

Secure Computing in Enterprise Cloud Environments



"In the battle of security versus convenience, convenience always wins."

George Reese - Executive director and senior distinguished engineer, Dell's software group.

Contents

Which Cloud Model is Right for Your Data?	3
Understanding Cloud Models	4
Cloud Security Myths	7
Public Cloud Security Issues	10
Private Cloud Security Issues	14
Data Security in Multi-Tenant Clouds	17
Compliance and Risk Management	21
Loss of Governance	26
Security Measures	29
Ten Step Plan for a Secure Cloud	30

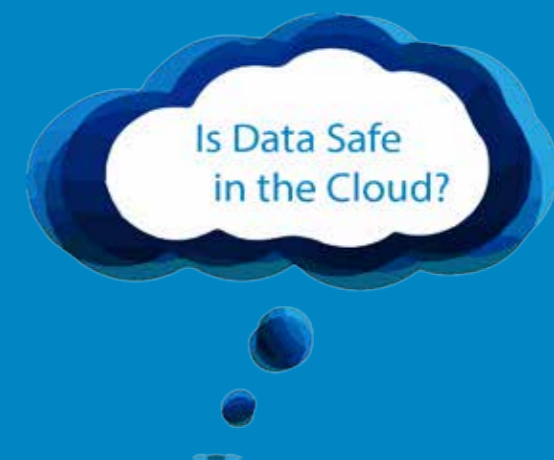
Which Cloud Model is Right for Your Business Data?

Firstly, it is essential to realise that data differs from case to case. A cloud model where data is stored in a multi-tenant public cloud may be perfectly serviceable for one business but totally inappropriate for another.

It's impossible to protect your data and network without first understanding the architecture of your cloud and where your data resides. For some businesses, cloud consists of areas on an overall IT network infrastructure. For others, it may be only one or two SaaS (Software as a Service) applications.

Storage is an obvious area of cloud infrastructure that is gaining appeal now that data transfer speeds allow LAN-like (local area network) operating speeds. In the past, SAN (Storage Area Network) would have been limited to one or two physical locations containing many physical and logical drives. Today, the rapid adoption of cloud services means that business data can reside in many physical locations and is more difficult to manage using traditional forms of GRC (Governance, Risk and Compliance).

Additionally, allowing many devices to connect to your network creates another set of vulnerabilities - requiring a rethink of the traditional GRC methodologies. Many businesses already use cloud computing solutions without any strategy because cloud computing is usually the fastest way to cater for business needs. In many cases, SaaS providers have a ready-made product that exists because the market demands it. SaaS speeds-up innovation in established businesses and it is a driving force in the start-up community, but it is not ideal for every situation. Your organisation's needs should always come before the solution. That may seem like common sense, but poor planning, often results in a poorly executed cloud environment.



Understanding Cloud Models

The three main cloud models are:

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud

The three models are simple to define, but the act of identifying which cloud is best for your business should not be a priority. It is more important to choose cloud services that suit your specific business needs than it is to ensure your business uses a private cloud because of the assumed security that comes with isolated IT infrastructure.

To clarify the differences between cloud models, here are some simplified definitions:

Private Cloud

A private cloud, in the purest sense, is infrastructure and software residing on your own IT equipment and managed by your own IT staff. However, it's possible to have a VPC (Virtual Private Cloud) so that your business outsources its cloud to benefit from lower capital expenditure and maintenance costs.

A VPC is a logical private cloud, unlike a true private cloud that is physically isolated compute and storage. For most businesses this offers more than enough

isolation and apart from sharing a datacentre, there is little to distinguish a VPC from physically private cloud infrastructure. It's possible to create a private cloud with an on-demand self-service system that acts in the same way as many of the larger public cloud providers. This allows businesses to expand when required and dispose of unwanted infrastructure to free up resources when possible.

Businesses with highly sensitive data - or those that want to maintain more control over data and IT resources - often use private clouds for this reason. Some businesses that build their own private clouds actually become cloud providers to offset the expense of their hardware and running costs.

Public Cloud

A public cloud is generally a service like Google Cloud, Microsoft Azure or Amazon AWS; all of which provide off-the-shelf solutions for businesses that want to access virtually any level of compute and storage capabilities. It is important to understand the data you control and the laws that govern your data before you can decide on a suitable cloud environment for your business.

You need to be clear on how much understanding your customers have on your data storage, how to plan and manipulate that data and how various changes may affect your decision to use datacentres in specific locations.



Hybrid Cloud

A hybrid cloud model suits most businesses in today's modern IT environment. Some applications that we pay for in the form of SaaS will always run on the application provider's servers and the price we pay will encompass software, processing and storage for any data we collect.

Some businesses undoubtedly have legacy applications and that means some data remains on our in-house network storage.

Cloud is a driver of innovation; so as we place new IT demands on businesses, most often the best solution is cloud-based and therefore will result in a gradual migration for the majority of IT departments. Many start-ups are already working entirely in the cloud because of lower costs.

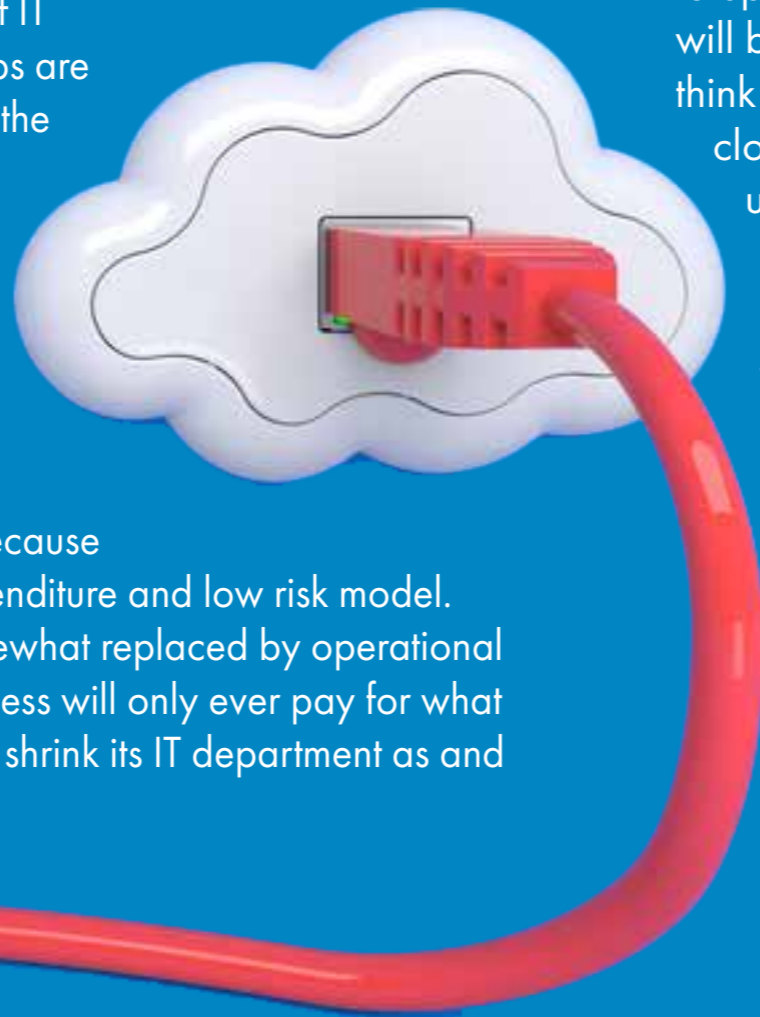
Choosing the Cloud for You

Without doubt, start-ups should consider being completely cloud-based because of the reduced capital expenditure and low risk model. Capital expenditure is somewhat replaced by operational expenditure, but your business will only ever pay for what it needs and can grow and shrink its IT department as and when change is needed.

