Mitigating Risks and Negotiating Terms for Cloud Services

Michelle Tyde

Daily Report

September 6, 2016

Cloud computing services (the outsourcing of information technology services via the internet) continue to evolve rapidly in the technology industry due to greater flexibility and economy. According to the research analyst Gartner, the use of cloud computing will become the bulk of new IT spend this year.

Providers are able to offer low-cost, flexible solutions because they standardize their offerings for multiple customers. Customers benefit from the cost savings, flexibility and scalability of the services.

The downside to cloud services are that providers are less likely than traditional outsourcing providers to adapt their solutions to a customer's needs or negotiate contract terms. Moreover, cloud computing services can be a double-edged sword; many of the benefits create significant legal risks, including data loss, security breaches and service availability issues.

These risks need to be carefully evaluated and mitigated during the provider selection and contract negotiation process. Knowledge of cloud offerings (both the service model and methods as well as the vertical supply chain or laying of providers in the industry) is key to risk mitigation.

Cloud Service Models

Cloud computing has several service models and deployment strategies, which have emerged in response to the specific needs of customers. Each provides different levels of control, flexibility, management and risk.

There are three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

IaaS provides access to virtualized computer resources (e.g., servers, networks, storage, and systems software) on a pay-per-usage basis over the internet. IaaS is designed to augment or replace the functions of a data center and provides the highest level of flexibility and management control over IT resources. Amazon Web Services, Rackspace and Google Compute Engine are IaaS models.

PaaS provides an outsourced platform that allows customers to develop, test and manage web applications. PaaS models include Google App Engine, Microsoft Azure Services and SalesForce's Force.com.

Software as a Service (SaaS) provides software applications that are hosted by a provider and made available to customers over the internet. SaaS is the most widely used and known form of cloud computing and includes Google Apps, Microsoft Office 365, Citrix GoToMeeting and Citrix WebEx. IaaS and PaaS give the customer more control than does SaaS.

Cloud deployment models include the private, public, community and hybrid cloud. Each represents a specific type of cloud environment, distinguished primarily by ownership, size and access.

The value and risk in each deployment model varies significantly. The public cloud is the most popular and widely used, while the hybrid continues to grow due to the balance it provides customers.

The private cloud provides a dedicated infrastructure that is operated solely for one organization. Private clouds provide a greater degree of flexibility and control over data security and storage and are more

reliable, but are the most expensive. The public could is made available to the general public by a provider who owns, operates and hosts the cloud infrastructure and offers access to users over the internet. Since users "share" the public cloud, this model offers the greatest flexibility (on-demand scalability) and cost savings (pay-as-you-go model). The public cloud, however, has increased security risks, and reliability can be problematic.

The community cloud infrastructure is a multitenant cloud service model that is shared among several organizations and is governed, managed and secured commonly by all the participating organizations or a third-party managed service provider. Community clouds are a hybrid form of private clouds, built and operated specifically for a group that shares common goals. With the community cloud, the costs of deployment and access are spread over fewer users than the public cloud, but there are more users than the private cloud.

The hybrid cloud is composed of two or more clouds (private, public and/or community clouds) that remain separate but are bound together, offering the advantages of multiple deployment models. A hybrid cloud increases the flexibility of cloud computing as businesses can take advantage of the cost-effectiveness of public cloud computing while also enjoying the security of a private cloud.

Since each cloud model and deployment method offers varying degrees of flexibility, efficiency, data security and cost savings, it is important to select the model and deployment method best suited to a company's needs and to manage the associated risks. Key considerations include whether the outsourced service is business critical, the size of the company, regulatory or compliance issues, and the sensitivity of the outsourced data.

For example, public clouds work better where the outsourced service is not critical to the business and the outsourced data is not sensitive. Private clouds and IaaS and PaaS are better suited for companies in highly regulated industries such as financial services and health care, where security and compliance issues are driving concerns.

Legal Challenges and Risks

While the economics and scalability of cloud computing are compelling to companies—lower operating costs, the lack of capital expenditure, the ability to quickly scale services and the ability to outsource maintenance—the risks can outweigh the rewards. Significant risks include vendor reliability, security, service performance and data portability. While security remains a concern with cloud offerings, it is increasingly cited as a benefit as large cloud service providers typically have the ability to support more robust security systems and platforms than are practical for most individual businesses.

