INFORMATION & DATA SECURITY IN THE PUBLIC CLOUD

The Process Every Enterprise Should Think Through

Featuring research from

Gartner®

TABLE OF CONTENTS

ABSTRACT	3
INTRODUCTION	3
Public clouds: fundamental characteristics	4
Separating data in multi-tenant environments	4
Why cloud computing is resilient	5
Security – pertinent pain pressure points	5
Mitigations – steps every cloud user should consider	6
Additional levels of security	7
Conclusion – what you need to do next…	8
Gartner: Privacy in the Cloud	9
ABOUT RACKSPACE	17
Rackspace Hosting	17

Summary

Cloud computing is now accepted as the greatest change in the technology industry since broadband Internet became mainstream. While enterprises welcome the business agility and flexible economics of the cloud model of IT, there are natural concerns regarding cloud security.

The purpose of this guide is to set out in straightforward terms the risks associated with cloud technology and the mitigation options available, to help buyers find a solution that fits their needs.

For more help making your choice, please contact Rackspace – the home of Fanatical Support®

Introduction

Cloud solutions should be selected and evaluated with security in mind, to avoid costly and time consuming mistakes

Enterprise customers considering a move to cloud computing have voiced concerns over security in this new computing paradigm. Over and above apprehension focused on traditional vulnerabilities, new areas of concern including data regulation and compliance now come to the fore.

Compliance concerns may relate to data protection, PCI standards, Sarbanes-Oxley, rulings made by the Information Commissioner's Office and the DSS. While initial resistance to cloud computing may be borne out of unfamiliarity, even educated users may have legitimate concerns.

A string of public data breaches during 2011 has not helped the safety image of Internet-based services and systems. Internationally, we have witnessed Sony's PlayStation Network being compromised and 70 million gamers' personal details being hacked. Closer to the UK, we have seen the Information Commissioner's Office issue Surrey County Council with a £120,000 fine for a serious breach of the Data Protection Act. Suddenly, online data storage has never been a more sensitive and contentious issue.

Essentially, companies are concerned about what happens to their data when it moves to the public cloud and steps outside of their premises and into a hosting centre. For full public cloud deployments, this 'migration' necessitates a move for data and applications from a dedicated infrastructure to a multi-tenant infrastructure.

This need not be a concern if sensitive data is held back from the cloud model; this need not be a concern if critical applications are sent to the cloud, and this need not be a concern if a company's cloud-based applications have cloud-compliant licensing options. But whichever technical steps are taken, the fundamentals remain true: the cloud solution must comply with a customer's security policy. Cloud solutions should be selected and evaluated with security in mind, to avoid costly and time-consuming mistakes.

Point to note: The information contained in this white paper relates to the public cloud. For private cloud, Rackspace also offers other options for greater protection and security.

Public clouds: fundamental characteristics

Before we go any deeper into security issues, let us just lay down the parameters by which we measure a public cloud. Based on the standard cloud computing model including options for both applications and storage, the public cloud is accessed over an Internet connection on a pay-per-usage model and therefore has exceptional scalability.

With the ability to provide new 'instances' of public cloud servers within minutes, this computing model is attractive to companies with variable demand cycles who want to avoid capital expenditure on physical units that will experience inefficient and costly periods of disuse. It is also ideally suited to any transient IT requirement, whether this be for test and development environments, for seasonal capacity, or for time-bound projects.

All virtual machines are segmented in memory and have no cross-memory access

Inherent to its very nature then, the public cloud is not an on-premise computing solution i.e. the physical server units that power the public cloud are housed within a data centre in another location. Further distancing cloud customers from the details of where its data will reside, the customer trusts the cloud provider to place their cloud data and applications on an unspecified server inside its data centre. This in itself may appear to be a concern to the customer, but it is in fact a security layer in its own right i.e. no one cloud customer will know if their data is housed next to that of a competitor.

Separating data in multi-tenant environments

Cloud computing uses industry-standard hypervisor technology to enable the sharing of physical servers by more than one customer - and this ensures that all virtual machines are segmented in memory and have no cross-memory access. In a cloud server, the hypervisor drives the dedicated partition between the two data blocks and there is also a separation of memory so that no two volumes can accidentally share the same memory blocks. Each cloud server is allocated a fixed block of memory and in a Rackspace cloud, the open source Xen and/or Citrix Xen Server hypervisor is responsible for this.

