Are Your Data Secure in the Cloud?

John Nye, CISA, CISM, CRISC, CISSP, is the director of technology risk solutions at ProcessUnity *(www.processunity.com)*, a cloud-based provider of governance, risk and compliance (GRC) solutions. He is responsible for the governance of ProcessUnity's Software as a Service (SaaS) solutions and advises clients in the art of third-party vendor risk management. Nye has worked with firms such as @stake, Symantec and Moody's as an assessor of third-party risk and has served as an information security executive for a midsized technology service provider, protecting information and managing corporate risk from both sides of the due-diligence table.

I was involved with hosting my first Internet-accessible, web-based, multitier, multitenant, shared infrastructure software solution in 1998. It was an x.509 digital certificate authority. Back then we didn't call it a "cloud solution," but we might today. In the years since, I have been involved in two other cloud solutions: a customer contact campaign management (auto-dialing) solution for call centers and, in my current role, a governance, risk and compliance solution with a focus on vendor risk management. All three of these solutions offer some common traits to subscribers:

- Access to specialty expertise
- Streamlined or even transparent upgrades and maintenance
- Effortless scalability
- A chance to share their confidential data with a trusted third party
- The opportunity to rely on a vendor for the success of a critical business process

Clearly, there are pros and cons in this list. In a differential comparison against on-premise solutions, the traditional benefits of outsourcing—access to expertise and seamless technology operations—can usually be achieved within the enterprise at some reasonable expense. Tactically, a business is usually better off selecting the best solution, regardless of whether it is internal or outsourced. Strategically, outsourcing can allow an organization to focus on its core competencies. Regardless of the business drivers for outsourcing, once appropriate third-party management and governance is included, outsourcing is not necessarily a material cost saver.

However, when one adds the massive scalability of cloud solutions to the outsourcing equation, the economics change drastically. The economies of scale achieved through the use of cloud solutions drive costs down to the point where they are difficult, possibly even negligent, to ignore.

For some organizations, the decision to move to the cloud is both obvious and instant. For others, cloud solutions represent intolerable risk. Certainly the challenges of assuring quality, protecting information and meeting service availability requirements in today's extended enterprises are present in the cloud, just as they are with other outsourced solutions. Yet in the cloud, these risk factors are more greatly feared. Why?

The answer is simple: fear of the unknown. This is true in two ways. First, transparency can be a challenge. The word "cloud" itself seems to say, "You do not need to know what is inside." Indeed, the icon of a cloud, so familiar as the shape of the Internet on network diagrams, tells us that what is inside is large, complex and irrelevant to the discussion. In the traditional notion of an enterprise with a clearly defined perimeter connected to the Internet—an external and untrusted entity—this obfuscation of complexity and expression of irrelevancy is completely reasonable. However, when outsourcing a business function to a cloud provider, nothing could be further from the truth. As risk management professionals, part of our responsibility is to evaluate the risk of outsourcing to third parties and to assess or audit their controls. It is our job to look inside the cloud, but, unfortunately, this is not always possible and, indeed, the right to audit seems to be more challenging to obtain as the cloud provider becomes larger and more cost-effective.

Second, cloud providers frequently implement familiar controls in unfamiliar ways. Let us take the simple example of comparing an on-premise enterprise software solution to a Software as a Service (SaaS) cloud solution. When the enterprise wants to regulate access to its data, one of the most common controls is to host the applications that contain the data inside its firewalls to prevent unwanted access via the Internet, which is to say, the enterprise uses network-based source Internet Protocol (IP) address filtering. Unfortunately, this technique does not work for many cloud providers. For example, when clients access solutions over the Internet and multiple clients share a single platform, universal access is allowed.

Certainly, firewalls should be in place, but they allow, rather than prevent, access to key applications via the Internet. Fortunately, the control objective is to regulate access to the data, not the application. So, instead of using a network-based solution (i.e., a firewall) to indiscriminately regulate access to the application, one can implement the source IP address filtering directly in the application to regulate access to the data. In this way, desired policies can be enforced on a per-client basis,e.g., by limiting access to a client's data to users connecting from that client's enterprise.

This is just one example of how a control might be implemented differently by a cloud provider than a typical enterprise or even a noncloud service provider. For those of us whose role as a risk manager includes evaluating whether our cloud providers are achieving the necessary control objectives, we need to be prepared to understand how our cloud providers operate in order to evaluate the design and effectiveness of their controls. And, we will want to consider how such control designs change the traditional priority of other controls.

Let us take another look at the previous example. In the case of the on-premise enterprise application, the firewall meets (at least) two control objectives. First, it authenticates the user's source IP address to ensure that the user is onsite at the enterprise. Second, it protects the application from attack by Internet-based attackers. In the case of the cloud solution, the source IP authentication has been moved to the application, but that application has been exposed to the Internet, thereby modifying its attack surface and exposing it to new threats. Clearly, application security controls should be a higher priority for the cloud application than for the on-premise enterprise application. Not only is the cloud application exposed to the Internet, it is also responsible for some of the controls previously provided by the firewall.

> "Be prepared to understand how your cloud providers operate in order to evaluate the design and effectiveness of their controls."

