Cloud Control

Managing the Risks of Engaging and Terminating Cloud Services

Brian Y. Boyd, J.D., CIPP/US

According to a recent survey of *Harvard Business Review* readers in large and midsize organizations, 70% said their organizations had adopted cloud computing. Of these, 74% said it provides a competitive advantage. This potential for cost savings and increased business efficiencies helps explain why cloud use is expected to continue its rapid growth. But there are associated risks with cloud use, and they can be summed up in a single word: control.

When an organization utilizes a cloud service, it gives up a measure of control over the security, availability, and quality of the data or service it entrusts to the cloud service provider (CSP), but it remains responsible for the data. When the relationship with a CSP ends, regaining that control can be challenging. Therefore, before an organization engages with a CSP, it should go through the process of gathering requirements, performing due diligence on the prospective CSP, and contractually protecting its expectations and interests.

Organizations recognize the advantages cloud computing can provide, but the many risks that come with storing data in the cloud must be considered as well. This article spells out the due diligence organizations must do before contracting with a cloud provider, as well as the proper way to manage the end of such a relationship.

Classifying Cloud Solutions

First, while the phrase "cloud computing" has burst into the lexicon, its meaning remains as nebulous as clouds themselves. *The cloud* has spawned "public," "private," and "hybrid" clouds, among others. And from the cloud comes a litany of "as-a-service" offerings, including software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and more.

The catchphrases themselves are unimportant, but the conceptual distinctions are important to any organization moving into the cloud. Options range from a blank slate of hardware infrastructure in the cloud that is dedicated to a single business client (IaaS in a private cloud), to niche cloud-based software that serves a narrow function for anyone who purchases the service (SaaS in a public cloud), and many variations in between. In short, not all clouds are alike, and not all cloud services are alike.

Rarely will an organization have all its technological needs satisfied by a single CSP; usually some IT functions and data will be kept in house. So, an organization first must have a clear understanding of its goals in moving some part of its business to the cloud. For what business process or information will the cloud be used? Is cost savings the motivation for leveraging the cloud, or is it the promise of improved data access and transparency, faster system performance, redundancy, or something else? These questions should guide an organization as it progresses through the request for proposal, due diligence, and contract negotiation processes.

Gathering Cloud Solution Requirements

The most common business use for the cloud is simple data storage because the cloud offers space that is low cost, easy to access, and almost infinitely scalable. In other cases, an organization may choose the cloud to gain access to the CSP's powerful data analytic tools, or to run algorithms to define market segments, or to identify emerging product or service demands.

However simple or sophisticated the need might be, the focus should first be on what requirements apply to the data that will be shared with the CSP. This includes data the CSP will store, data the CSP will have access to, and, in some cases, data the CSP will generate itself.

Determine Privacy, Security Requirements

Many data security and privacy laws and regulations apply to businesses, based not only on their industry, but also on the nature of the data at issue and how that data is acquired. For example, personally identifiable information (PII) in the form of 1) medical, 2) credit, or 3) employee records can each implicate different legal requirements.

Some privacy requirements apply to particular industries, such as the Graham-Leach-Bliley Act (financial), the Health Insurance Portability and Accountability Act (HIPAA), and the Defense Federal Acquisition Regulation Supplement, to name a few.

Other laws, such as Massachusetts' data security law and the EU Data Protection Directive, apply to virtually any organization maintaining PII on individuals residing within the statute's jurisdiction.

Identify Other Obligations

Data also may be subject to contractual obligations or constitute an organization's own trade secrets, requiring special treatment or protections. Before CSP selection can begin, an organization must determine what legal

No insurance will completely compensate for the losses associated with a high-profile data breach, not the least of which are reputational.

obligations arise from the data and incorporate those requirements into its due diligence and contracting process.

Performing Due Diligence

At this point, an organization has gathered the information it needs about its cloud service goals, what information it will share with its chosen CSP, and the security and privacy duties that govern the handling of that data. With that foundation set, the organization must next look into the provider's financial condition, insurance, security, data center locations, disaster recovery plan, reputation, and clientele.

Assess Financial Conditions

Entering a relationship with a CSP that is not financially sound can have serious consequences. For example, in the pending action *GlaxoSmithKline LLC v. Discovery Works Legal, Inc*., the pharmaceutical giant alleges that its e-discovery service provider, while "apparently spiraling toward insolvency," threatened to destroy terabytes of sensitive information unless it was paid a ransom of more than $80,000.