The function of the hypervisor, then, is to allow multiple virtual servers to co-exist on the same physical host machine. The hypervisor ensures that the performance of one virtual server is segregated from all other virtual servers and it also serves to separate all other virtual servers from a security perspective. It is worth noting that many public clouds including both the Amazon and Rackspace clouds use flavours of the proven Xen hypervisor, providing an extra level of confidence as to the robustness of the solution.

Even with this built-in resilience to accidental cross contamination, hypervisors are not immune to security exploitations. It's been reported[1] by IBM security researchers that up to 35% of servers tested had escape-to-hypervisor vulnerabilities, meaning that one VM could affect other VMs. In an industrial-strength cloud, far fewer servers should be vulnerable, but this highlights the need for very clear thinking when deciding what data or apps to house in the cloud.

Why cloud computing is resilient

The distributed nature of public clouds creates a degree of resilience in itself. When a customer virtualises their own physical server, a failure of the host server will inevitably result in failure of all the guest servers housed on that host. In well designed cloud solutions, guest servers are by design distributed across different host machines, specifically to avoid this problem. This means that when a physical host machine fails on the cloud (as they inevitably will in due course) the impact on individual users is minimised.

The same distributed design approach applies to cloud storage – typically data stored in public clouds is replicated across physical infrastructure, to mitigate the impact of any single physical failure – for example Rackspace replicates all data stored in Cloud Files into three different areas of each data centre. Note that the location of the data is commonly specifically identified to customers – although there is much discussion that "you never know where your data is once it's in the cloud", this is rarely the case with Infrastructure-as-a-Service solutions.

The biggest threat to IT always comes from internal threats

In addition to these built-in elements of redundancy, as cloud technology evolves, it is also becoming more feasible to build cloud infrastructures that are designed to withstand failure of individual components. Resilient solutions – ones that duplicate infrastructural components, as protection against failure – have traditionally been a rather costly solution. However, public cloud services are much lower cost than traditional dedicated services and on clouds that support cloud load-balancing, resilient solutions are now much more affordable.

Security – pertinent pain pressure points

Among organisations considering a move to the cloud, security concerns are often raised at every level of the business as little more than a technically phrased knee-jerk reaction. These alerts are typically driven above all by the FUD-factor i.e. fear, uncertainty and doubt. Businesses feel some kind of loss of control as data moves off site to be controlled by some new and seemingly unknown technology power.

Companies often feel that they have been working with security policies that have been 'good enough so far' in the pre-cloud era. Interestingly, almost every IT security survey you will read suggests that the biggest threat to IT always comes from internal threats. But leaving this reality aside for a moment, cloud is still a new technology and by definition then: companies say that they don't know what the vulnerabilities will be in a post-deployment scenario.

[1]IBM X-Force® 2010 Mid-Year Trend and Risk Report, August 2010, Page 55 – see: ftp://public.dhe.ibm.com/common/ssi/ecm/en/wgl03003usen/WGL03003USEN.PDF

So there is scepticism here, but the reality is that although cloud computing is new, it is not very different at all from the virtualisation practices that have been going on in many companies for more than a decade now. What is perhaps not so clear is how all the nuts and bolts fit together when you move virtualisation to the cloud, as it now happens under the auspices of the cloud provider.

So it appears to businesses that they have to just take this element of their IT model on trust i.e. the status and parameters that govern the host devices, the networking layer and where exactly the virtual machine in use is residing. Of course, a simple conversation with the service provider in question overcomes this issue – and, if the provider in question is not willing to talk to you and provide this level of transparency then you will would be best advised to look elsewhere for your cloud computing.

Mitigations – steps every cloud user should consider

For many companies, the issue that needs to be addressed is the question of how data is processed and stored in the cloud. The reality is that the process and actions traditionally taken by security-aware organisations to secure their own on-premise infrastructures are the same steps that need to be taken to ensure security in the cloud.

A review of the company's existing security policy and of how cloud plays against it, may be all that is necessary. Moving to the cloud does not necessarily mean reaching a new compliancy level, rather it requires a clear understanding of how cloud can be implemented and used within existing policy guidelines.

There is much that organisations can do to prepare for the cloud in terms of provisioning for appropriate levels of business security before they migrate. A simple first step is to consider whether some or all data stored in a public cloud needs to be encrypted. Public cloud is by nature Internet-accessible, and each organisation's security policy should give guidelines on encryption use for sensitive data.