Existing businesses should not make the mistake of taking what they have and then trying to replicate this in the cloud. Having an effective cloud strategy will do far more than increase availability to a mobile workforce. Effective use of the cloud will centralise your IT, reduce costs and increase productivity.

Most businesses have applications that exist outside of the cloud that function perfectly. If it makes sense to move legacy applications to the cloud, move them. If not, then don't. It's as simple as that. Ultimately, it will boil down to a cost issue. At some stage, you will need to upgrade or replace your SAN and perhaps that will be the time to move to the cloud. In the meantime, think about where your business can benefit from cloud technology without disruption or incurring unnecessary costs.

Even something as simple as moving your business email to the cloud will produce massive increases in productivity. For most businesses, a cloud strategy will involve the use of new cloud appliances (IT instances with a single function such as Enterprise Document Management) to replace existing methods on local networks.



What About Data Laws?

People often worry about data laws that govern a particular territory. The following guideline is appropriate for businesses that collect customer data and are subject to the Data Protection Act; protecting the rights of citizens in the European Economic Area.

“Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

As many datacentres are off shore or their whereabouts are unclear, businesses that hold sensitive customer data should fully consider whether its cloud operations adequately protect customer data. The UK’s Information Commissioner’s Office released guidelines for assessing a locations’ suitability in a document named ‘Assessing Adequacy International data transfers.’ This document is available from the Information Commissioner’s website or by visiting the following URL: <http://goo.gl/Yus3sg>.



Cloud Security Myths

Cloud computing has been the subject of many myths regarding security. Most people don't realise that cloud security issues are not unique or recent problems. We face the same issues as we have done for many years, but people's perceptions have changed. A perceived lack of control has undoubtedly contributed to the change in some people's perceptions, but there is no reason why a cloud environment should be any less secure than your existing datacentre set-up. On that note, one of the first myths to clear up on this matter relates to compliance.



Myth – Compliance is Security

You will often hear about cloud security requiring compliant devices and IT managers place a lot of value on compliance. IT managers often want their IT to exist in a world where they are confident that the business is meeting with traditional GRC requirements. The truth is that compliance is not a guarantee for security. Compliance only certifies that processes and security measures are correct at any particular time. Compliance often requires human interaction to follow guidelines and procedures; errors are always likely to occur when businesses depend on human input rather than automation. This does not mean compliance has no place in enterprise IT as it certainly serves a purpose, but it's unwise to think that compliance equals security.

Myth – Clouds are not Securable

This is one of the most common and frustrating myths; clouds are most definitely securable. Different cloud providers will have varying levels of security and so one cloud provider may offer a more suitable cloud model for your business than another. There is no one-size fits all solution for cloud security. Instead, businesses must design security to suit the chosen cloud model in the following three critical areas:

1. Control enforcement layer
2. Control management layer
3. Security management layer

The technology to deploy cloud infrastructure with these three critical elements of security already exists and is in use in enterprises all over the world. To learn more about these methods skip to Chapter 9.



Myth – Multi-Tenant Clouds are Vulnerable from Attack by Other Tenants

Virtualisation is the cornerstone of a secure and trusted cloud. Most cloud providers separate tenants at the compute or hypervisor layer rather than at a database level. Essentially, this means that there is no logical connection between tenants and also means that the virtual machines each tenant runs in the cloud are independent of others. This is made almost impossible by the fact that tenants operating a virtual machine would need to elevate their privileges to take control of the hardware at the virtual machine monitor or below. Skip to Chapter 9 to see how providers separate multi-tenant cloud applications, networks and compute and storage.

Myth – Internet Threats are more of a Problem When Your IT Infrastructure Exists in the Cloud

Many threats that affect businesses with an internet presence have been around for many years. Moving a network to the cloud will not make it any more vulnerable if you have adequate security in place (see Chapter 9). A network is only as secure as its weakest point and even traditional IT networks will have a point of entry that a determined hacker will exploit.

Most hacks are opportunistic and occur because of poor security or a complete oversight in a certain area. As previously mentioned, designing security measures to suit your data and cloud portfolio is the only way to ensure your safety - this is no different from the approach you should take with an internet presence. After all, you would provide similar, but slightly different security measures, if your business offered SaaS applications to one customer and retail or point of sale services to another. Both will access a database that requires protection.

Myth – Security Certifications Provide Assurance to Cloud Users

Security certifications are undoubtedly useful in all areas of IT and many that exist for traditional IT environments (PCI-DSS for credit cards, SSAE 16 [see SAS 70] for financial services etc.) are valid for businesses working and delivering services in a cloud-computing environment. However, security certification alone is insufficient as a security measure. Businesses still need to assess the security SLAs in any agreement with a cloud provider.

Certification is constantly improving and many of the most popular cloud providers have US FISMA (Federal Information Security Management Act) certification; providers such as Google Cloud, Microsoft and AWS will certainly use the latest auditing standards.



Public Cloud Security Issues

If you read the myths in Chapter 2, some of your fears about cloud security issues may have disappeared. Unfortunately, some risks are very real. It's important to understand that all IT infrastructures have vulnerabilities; knowing and understanding them is half of the battle.

This short list is *not exhaustive*, but simply being aware of these issues can help you decide how to deploy cloud-based IT within your business.

These aspects of security pose a risk to a multi-tenant cloud user, but some are also risks for other types of outsourced cloud-computing infrastructure.

Data Recovery on Newly Provisioned Cloud Space

It's possible in some circumstances to access data that resides in memory, which was left there by another tenant. This data has no index so will have no structure. However, a hacker who knows how to

access this data is most likely able to run software that recognises clusters as well as software to follow the fragmentation and reconstruct the data.

As data is stored in memory locations as either a 0 or a 1, a full format is required to erase the data completely. In some cases, when customers no longer require storage, a quick format frees up the spare capacity, but this only removes the virtual drive index and does not reset all the memory locations to 0. The chances of a tenant finding your business' sensitive data are very low, but it is a risk nonetheless.



