KAYE SCHOLER

Big Weather And Cloud Computing: Lessons From Sandy

The broad path of Hurricane Sandy shows us that the same storm that destroyed your primary computing center can also destroy your backup site located in another state and hundreds of miles away. Cloud computing can mitigate geographical risks of extreme weather. Put another way, clouds in a storm can be a good thing.

Industrial-strength cloud computing can be an important part of a company's IT ecosystem. Cloud computing can provide a way to replicate and store data in a geographically dispersed manner. The data can then be restored when, because of adverse weather or natural disasters, the backup facility cannot be reached, cannot be manned because is inaccessible by travel or Internet employees, and cannot function because of the damage it sustained. Cloud computing can provide redundancy necessary in an emergency. It can also allow a company's employees — and the company's customers — to access data and computing services from remote locations and using mobile devices.

Companies depending on Big Data can also benefit from cloud computing during emergencies, including companies whose business require sophisticated analytics performed on large data sets. It is a given that businesses today have access to tremendous amounts of data. The challenge is not just to collect data, but to analyze it and make decisions based on the data. But making decisions is not the end of the story. The ultimate purpose of making decisions is to achieve good business outcomes. Cloud-based Big Data provides a means to continue operations when other data centers are unavailable because of superstorms. This highlights that increasingly the job of the chief technology officer is to manage computer services and select software.

"The challenge is not just to collect data, but to analyze it and make decisions based on the data. But making decisions is not the end of the story."

Not all cloud computing systems are created equal. Well-designed due diligence is required before the disaster so that the right cloud vendor provides the right services after the disaster. The due diligence needed is different from that used in traditional artisanal IT outsourcing. Cloud services are delivered to

About the Author

William Tanenbaum is chair of the Intellectual Property, Technology & Outsourcing group at Kaye Scholer LLP. He was named as "Lawyer of the Year 2013" in Information Technology Law in New York by Best Lawyers in America and ranked in Band One in Technology and Outsourcing in New York by Chambers. The group was ranked in the First Tier in New York by U.S. News & World Report. He is a past president of the International Technology Law Association and is currently a Vice President in the New York Metro Chapter of the Society for Information Management, an association of senior IT executives. He is a graduate of Brown University and Cornell Law School. He can be reached at ***william.tanenbaum@kayescholer.com***

This article originally appeared in *Law360* on November 2, 2012.

the customer by a provider and an interwoven collection of subcontractors and upstream IT companies sometimes referred to as the "Stack."

Due diligence requires investigating not only the direct provider but the companies in the Stack, and not only technical ability, but also financial stability. Many companies in the Stack that support the cloud provider are not visible to the customer, and may be small and may not have the financial strength to provide the technology or necessary support to the cloud provider when an emergency arises. This can lead to legal problems. For example, if the small company encounters problems, the cloud provider may lose the legal right to use technology on which the customer relies.

> ***"Not all cloud computing systems are created equal. Well-designed due diligence is required before the disaster so that the right cloud vendor provides the right services after the disaster."***

Ensuring good cloud-based services requires well-focused contracts that anticipate the difficulties that will arise when IT services must be provided during storms and other emergencies. Lessons learned from IT outsourcing experience can be applied to cloud computing contracts. Because cloud providers are delivering services rather than technology, service levels must be carefully defined; the scope of services must be clear; the division of responsibility between the provider and the customer must be correct; and the special services required in an emergency must be defined properly and priced correctly. Two special contractual requirements are advisable.

The agreement must obligate the cloud provider to cooperate with the customer's other IT providers during the emergency; this will require modifying confidentiality provisions to allow all the providers in the company's portfolio to share information and access their technologies in an expedited manner. Force majeure and disaster recovery provisions should be combined. An event which constitutes a disaster under the disaster recovery plan should not, through contract drafting, also constitute an act of God under the force majeure provision that gives the providers a get out of jail free card and the right to suspend services. It is not a question of if a disaster will occur but when, and the contract should be written to require the provider to plan for and be able to provide services during the emergency.

> ***"It is not a question of if a disaster will occur but when, and the contract should be written to require the provider to plan for and be able to provide services during the emergency."***

Finally, cloud computing provides data privacy and data security risks that generally are not present in traditional IT outsourcing. These must be addressed through special contract provisions that often must be added to a cloud provider's standard agreements to provide customer protection.