[InsideCounsel].com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
May 2, 2014


Carrying your umbrella when navigating the cloud

With cloud computing comes significant concerns about security, integration and governance

BY CY MORTON, SETH A. NORTHROP

Cloud computing continues to fill the enterprise troposphere. A recent 2013 IDC survey reported that 61 percent of enterprises have at least one application that is cloud-based in their organization, and total investment by enterprises was up over 10 percent since 2012. But, with cloud computing comes significant concerns about security, integration and governance. Although individual users of cloud computing may lack the necessary leverage to drive and shape agreements between themselves and cloud providers, enterprises can increasingly shape cloud agreements. Being proactive in this process can mitigate corporate risk when the clouds gray.

Rain gear for your data: Data privacy and security

One of the greatest fears of an enterprise engaged in cloud computing is that placing corporate data in the cloud increases the risk that data will be subject to breach. Although there have been some high profile breaches of cloud-based storage systems (Expedia, Epsilon Data Management's email marketing systems, Sony's online entertainment system, for example), the prevalence of cloud-based breaches remains fairly low, particularly in relation to non-cloud-based breaches. The nature of cloud computing, however, ought to make security and data governance a paramount concern for organization pushing business data into the cloud. There are therefore several issues organizations investigating cloud services should consider:

Focus on due diligence: An important consideration in any sourcer/provider relationship is pre-contract due diligence. During due diligence, an organization should investigate the security policies of the provider, how the provider responds to government data requests, previous security performance, and recent intrusion testing results.

Seek notification provisions: Seeking contractual requirements for expeditious notification in case of breach can help minimize the damage of a breach, avoid embarrassing disclosure of the breach by a third-party, and provides the customers of cloud services the ability to start meeting data privacy regulatory obligations. Likewise, many provider agreements expressly allow them to disclose customer data in case of subpoena or other legal process. Organizations storing data in the cloud should insist on notification of such requests so that they know data has been provided to other parties.

Seek comprehensive audit rights: One of the most important components of a governance regime is access to information. Although pre-contract due diligence will provide insight into the operations and policy of a provider, audit rights will be essential in order to ensure continued compliance with regulatory obligations and consistency with established security policies.

Limit where data will be located: Organizations should insist on contractual terms that clearly define where data geographically resides and provisions that identify who can access or manipulate the data. For example, there should be restrictions on moving data to additional third parties without consent or storing data on off-shore servers. Allowing data to move across jurisdictional lines can have profound implications on controlling regulations, may impact the organization's own regulatory and contractual obligations, and may limit remedies in case of breach or failures.

Negotiate data deletion provisions: If data is particularly sensitive and the relationship with the provider untested, consider negotiating terms related to how data will be deleted should it be necessary. Various techniques can be deployed to help ensure a more robust removal of data from stored drives and providers may be willing to provide confirmation and/or copies of the materials removed from its system when requested.

Encrypt: No provider will be immune from governmental requests for data or fully secure from breach. Where possible, insisting that data be encrypted will help provide an additional level of protection of data stored within the cloud.

When the cloud dissipates: Availability

Loss of availability continues to present significant risk to organizations leaning on the cloud. One of the most notorious such outages impacted Amazon's cloud services over the holiday season of 2012. Amazon's outage impacted numerous high-profile web properties including Netflix. How should organizations structure agreements to minimize the risk of availability?

Understand the vendor's backup and recovery procedures: Whether in due diligence or throughout the course of the agreement, it is important to fully understand the backup and recovery procedures of the vendor. Often, vendors have an expectation that its customers are responsible for backing up critical data — if that is the case, it is important to know so that your organization can take preventative measures or negotiate terms that ensure data is protected.

Understand and negotiate SLAs: Negotiating cloud provider service level agreements (SLAs) is far from the norm. However, coming to the table with specific and reasonable expectations may open the door to customized SLAs. Seeking customized SLAs will better align availability with your desired user experience. However, more important, taking time to understand SLAs will provide a better benchmark to compare competing cloud provider offers.

Request RCAs: In order to help avoid repeat outages, organizations seeking to use cloud services should request root cause analyses when outages do occur. This will assist the organization's governance organization to maintain a handle on the environment and whether outages are foreshadowing more damaging problems in the future.