Authentication and Access Controls

Your cloud provider's choice of authentication is one of the most important aspects of cloud computing. Authentication, authorisation and access controls are different depending on which cloud provider you choose. However, two-stage sign-ins and the kind of internet security that we have come to expect, when secure data resides on systems, is the minimum.

Some people feel it's important to know who has access, or how many people have access, to your account thanks to their higher privileges. Having great support where hundreds of live agents can resolve your issues in the least amount of time is great. However, what data becomes vulnerable because of higher privileges and does this pose too great a risk for your customer or other sensitive business data?

Hosting data in locations where tenants share namespaces is also a big no-no for security. Tenants should have individual namespaces rather than have their data stored with location identifiers that relate

to drives or physical locations. For many users, these issues are hardly worth the consideration because most cloud providers deal with them as part of their own best practice methodologies, but they still exist as a minor

risk if you are not sure. Evaluating risk is always a key process when formulating a cloud strategy. In reality, things like namespaces are rarely an issue. Even website hosting providers separate accounts with individual namespaces, but having faith in your cloud provider without knowing how they operate their systems is foolhardy.

Having adequate, centralised access controls not only helps avoid the risk of unauthorised tampering in your cloud deployments, but also eases the burden of managing large numbers of users for each application. It also makes it easier for users who would only need to manage their access details for the business' cloud rather than having separate login details for each application.



Virtual Machine Escape

A virtual machine escape would involve a tenant elevating their status from the user of a virtual machine that is logically isolated, to the status of a user that has control of the layer above the virtual machine. A virtual machine escape is a very difficult hack for even the most determined malicious user. This is because the vulnerability involves a guest moving its status from the guest to the host of the virtual machine.

Hackers who want to access their neighbour's data would attempt to exploit a number of known vulnerabilities to effectively 'escape' from the constraints of the service provided to them by the cloud vendor and gain greater access rights or access areas of memory used by other tenants. Luckily, vendors usually have safeguards in place to prevent this from happening, but known exploits remain unknown until they are exposed and suitable security patches are created. In these circumstances, it's essential to understand where the responsibility for data lies within your business and where it lies with your chosen cloud providers.

Ultimately, the responsibility lies with the data controller; in which case your business is ultimately responsible for any losses. However, if you perform proper due diligence and seek reassurance while choosing a cloud provider, it may be possible to deflect a portion of the blame to your cloud provider and protect your business' reputation. You should always understand the

agreement you have with your cloud provider and be sure that you are aware of your responsibilities, too.

Amazon, one of the leading cloud providers, states that although Amazon Web Services secures the underlying infrastructure, customers are responsible for securing anything they place on its infrastructure. This is where communication with your provider is paramount to a successful and secure business. Each provider is different from the next and just as Amazon advises, your IT people should talk with the security experts at your chosen provider.

DDOS – Distributed Denial of Service

Malicious users have hijacked servers in the past for reasons that range from ransom to protests, but the result is that businesses using those servers suddenly find their applications inaccessible. If your business relies on the use of its CRM, this could render your business inoperable. Hackers often execute DDOS attacks with something as simple as a script sending thousands of simultaneous requests to the server. This would place an unusual load on the server and that would slow or completely shut down the service your business relies upon.



A DDOS attack can cause many problems for businesses using a SaaS solution, whereby the software or the server on which it resides is either a target for an attacker or an unknown victim that hosts the malicious script used to administer the attack. DDOS attacks are also a possible problem if you share a server with organisations that potentially have enemies and your cloud provider provides an elastic compute. Elastic compute allows tenants to increase the amount of processing power they utilise to accommodate increased activity.

In most cases, your requested compute availability is reserved and you would be unaware of the problem faced by neighbouring cloud tenants. The cloud provider should also have measures to prevent this from becoming an issue for any of its tenants, but decision makers should be aware of these issues and have reassurances before making a commitment to a cloud provider.



SQL Injection

SQL injection is one of the greatest risks to any enterprise that has a log-in or access point available online. Businesses that rely on SaaS applications are reliant on the provider for security. Alternatively, your business could place client data at risk if you offer cloud-based applications to customers and fail to take proper precautions to avoid or reduce the risk of exploitation by SQL injection (see Chapter 9 for precautions).

Data belonging to tenants or users of SaaS applications is at risk if an application provider's database is particularly vulnerable to SQL injection; even if the application developers create a user log-in interface with precautions in place. A malicious user could use simple SQL code to return data that belongs to other users if they understand how the application provider constructed the multi-tenant database. Alternatively, some hackers are able to steal the session ID of users so that the application is unaware that an unauthorised user is accessing a restricted area.

Vulnerabilities related to SQL injection are often the most publicly exposed. In the past, hackers have accessed databases with confidential information and published the contents online. SQL injection is a massive topic in itself, which is why it deserves serious consideration during the decision-making process.

Private Cloud Security Issues

As you would expect, private clouds are innately more secure, but this is only true if you take the necessary steps to secure it properly. Afterwards, it's important that everyone in your business is on-board with the governance, risk and compliance that you set to protect your data. You can only really have a secure private cloud environment when all areas of the business properly understand the issues surrounding GRC, not just the CIO.

The rapid growth of cloud services used within businesses often means that it is difficult to limit business use to a private cloud. Many employees with budget control or expense account coupled with the availability of low-cost SaaS applications are contributing factors. Budget controllers may add an application as an expense and by-pass the traditional GRC constraints, which can adversely affect the CIO's ability to manage data responsibly. However, when strict GRC controls are in place, securing a private cloud and the data that resides on that infrastructure is considerably easier. Nevertheless, there are still some security issues to understand.



Building or Outsourcing a Private Cloud

To begin with, many cloud providers offer a private cloud service that we should really call a virtual private cloud, as this description is more appropriate. Hardware manufacturers, such as Dell, will still build private clouds for clients, but many businesses want an off-the-shelf solution. Those businesses want all the ease of use and rapid expansion afforded by the largest cloud providers such as Google, AWS and Microsoft and they want it quickly, but they also want the security benefits of a private cloud set-up.

There is always a fear that virtual private clouds will have the same security issues that affect multi-tenant clouds. This makes it important to speak with your cloud provider to seek assurances that your hardware is not just logically, but physically, separated from other tenants. Some cloud providers achieve the physical separation by reserving compute, memory and storage. That sounds like a reasonable agreement, but you need to ensure that your reserved cloud facilities are in fact the same physical compute and memory locations. This will avoid the vulnerability mentioned in Chapter 4 that described how a previous user's data is accessible to other users on newly provisioned hardware.

If you are not confident in the response from your cloud provider or you regularly handle data that is extremely sensitive, then you should really consider a private cloud in the true meaning of the term. A truly private cloud involves owning your own datacentre, compute and networking with no tenants vying for resources. Even with a private cloud set-up, risks still exist and here are some of the better-known vulnerabilities.