The risks associated with provider lock-in, however, are commonly overlooked but substantial. Lock-in (dependence on a provider) occurs when a customer cannot easily transition to another provider without substantial costs, legal constraints or technical incompatibilities (the customer is unable to retrieve and port its data, or there are interoperability issues when transitioning the services). Such risks can be mitigated by negotiating certain contractual protections.

Contract Review and Negotiations

Cloud providers regularly promote their service benefits, capabilities and credentials, while providing little, if any, contractual recourse to the customer for failure to meet such claims. Cloud services are typically offered on the provider's standard terms and conditions (often a click-wrap agreement or other online terms of service), which heavily favor the provider due to the commoditized nature of the services.

Cloud service agreements are also often multilayered, including terms and conditions, an acceptable use policy, a privacy policy and a separate service level agreement. While cloud offerings have traditionally been non-negotiable, providers are increasingly more flexible, particularly for large customers, enterprise-grade offerings, and for IaaS, PaaS and private cloud service offerings. SaaS deployed on a public cloud are the least negotiated due to the shared infrastructure.

For other offerings, the terms most often negotiated are price, term, data-related issues, service-level agreements, limitation of liability, termination rights and the provider's ability to unilaterally change service features and/or policies. Technical areas, such as the variability of service elements, are generally non-negotiable.

The larger the deployment and commitment (i.e., term and revenue), the more leverage a customer has in negotiating favorable terms. Even if a provider claims that the contract terms are offered on a take-it-or-leave-it basis, providers negotiate to secure deals that are financially or strategically advantageous or have a reputational value (e.g., being able to publicize the deal).

Legal counsel should be engaged early in the negotiation process to ensure that the services are provided on terms that mitigate the risks. Some lawyers mistakenly try to negotiate cloud contracts as software licenses or technology acquisitions when in fact they are contracts for services. Understanding the unique features and risks of cloud service offerings is integral to successful contract negotiations.

Below is a summary of some of the key contractual issues that should be carefully reviewed, evaluated and negotiated depending on the nature of the services (such as whether it is mission critical for a customer), the type of data being processed, and the cloud model and deployment method. Other issues include security, warranties, limitation of liability, intellectual property rights, insurance and force majeure.

Term

From the outset, the term should be carefully considered. While traditionally cloud services have been provided on a pay-on-demand basis, increasingly providers are requiring minimum term commitments: 1 to 3 years, particularly in exchange for negotiated pricing discounts.

Typically, cloud agreements do not require the provider to make service enhancements, and thus a customer risks being stuck with outdated or inadequate services when making a term commitment.

Evergreen provisions should also be carefully reviewed, as providers frequently have the right to raise fees during renewal terms without sufficient notice to the customer or a cap on the increase.

Data Issues

There are a number of significant data-related issues unique to cloud services, since control of a customer's data is in the hands of the provider (that is, the provider controls access to the data, as well as the data schemas and storage format).

While cloud agreements commonly include confidentiality and security provisions, they provide little or no protection regarding data ownership, integrity, loss or access. For instance, cloud agreements are often silent on the issue of data ownership (creating an ambiguity), specify ownership by the provider, and/or give the provider broad rights to use customer data.

Thus, negotiate terms that (1) broadly define customer data (e.g., data input, processed or created by the customer using the cloud services or generated by a customer's use of the service), (2) specify the customer's ownership rights to such data, (3) limit the provider's ability to access and use customer data, even in aggregated, nonidentifiable form for sensitive information, and (4) permit the customer to readily and easily access and retrieve data in a useable format.

Depending on the nature of the data being processed by the cloud service, specified business continuity and disaster recovery obligations should also be negotiated into the agreement. While many providers have business continuity or disaster recovery plans, if the contract fails to incorporate such into the agreement, there is no obligation for the provider to adhere to such requirements. To increase its profitability, the provider can unilaterally change such protections, to the detriment of the customer.

Data access and portability, both during the term and upon the expiration or termination, are also significant issues to negotiate to avoid lock-in. Even if the contract clearly defines data as being owned by

the customer, retrieving and porting data (including metadata) into other systems and services is not an easy and straightforward process, and the costs involved might present a barrier.

