By Mary Siero

Secure Cloud Computing
Another Lesson from Mythology...

Freedom that gives you no worry, anytime, anywhere computing... that is the lure of the cloud.

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

Science and technology lead to culture change and the cloud is the latest technology to offer the promise of a game changer. Since the hospitality industry is all about culture, the cloud is the latest vehicle to offer the opportunity for change with the next big advance in providing guest services.

The biggest question on everybody's mind is, "Is the cloud secure?"

To answer this question, it might be helpful to look at Greek mythology. As legend has it, the infant Achilles was dipped into the river Styx by his mother Thetis in an attempt to make him invulnerable. She held him by the heel of his foot as she lowered him into the magical waters. Achilles' undipped heel left an area of vulnerability, a weakness which later led to his death when Paris shot a poisoned arrow into that heel. What if this vulnerability had been discovered before Paris shot the fatal arrow? Achilles may have lived to fight another day. The moral for us is that weaknesses may not be apparent, but can be compensated for if they are identified. With this in mind, the best way to approach cloud computing is with a combination of knowledge and caution.

The cloud has many benefits that can truly enable you to transform your business by either keeping pace with the changes in culture or creating a new culture of experiences for your guests. Taking the time to understand how to prudently select your cloud services provider and build in the controls to manage your risk in the cloud environment will open the doors that eluded Achilles.

The best place to start is with the controls offered by your cloud services provider. Historically, you would have requested a SAS 70 report which covered security in the form of operational security. SAS 70 ensured that the service provider backed up its systems and implemented redundant controls to minimize the risk of data loss that resulted from inadequate operational processes or environments in the mainframe world that was predominant during that time. Today, mainframe processing is being usurped by powerful and complex client server environments. It's a different day and the rise in popularity of the Internet and the more nimble technologies that support it also give rise to new safeguards that need to be addressed to protect your data.

In a progressive move, the American Institute of Certified Public Accountants (AICPA) has upgraded SAS 70 to SSAE 16 in keeping with this change in culture.

Beginning June 15, 2011 auditing firms began auditing to the new SSAE 16 standards.

SSAE 16 retains the Type 1 (discreet point in time) and Type 2 (period of time) report designations. The old SAS 70 requirements (operational controls and safeguards) are now incorporated into a Service Organization Control One (SOC 1) report. In order to take it to the next level, two additional reviews have been added to address controls related specifically to data security and protection, and to round out the best practice implementations of data security. These reviews are designated the SOC 2 and SOC 3 reports.

With this in mind, when you select a cloud provider, you want to ensure that they are in compliance with the SSAE 16 SOC 2 standards to add assurances that your data is protected.

The second thing to verify is that the auditor who performed the audit of the cloud provider is cloud aware. Being cloud aware is important because it means the auditor understands the operational model of the cloud and knows what controls are important to the data that is housed in the cloud. For instance, joint tenancy is a key cloud model employed to keep costs down. Auditing data in a joint tenancy environment should include special precautions to ensure that compartmentalization of the data is adequate and controls to manage this compartmentalization are included as part of the audit. Since joint tenancy is not a model commonly used in on-site data centers or in data center outsourcing, specialized knowledge is required for this type of audit.

A third important consideration for cloud computing is the location of the cloud services. The physical location of the servers that house the data may introduce different legal or regulatory considerations. For example, the European Union (EU) has specific privacy laws, different from U.S. privacy laws, which are applied to data that is housed there. If your service provider locates your data in one of the EU countries, your data is subject to those laws. Likewise, states in the United States may have or may be considering laws that your data will be subject to if it is housed within that state. Lastly, regulatory agencies that govern your industry may have requirements related to the location of your data.

These three practices, 1) request a SSAE 16 SOC 2 report, 2) ensure that audits are conducted with cloud-aware auditors, and 3) know the location where your data is housed, are good starting points in moving to the cloud.

Part II of this article will discuss various contractual provisions you should consider before you sign the contract to move your sensitive data into the cloud.

MARY SIERO, *CISSO, CRISC, is the principal at Innovative IT in Las Vegas, www.inovativeitlv.com.*