Threats from Within and Spoofing

Thanks to the secure nature of a private cloud set-up, many attacks originate from people who have direct access to the network. While it is often impossible to anticipate attacks by employees from within an organisation, understanding that the employees may be an unconscious partner in the attack will help a business build more robust authentication and access controls.

It is possible for someone intent on penetrating a network to spoof (emulate) users or devices on a network if they are in the general proximity and the network uses wireless connectivity or the intruder has access to the wired network. Chapter 9 suggests ways of detecting and preventing access to devices you suspect of being 'spoofed'.



Non-Compliant Devices and Services

The growth of 'Bring Your Own Device' policies has been exponential, but uncontrolled devices on a private cloud are a security concern. A network is only as strong as its weakest point and without having control over the devices that access the network, you risk exposing your data. Despite access and authentication controls, allowing any device to connect without the proper security creates a potential access point for an attack. Even opening a browser on a non-compliant device, while accessing the private cloud, is a security risk.

GRC breaches are another worry where end-users take data outside of the GRC controls to facilitate their immediate needs. This could be something as simple as transferring a large file via Google Drive or Dropbox rather than creating an account on the chosen internal collaboration software and giving a customer or outsourced team member complete access. Allowing new devices to access your cloud is inevitable, so plan to facilitate collaboration within a controlled environment.

Poorly Configured Security

As every deployment is different, it's easy for IT departments to overlook areas that pose a threat. Some security tools that work well with physical hardware will require additional steps to work properly with a virtualised cloud set-up. For example, a security tool that functions by monitoring traffic will not function if the traffic produced by the application deployment means moving data is from a physical network to a virtual implementation.

This makes IDS, sniffers and traffic monitors redundant unless the hypervisor is able to offload traffic through correct configuration, as data no longer travels through the monitored switches. A greater number of virtualised instances will only add to the complexity and will require thorough planning. Rapid deployment and unfettered cloud growth clearly pose risks that are difficult to control unless the correct GRC controls are in place. On-demand self-service is a 'must-have' feature of modern IT, but innovation and expansion does not need to jeopardise existing operations if your IT people properly configure your security.



Inadequate Penetration Testing

Regardless of how much planning went into your private cloud deployment, vulnerabilities will exist. Penetration testing is an important part of security and should take place regularly – especially where on-demand self-service clouds are a feature of the business IT set-up.

Businesses often overlook penetration testing, but a successful round of testing will highlight more areas of concern than most businesses would like to exist. Software providers often release patches to remove vulnerabilities that may not exist in the software or in every cloud model at the time of deployment. Different data requires different levels of security. For example, the Payment Cards Industry council (1) requires businesses that collect payment card data to perform penetration testing.

Penetration testing should take place periodically and immediately after you implement significant changes to your private cloud set-up. You should be aware of your provider's TOS if you have outsourced your cloud infrastructure, as penetration testing could result in a breach and occasionally be misconstrued as a real attack. Always speak with the security people employed by your cloud provider before you begin testing.

Data Security in Multi-Tenant Clouds

It should now be clear that data in multi-tenant clouds is more at risk than if the same data is isolated from neighbours in a private cloud. However, it's important to understand that even in your private cloud there could be instances where you would consider two different departments of your business as tenants which should not have access to each other's data. Accounts and payroll data is highly sensitive and breaches could cost you dearly. Likewise, R&D may house intellectual property that is valuable and requires protection. This is why many of the principles that protect your data in a public cloud are applicable to private cloud set ups.

Most people reading this book will store or intend to store data residing in both public and private cloud environments. The increasingly complicated and dynamic nature of network topology for multi-tenant clouds means that there will never be a one size fits all security solution. Businesses should just strive to limit risk wherever possible, but it's important to remember that no IT set-up - on or offline, cloud or isolated network - will ever be completely risk-free.



Access Control Methodologies

While most public or multi-tenant cloud providers have adequate systems in place to deter, inhibit or completely block unwanted access, many problems arise from the lack of proper access controls. At one time, many cloud providers relied on a simple identification-based access control (IBAC) system, but that lacks flexibility and limits options when clouds begin to scale. That's why many administrators use a cloud system that allows users to become members of groups that have specific access privileges to applications and locations within the cloud. This system is a role-based access control (RBAC).

As the name suggests, RBAC allows access to users with a certain role. For example, administrators may have greater access than users etc. This works well for businesses that have a small cloud or a cloud with a small number of users, but problems can creep in when

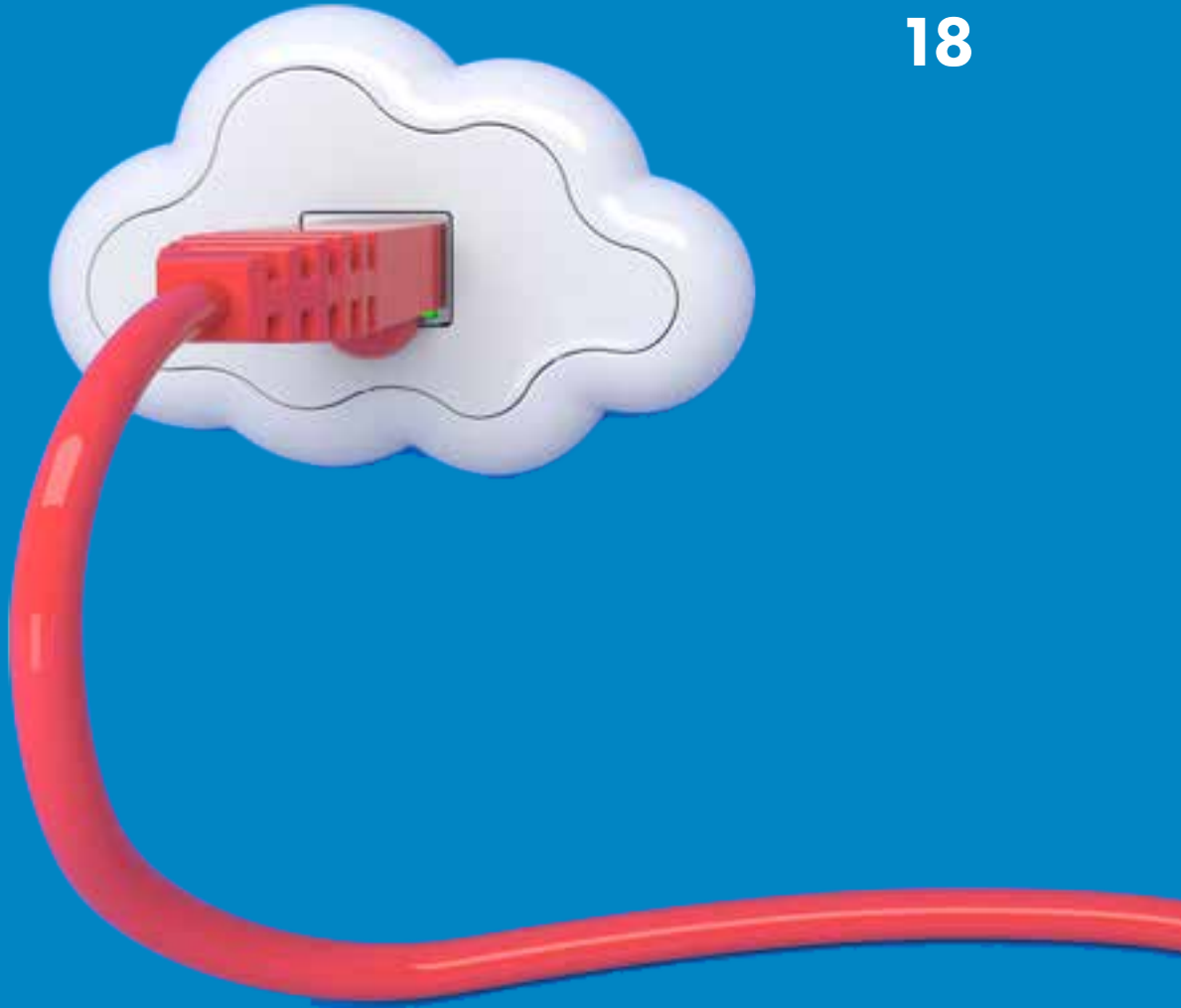
using this system in larger cloud set-ups. Imagine a large business with several locations or teams that access a private cloud with many users on equal access levels that should not really see data from each other's area of work. Clearly, sales, payroll and accounts people in one location should not have access to data that belongs to their peers in another.