Thus, negotiate obligations for the provider to provide data in a specified format (to ensure it is usable) upon request at any time during the contract (regardless of whether a party is in default or breach under the agreement), and within a specified period of time upon the expiration or termination of the agreement for any reason.

Service Level Agreements (SLAs)

Though many cloud service providers offers SLAs, contractually most provide woefully inadequate protection for the customer, as the remedies offered and contractual limitations on the SLA do not match the cost to the customer of a potential service disruption. SLAs are frequently the only type of warranty provided for cloud services, and thus, the SLA provisions are essential to ensuring performance by the provider.

Terms that negate the SLA include (1) limiting the customer's remedy for failure to meet the SLA to a capped amount of service credits, (2) extensive and vague carve-outs to the SLA that can lead to a dispute as to whether a service failure actually occurred, and (3) putting the burden of SLA violation notification and credit requests on the customer.

While SaaS and public cloud providers will generally not negotiate the system uptime requirements (e.g., 99.5 percent, 99.7 percent, 99.9 percent), other terms should be negotiated for all models and deployment methods. For example, the carve-outs should be clear and limited, and the contract should detail how service availability is monitored (by the provider, the customer, or a third-party performance management provider), how incidents are reported and addressed (response times), and the parties' corresponding responsibilities.

Furthermore, it is imperative to negotiate additional remedies for service interruptions/outrages, including the right to conduct a yearly comprehensive review, the right to have a "sit-down" meeting by the parties' executives for repeated failures, and termination rights if interruptions/outages are "chronic" or "excessive," otherwise providers tend to have little incentive to address service issues.

Moreover, it is a grave mistake to rely on the right to terminate for material breach as a remedy for repeated service interruptions or outages, as some courts have found that where the SLA specifies that a customer's sole and exclusive remedy is credits, such provision nullifies the customer's right to terminate for material breach. Accordingly, experienced counsel will push aggressively in negotiating the SLA, particularly if the service is critical to the customer's business and/or the term and financial commitments are significant.

Termination

It is not uncommon under a provider agreement for a customer's right to terminate to be vague and limited, and for the provider's right to be broad and extensive.

For example, cloud agreements frequently allow the provider to suspend services or terminate the agreement for nonpayment, without any notice to the customer or cure period. This can be detrimental if the service is integral to the customer's business.

Specific provisions addressing how a payment dispute will be handled should also be negotiated (such as allowing disputed amounts to be paid into escrow pending resolution) to avoid being "forced" to pay disputed amounts to prevent a service suspension or termination. Another termination issue to consider is whether an end user's conduct should give rise to termination of the services or limited to termination of the offending end user's access to the services.

Negotiating an exit strategy upon termination with respect to the transitioning of the services and porting of data is also key to mitigating the risk of lock-in. Provisions should address the process and timing for porting data and transitioning the services either in-house or to another provider, the format in which the

data will be ported, what assistance (tools or services), if any, the provider will provide, any applicable fees and expenses, and the timeline.

Finally, if the service processes personal information or sensitive data, include specific data deletion requirements to ensure that the deleted data is not recoverable, as many providers do not automatically utilize secure data deletion practices because of the cost involved.

Conflicting Terms/Provider's Ability to Change Service Features

Commonly the provider's contract will incorporate by reference other applicable terms and conditions, policies, etc. Carefully review all applicable terms, even if they are non-negotiable, to ensure they do not conflict with negotiated provisions (remedies for SLA failures) or contain provisions that limit the service offering (permissible usage limits).

Furthermore, providers often have the right to unilaterally change service features, terms, or applicable policies (e.g., business continuity plan). Negotiate adding a conflicting terms provision and requirements that (1) any unilateral changes not degrade the service or weaken the security requirements or (2) the provider will notify the customer in writing of any changes, and give the customer a right to terminate without liability if any of the changes adversely affect the service or the customer's use thereof.

Conclusion

As the cloud computing industry continues to evolve, providers are increasingly willing to negotiate certain contract terms to remain competitive.

To maximize the cost savings and other benefits of cloud services, mitigate the risks by carefully reviewing all applicable terms and policies and negotiating key contractual protections.

Michelle Tyde, counsel at Kilpatrick Townsend & Stockton, focuses her practice on intellectual property/technology transactions and privacy and data security matters.