Heads In The Clouds: Understanding Cloud Computing And Its Risks

February 01, 2011

The term "Cloud Computing" is coming up more and more often in the press, and in questions from clients. But what is cloud computing really? And what kinds of issues and risks do clients need to be thinking about when considering "leveraging the cloud?" **What is Cloud Computing anyway?**
Just about every business uses software applications of one type or another. Some applications, like word processors, spreadsheets and graphics tools, run on each user's desktop. Other applications, such as accounting packages, email servers, inventory management systems, document management systems, time keeping packages, and customer relationship management systems run on centralized servers that support multiple users at once. In many cases, those servers aren't even in the same office as the users who access them. Instead, the servers are centralized in a data center managed by the business, and users access them through the company's network. IT personnel at the company are responsible for maintaining the servers, installing updates, making backups, and ensuring the servers are secure. The move to "cloud computing" is really all about outsourcing data center operations to a third party vendor. After all, why should a business have to purchase servers and maintain a data center to run applications? Wouldn't it make more sense to have a company that specializes in running a data center or a particular type of application "rent" time on its computers instead? That way, instead of a company running an application on its own computers in its own data centers, the company can contract with an expert vendor who runs a data center that is shared by many users. The vendor takes care of all the hardware and (in many cases) software licensing costs, is responsible for applying updates and making backup copies, and generally running the data center or application. The company's users access the same applications as before, except that they are accessing them over the Internet, instead of over the company's internal network. In many cases, in fact, the users don't even notice the difference. To them, the application is just "out there somewhere in the cloud." **Why Bother?**
In many ways, cloud computing makes a lot of sense. Since the vendor can support many different customers, they can take advantage of economies of scale. The company's capital costs are reduced as well since it doesn't have to maintain and upgrade its own computers. Labor costs are also

reduced since the system administrators at the vendor take care of running the data center, instead of requiring the company to hire personnel to do that job. In addition, there's the magic of competition driving prices down since many different vendors can compete for the company's business. Some of those vendors may even be outside the U.S. in countries like India with good technical resources, and lower labor and regulatory costs. So long as the connection is fast enough, the user never knows the difference. As a result, moving to the cloud can save money and allow for more flexibility than the company would have if it had to purchase and maintain its own equipment.

OK, So What's the Rub?

As much as cloud computing might seem to make sense financially, there are some downsides, and some of the most important downsides are on the legal front. The nub of the problem is simple: the company is giving up control of data that it needs and, in many cases, has an obligation to protect. For example, suppose a company were to move its document management system to the cloud. What would happen if the vendor ran into a problem and that system wasn't available for a day? For one thing, the company would have a lot of difficulty getting any work done. For another, it's possible that deadlines would be missed and the company's customers would be put in a bad position as a result, potentially leading to litigation. For a real disaster scenario, imagine that the company gets into a dispute with the vendor and the system is "turned off" while the dispute is worked out. How will the company be able to meet its obligations when its documents and, possibly other systems, are no longer accessible? And, more importantly, what will its E&O carrier say when confidential documents, potentially documents with the names and addresses or financial information of its customers, are exposed because of a security breach at the vendor's data center? How well will the "not my fault" excuse go over during resulting litigation? What if the vendor is serving a bank or other entity subject to regulatory oversight? Will the regulator allow the bank to shift the blame to the vendor when something goes wrong? All of these scenarios are possibilities and, therefore, risks that have to be assessed before the decision to move any given system to a cloud computing infrastructure can be made. Some of these risks can be dealt with technologically by maintaining backup and fall-over systems. Other risks need to be dealt with from a legal perspective, most often in the contract between the company and the vendor, or in the form of due diligence reports on the vendor that help demonstrate the company acted responsibly during the selection process, and audit clauses that permit the company to update that due diligence over time. The trick is being able to identify and understand the risks, and knowing the options for addressing them. **So the Cloud is Bad, Right?**

No, it's not bad, it's just a tool that creates some new risks that have to be understood, considered and managed. Many can be mitigated with technology, while others have to be addressed legally. Despite those risks, however, the move to cloud computing is only likely to accelerate over the coming years. We as legal advisers should expect more questions regarding the inherent risks and the potential strategies for dealing with them. We also need to be prepared to advise clients if litigation arises because something goes wrong in the cloud, and, preferably, regarding steps they can take up front to help avoid that potential outcome, or at least make it easier to respond should the unthinkable come to pass. If you feel that your business may be impacted by this information or

have any other questions related to intellectual property, please contact Ty Giltinan at 813.229.4241 or tgiltinan@carltonfields.com.

Authored By

William Giltinan

Related Practices

Intellectual Property