In this instance, an attribute-based access control (ABAC) is more suitable, but can be difficult to administer in some circumstances. For example, a user with a certain role accessing via a specific log-in location attribute may be sufficient for some businesses, but it would depend on the data that requires protection.

Data Encryption

Data encryption during transit and at rest is one of the most practical forms of protection because it then provides a level of security from guest to hypervisor escape attacks. However, not all cloud applications and cloud storage options are equal.

Businesses should always encrypt sensitive data in transit and at rest. Many cloud providers will offer packages where the customer decides what level of control it wants in the encryption key management infrastructure (KMI).



Managing your own encryption keys can be a complex choice and in some circumstances could require a bespoke solution, but there are many applications available to simplify the process. A complete solution that handles endpoint encryption is one of the best ways for enterprises controlling sensitive data to operate in the cloud. Look for a package that will facilitate a BYOD environment and ensure regulatory compliance within your operating territories. Dell Data Protection is an example of a package that will reduce your business' deployment timescale by meeting industry and international guidelines.

There may be other providers with similar capabilities, but here's a snapshot of what Dell Data Protection covers:

Industry regulations:

- PCI DSS
- Sarbanes Oxley (SOX)

US Federal & State regulations:

- HIPAA and the HITECH Act
- Gramm Leach Bliley Act California—SB1386
- Massachusetts—201 CMR 17
- Nevada—NRS 603A (which requires PCI DSS) and more than 45 other State and US jurisdiction laws

International regulations:

- US-European Safe Harbor
- EU Data Protection Directive 95/46/EC
- UK Data Protection Act, German BDSG

Your business may simply require good data protection even though you are not subject to the guidelines of any governing body. The Dell product is a good benchmark to use for comparison when deciding on what option is best for your business as this is an enterprise-wide security solution.

Having to micro-manage every area of your data security can be a costly and time-consuming process. However, there are packages that help KMI and related tasks and your cloud provider will usually advise you on the best option for your deployment.

SaaS is Multi-Tenant

Businesses using SaaS applications should be aware that many SaaS offerings operate with a shared database among its customers. This means that each customer accesses the same database, so the segmentation is far less secure than installing the same software on your own servers, whether those servers exist in an IaaS or PaaS environment.

For example, enterprise content management software creator 'Alfresco' offer a fully outsourced solution that would require some scrutiny from businesses that want to store their documents and collaborate with users online.



Alternatively, a business could use the self-hosted version of Alfresco or other offerings such as Microsoft's SharePoint to achieve the same goals in a more secure environment.

Some research into the SaaS application's security capabilities is called for if an application is unavailable for installation on your own servers and it is the best or only option for your business needs. Ask the application provider the following questions:

1. How do you protect data at rest?
2. How do you authenticate and authorise access?
3. What are the SLAs for dealing with breaches and how do you mitigate risk when or if a breach occurs?

Only consider trusting any SaaS application with sensitive data following satisfactory responses.



Compliance and Risk Management

Maintaining control over your cloud-based system is crucial to limiting risk and effective governance is achievable with the right planning. Software is key to enforcing GRC policies in a cloud-computing environment. Even something as simple as implementing secure passwords will mitigate risk, so clearly some GRC control is better than not having any.

Effectively, GRC (Governance, Risk and Compliance) is nothing more than a business objective that uses an understanding of risk within the business to create compliance rules to improve control or governance of data.

The GRC acronym in its simplest definition stands for:

Governance – How you set your data policies and how they are executed.

Risk – Using risk management to limit the likelihood of a negative impact to business objectives by avoiding uncertain processes and practises and mitigating risk through the application of suitable controls.

Compliance – Adhering to regulatory guidelines and applicable laws as well as internal policies and management decisions. Not all data within an organisation is coverable with GRC controls because

it would create a situation whereby everyday activities are unable to function.

For most people involved in GRC controls at larger organisations, the above definitions are too simplistic. But it's impossible to nail down an exact definition because, as with many things in cloud IT, there is no standard set to fit all businesses.

You should decide which processes and workflows require monitoring before deciding on a GRC tool for your business. It is easier to find the right tool for the job when you have a rough idea about what that job will be, even if you are only estimating your needs. This reduces the chances of costly or disruptive process changes to suit your GRC system at a later date.

However, you should also be aware of the tools on the market. Many GRC tools will integrate with datasets directly to ensure compliance with certain regulations that affect data controllers.

Enforcing GRC

Clearly, not all data is the same. Whatever data your cloud IT processes, stores and recalls, there will be some that is subject to your GRC controls - even if it is not a regulatory requirement. However, regulated data has to meet the guidelines set by the regulating authority.

One of the easiest ways to ensure compliance with your industry regulators is to use a centralised GRC system that is already effective for businesses in your industry. Many enterprise-level security systems use the Unified Compliance Framework (UCF) within their products including Qualys - a leader in the security industry and founding member of the Cloud Security Alliance. Many managed service providers use Qualys technology, including Dell SecureWorks. Essentially, the UCF, Qualys and SecureWorks are good benchmarks for any business that has to decide which GRC tool will work best for its cloud-based data.