Equally it is best practice that all servers, whether cloud or conventional, should be protected by a firewall. For cloud servers, the standard software firewalls are Windows Firewall (for cloud servers running a Microsoft OS) or iptables (for cloud servers running Linux). On most clouds, configuring software firewalls is a customer responsibility – alternatively customers of Rackspace's "Cloud Servers with a Managed Service Level" can also request advice and assistance to set up firewalls to comply with their policy.

Additional levels of security

Organisations that need higher levels of security should look to hybrid hosting (e.g. Rackspace's RackConnect service) to combine cloud computing with enterprise security solutions.

Hybrid hosting combines cloud hosting with traditional IT. This means that an organisation using hybrid hosting can configure their cloud infrastructure to sit behind any or all of a range of proven defence solutions, including:

- dedicated hardware firewalls: these are frequently specified by customer security policies and are also a common requirement for regulatory compliance
- DDoS Protection: these solutions protect against malicious attempts to swamp websites by launching such large volumes of otherwise legitimate requests, such that the website capacity is overwhelmed
- Intrusion Detection Services: these services highlight the fact that a security vulnerability has been exploited

Organisations that need higher levels of security should look to hybrid hosting

A typical application of such a hybrid solution would to be to enable a content library to be securely hosted in the cloud. In this example, large volumes of static content (images, documents, files etc) can be hosted in a flexible and cost effective way using cloud storage. Using a hybrid solution means that dedicated security appliances can be used to managed secure access to that content library. If transactional capability is also required (e.g. for PCI-compliant sales of that content), then this can be included in the solution using a dedicated server infrastructure.

Organisations can use hybrid solutions to build web servers that can survive sudden spikes. All leading cloud-based servers are available with an API, to enable provisioning to be automated into user applications. This means that when capacity thresholds are passed on a primary dedicated web server, additional cloud-based web servers can be provisioned automatically. Once demand falls again (as it typically does) those cloud-based web servers can be de-provisioned to save cost. Since the solution is hybrid, transactional activity can be always be handled securely by the dedicated elements of the solution.

Finally, hybrid solutions can be used as a way to add a termination point for a Virtual Private Network (VPN) into a cloud infrastructure. This would be useful to enable secure uploading to cloud servers, or to secure a pool of cloud servers e.g. for batch processing.

Conclusion – what you need to do next...

- If your company is about to consider a move to the cloud computing model of IT delivery, then remember that the same level of security provisioning should be accommodated for wherever your data resides. The cloud is no different. So, review your security policy (what are you protecting and what are you protecting this from) against the capabilities and limitations of the cloud itself before you embark on a cloud migration programme.
- Decide which parts of your infrastructure can and cannot be delivered into the cloud. Naturally, there will be a separation of data, a separation of applications and a separation of mission-critical relevance and sensitivity among the different technology modules that make up your company's whole IT 'stack'. Being able to audit, configure and manage different datasets and data streams is a pre-requisite if you are to intelligently move towards a public and/or hybrid cloud-based model of IT services.
- Get moving – those who delay will be overtaken by their competitors!

From the Gartner Files:

Privacy in the Cloud

Many IT organizations encounter resistance from legal, compliance or risk managers when considering cloud computing for personal information. Security and privacy concerns are currently the most visible inhibitors to cloud computing (see, for example, "Private Cloud Computing Plans From Conference Polls"). This will change when organizations decide that some of these concerns are without basis and that the remaining risks can be mitigated or accepted. This research is relevant for IT departments, privacy and information security officers, business units, and compliance and risk managers.

Key Findings

- Most organizations are reluctant to use cloud services when this involves a transfer of personal information to the cloud.
- Some organizations transfer personal information to the cloud, despite widespread legal concerns. They have found ways to comply with applicable privacy laws – for example, by implementing a privacy program with contractual privacy guarantees or encryption.
- Many organizations have evaluated cloud computing and the impact on privacy in 2010. The number of organizations that move from pilot to production will increase rapidly in 2011.

