InsideCounsel

Technology: 5 key cloud computing concerns

Before signing a contract with a cloud computing vendor, it's important to consider issues such as compliance, reliability and pricing

BY JOHN COWLING, DANIEL NELSON
September 14, 2012 • Reprints

In part one of this series, we discussed the issues of security, interoperability and vendor lock-in issues in cloud computing contracts. In this installment, we will discuss the five issues of regulatory compliance, reliability, complexity, privacy and pricing.

1. Regulatory compliance

Compliance touches on many issues, depending on the industry and requirements of the customer. Compliance is an issue that, along with security and privacy, often inhibits the adoption of cloud computing. In many cases, however, these issues can be addressed with a combination of contract provisions, careful vetting of vendors, the adoption of granular security procedures and, to some extent, insurance protections. A detailed discussion of the contract issues is beyond the scope of this article because the concerns vary substantially depending on the type of business. Companies should consult counsel that is familiar with the specific regulatory requirements of the business.

Customers need to address and understand, in the contract with the cloud provider, what happens when they must respond to legal discovery or a regulatory subpoena. Like the horizontal interoperability issue, the format for the extracted data, the length of time needed to extract the data, the vendor's ability to search and cull the data and the cost of extraction are all important issues.

2. Reliability

The service level agreement (SLA) should cover reliability. Availability, bandwidth and vertical interoperability should be addressed with as much specificity as necessary. The remedies, as explained in our last column, should, if possible, to incentivize the vendor to comply with the reliability requirements.

Availability numbers can be deceiving. A guarantee of 99 percent availability actually means that the service could be out for an entire day every 100 days. Many availability provisions do not address throughput or bandwidth. The service could be up, but unacceptably slow, and still be considered "available" under the contract. Customers should also understand that there may be exceptions in the contract that do not count towards the availability or related guarantees, such as the service being down for maintenance as the result of events outside of the vendor's control. This is not to say that cloud vendors should be expected to guarantee 100 percent availability or ideal throughput all of the time, but only that both parties should understand and properly document their expectations.

3. Complexity

Complexity is a subset of interoperability and intersects with other issues such as regulatory compliance. It is often addressed through careful planning and in a meaningful and granular implementation and testing process. Like enterprise resource planning projects, cloud computing projects require a detailed understanding of the customer's workflows and the scope of work. Customers should beware of vendors promising that "we can do that" if the vendor does not take the time to understand the client's business needs. All too often, the sales promises turn into vague scope-of-work requirements in the SLA and problems during the testing and implementation phases. On the vendor's side, the customer's failure to commit the resources necessary to implement the project may also create problems. Spending time on all of these issues at the beginning of the relationship and incorporating the understandings into the contract gives the project a better chance at success.

4. Privacy

Privacy in the context of cloud computing contracts, apart from security issues, is primarily related to two types of data: personally identifiable information such as financial information (primarily names and addresses combined with social security numbers, credit card numbers or other bank account information) and personal medical information. If this type of data is relevant, the contract should cover the steps taken to protect the information,

encryption, access by system administrators, procedures to report breaches and allocation of the risk of loss between parties in the event of a privacy breach. Insurance coverage may also be an issue. Note that the customer often cannot successfully transfer responsibility for privacy breaches to the vendor and will have to settle for indemnification or similar provisions.

The use of cloud services also creates issues under international privacy laws. Data centers may be located in many countries and may result in the inadvertent application of foreign privacy laws or run afoul of trade or export restrictions.

5. Pricing

Pricing is usually straightforward. (The vendor lock-in section of our previous column addressed price escalation). Most pricing issues are the same as those of other IT contracts. Customers should pay attention to the cost for training and implementation; the level of support included in the contract price; the nature and cost of extra support; the cost of enhancements; annual fees for maintenance and upgrades; travel expenses for onsite visits; and the expense of increasing processing power, data storage and bandwidth if needed.

About the Author

John Cowling

John F. Cowling *is an attorney in the St. Louis, Missouri office of Armstrong Teasdale. He practices primarily in the areas of commercial litigation, environmental litigation and information technology law. He has employed computers and litigation technology in his practice for many years. Additionally, he is the President of Lawgical Choice, an Armstrong Teasdale subsidiary, that provides legal technology services to law firms and legal departments.*

About the Author

Daniel Nelson

Daniel C. Nelson *is a partner in the St. Louis Missouri office of Armstrong Teasdale. He works primarily in the area of commercial litigation, with a particular emphasis on contract, real estate, sale of goods, securities and internal governance*

issues. He is the leader of the firm's Real Estate Litigation and Electronic Discovery practices.