Risks of the cloud

How to address potential pitfalls before moving ahead with cloud computing

Interviewed by Sue Ostrowski

Service providers are touting the benefits of cloud computing, and more and more businesses are moving to the cloud. But beyond the benefits, there are also dangers, and companies should consult with an attorney to ensure that the language in the contract will protect them, says Bill Cramer, senior counsel at Dykema Gossett PLLC.

"Service providers like to emphasize the potential financial benefits by saying that inside every cloud is a silver lining," says Cramer. "However, inside some clouds, there is golf-ball-sized hail. When you give up your computing needs to a third party, you give up control and expose yourself to potential liability."

Smart Business spoke with Cramer about contractual issues to resolve before moving to the cloud.

Bill Cramer
Senior counsel
Dykema Gossett PLLC

What legal issues do companies need to be concerned about when moving to the cloud?

You need to protect yourself in contracts with your service provider. With your own network, you control your security. But if you move your computing needs to a third party, you lose that control.

The contract should address how the hardware is protected from both outside and inside intruders. Does it require security guards or alarms? Does it limit access, require background checks, and have entry and exit logs? How does it protect data from electronic intruders? Does it have passwords to access systems? Does it encrypt data when it is stored and transferred to and from the Internet?

The contract should require segregation of your data from other companies' data, because you don't want your data mingled with that of another company. And if you are subject to regulations such as HIPAA or PCI, make sure the provider is contractually obligated to meet those standards.

Further, how often does the provider update system software? If it doesn't keep its software up to date, your information may be at risk. You should expect your information to be at least as secure off site as it is in your own building, and your contract needs to set out what the provider is doing to protect it.

How can a company address uptime requirements and remedies?

While with your own network, you don't have control over unexpected failures, you do have control over how you respond. But once you move into the cloud, you lose that control. Specify in your contract how information is stored online: At a minimum, there should be some level of redundancy, and preferably some level of error correction such that failure of a hard drive doesn't take your system offline.

Second, where is online information stored? Are there multiple copies at multiple locations, so if there is a catastrophic failure at one site, is there a secondary site where service will continue so you can maintain your business?

Third, if the cloud becomes inaccessible for a short period, is there any definition of 'short period?' A service provider may promise 99.9 percent accessibility, but over a year, that's more than eight hours of unscheduled down time. Further, some providers don't start counting such interruptions as down time unless the interruption lasts more than five minutes.

Fourth, does the provider make periodic backups of data and have an applicable transaction log so it can recover data if there is a software problem? Fifth, the provider should have a cluster of computers with multiple redundancies so if one is taken down for maintenance, it doesn't affect service.

Finally, your contract should specify what level of support you can expect when there are problems.

What should the contract cover regarding liabilities to third parties?

You may become liable as a result of a breach in security, resulting in notification requirements, which can be expensive. You may be accused of patent infringement because of the provider's services. It's important to spell out in the contract that the provider is on the hook to indemnify you for your costs, as well as to provide for your defense if you are sued.

How should the contract address remedies?

The contract is empty unless it ultimately provides a remedy. Typically, contracts have limits of remedies, for example, if service fails, you don't have to pay for that service. But you need to put a dollar value on what it means to your business to be offline for a minute, an hour, or a day. The provider may offer credit for down time, however, that credit has to be enough to incentivize the provider not to fail. For example, an hour of unplanned availability should result in more than an hour of credit, so that the provider has an incentive to get it right.

What if the move to the cloud fails?

You need to have a graceful retreat. Even with a competent service provider, a good internal team and a solid migration path, it still may not work as you expected. Start slowly, preferably with a pilot project that won't cause too many headaches if it fails.

The contract needs to have a migration path to retreat, to recover data and software from the provider and bring your information back to your facility. This can be difficult if you didn't expect it. It may take weeks to retrieve your data and software from the cloud, and during that time, how do you conduct your regular business?

To ensure all your bases are covered, look to a law firm that has experience dealing with the specifications, technology and provisions of service that can examine the contract for missing but essential terms and terms that carve out big exceptions in the provider's obligations. <<

BILL CRAMER is senior counsel at Dykema Gossett PLLC. Reach him at (214) 462-6418 or wcramer@dykema.com.

Insights Legal Affairs is brought to you by Dykema Gossett, PLLC