INTRODUCTION

Cloud computing and SaaS arrangements are growing increasingly commonplace, and the benefits of getting IT out of the infrastructure business are obvious. While the technology is rapidly maturing and moving from novelty to commodity, negotiating contracts with cloud vendors can be a challenge.

What if sensitive customer data are stolen from your cloud provider? Who foots the bill if aliens (or government actors) abscond with your provider's servers? Who is liable when the lawsuits start flying?

One of the critical concerns of cloud computing is data security, especially with the recent focus on data theft. While you may think you "own" the data that your provider uses and gathers on your behalf, detailing the ownership of data in the contract with your service provider is critical.

Data encryption; a right to audit security procedures and data centers; a requirement to be notified immediately of any security breach; and a requirement to allow an outside auditor to assess controls and procedures for storing, handling, and transmitting data, should all be detailed in the contract.

Ownership of data is not be left to assumptions. The contract should clearly state that all data are owned by the client and contain a provision that, at the termination of the contract, the provider should agree to deliver a copy of client data and permanently destroy all copies of the data in its possession.

We have all seen the dreaded "limitation on liability" clause in everything from amusement parks to complex vendor contracts, and working in the cloud is no exception. The first iteration of a contract is always in favor of the drafting party, and cloud vendor contracts are no exception, especially around limitation on liability clauses.

The provider typically includes a provision that limits its liability to a fixed amount, often based on fees paid to the provider. If you are served with an expensive lawsuit related to a customer data breach, or suffer damages to your business when the provider has a technical problem, this is unlikely to cover the damages if the breach or outage was a result of the cloud provider's negligence. With SaaS fees falling to commodity prices, a liability based only on fees paid to the provider can leave your company overly exposed.

In today's data-dependent world, businesses must work smarter and faster to stand out from the competition, deliver new products, and achieve results. Regardless of industry, geography or size, now is the time to consider what you need from your data in order to succeed in this new business landscape, and what you must do to ensure these needs are met. For instance, the new Intel® Xeon® Scalable processors have been designed to accelerate analytics as well as artificial intelligence, providing a more scalable, agile, and efficient platform with increased security features for all enterprise use cases.

Force majeure clauses (sometimes called "Acts of God") are unforeseen circumstances that would prevent the cloud provider from delivering on their promised services, oftentimes services for which you have paid in advance.

These scenarios could range from the relatively mundane-such as a key communications link being severed by a wanton backhoe-to all manner of natural disasters, terrorist incidents, and yes, even little green men from Mars shutting down your provider.

While you cannot expect your cloud provider to stay up and running through every unforeseen disaster scenario, clients should protect themselves from paying for a service they cannot use.

A contract should only allow a force majeure clause to apply if the provider is in compliance with its backup obligations and the client should receive a credit for each day of interruption, and be allowed to terminate the contract should the force majeure event last more than an agreed-upon time.

In short, your cloud provider should not be able to claim force majeure if that "state-of-the-art backup data center" is really a closet in a strip mall and cannot handle the demand if the primary data center fails due to an earthquake.

Similarly, ensure you understand how your provider will handle your data in the event of a government subpoena or other action. When you control the data you may have time to get your legal "ducks in a row" should a government action take place,whereas your cloud provider may simply turn over anything and everything related to your business without a prior agreement in place.

When bad things happen to good companies

While cloud can be cost effective and allow for innovative new capabilities, it is obviously not without risk. On what seems like a regular basis, we hear about providers "losing" a batch of backup tapes with sensitive customer information, or a security breach resulting in a similar loss.

Several protections, including provisions that "indemnify, defend, and hold harmless" the company engaging the cloud provider to be provided should the company be sued as a result of the provider's negligence.

In addition to legal concerns, many players in the cloud space are relatively new and untried, and some are bound to fail as the market matures. For a particularly risky provider, or in a situation where you cannot easily recreate the data held by your cloud vendor, it is recommended that your data be escrowed with a third party, and that contractual provisions require the vendor to return your data and destroy any copies before turning off the lights and skipping town.