Data Protection

Firstly, a little background. Data protection can mean many things in many environments, but there are most likely one or more regulatory authorities that stipulate what data protection means to your business. As soon as you employ staff and have access to their personal data, you are effectively a data controller.

A data controller is a person, corporate entity or any group/organisation that is recognisable in law. The exact definition for a data controller is:

A person who (either alone or jointly or in common with other persons) determines, the purposes for which and the manner in which any personal data are, or are to be, processed.
(2)

The UK Data Protection Act (DPA) regulates the use of personal data and has many guidelines about how and why those who have access can use and store that information. Chapter 5 touched lightly on how a business can ensure compliance with the DPA and other similar authorities in different territories, but there is far more to data protection in the cloud than encrypting data.

Understanding Data Controller Obligations

The DPA also regulates the processes a business undertakes in the performance of everyday tasks. The UK Information Commissioner states that any of the following actions constitute the processing of data and are therefore subject to regulation (2):

- Organisation, adaptation or alteration of the information or data.
- Retrieval, consultation or use of the information or data.
- Disclosure of the information or data by transmission, dissemination or otherwise making available.
- Alignment, combination, blocking, erasure or destruction of the information or data.

Effectively, any data you collect or process that belongs to customers or employees falls under the regulatory authority of the DPA. That's for when you're conducting business in the UK; there are similar authorities in Europe and North America.

Where Data Protection and Cloud Computing Meet

Cloud computing technology aids rapid growth in IT systems and provides the freedom to operate in new territories at a moment's notice. That freedom makes it critical to control your business data in a framework that protects against regulatory breaches following a data leak or inappropriate use of data.

Although cloud computing presents many new challenges for businesses, the correct application of GRC solutions often results in a better organisation and easier regulatory compliance. Sourcing a suitable solution to Identity and Access Management (IAM) involves acquiring a suite of applications to suit your specific needs.

Applications such as Quest.com's Identity Manager coupled with SecureWorks should work in harmony, as they are now both Dell acquisitions. Other developers in the market will have products that work well with competing managed services. However, experience suggests that using one source for your cloud security/GRC avoids the problem of overlapping services and conflicting governance issues.

Protecting Data on Mobile Devices

Cloud computing is an enabler of mobility. Enterprise Mobility Management (EMM) is another area that requires a high level of access control. BYOD is an increasing necessity for businesses with highly mobile employees and some that just find it beneficial to access their work email and collaboration software on their own devices from any location. There are many ways to ensure access controls are maintainable on almost any device, but not all have the required capabilities for users to access a secure workspace with Data Loss Prevention Technology (DLP).

Ideally, your chosen EMM product should work with hypervisor technology when installed on the device. Data should always undergo encryption and at the bare minimum sit in a logically isolated environment with policy enforcement and remote access capabilities for administrators.

A typical EMM suite should empower IT administrators with the following features:

- Password management
- Device registration and monitoring
- Locate, lock and wipe capabilities
- Monitor individual and group policies
- Instant or real-time report availability
- Compliance alerts and granular events
- Audit trails
- Application distribution

Many of the EMM products in the market have the listed features (including Dell's). Again, choose a provider that interacts seamlessly with your cloud security and choice of GRC monitoring/enforcement - Connected security is all about integrating protection for as many of your network locations as possible and that is really only achievable when applications and your network deployments work with synergy.

Loss of Governance

Loss of governance occurs when the organisation does not have control over the infrastructure on which its compute and storage takes place. This can have implications for businesses using data that falls under certain regulations because many regulations restrict the transfer of data outside of the control of the organisation. The geographical location of data can also present problems for an organisation that has to abide by the rules of regulatory authorities.

Governance is one of the key challenges for cloud deployments. Many businesses use SaaS that instantly contravene regulations because the organisation lacks control of the infrastructure that houses data entrusted to it by a third party. Even with PaaS, businesses only share control of the hosted application and virtual machines with the provider. Strictly speaking, only dedicated IT in a truly private cloud environment prevents sharing of control with a provider.

In 2010, the University of Oregon identified the loss of governance as high risk with a high probability that it will happen at some point in an IaaS environment (3). Thankfully, the market reacted to a demand for better control and the widespread loss of governance is less of an issue today.

Improvements in the governance landscape is partly due to the growth in cloud-skilled IT professionals managing private clouds or merging a business' own infrastructure to create hybrid deployments, but the major providers have acted too. Many cloud providers work with security product developers and managed security service providers to ensure that data is secure and only unencrypted when viewable to data controllers.

Some international regulations have issues with data ownership, confidentiality and jurisdictional storage that occur when businesses share governance, which some businesses circumvent by using enhanced contracts with providers. However, the validity and effectiveness of a contract remains untested in a court of law. The retention and disposal of data are often features of these contracts as some cloud providers have held on to data after an organisation has stopped using their services.

Retention of data is rarely for malicious reasons. In some cases, businesses have defaulted on payments or become insolvent and failed to inform the cloud provider of the situation. The provider has held on to data to ease the reuptake of its services as quickly as possible if the business' credit card starts working again.

What Every Business Needs to Know

It is important to remember that delegating governance and management of your business' cloud services does not discharge your organisation from the ultimate responsibility of protecting its business and customer data. Who is able to access, delete and replicate data is a critical concern for businesses operating in a highly regulated industry. When a business solves those issues through effective controls, how does the organisation enforce the policies?

Organisations that consider both infrastructure and security governance at each decision stage will have a much more secure cloud deployment than the same deployment with retrospective governance controls.

Governance Planning – What and When

The stages of cloud deployment may differ between businesses because each will have unique requirements, but decision stages are essentially the following:

1. Cloud strategy
2. Design of cloud architecture and deployment
3. Vendor selection and the negotiation of contracts or cloud architecture acquisition
4. Resource provisioning and subsequent management
5. Operation management

Each stage of planning will present challenges and sometimes it is useful to speak with several cloud providers during the decision-making process. Investigate what tools are available that will help your organisation streamline GRC controls.

Security Measures

As with all chapters of this book, the information contained in this section is only supplementary to your own risk assessments and penetration testing. While the following methods of protection are useful deterrents, software and hardware configurations are constantly changing and presenting new challenges for secure computing in the cloud.

Cloud users should consider outsourcing their firewall service to a reputable company that provides the following features in their managed firewall:

- IPS/IDS
- Firewall
- Anti-virus
- Anti-spyware
- Application control
- Content filtering
- Wireless LAN
- VPN tunnels
- Multi-WAN support

Precautions

Some precautions will instantly add layers of protection without adding additional expense. They are not replacements for comprehensive security software or hardware.

Segregate Data and Limit Internet Access

Demilitarised zones (DMZs) are a cost-effective security measure because it reduces the routes available to network intruders to just one or two ports. Use a DMZ for anything that needs access to the Internet such as web and mail servers. Then you can protect areas of your infrastructure that contain sensitive information, such as your MySQL servers.

