-ordinating with the cloud provider's technical teams to create a set of processes and SLAs jointly. In the real world, however, most cloud service customers are at the mercy of a provider's standard terms and conditions. This can make it difficult for organisations to gain the level of detail to which they are normally accustomed. In the absence of this information there are a number of key steps that can be taken to improve incident response.

- **Document and (if possible) test the cloud provider's response processes**. In the event of an incident, having a clear understanding of the customer's and provider's obligations, and of the demarcation of responsibilities between them, is essential. Knowing what to expect – in terms of both actions and service levels – will help to ensure a calm and analytical response to an incident. Covering the basics in advance, such as ensuring the cloud provider has the incident manager's correct contact details on record, will help to maintain the integrity of the incident response and escalation process.
- **Agree and implement a recovery plan**. If a service outage occurs, or data becomes lost, ensure that a clear plan exists to maintain continuity, such as switching to alternative back-up services. Disaster recovery and business continuity planning must also account for cloud services, with regular reviews to ensure that any service changes enforced by the cloud provider are considered.
- **Focus on communication**. In the event of an incident, having a clear communications policy to ensure internal and external customers are kept up to date is critical. Without this, confusion and miscommunication can often cause more damage than the original incident – especially where a security breach occurs and forensic investigation is required.

Conclusion

This paper has aimed to provide a concise guide to some of the security considerations affecting cloud services.

The use of cloud services creates a shared ownership of risk between the organisation which owns the data and the service provider. So organisations need to think differently about how they ensure the confidentiality, integrity and availability of their data. Making sure that information security requirements are addressed right at the start of any cloud adoption process, and ensuring that reputable cloud providers with the relevant accreditations and certifications are selected, will allow businesses to reap the benefits of cloud while minimising risk.

Those requirements have to include clear and simple classification of data in order to assess the impact of any compromise; appropriate controls on access; effective and appropriate use of encryption to provide additional security support; and a clear planned approach to respond to any incidents if they do occur.

Cloud offers clear business benefits, but organisations must recognise that behind a simple service model lie risks that are ignored at their peril.

About Mason Advisory

A simple approach to complex challenges: Mason Advisory is an IT consultancy that does things differently. We're experts in IT who match technology know-how with commercial and business sense.

Businesses come to us because we solve complex business challenges through intelligent use of IT. We're here to help clients set their strategy and then deliver on those decisions.

And because we're independent, you know you can have confidence that our conclusions meet your needs. For 20 years, organisations of all sizes have trusted our consultants to deliver IT with an impact.

Contact us

If you would like to discuss how we can support you please email contact@masonadvisory.com or call +44 (0)333 301 0093.

www.masonadvisory.com