Recommendations

- Seek acceptance for moving personal information to the cloud by engaging with relevant internal and external roles, not just with legal advisors.
- Consider the applicable jurisdiction ("legal location"), as well as the physical location of data storage, to address both legal and political concerns.
- Put pressure on providers to commit to the location of cloud data centers (or even to change it), and ask under which conditions they will hand over personal information to law enforcement agencies and tax and financial auditors.
- Treat personal information like any other valuable information, and apply best practices for information security and risk management.

STRATEGIC PLANNING ASSUMPTION

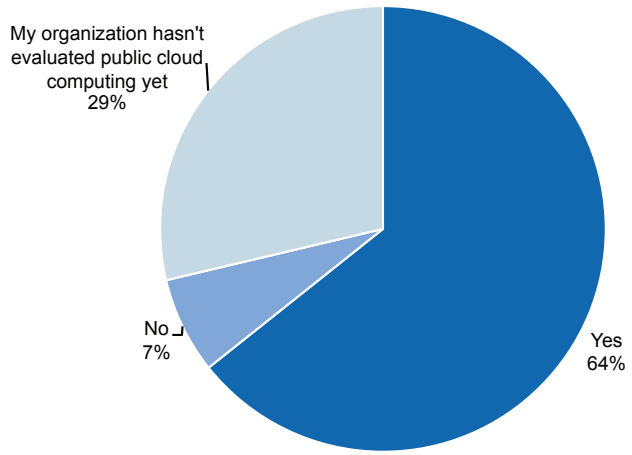
By 2014, less than 10% of enterprises evaluating public cloud computing will view privacy concerns as an exclusion criterion.

ANALYSIS

What Gartner Clients Think About Cloud Privacy

Many organizations see privacy at odds with cloud computing. In a Gartner conference survey conducted in November 2010 (n = 143), 64% of respondents said that their organization views privacy concerns as a criterion for exclusion when evaluating public cloud computing.

Figure 1. Privacy Concerns as a Criterion for Exclusion



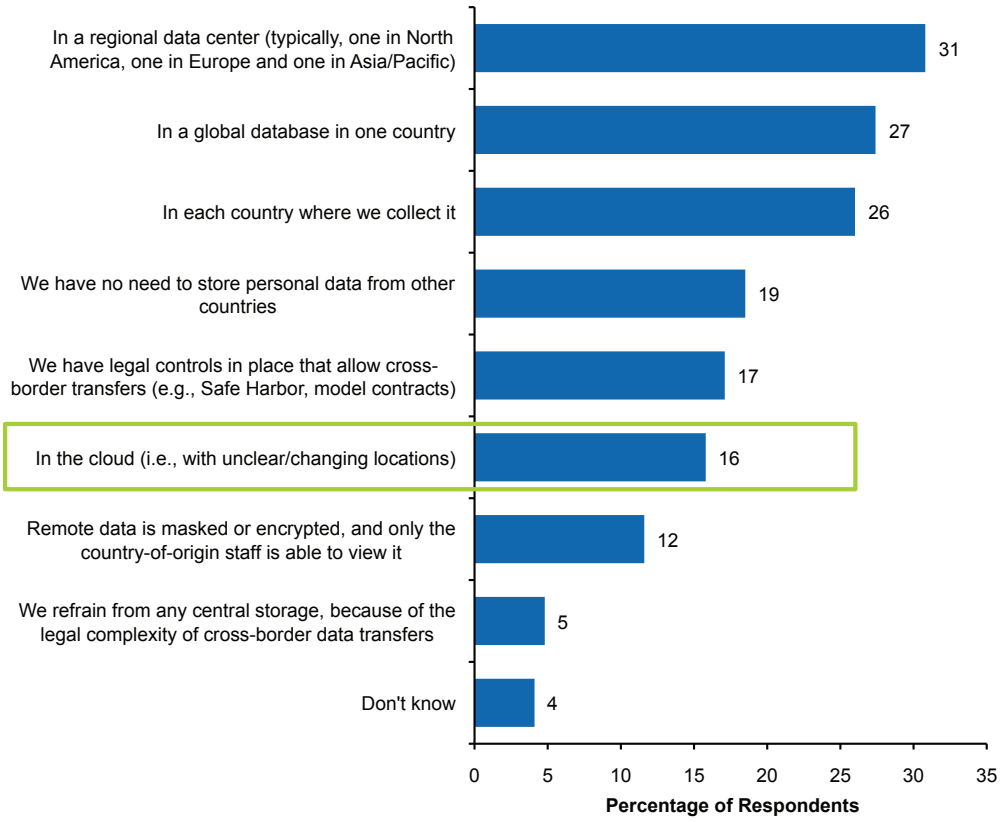
Source: Gartner (February 2011)

Figure 1 shows results from the survey question: "When evaluating public cloud computing, does your organization view privacy concerns as a criterion for exclusion?"