Use a VPC where possible

Place your DMZs within a VPC. VPCs have several advantages when using a public cloud:

1. Your IT security doesn't need to track the new IP of each instance as they start and stop.
2. Many cloud providers have VPC security groups that enable outbound filtering.
3. DMZs and Private segregation are easy to organise and apply security settings because you can have different settings for each IP range.

Use Two or multi-Factor Authentication

Almost every cloud provider gives users the option of a two-stage authentication. Even free email accounts use this as a security measure so it would be irresponsible to ignore the option and rely on a simple username and password for access to your critical data.

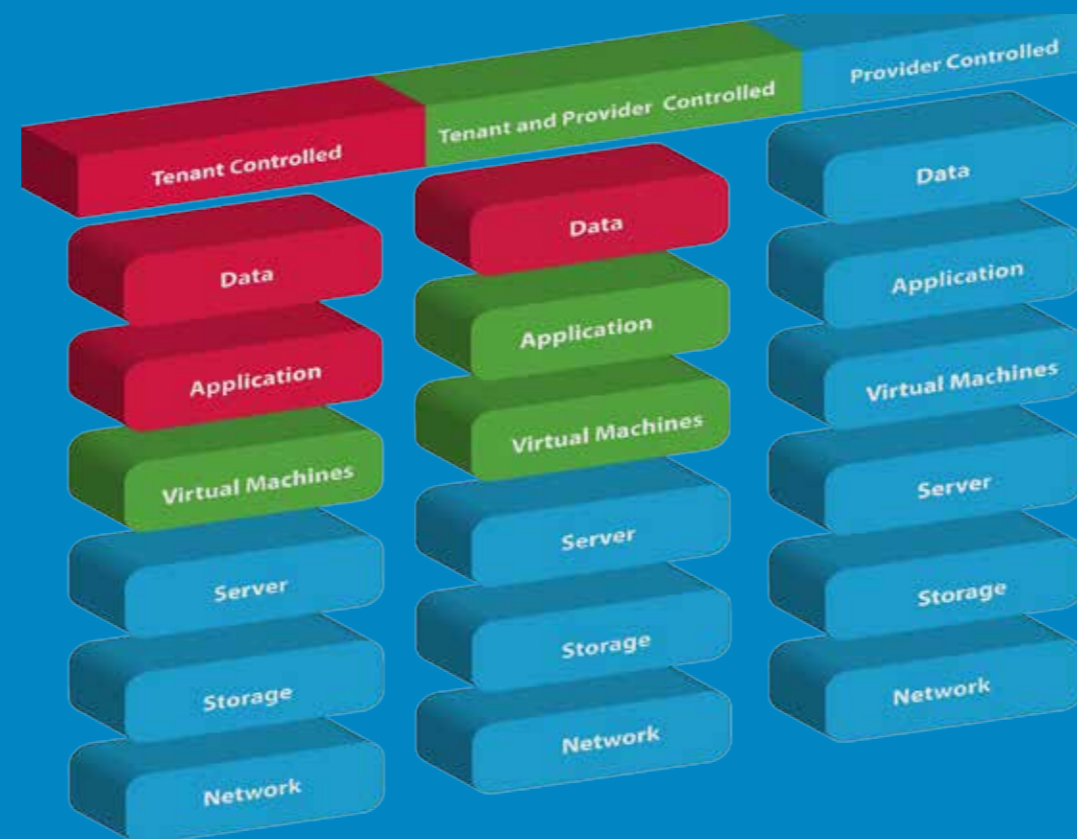
Encrypt Sensitive Data at Rest

Businesses should encrypt both offline and cloud disk images that contain sensitive data. Virtual disks and backups are easy to clone following a successful attack. Encrypting data at rest is an essential security feature that every business should employ. Decide on an encryption key manager to ease the process at the deployment planning stage as this will save time later. Some encryption solutions (such as Dell DPP) use remote management, audit and policy settings.

Ten Step Plan for a Secure Cloud

Every cloud deployment is different because of a seemingly infinite amount of diverse application and hardware configurations. All cloud security should follow a risk-based approach with suitable actions to remove or limit any identified risks. However, new risks emerge constantly and vulnerabilities require patching; so it's important to have a solid framework in place that makes security management easier.

It is important to understand who controls what in when planning security SLAs and implementing controls. Any business that relies on a cloud provider for security should have understand how the service or infrastructure provider's security protects the organisation's data. The business may need to implement further security measures if the standard offering is insufficient. The diagram below explains where the responsibility for security and control lies in most deployments



Ten Step Plan for a Secure Cloud

Every cloud deployment is different because of a seemingly infinite amount of diverse application and hardware configurations. All cloud security should follow a risk-based approach with suitable actions to remove or limit any identified risks. However, new risks emerge constantly and vulnerabilities require patching; so it's important to have a solid framework in place that makes security management easier.

1. Plan and Agree GRC Internally and with Cloud Providers

The need for effective GRC has been a feature of this publication. Your organisation's GRC should follow an extensive risk analysis that allows you to set controls in place to mitigate the risk. Your contract and service level agreements with any cloud provider should reference compliance and security policies wherever necessary.

Reporting of security breaches is a time-critical factor when dealing with regulatory authorities, so ensure this is a feature of your contract. You should also have a solid grasp of where the responsibility for securing your cloud deployment falls within your organisation and where you delegate or share responsibility with the cloud provider. The previous diagram helps explain where responsibility lies in simple terms, ultimately, as an organisation entrusted with data the responsibility lies with your business. Using providers with ISO 27001 certification is a good place to start, but you should always vet the provider's security.

2. Audit Processes to Check Effectiveness

Frequent audits of IT systems ensure your organisation is effective at enforcing policies that may be internal or external requirements. Cloud providers will usually provide reports from an independent auditor and this should feature as an agreement on your contract.

Access to information relative to an application audit event is also important to ensure hosted or SaaS applications continue to meet the regulatory compliance needs of the organisation.

Auditors and organisations using cloud should consider the following areas of security:

The cloud provider risk and control environment related to cloud services provision.

The cloud provider should be able to provide customers with transparency when a business or auditor questions the day-to-day activities of employees, including how the provider handles access and authorisation. Each business should have a complete understanding of the isolation methods used to protect their data, especially in a multi-tenant environment.

Access to audit trails that span services of the cloud provider.

Access to audit trails is essential for any business when testing the effectiveness of its security controls. You should see evidence of authentication and authorization event logging and management information that meets

your security and compliance policies. Information gathered during the audit should demonstrate the effectiveness of the security measures against known threats. It is impossible to audit for the unknown.

How the provider allows organisations to self-manage and secure cloud services.

Self-management and the ability to monitor cloud usage is an absolute necessity for businesses using IaaS. Self-management enables the business to run audits, as well as grant or remove access and authorisation to users. The business also has complete access to how those users and the business itself uses hosted applications and services.

