Taking the Risk Out of Cloud Computing

By Robert J. Scott
Sept. 16, 2010

Business executives are beginning to recognize that cloud computing offers real benefits. Low upfront and maintenance costs, utility billing, on-demand scalability, and access to enterprise-level software represent clear advantages for any organization.

Cloud computing is a format that delivers software and related services to end users over a network, typically the Internet, instead of being installed on a local computer or server. Cloud computing can legitimately deliver greater speed, flexibility and tangible IT cost savings; three reasons why businesses should not disregard the cloud as hype. But before entering into a cloud agreement, there are significant risks that need to be addressed in the agreement.

Business Continuity Risks

Relying on software delivered over the Internet inherently creates business continuity risks. Businesses can be significantly impacted by service interruptions and insufficient post-termination data access. To address the service interruptions risk, cloud vendors typically provide some level of guaranteed service uptime with a detailed method for remedying circumstances when guarantees are not met. Generally, these service levels are contained in a document known as a Service Level Agreement (SLA). To avoid costly surprises regarding accessibility to business-critical software, the customer should read and fully understand the SLA. Besides service level guarantees and remedies, a good SLA will contain service definitions, disaster recovery provisions, customer duties and software management and upgrade practices.

Also, because all agreements eventually come to an end, it is equally important to manage the risk of data loss upon termination of the contract. The agreement should specifically require the vendor to provide the customer with access to all customer data upon termination, for whatever reason.

Intellectual Property Risks

Cloud computing implicates issues with confidential information, copyrights and trademarks. When entering into cloud agreements, careful consideration should be paid to provisions dealing with use and disclosure of information, ownership of software, and which party owns what intellectual property at the end of the term. In some circumstances, a customer may store trade secret data in the cloud. Both parties must understand the nature of the data stored in the cloud, and where necessary, address any trade secret issues with indemnity and insurance provisions to balance risk.

Some customers require customization of the cloud offering to integrate into their software environment. If the customization is performed by the vendor, the parties should consider whether the custom code is owned by the customer as a "work for hire" or is retained by the vendor. Also, cloud contracts should detail whether enhancements and customizations are available to the vendor's other customers. Finally, at termination the contract should set out whether ownership rights remain static or shift from one party to the other.

Regulatory Compliance Risks

Regulatory compliance is becoming the most vexing issue facing the cloud computing industry. Legislatures are tackling the issue of data privacy in different ways, making compliance a troublesome task for many companies. Since customers sometimes store statutorily protected information in the cloud, vendors are forced to consider how to comply with these data security regulations. Traditionally, vendors prefer to disclaim all liability for failures to comply with data security statutes. Customers should not and, in many cases, cannot agree to this type of blanket disclaimer of liability. Some data security statutes, such as HIPAA and Massachusetts Data Privacy Law, require companies to ensure that third-party service providers meet specific security requirements.

Liability Risk

The risk of legal liability is a major concern and must be addressed in the limitations of liability, indemnification, and insurance provisions in a cloud contract. Legal liability looms for both the vendor and the customer. For instance, a service interruption could continue for a significant period of time (business continuity), a third party could bring suit against the
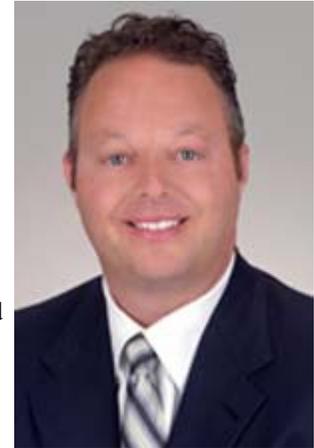
vendor for infringement of proprietary software (intellectual property), or a vendor could inadvertently leak customer data (regulatory compliance).

Vendors typically approach the liability issue with a pure avoidance strategy: the vendor disclaims all liability for failure to comply with applicable laws or data loss. From the customer's perspective, this provision is completely unacceptable. Instead of issue avoidance, the parties can balance risks and liabilities using insurance policies to transfer the risk to an insurance carrier and then tailor the indemnity and limitations of liability provisions to implement the insurance coverage. By ensuring these liability provisions specifically address business continuity, intellectual property, and regulatory compliance issues, the parties can apportion risk commensurate with the value of the cloud service.

The Good News

Companies that are quick to adapt to the cloud model may achieve greater flexibility and speed to adjust to market opportunities. But entering into cloud computing contracts without understanding the inherent risks can cripple an otherwise healthy organization. The good news is these risks can be mitigated, so long as they are recognized, by ensuring that cloud agreements identify each risk, utilizing tools such as insurance, indemnity and limitations of liability to meet the risk balancing objective.

Robert J. Scott, JD, is managing partner of Scott & Scott, LLP, a Dallas-based intellectual property law firm. He has a national practice representing clients on issues where technology, media and the law intersect. Robert has become a trusted resource on data privacy and network security, intellectual property, copyrights and trademarks, Internet law, software defense, and IT service contracts. He may be contacted at rjscott@scottandscottllp.com.