However, not all organizations share this view. In Gartner's yearly privacy survey (n = 146), conducted in December 2010, some organizations (16%) clearly acknowledge that they have already moved personal information to the cloud. These numbers are highest in manufacturing and communications/media, and very low in banking, insurance, government and healthcare.

Figure 2 shows results from the survey question: "Where and how does your organization store and process personal data?"

Figure 2. Personal Information in the Cloud



Source: Gartner (February 2011)

Moreover, 31% of respondents also said that they store personal information in a regional data center (rather than in the country of origin). A global database is also not unusual (27%). All these responses mean that personal information has left the country in which it was collected. While many organizations – especially in Europe – seem to believe that it is illegal to store personal information in the cloud, others have done exactly that. The following section describes some of these misconceptions and explains Gartner's view, based on client interactions since late 2009.

Myths and Realities About Cloud Privacy

Concern: Moving personal data to the cloud is against the law.

Clarification: Gartner has spoken to many organizations, and not one of them could name a law that explicitly forbids cloud computing. Many legal advisors interpret existing laws to mean that such a prohibition exists, but this interpretation will change over time as more organizations embrace the cloud-computing model. Gartner is not aware of a legal case in which an organization has been fined because it moved personal information to the cloud. Even where companies have not protected personal information adequately outside of the cloud environment, monetary fines have been rather moderate (typically, tens of thousands of dollars/euros). Substantial fines (a million dollars/euros or more) have, in most cases, been assessed only to companies that engaged in illegal surveillance and/or have refused to collaborate with data protection authorities once the incidents were made public.

Concern: Moving personal data to another country is forbidden.

Clarification: The EU Privacy Directive is quoted in that context, and it is true that there are provisions about international transfers in the directive and in implementing laws. However, the law doesn't say that international transfers are always forbidden. It says that international transfers are allowed only if certain conditions are met, and there are defined and proven ways to establish these conditions (see Note 1). On the other hand, some organizations might have their own requirements to keep personal data in the country – for example, employment records of an intelligence agency or telecommunications records captured for a law enforcement agency.

Concern: There are legal requirements regarding the physical storage of personal data.

Clarification: Most laws do not relate to the physical location of data – they relate to the legal location of data. In other words, the legal entity that holds the data determines the location – and not the location of the server, the citizenship of the individual or the place of collection. Where the cloud service provider and the organization that consumes cloud services are legally registered in the same jurisdiction, companies have taken the position that there is no legal problem, because the contractual obligations can be enforced locally.

However, contractual terms can vary widely. In some cases, they might include the EU's model contracts for privacy; in other cases, they are a negotiation between the cloud-service-consuming organization and the cloud provider and, essentially, a question of purchasing power. Some organizations that want to put data into the cloud have already signed contractual agreements with *their* clients to store data locally, making a move to the cloud impossible. Moreover, clients occasionally report the requirement to physically store data in Switzerland or China, but this is usually industry-specific (for example, private banking).

Concern: We cannot engage with a U.S. cloud service provider, because the USA Patriot Act gives U.S. authorities unlimited access to personal data.

Clarification: This situation is not specific to the U.S. All countries have rules in place that allow law enforcement authorities to access personal information hosted by third parties in case of terrorism or severe crime, or to protect national security. Rules vary. In some cases, a search warrant or a court order is required; in other cases, a subpoena is sufficient (which can take the form of a national security letter in the U.S.). In some cases, authorities must precisely specify the data they are looking for; in other cases, they can take a larger snapshot of a data store. In some cases, they can sift through historical data; in other cases, they can access only the most recent data (a so-called "quick freeze").

The main reason many organizations are concerned about the USA Patriot Act is that this law has such a remarkable name. According to Gartner's 2011 compliance survey (n = 185), 14% of respondents have already received a request for information based on the USA Patriot Act. However, authorities in other countries, including the organization's home country, might have access as well. About 32% of respondents said that they have had to hand over data to support a criminal investigation.

Concern: Everybody else is already moving to the cloud; only we are overly concerned with privacy.

