@ISACA
RELEVANT, TIMELY NEWS
Volume 15, 20 July 2011

Top 5 Questions to Ask Cloud Providers About Information Risk Management and Security Before Engaging With Them

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. **What level of visibility into your cloud environment are you willing to provide to me as a customer?** Visibility is one of the key concerns when engaging cloud providers with all flavors of their services. Often, cloud providers are willing to give you visibility into a set of logical containers they establish for you but limit your ability to peer under the hood to see how they design, implement and operate the supporting infrastructure. Unfortunately, this limits your ability to properly assess risk or enable controls to adequately secure your environment, since you can easily be impacted by operational activities or attacks that may be directed at the underlying infrastructure or carried out by an insider within the provider's organization. If you are running in a private cloud configuration, I suggest requesting the ability to review a read-only mirror feed of all operational and system-management activities associated with the technical infrastructure supporting your services, including server, network and storage elements. You can then use this level of visibility to support a trust-but-verify approach to risk management and security with your provider, which is something that the provider should be able to support in this configuration.

1. **What are your availability guarantees and resiliency capabilities and how do you support them?** Recent outages, such as Amazon's EC2 multiday outage, have brought to light the fact that many cloud providers do not have robust business resiliency capabilities (e.g., command and control, business continuity, disaster recovery, incident response) in place to effectively address broad-based disruptions to their capabilities and infrastructure. It is important to understand the existence and comprehensiveness of a provider's capabilities as well as their level of maturity. It is also important to understand the requirements they have for you as a customer to be able to take advantage of these capabilities in advance of a business-impacting incident.

2. **What guarantees of risk management and security are you willing to provide to me as a customer?** Unfortunately, if you look closely at many of the agreements and terms of service that are required for organizations or users to execute to use cloud services, you will find most providers offer little or no guarantee of appropriate risk management and security of either their or your environments. In fact, by default, many cloud providers typically make it the responsibility of the customer to properly protect the capabilities and services they utilize as well as their data. Without enhanced visibility into and control of the underlying information infrastructure that supports the capabilities and services you contract for, it is almost impossible for you as a user to effectively secure your environments and the data included within them. Often, cloud providers will offer you a series of security technologies that you can implement in your environment at your cost to help you enhance your own security, but this still does not solve the challenges associated with underlying information infrastructure, which can adversely impact you as well.
3. **How do you protect yourself and the solutions and services that I purchase from you from denial-of-service attacks?** From a risk management and security perspective, one of the Achilles' heels associated with cloud solutions is the denial-of-service attack. If users are unable to connect to or take advantage of the cloud environments, then they are essentially useless. In the case of cloud infrastructure, this is a bigger concern since an adversary may be attacking the provider or another customer of the provider that has no relationship to your organization, but it still can have a direct impact on you and other customers. Unfortunately, these attacks are relatively easy to carry out and can be very effective, if an adversary is motivated and capable. This has been seen recently by the attacks carried out by the group known as "Anonymous." There are various ways cloud providers can attempt to defend themselves from these types of attacks, which can include having reserve network capacity available; implementing and operating technology specifically designed to capture and redistribute attack traffic; establishing, testing and maturing incident response procedures specific to this type of attack; and even having reserve data centers available that are connected to alternative networks and mirror your environment and associated data on a regular basis.
4. **How comprehensive and mature is your information risk management and security program and the capabilities it provides to your organization?** Information risk management and security are typically 75 percent people,

process and procedure and 25 percent technology. It is important to understand how seriously and comprehensively a cloud provider recognizes this paradigm and also the maturity of its associated capabilities. If the cloud provider's primary evidence of the comprehensive nature and maturity of its program and capabilities is to identify and demonstrate the technologies that it has in place or the certifications it has earned from third-party organizations, such as the Payment Card Industry (PCI) Security Standards Council or the Cloud Security Alliance (CSA), this could be a warning sign about its level of focus or ongoing support. Unfortunately, technology works only as well as the people, processes and procedures that are used to leverage and support it, and industry certifications tend to set the minimum acceptable level for risk management and security capabilities, not the ideal or appropriate ones. In fact, the use of third-party certifications as proof of capabilities often leads to the use of security-by-compliance as a risk management strategy instead of the operation and support of a properly funded comprehensive information risk management and security program. When evaluating capabilities of cloud providers in this area, ask to review the structure, mechanics and evidence of regular and consistent use of their programs for the services for which you are contracting. This can include a review of their approach and capabilities associated with threat and vulnerability management; integration of risk management and security capabilities in their business and operational processes; a governance model that supports their program; and metrics and measures they use to monitor the effectiveness of their program and capabilities on a regular basis.

The following publications related to cloud computing are available from ISACA: *IT Control* ***Objectives for Cloud Computing***, ***Audit/Assurance Program: Cloud Computing Management*** and ***Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives***. In addition, ISACA offers the **Cloud Computing Group** in the Knowledge Center and further guidance on the **Cloud Computing** page of the ISACA web site.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.