Only a small percentage of CSPs are public companies, which makes it more difficult to access their audited financial statements. If a CSP can prove it has the backing of significant institutional investors, this can provide a measure of assurance.

It is worthwhile to look at whatever financial information a CSP is willing to furnish. However, because CSPs operate in an emerging market, many are start-ups and their financial profiles will likely compare unfavorably to traditional outsourced service providers. This is particularly true for CSPs that provide specialized or patented SaaS and less true for CSPs that offer more generic IaaS or PaaS, of which there are more. Therefore, while the risk of dealing with nascent CSPs is real, it should be assessed with an understanding of the competitive environment they operate in.

Check Customer Base

Since financial due diligence may not yield a clear picture of a CSP's long-term stability, alternative forms of inquiry are all the more important. One indicator of a cloud provider's staying power is the profile of its existing customers. While there may be some appeal to being a cloud provider's largest and most important customer, generally that is not a position an organization wants to be in.

A CSP that builds its business around a single customer may do everything it can to keep that customer happy, but it may also become desperate if faced with the prospect of losing that customer, as the *Glaxo* example illustrates. If an organization wants to part with its CSP for any reason, it will need the utmost cooperation from its outgoing CSP to facilitate a smooth transition. That cooperation will be difficult to secure if the CSP is about to shut down.

Verify Insurance Coverage

Insurance is another consideration; it is an essential component of a CSP contract. Cybersecurity insurance is particularly important. Indemnity obligations in the event of a data breach are provisions that are often debated, if not contested, in contract discussions with a CSP.

From the organization's perspective, it is storing its data in the CSP's castle. From the CSP's perspective, the organization holds the keys to the castle. In truth, if the castle is breached and data is lost, it can be difficult to determine whether the CSP or the organization is responsible. While indemnity – which is the CSP's promise to pay for the cost of the organization's possible loss or damage – may be an option, cybersecurity insurance is sometimes an easier solution.

Wherever an organization's data resides, it remains the property of that organization, and any contract should stipulate as much, particularly as it relates to PII and the organization's intellectual property. If a CSP has a data breach involving the client's PII, the client, not the CSP, could be responsible for costly notification requirements; this is the case in 47 U.S. states.

Cybersecurity insurance might cover that expense, but not all cybersecurity insurance is alike. An organization may have its own cybersecurity insurance that covers a data breach, even one involving its third-party CSP, but many cybersecurity policies do not provide this coverage. If a CSP has cybersecurity insurance, it may cover only the losses suffered by the CSP itself. A CSP that has so-called third-party cybersecurity insurance may be able to offer coverage to its clients, and those clients should seek to be identified as an additional insured on such policies.

Check Security Measures

Another important aspect of cloud vendor due diligence is determining how secure your company's data will be. No insurance will completely compensate for the losses associated with a high-profile data breach, not the least of which are reputational. If a CSP will provide simple cloud-based storage and nothing more, an organization might achieve the greatest level of security by storing the data in encrypted form and retaining the encryption key (without providing it to the CSP). But in many contexts, particularly in many SaaS solutions, encryption of all data in the cloud is not a feasible solution. Then the admonition of "trust, but verify" is apropos.

However an organization chooses to satisfy itself regarding a CSP's security, those rights and obligations must be carefully documented in the contract. Moreover, organizations should ensure that the security verification process is ongoing throughout the term of the contract.

Even where the best security practices are faithfully followed, data breaches can occur. But the impact of a

Whatever the organization's requirements are for system performance and availability, they must be documented in the service level agreement.

data breach can range from a public relations challenge to a business-ending catastrophe. The difference can hinge on what measures the affected organization took to ensure the security of its data. An organization that suffers a data breach through a respected, ISO 27001-certified CSP will be treated with more understanding by the public and regulators than one that lost data by contracting with a three-employee start-up that had no strict security practices.

Confirm Location of Stored Data

A related component of due diligence is learning where a CSP will physically store the data. This is another instance in which the distinctions between a public and a private cloud become important. In a public cloud, the provider typically stores the data of multiple clients on shared physical resources at data centers that are often scattered across the globe. A private cloud implies dedicated physical resources to a specific client, a configuration that should give the client more say over the location and conditions for storage.

The location of a cloud provider's data centers can be important if, for example, an organization handles PII of EU citizens. The EU Data Protection Directive forbids the transfer of such PII outside the EU and a handful of additional jurisdictions without specific legal assurances on how the data will be handled.

An organization could unwittingly run afoul of such rules by selecting a CSP with data centers inside and outside EU-approved jurisdictions. For instance, co-location of data is a standard disaster recovery practice, but this innocuous practice could violate privacy laws if data in the EU is backed up to a location outside the EU.