Clarification: The opposite is true. At the time of this writing, Gartner is not aware of any company that uses public cloud services with a shared infrastructure for the processing of personal information in Europe, the U.S. and beyond on a large scale in production. However, there are many examples of companies that use cloud services in one country (often in the U.S.), in a specific business unit (or in headquarters), or on a small scale (maybe 100 users). Many cloud initiatives are in demo, prototype or development status. We found one company that uses e-mail in the cloud for tens of thousands of users in all the countries in which it operates. This was in production only since January 2011. However, this company uses a dedicated infrastructure (private cloud), not a shared infrastructure (public cloud).

Concern: Cloud computing is very different from software as a service (SaaS), and this makes privacy compliance much harder.

Clarification: There are certainly conceptual differences, but from a regulatory privacy perspective, there should not be any difference. In both cases, the data-collecting organization (the data controller) hands over personal information to

a third party (the data processor), which can be either a cloud service provider or a SaaS vendor. The differences between cloud computing and SaaS are mostly a matter of perception (that is, "I know where my data is," or "I don't"), and consequently, there are differences in the level of risk that enterprises see in both models. Organizations find it much harder to believe that personal data is well-protected if they can't physically audit the server.

The Way Forward

In many situations, the business case for moving personal information to the cloud is compelling (for example, for human resources or CRM, collaboration, or simply e-mail in the cloud). Legal concerns will erode quickly. Privacy regulations will become stricter this year (updates to U.S. and EU privacy rules are pending), but significant fines for organizations that simply move personal information to the cloud are unlikely. However, there are not only legal concerns. Political and cultural concerns are already important and will overshadow legal concerns as those get addressed by contracts and new interpretations of existing laws. An organization that uses cloud computing, but has to report a privacy breach and a loss of personal information, will certainly suffer reputation damage, even if it complied with all relevant laws, regulations and standards. Consequently, organizations need to conduct a risk assessment that takes into account legal, technical and reputational risks.

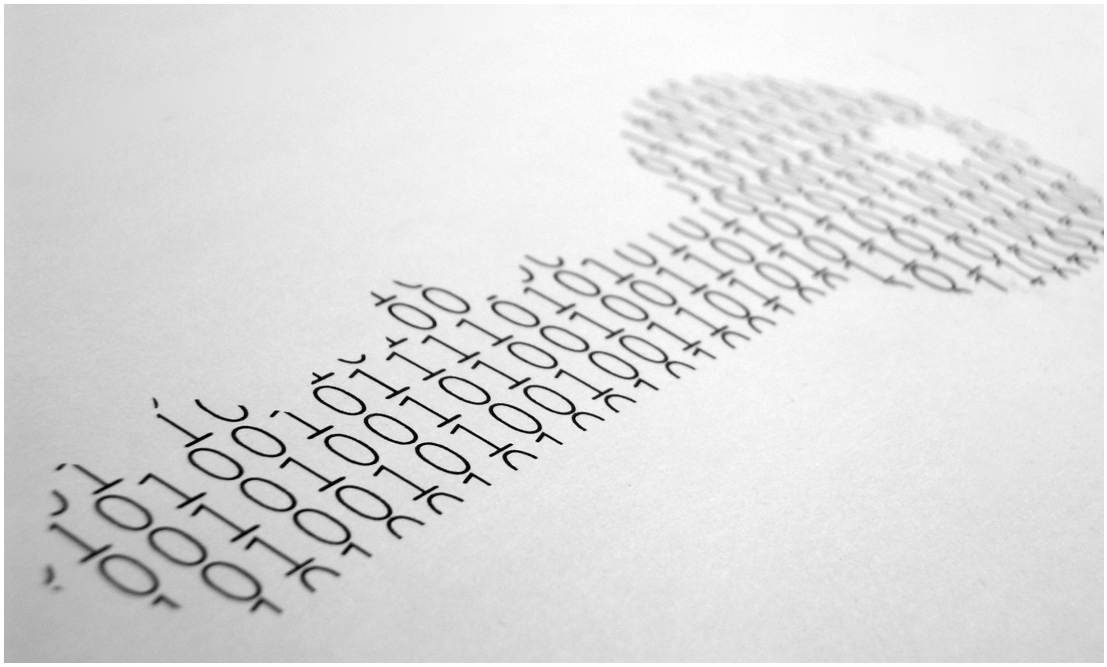
The following list of recommendations will help organizations to implement strategic, procedural and technical controls that facilitate the use of cloud services for personal information:

