TEXAS LAWYER
JUNE 24, 2015
An ALM Publication
www.texaslawyer.com

CONSUMER PROTECTION

Business Continuity Risks for Hosted and Cloud Services

BY JULIE MACHAL-FULKS

Credit: iStockphoto.com

Businesses are increasingly interested in controlling costs related to services that were traditionally performed by internal employees. They are also looking to save costs related to hardware and software necessary to business operations. Accordingly, companies are reviewing availability of hosted or cloud solutions for software and hardware availability, network monitoring, accounting services, human resources services, and many others.

Cost of services plays a big part for most companies considering outsourcing a portion of business operations. Counsel for businesses that are considering hosted or cloud services arrangements should encourage the business teams to look past the costs to some of the business continuity risks both during the agreement and after one of the parties terminates the agreement.

While there may be many other risks in a hosted or cloud relationship, the ones that have the highest impact on business continuity include availability, accessibility, data loss and recovery, escrow, acquisitions and divestitures, and continuity after termination.

1. Availability. One of the most important business continuity concerns for companies who outsource is the availability of the software, hardware or services. If a company that depends on accessibility to its email at all times outsources its email management to a third party, the third party (and possibly others) are now in control of maintenance windows, scheduled outages, and other availability of the system.

The contract should reflect what latitude the service provide has to render the service unavailable before and after business hours. The contract should also include remedies for failure to provide the promised access to the software or services.

2. Accessibility. If a business requires restricted access to its data, the contract with an outsourced vendor should clearly outline the authorization process. Whether it is a background check for all of the vendor's employees, identification of every team member in advance, or a segregation of data or records, the parties need to include all security and investigation concerns in the agreement.

If the customer wants to be notified immediately upon a change in the vendor's team members, the contract should include a provision identifying the time and method of notification.

3. Data loss and recovery. Businesses often consider outsourcing their data management to decrease risks associated with disasters and data loss. Because the third party may have access to sensitive data, the businesses generally use a careful vetting and selection process to identify the desired vendor.

What many businesses do not do carefully is identify in the services agreement all of the expectations about data availability in the event of an outage. It is not enough to identify the service provider as the responsible party when it comes to data—the customer must also identify remedies if the service provider fails to produce the required backups or data during an outage.

4. Escrow agreements. Many large enterprises rely on hosted services for their core business operations. For instance, a financial institution may have their entire customer interface built on a platform hosted by a third party. If that third party becomes insolvent and ceases operations, the large enterprise must have a way to continue operations.

Customers that are concerned about the ability to continue business operations if the service provider or its services disappear often rely on agreements that keep the necessary source code or other operational data in escrow. The large enterprise can retrieve the source code or the data from the escrow holder in the event that the service provider stops providing services.

5. Acquisitions and divestitures. Companies that plan to make acquisitions and divestitures during the term of the services contract need to discuss and document the consequences of the acquisition or divestiture.

When a company plans to make acquisitions during the term of the agreement, there is often a need for increased usage. The costs to increase the number of users, the number of devices, or the number of software licenses should be articulated in the agreement so that the acquiring company is able to calculate the total acquisition costs.

If a business is expecting to divest a division or a subsidiary, it is often important to identify whether the number of users, devices, or licenses and the associated costs can be decreased. For instance, if a customer is being charged by the service provider for hosting 3,000 users, can the customer decrease the number of users to 1,500 after a divestiture and pay only half the fees remaining under the contract? In many instances, contracts do not allow any revisions that decrease the contractual monthly fees.

Some companies that are divesting a subsidiary enter into a transition agreement that allows the recently divested entity to continue using the third-party's technology services during a transition period. Many hosting agreements prohibit this type of arrangement. A company that is anticipating a divestiture should include appropriate revisions in the hosting or services agreement to ensure that the transition services are allowable during the term of the agreements.

6. Continuity after termination. Many customers are surprised when they terminate a hosted or cloud services agreement and experience difficulty retrieving their data in a usable format without paying substantial fees to the service provider for transitioning the data to a new provider or back to the customer. Continued access to data can be a critical requirement for most customers, and many do not address the issue in the agreements.

Companies that are considering hosted or cloud services agreements must ensure that the expectations for transitioning of critical data are discussed as part of the vendor selection process and documented in the agreement between the parties. The discussion should include whether the vendor will return all of the data, the format the data will be in when it is returned, and the cost, if any, to return the data.

Because the use of hosted and cloud services is increasing the marketplace, companies need to evaluate each of the business continuity risks that is inherent in a hosted or cloud services relationship. The ability to discuss and potentially minimize the risks can increase the likelihood that the relationship will be a successful one for both the customers and the vendors.

Julie Machal-Fulks is a partner in Scott & Scott in Southlake, where she leads a team of attorneys in representing and defending clients in legal matters relating to information technology.