By Mary Siero

Secure Cloud Computing

Protect Your Data with the Right Contract

This is Part II of a two-part article on the security of cloud computing.

In Part I of Secure Cloud Computing we discussed the changes in the audit provisions for cloud service providers, moving from the SAS 70 Audit to the SSAE 16 (SOC 1,2 and 3) Reports as one component of mitigating the vulnerabilities of cloud computing. Another important component is the contract.

Jay Mohr once said, "Unfortunately there are no mulligans when it comes to … contracts." This article will focus on three of the important terms specific to contracts with cloud service providers to help you avoid needing that mulligan.

Fundamental to the success of cloud service providers is the concept of joint tenancy. In order to take advantage of resource optimization and economies of scale, cloud service providers use virtualization technologies to locate applications and data from various clients on a single server. In some cases, where you are taking advantage of software as a service (SaaS), your data may be in the same database with other clients.

Protecting your data in a joint tenancy environment can be accomplished by contractually obligating the cloud service provider to provide you with a warranty related to your data availability that meets your business needs. This warranty should state that availability of your data will not be impacted by any adverse events impacting the data of any shared tenants. As part of this, you should take the time to understand what controls are in place to ensure the integrity and authenticity of your data, including secondary data like metadata and log files. For example, if there is a legal seizure of a shared client's database, you will want the cloud service provider to warrant that it has processes and procedures in place so that your data availability will be unaffected.

In cases where your company data is resides in a database along with the data from other companies, review the methodologies to compartmentalize the data and the controls in place to prevent data leakage from one company to another. If the data is encrypted, the management of the encryption keys should be addressed.

The second important term to address is related to compliance, as there are some distinct differences created by cloud computing.

"Is the cloud secure?"

Identify where your data will be located, or even where it will not be located. Within the United States there is no federal legislation that covers the definition of personally identifiable information (PII), protection of PII, or customer breach notification conditions and requirements. As a result, these matters are typically covered by state statutes and vary from state to state. Furthermore, if your data is stored or located in a state different from the state in which you collect it, you could be subject to multiple jurisdictions regarding its protection and notification, an environment typical for hospitality chains.

If your data is located outside the United State, learn about the data privacy laws of the country in which it is stored and obligate your provider to comply with them. Italy, Russia and the European Union all have more stringent data privacy requirements than the United States. Make sure your cloud service provider contract for data stored in any of these locations reflects those laws and that they won't adversely impact your business processes by complying with them.

Another compliance issue to incorporate into your cloud services provider contract is your ability to perform compliance activities on your systems and data in the cloud. For example, PCI requires an annual penetration test; make sure your contract gives you the right to conduct these tests or performs them for you in a manner that satisfies your requirements and provides you with the necessary documentation to prove compliance.

Specific contract language relating to discovery, litigation hold, subpoenas and expert testimony should also be included. These contractual provisions should ensure proper disclosure without contamination, as requested.

The third term to make sure you address in your cloud services provider contract is breach notification. You need to be notified if your data has been breached, but, what if a shared tenant's data has been breached? Will your provider notify you in that situation? Should they? If your data is in a combined client database, you will likely want to know if a shared tenant's data was breached unless you are confident that the wall separating your data from theirs is not only effective, but impenetrable.

Including these three important terms in your cloud service provider contract will allow you to save your mulligan for another day.

MARY SIERO, *CISSP, CISM, CRISC, is the principal at Innovative IT in Las Vegas, Nev., and can be reached by visiting www.innovativeitlv.com.*