Check Continuity of Operations Plans

Data co-location is just one potential component of a CSP's broader disaster recovery program, which also must be the subject of the due diligence process. Here, it is important to distinguish between a CSP that merely backs up data and one that has a tested disaster recovery program. If a CSP's service becomes unavailable due to a catastrophic failure, the fact that the vendor has the data backed up at a secure location will be of little comfort. The client organization needs a live, operative system, not just a static and inaccessible archive of data.

Similar to disaster recovery is a CSP's commitment to a service level agreement (SLA). An SLA sets out the CSP's obligations to keep its service running in the ordinary course of business. Based on the requirements-gathering stage, an organization should know how much downtime it can tolerate.

If the CSP is simply providing archived data storage, an organization may not need instantaneous 24-hour access to that data. If, on the other hand, the CSP is providing an SaaS solution that will manage high-frequency customer orders, any downtime will jeopardize the organization's revenue.

Availability comes at a price. And this is another area where the distinction between a public and a private cloud impacts the level of control an organization will have over its CSP's service. For example, routine maintenance cannot be scheduled to accommodate one particular cloud service client in a public cloud. In a private cloud, by contrast, a client can work with its cloud provider to mitigate the impact of downtime related to maintenance.

Whatever the organization's requirements are for system performance and availability, they must be documented in the SLA with appropriate remuneration and termination options if the CSP fails to perform to the required standards.

Planning for the End

Once due diligence is complete and the prospective CSP has agreed to the client's contractual requirements, the next step is to focus on the possibility of the relationship between the CSP and the client ending, amicably or otherwise. Business relationships can end for any number of reasons, but there are particular risks associated with the termination of cloud services that must be addressed in the contract.

First, like a traditional software license, SaaS may infringe on a third party's copyright, patent, or other intellectual property rights. Organizations should generally expect that CSPs will defend and indemnify them if they are drawn into a lawsuit over such infringement. However, CSPs will often place limits on their indemnity obligations, and if the CSP's service is found to infringe, the client may be forced to stop using it.

Establish Data Withdrawal Protocol

If the relationship between an organization and its CSP ends, the client's chief concern is to get its data in a usable form. Over the life of the relationship, the CSP has likely accumulated a great deal of data on the organization's behalf. In many instances the data may be incorporated into a database or proprietary CSP software in a manner that makes it unusable in a flat file. Imagine a complex database of customer information returned to the organization in a heap of plain text, or imagine data from geolocation tracking software returned to the client

in a string of longitudes, latitudes, dates, and times. The format in which an organization will want to receive data will depend on the cloud service at issue. XML and JSON are flexible file formats in certain circumstances.

Even if the desired protocol and file formats are carefully specified, an organization will almost always need some flexibility from the CSP in transitioning the existing cloud service to the client itself or to a new CSP. Contracts must carefully set out the CSP's obligations during this transition period and must be binding regardless of the circumstances for ending the relationship.

Spell Out Transition Costs

Of course, a CSP will expect to be paid for such "transition services," and it should be paid as an incentive to see the process through. Costs arising from a termination or transition of services should be carefully noted in the contract. And when the separation is complete, the client should have contractual assurances that its data has truly and irrevocably been deleted by the terminated CSP.

Consider Source Code Agreement

Sometimes, however, a CSP may be unwilling or unable to cooperate in an orderly termination of its services. In these cases, a source code escrow agreement might offer assistance because it allows the organization, at least theoretically, to recreate the CSP's service without the CSP. It also offers leverage because a CSP that is resistant to cooperating in transitioning its services may reconsider when faced with the possibility that its proprietary source code could otherwise be turned over to the client.

Still, source code escrow arrangements are rife with pitfalls in practical application, so an organization should not place much stock in the assurances they can provide. Finally, an organization should make certain that its agreement with a CSP and any escrow agreement protects it in case of the CSP's bankruptcy.

Make up, Don't Break up

Perhaps the only thing more difficult than selecting a CSP is breaking up with one. Pulling the plug is not a viable option. An organization should always assume that terminating a CSP will be more difficult, costly, and time consuming than it expects. Generally, both the client and its CSP are better off mending fences than parting ways. But if the relationship must end, the due diligence that was performed at the outset and the proper contractual protections will minimize the pain and help facilitate an effective transition. **END**

Brian Y. Boyd, J.D., CIPP/US, can be contacted at bboyd@carmodylaw.com. *See his bio on page 47.*