- **Trust:** When the legal uncertainty and the fast pace of technology change are considered, privacy in the cloud is, to some degree, a matter of negotiation between the compliance officer, executive management, business units, legal counsel, privacy officer, IT security, risk management, works council and data protection authorities. Involve relevant parties early in the process, and ensure that company management makes a decision based on an assessment of business, project, legal and IT risks.
- **Physical location:** Even in the cloud, personal information must be stored somewhere in a data center (or in several data centers). Choose a cloud provider that reveals its data center locations. Ideally, the provider will commit to keeping personal information in your geographic region (even though this might not be legally required). This will help to explain how personal information is protected appropriately. People like to be able to conduct on-site visits, and physical proximity to the data center facilitates such visits.
- **Legal basis:** Engage the services of legal advisors who understand international privacy laws. In many cases, these will not be your company's lawyers, but specialists in international law. Do not ask them whether a move to the cloud is legal. Ask them to put in place legal controls so that a move to the cloud is legal. Such controls can be a Safe Harbor certification, EU model contracts, individual consent or binding corporate rules. Ask that a local subsidiary of the provider sign the contract with your organization (for example, a legal entity in Ireland) if the headquarters of the cloud provider are located in another country (for example, in the U.S.).

- **Providers:** Put pressure on your cloud provider to take your concerns seriously, and ask your provider to evaluate whether the following options are economically feasible: (1) Establish a cloud data center in your region, and commit to storing and processing your personal information only in that data center; and (2) establish a legal entity in your region, and allow this entity to sign contractual clauses for privacy protection.
- **Law enforcement access:** Require the cloud provider (contractually) to inform you when law enforcement authorities request personal information that you have put in the cloud. If the cloud provider does not make any commitment regarding the location of its data centers, then you cannot rule out that the provider stores personal information in a country that is known for human rights violations. Ask the provider to explain under which conditions it responds to access requests.
- **Auditor access:** Financial and tax auditors need direct access to the data they want to audit (including personal information). Some interpret this to mean that data must not be stored in the cloud. However, the rules are changing, and some auditors accept the option of conducting the audit remotely (as long as access at the time of audit can be guaranteed). When you contemplate the need for on-site and remote audits, include industry-specific audits in this consideration – for example, U.S. Food and Drug Administration (FDA) audits.
- **Legal discovery:** Consider conflicting legal requirements. Parties to a civil litigation in common-law countries (for example, the U.S. and U.K.) might request a cloud provider to hand over information relevant to their case (including personal information), whereas parties in non-common-law countries (for example, Germany and France) might demand that the provider does not transfer such information, due to privacy law restrictions. Ask the provider which practice it would follow.
- **Standard of due care:** Evaluate whether the provider protects personal information appropriately. Absent of any detailed technical guidance from regulators, focus on best-practice controls, such as encryption, segregation of duties, role-based access, monitoring, and alerting, as described below.
- **Protection:** Encrypt personal information at rest in the cloud and in transit. It is more important that information is encrypted, not how it is encrypted (such as algorithm and key length). If possible, encrypt in a way that only the client has the keys. Some legal experts argue that encrypted personal information does not have to be treated as personal information (because it is just binary data), and that privacy laws do not apply.
- **User access control:** Limit user access to personal information in the cloud. Do not use shared accounts. Give access only to individuals who have a need to know (and, ideally, not to the provider). If possible, give user access only to individuals who are employed in the jurisdiction where personal information was collected, because those individuals are bound by privacy laws in that jurisdiction. Note that viewing information is considered access to information, even if this access is read-only and done remotely (for example, with a thin client such as Citrix Systems).

- **Privileged-user access control:** Ask current and prospective cloud service providers how many of their administrators can gain access to customer data, and demand a detailed explanation about how misuse is controlled. Ideally, do not allow administrators access to personal information. Encrypt and/or mask personal information, if possible. If administrators have a need to know, then they should use a standard user account.
- **Masking:** Replace personal information with pseudonyms in a way that business processes in the cloud do not have to be changed, yet sensitive information is not exposed. This is known as "data masking," "obfuscation" or "tokenization".
- **Tagging:** Make sure that personal information is tagged with a country name if it cannot be stored in that country (that is, if it's stored in the cloud). That way, you can apply country-specific policies and comply with country-specific laws.
- **Segregation:** Ask the cloud provider how data from different clients is separated (for example, in different folders, different virtual machines or different database tables). You don't want your information to be included when hackers or law enforcement agencies grab information from other cloud clients.