3. Map how you will manage people, roles and identities

Access and authorisation is a major consideration during the planning stage of a business' cloud computing. Cloud providers must enable organisations to assign privileges and users to groups to limit the capabilities of some while empowering other employees in the business. Identity and privilege management along with the ability to add attributes to applications, resources and users are essential tools for cloud security. Using appropriate identity and access management within a cloud deployment ensures accurate logging of activity and provides a traceable route that is essential when auditing.

4. Protect Data

The risk of theft and disclosure to unauthorised entities and modification of data are core considerations. The distributed nature of cloud deployments creates added risks, which makes data encryption at rest and in motion an essential feature. View the standards contained in ISO 27002 (5), which is entitled 'Information technology — Security techniques — Code of practice for information security controls.' Also view ISO/IEC CD 27017 (6) which is in development, but is scheduled for publication in October of 2015. The International Standards Organisation states that ISO 27017 is a code of practice for information security controls for cloud computing services based on ISO/IEC 27002 (6).

5. Maintain Privacy Policies

Personal and Identifiable Information (PII) is an ever-present concern in modern IT environments. Businesses using a public cloud, even if that deployment uses VPCs, should be familiar with ISO/IEC 27018:2014. The standard is the code of practice for the protection of PII in public clouds. As mentioned on numerous occasions in this document, the responsibility for PII remains with data controllers even when delegating services or using cloud providers.

A legally binding agreement is sometimes required to satisfy regulatory requirements when a business uses cloud services that will subsequently have control and possible access to sensitive data. Properly defined privacy policies within a business are essential to secure operations and to add validity to any legal agreements between an organisation and the cloud provider it employs.

6. Secure Business Critical Applications

Application security begins at the design stage and continues all the way through the lifecycle. Securing applications from both internal and external threats requires enforcement of security policies and the adherence of operational processes. Inadequate security policies or poorly executed enforcement is a primary concern for businesses.

Cloud infrastructure presents security challenges for providers and application developers that amplify when the cloud grows. Virtual machine and application sprawl make auditing and remedying the situation difficult. The responsibility for application security lies with the data-controlling organisation in both IaaS and PaaS environments and only passes to the cloud vendor when it is providing a SaaS application.

Understanding the provider's architecture, when using IaaS or PaaS, is a major factor when creating or deploying applications in the cloud. Authorisation and authentication is a priority in an IaaS environment, as is the ability to audit effectively. Organisations that use PaaS services will need confidence in their provider along with the strength of the agreed contract and SLAs.

7. Secure the Network

Perimeter security that protects on-premise networks should work with a Unified Threat Management (UTM) option designed to work with clouds. A secured network would screen traffic, detect and prevent intrusions while logging information for later use. This must take place both in the organisation's premises as well as the cloud.

The use of logging can cause an issue with some cloud providers, because of the possibility of logging sensitive data. Incident handling and reporting should also feature in an organisation's network security solution as it does with all other areas of where the business monitors traffic and enforces security policies.

All organisations must be aware of the precautions taken by cloud providers when relying on a provider of virtual local area networks (VLAN), rather than a physical LAN. Incidents of VLANs allowing attacks to take place where users gain access to other network users are rare, but ask the question of any cloud provider where your systems share a physical network. The use of software firewalls is essential for each instance that uses a VLAN on a physical network that it shares with neighbours in a multi-tenant environment.

8. Secure the Physical Location of the Network

The physical location of an organisation's datacentre may become a target for attack if motivated individuals are unsuccessful when attempting remote access. The amount and type of security an organisation employs will depend on the data stored.

Even with relatively low interest data, other datacentre tenants could be the target for an attack. Ask the cloud provider to explain what measures are in place in case of a physical attack or if environmental factors put your data at risk. Does the datacentre have an alternative power source? What controls are in place to ensure the datacentre copes with environmental incidents? All these questions are important.

Planning for data controls and misuse of access should take place before thorough and frequent training of properly vetted personnel. This is a necessity for both the organisation and the cloud provider that it employs. Establish a continuity plan or include the plans in SLAs and a legal contract with your provider.

9. Create and Maintain Manageable Security SLAs

Service level agreements will and should contain information that holds both the organisation and the cloud provider accountable for their respective roles in protecting the organisation's data. Breach reporting should form part of the agreements and in some cases with reports flowing both ways depending on where and how the breach occurs.

Statements to ensure cloud service providers bound by SLAs pass the same responsibilities on to any third party providers are used to facilitate the needs of the employer organisation. SLAs should also contain standards to meet with agreed performance metrics that the organisation and cloud provider periodically reviews. Metrics are an essential element of SLAs because they help measure the effectiveness of security policies and operating processes.

10. Know How to Terminate a Cloud Service Contract

The cloud service agreements are not life-long commitments. It could be time to move as soon as security metrics fall below acceptable levels or the capabilities of a cloud provider are less impressive than that of a competitor. Whatever the reason, plans for removal of data, logs and audit trails must be visible when an organisation no longer wants to use the cloud provider. The only exception to this rule is when local or international laws that govern the data stored by the cloud provider, on behalf of the business, require its retention.

Will I Then Have a Secure Cloud?

No IT environment, cloud or on-premise can ever be completely secure even after extensive planning and taking every possible precaution. Your business can simply manage and mitigate risk with good governance and enforcement of security policies.

Works Cited

1. PCI Security Standards Council. Information Supplement: Requirement 11.3 Penetration. s.l. : PCI Security Standards Council, 2008.
2. Information Commissioner's Office. Key definitions of the Data Protection Act. <http://ico.org.uk/>. [Online] [Cited:] http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#type.
3. Betcher, Thomas J. Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners. Unversity of Oregon. [Online] Febraury 2010. [Cited: 09 September 2014.] <http://aim.uoregon.edu/research/ebriefings/eb-betcher.php>.
4. International Organization for Standardization. ISO/IEC 27002:2013. www.iso.org. [Online] [Cited: 11 September 2014.] http://www.iso.org/iso/catalogue_detail?csnumber=54533.
5. International Organization for Standardization. ISO/IEC CD 27017. www.iso.org. [Online] [Cited: 10 September 2014.] http://www.iso.org/iso/catalogue_detail.htm?csnumber=43757.
6. Covington & Burlington LLP. The USA PATRIOT Act and the Use of Cloud Services: . www.insideprivacy.com/. [Online] [Cited: 09 10 2014.] <http://www.insideprivacy.com/PatriotActQA.pdf>.

Notice:

This document may be copied and distributed in its full and unedited form. No permission to edit the content of this document is granted or implied.

Distributors do not have permission to charge any fee for copies of this document.

Permission to quote and reproduce snippets is granted provided full credit is given to the original work.

Written under commission for iProspect, 5th Floor, 10 Triton Street, London, NW1 3BF

United Kingdom Author Shaun Thomas Copyright © All Rights Reserved.