Availability, however, is not only impacted

May 2, 2014

InsideCounsel.com

BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS

by server or network outages. As the competition among cloud providers intensifies, the risk that certain providers will go bankrupt also increases. Recently, this played out when the cloud provider Nirvanix — an IBM storage partner — filed for bankruptcy protection. Here are some tips to consider when negotiating cloud services agreements that will help minimize the impact of a provider declaring bankruptcy:

Conduct extensive financial due diligence: Although due diligence surrounding a provider's technical capabilities is intuitive, financial due diligence is not. It is, however, important that organizations considering cloud providers investigate the financial health of the provider to gauge the risk that their data is held hostage by bankruptcy.

Seek audit rights: Due diligence will only provide a snapshot of the provider's health at the onset of the agreement. That financial health can dramatically erode during the duration of a contract—particularly when it extends several years. At a minimum, the organization should insist on early notification of potential bankruptcies.

Ensure data ownership: In order to escape any ambiguity if a provider slips into bankruptcy, it is critically important that organizations negotiate terms that ensure clarity that its data only belongs to them and that the data is immediately accessible in case of bankruptcy. Without such terms, the bankruptcy estate may make removal of data difficult or the organization can be forced to negotiate with creditors on ownership of the data.

Hopping from cloud to cloud: Data portability

When things do go awry, an organization with its data in the cloud needs to be able to hop to another provider. There must, therefore, be terms negotiated into the cloud agreement that ensures data portability. Some key issues to consider include:

Seek to minimize contract term and termination charges: If the relationship sours, the last thing an organization wants is to have its data stuck with that provider. Given cloud services are becoming increasingly commoditized, it should be easier for organizations to seek shorter contract terms with minimal termination charges — this will allow the organization to move its data should the arrangement unravel.

Seek and enforce open standards: The more proprietary the methods to access cloud stored data, the harder it will be to migrate to other providers. Ensuring that the provider utilizes open standards in accessing stored information will substantially simplify transferability of the data should it become necessary.

Obtain transition assistance: In case termination is necessary either because of failures by the provider or a change of circumstance for the organization hosting data in the cloud, it will be essential that the agreement provide for some level of termination assistance. Often this will take the form of the provider guaranteeing service for a period of time after termination or guarantees on assistance to move data to alternative providers.

Ideas in the cloud: Intellectual property

Being dependent on a provider's tools and infrastructure may have an unforeseen consequence: exposing the organization to claims of intellectual property infringement. Likewise, continued development by the provider or the organization on the data sets, tools, or architecture may give rise to disputes surrounding ownership of the new works. Addressing these issues in the front end of the agreement can significantly mitigate disputes.

Seek indemnifications: When claims of infringement arise related to the cloud provider's service or tools, indemnification provisions will help protect the organization merely hosting its data in the cloud.

Define ownership of derivative works: Rarely will the provider or the customer remain stagnant through the duration of the agreement. The customer of the cloud provider may make improvements to the cloud interface, the provider may improve tools, or both parties may contribute to improvements in hosted applications. Defining who owns what and when will significantly reduce disputes later should the relationship between the parties change.

Navigating the storm: Issue resolution

Unfortunately, some cloud services relationships will end. Ensuring a smooth termination will help ease the impact. Some portions of the cloud services agreement that deserve particular attention include:

Be cautious of limitations of liability: No cloud provider will accept unlimited or expansive liability should things go awry. But, organizations hosting data in the cloud should be cognizant that caps on liability unduly shifts risks. At a minimum, caps on liability can serve as an important data point when comparing cloud services agreements.

Review dispute resolution provisions: How disputes are to be contractually resolved can have significant consequences for the complexity and costs associated with addressing problems that arise. For example, there may be venue and forum restrictions limiting disputes to certain states and types of courts (state or federal), or, they may require binding arbitration or informal dispute resolution.

Conclusion

Leveraging the cloud need not be a stormy endeavor. Careful investigation, planning, and execution will assist enterprises seeking greater flexibility and efficiencies when hosting data and applications within the cloud.

About the Authors

Cy Morton
Cy Morton, partner, leads the Patent Office Trial Practice at Robins, Kaplan, Miller & Ciresi L.L.P. He can be reached at CMMorton@rkmc.com or 612-349-8722.

Seth A. Northrop
Seth Northrop is a trial attorney at Robins, Kaplan, Miller & Ciresi L.L.P. whose practice focuses on intellectual property and global business and technology sourcing. He has substantial experience with complex business litigation involving various technologies including software and hardware design, analytics, networking, database, and E-commerce systems. sanorthrop@rkmc.com.