So here are some legal strategies for successful cloud?

In order to obtain successful cloud-based computing services, with the benefits of safety and security as well as legal compliance, an organization must first make an informed business decision about the type and sensitivity of data and service it plans to migrate to the cloud, specific configurations and type of cloud service required (e.g., private, hybrid or public), in order to comply with the organization's legal obligations. Prior to contracting with a particular cloud service provider the enterprise should insist upon transparency, identifying all of the parties involved (e.g., subcontractors), the data process flow, uses and locations. A detailed audit and assessment of the cloud service provider's security protocols and technology is recommended, and a roadmap of the service provider's future plans is also helpful. As well, a migration plan should be developed, including an assessment of current state architecture, applications, data and performance metrics, so that one knows what needs to be changed and to have a baseline to make future service level measurements meaningful. Similarly, a transition plan for exiting the cloud service relationship should be constructed in advance.

Second, the organization must properly negotiate and draft the legal contract between the organization and the cloud service provider. Organizations sometimes find that cloud providers, in particular the low-cost online service providers, present “take it or leave it” contracts that are non-negotiable. The risks of doing business with these cloud service providers and accepting their boilerplate contracts are that many of them:

- lack critical enterprise-protective terms,
- do not adequately protect the customer's data,
- do not contain any guarantee as to quality of service, and
- allow for more liberal usage of personal information, which would not be sufficient for an organization to meet its privacy and other legal obligations.

Often, cloud service contracts fail to deal with proper transitioning of the data and services to another cloud provider (or back to the customer organization) when the contract or the relationship comes to an end, leaving the organization vulnerable to loss of, or inaccessible, data and interruption of critical services. Generally speaking, more industry-specific

cloud offerings are available, but at costs which are higher than consumer-based or generic services that are more suitable to non-enterprise or non-regulated businesses.

Terms which need to be thoroughly covered in a cloud service contract include:

- ownership of data,
- termination rights and termination assistance,
- uptime,
- service availability,
- performance levels,
- security warranties,
- allocation of liability risk,
- privacy,
- data security and breach notification requirements,
- compliance with laws and regulations,
- representations about jurisdictional exposure of information and operations, and
- remedies for breach of the contract.

Cloud service contracts should also include proper terms dealing with:

- change,
- problem resolution,
- subcontracting,
- use of open source software,
- application re-development,
- ownership of any intellectual property,
- trade-secret protection,
- confidentiality,
- testing,
- data integrity,
- potential secondary uses of data,
- assurance of data segregation and isolation,
- encryption in transit and in storage,
- backup and data recovery,

- what happens to the data and the infrastructure upon termination of the agreement or in the event of a failure or insolvency of one of the parties,
- how maintenance or service interruption will be handled,
- what geographical limitations must be imposed,
- the right to audit the entities and the technology, etc.

The foregoing is not an all inclusive list. Each cloud service needs to be looked at separately and carefully analyzed to determine the full extent of the business and legal risks, before your legal counsel can advise on what contract terms are appropriate and which ones need to be revised.

The third step to achieve success with cloud-based computing is to implement appropriate internal organizational and transitional governance, policies and controls. Policies dealing with confidentiality, security, privacy, business continuity plans, ongoing risk identification and management, technical problem escalation, and electronic data retention need to be prepared or revised as well as disseminated, clarified and enforced throughout the organization. Data cleansing, encryption and backup activities may need to be incorporated into the

organization's business processes. Employee policies should also be developed or modified to deal with employee use of cloud-based services (in particular when accessed via their own personal devices for business purposes), such as e-mail for business correspondence, customer database/sales management, document sharing or presentations, etc. Business leaders as data controllers are accountable for their organization's use and outsourcing of data or other services to a cloud provider and must ensure that their organization's information management and privacy practices are compliant with the law and consistently applied across the organization at all levels.

Cloud-based computing can have numerous advantages and be accomplished successfully if all the legal considerations are taken into account. Failing to take the appropriate steps or rushing through to secure a cloud deal without thorough legal review, can have a large negative impact to the business and its stakeholders.