PUBLICATION

Government Releases Security and Privacy Guidelines for Cloud Computing

Authors: Alisa L. Chestler
February 07, 2012

In December, the National Institute of Standards and Technology (NIST) issued its "Guidelines on Security and Privacy in Public Cloud Computing" (Special Publication 800-144). The Guidelines provide a sobering and significant overview of the "formidable" security challenges for those utilizing the services of public clouds. The main premise of the document is to ensure that the end user clients understand their integral role in the privacy and security of data and applications maintained in a public cloud environment. While the Guidelines are generally geared toward federal agencies, they provide a concise resource for all companies considering a move to a public cloud environment.

As established in the Guidelines, there are many potential benefits for greater privacy and security controls in a public cloud, including better staff specialization, uniform platform strength, greater resource availability, robust backup and recovery, and data concentration which allows for less need for portable devices and removable media. However, there are certainly just as many concerns with public cloud computing, including system complexity which is an ever-evolving challenge, the complexity of logical separation to deal with the shared multi-tenant environment, utilization of the Internet as a delivery mechanism and finally, a loss of control by the client, to name just a few.

The Guidelines serve to remind the reader that the ultimate responsibility for ensuring that the privacy and security of the data and applications continues to reside with the company purchasing the cloud services. While much of the physical, technical and administrative safeguards are handled by the cloud service provider, the company will still retain responsibility for a significant portion of these safeguards. For a company considering a move to the public cloud, the role of due diligence should not be underestimated, and begins with the company identifying their own privacy, security and other organizational requirements for choosing the right cloud provider. The Guidelines also emphasize the need to "ensure that all contractual requirements are explicitly recorded in the service agreement, including privacy and security provisions, and that they are endorsed by the cloud provider." Involving an experienced legal advisor before the cloud provider is chosen can prove very critical in meeting both of these needs.

The Guidelines also remind companies that continued assessment of the performance of the cloud service provider and the quality of those services is a never-ending responsibility. Managing and mitigating risks are an affirmative and constant obligation for all companies, including those with data and applications in a public cloud environment.

To view "Guidelines on Security and Privacy in Public Cloud Computing," please click here.

If you have any questions about privacy and security issues related to public cloud computing, contact your Baker Donelson attorney.