In many cases, enterprises may have already moved personal data to the cloud and not even know it. Besides the obvious, such as payroll processing and customer call centers, they may have engaged a hospitality company to offer discount tickets and travel for employees, or they may offer health benefits to their employees. Implementation details might be opaque to the client. Whether these services are delivered as SaaS with a dedicated in-country infrastructure, SaaS with a shared remote infrastructure, or cloudlike with changing or unknown data centers, locations might be unknown to the client, or these implementation details might be changing. Companies that already engaged such service providers would be wise to consider exactly how much personal information about employees and customers they have provided to these service providers.



Evidence

Gartner conducted a survey of information risk management professionals in Germany, the U.S., Canada, the U.K., Australia, India and Japan. The survey population was 415 respondents. Respondents were knowledgeable of and/or responsible for risk management, security, business continuity, compliance or privacy processes within their organizations, and 146 respondents were responsible specifically for privacy. All respondents work for firms with at least 500 employees and $500 million in revenue. This is an annual survey. Field research was conducted in December 2010.

Note 1
Options for Cross-Border Transfers of Personal Information

Some countries allow transfers of personal information to other countries only if that information is protected appropriately. Canada has such provisions, but the EU's privacy directive is the most prominent regulation in this context. According to the interpretation of Directive 1995/46/EC, personal information may be transferred to countries within the European Economic Area (EEA) and Canada, Argentina, Switzerland, Israel and Andorra, because these countries' legal systems offer adequate protection. Transfers to the U.S. are possible (under certain conditions) if the receiving entity is Safe Harbor-certified. Transfers to any country are possible if the organization has implemented corporate binding rules (but only a very few have implemented this cumbersome process). Most organizations use the EU's standard contractual clauses (also called "model contracts"), especially because the new version of these contracts, published in May 2010, allows for data controller, data processor or subprocessor relationships.

In any case, it is crucial to determine who is the data subject (usually, the employee or the consumer), who is the data controller (usually, the organization collecting personal information), who is the data processor (usually, an internal or an external IT provider), and who is the subprocessor (usually, a service partner of the IT provider). The cloud service provider is typically the data processor or the subprocessor. Depending on the countries in question, the type of personal information (contact data or health information) may also play a role (for example, for health information transmitted to the U.S., the dispute resolution provider must be in the EU). Note that Gartner does not give legal advice. Please seek advice from qualified legal counsel.

Gartner RAS Core Research Note G00210881, Carsten Casper, 25 February 2011

About Rackspace

Rackspace Hosting is the world's leading specialist in the hosting and cloud computing industry, and the founder of OpenStack, an open source cloud platform. Rackspace provides Fanatical Support® to its customers, across a portfolio of IT services, including Managed Hosting and Cloud Computing. Rackspace was recognised by the 2011 Sunday Times Best Places to Work and the 2010 Financial Times Top 50 Great Place to Work in the United Kingdom for the sixth year in a row. The company was also positioned in the Leaders Quadrant by Gartner Inc. in their 2010 Magic Quadrant for Cloud Infrastructure as a Service and Web Hosting. For more information, visit www.rackspace.co.uk.

Rackspace Hosting

Global Headquarters
5000 Walzem Road
San Antonio. TX 78218
Phone: 800-961-2888
Intl: +1 210 312 4700S

UK Office
Rackspace Ltd.
5 Millington Road
Hyde Park Hayes
Middlesex, UB3 4AZ
Phone: 0800-988-0100
Intl: +44 (0)20 8734 2600

Benelux Office
Rackspace Benelux B.V.
Teleportboulevard 110
1043 EJ Amsterdam
Phone: 00800 8899 00 33
Intl: +31 (0)20 753 2301

Hong Kong Office
9/F, Cambridge House, Taikoo Place
979 King's Road, Quarry Bay,
Sales: +852 3752 6465
Support +852 3752 6464

Australia Office
Suite 14, Level 4,
3 Spring Street, Sydney
NSQ 2000
Phone: 1-800-722577