PUBLICATION

Cloud Computing: Vulnerabilities and Challenges

May 09, 2011

As recent events have shown, companies who use cloud computing must understand the associated legal and business risks and have a plan for managing those risks before a problem arises. Operating in the cloud certainly offers some business advantages, including lower cost, higher efficiency, flexibility, scalability and on demand provisioning. However, as the recent "Amazonpocalypse" has shown, cloud computing also has its limitations, and companies must understand those limitations in order to reap the benefits while simultaneously reducing the risks.

Amazon's data center facility in northern Virginia recently experienced a network event that created a shortage of capacity and resulted in a large scale outage for its customers, including noteworthy companies such as Foursquare, Quora and Reddit. This outage is particularly troubling when you consider that Amazon's web-based cloud services are often listed as a model or industry benchmark for similar offerings. During this outage, approximately 12 hours passed before Amazon made any progress in fixing the problem that caused several websites and internet services to crash or have limited availability.

While utilizing a cloud service provider helps companies lower costs, it also comes with the added risk of relying on a third-party to fix problems that may arise. In short, businesses should plan for potential failures by becoming educated on safeguards that are available, both contractually and operationally.

- Privacy and security issues are critical. With the advent of the cloud computing services, there's inherent vulnerability. There is no control or limited control over critical security areas and physical control is left to the cloud provider. It is important to understand what automated processes are taking place and address/understand audit and monitoring rights relating to the services provided, as well as data breach obligations.
- When negotiating the contract with a vendor, understand the terms of the service level agreements, which will help with business expectations. For example, Amazon promised its web-services customers that its data centers will be available 99.95 percent of the time. As part of your research relating to cloud computing vendors, understand the vendor's history of incidents and the vendor's incident response policy.
- It's vital to address disaster recovery and business continuity protocols and procedures to ensure that the proper procedures are in place for business resiliency. Other critical business issues include the financial stability of the cloud service provider, transition assistance, suspension and termination rights. There were several Amazon customers that did not have an outage because their planning accounted for potential issues.

In summary, outages are nothing new. Bottom line - outages will happen, whether they are in your office, your datacenter or the cloud. Be smart and get educated about the risk and benefits of the cloud. Legal terms and conditions are constantly evolving. Good planning on both the business side and the contractual side will be invaluable.

If you have questions about the challenges of cloud computing and how they may affect your business, please contact your Baker Donelson attorney or any of the attorneys in the Firm's Business Technology Group. You may also follow us on Twitter at @Baker_Tech.