Understanding how cloud providers operate is key. Without this information, you cannot understand their (or your) risk. And, if you do not understand their risk, you cannot determine if their controls are designed or operating effectively. To a fellow risk professional, such a mantra will come across as both obvious and academic. However, in the world of third-party risk management, where one-size-fits-all assessments are used in an attempt to compress standards-based, formal controls audits into assessments lasting only a day or two, the peril of assumption warrants the reminder. To avoid this mistake, particularly if there are time constraints, ask these questions about any cloud provider at the beginning of an assessment:

- What type of cloud solution is it (e.g., Infrastructure as a Service [IaaS], Platform as a Service [PaaS], SaaS), and how does that inherently impact control design?
- Does the cloud provider use virtualization or other new technology and, if so, how has the provider addressed the organization's control objectives as these new technologies reshape how the Open Systems Interconnection (OSI) model[1] is implemented?
- Has the cloud provider implemented provisioning tools? If so, do these tools enhance governance, inadvertently subvert the provider's security architecture, or both?
- The cloud is relatively new. How new, as a business, is the cloud provider and what does that mean about its financial and business stability?
- Cloud providers frequently do not want to manage their clients' individual users and, instead, support some form of delegated access management. What options are available from the cloud provider for access and identity management? What options are available for access control review and for log review? And, do these features meet the organization's governance and operational needs?

- Is the cloud solution stand-alone, or does it involve multiple providers (e.g., a SaaS solution hosted on a PaaS solution)?
- Is there an opportunity for risk concentration that would not be present in an on-premise enterprise solution? How does the organization's business impact analysis change if multiple applications are moved to the same IaaS provider? How many of the organization's peers outsource the same function to the same cloud provider and, if many, how would a potentially marketwide incident impact the organization?

These questions are hardly comprehensive, but they serve to focus one's perspective at the beginning of an assessment of a cloud provider. Understanding how cloud vendors operate allows you to move beyond fear of the unknown into the comfortable place of rational, risk-based decision making.

One of the most common questions I am asked—by colleagues, clients and lay persons alike—is: "Is the cloud secure?" In response, I point out that some cloud providers are more secure than others. But, typically, when I am asked this question, it is by someone curious about well-known, consumer-oriented solutions (such as Netflix), or one of the larger, business-oriented public cloud solutions (e.g., Google Apps or Amazon EC2). Insofar as we can agree that even the best-governed solutions can experience security incidents and that when we say "secure," we actually mean "well governed with effectively designed and operating controls based on a meaningful analysis of risk," my response is: "Most large cloud providers are probably secure, but without better access, I cannot prove it."

Although I have not been fortunate enough to have obtained direct audit privileges at all of the larger cloud providers that I have used, I am still generally comfortable using them. For example, a key part of any security program is a secure, repeatable host build and the ability to apply patches. Intuitively, I know that any organization operating millions of hosts is going to have host build and change management under control. My evidence is that they operate successfully—something they simply could not do at their scale without careful planning, superb consistency and excellent change management. But, such evidence is circumstantial. I am also of the opinion that most cloud providers, due to their specialization in one or a small number of solutions, can generally do a better job of securing those solutions than their clients. For instance, when I was responsible for the security and compliance of a cloud-based telephony autodialer, a number of controls specific to telephony fraud were implemented that only a handful of the roughly 400 clients would have understood. In this way, the organization's specialization allowed us to mitigate risk that would have gone unmitigated had the solution been on premise with clients.

From the perspective of a risk professional, one of the greatest downsides of using one of the public cloud providers is the inflexibility of the engagement model. Similar to business-to-consumer services, subscribers to public cloud solutions basically have to agree to the contract provided by the solution provider. It is unlikely that such contracts will grant meaningful audit rights or include other specific terms and conditions that may be desirable to the business or required by regulators.

This does not mean you have to give up on assurance completely. In the case of the business-oriented public cloud providers, security assurance documents (e.g., ISO 27001 certifications, SOC audit reports) are usually available for review by potential subscribers. Such documentation will likely answer many of the assurance questions and should be able to allow you to make a reasonable, rational, risk-based business decision about whether to subscribe to the service or not. Unfortunately, particularly if you are regulated, this may not be sufficient to meet your due-diligence obligations.

With smaller providers, these dynamics are reversed. You will be more likely to negotiate the contract you want and audit or assess the provider directly. And you had better do so because, as you move away from the mega scale of the largest providers, you will not be able to intuitively equate operational viability with good governance. The smaller the cloud provider is, the less you can assume and the more important due diligence becomes. Some will be very trustworthy while others will be too risky with which to engage. You will not know unless you take a close look.

Enterprise-grade solutions are rarely served by single applications. An on-premise enterprise architecture can include business applications cross-integrated with one another, authentication infrastructure, logging infrastructure, and the like. Cloud solutions are no different. It is not uncommon to engage a cloud-based SaaS provider only to discover that to get the most out of the application or to govern its use appropriately, it needs to be integrated with other business applications and technology infrastructure. Frequently, the solution is to engage more cloud providers to glue these pieces together. By the time you are fully

integrated with the cloud provider serving the initial business requirement, you may find that you have had to integrate with several additional providers to assemble a complete solution. If done correctly, a foundation of cloud solutions that integrates with and extends your enterprise architecture is created. Salesforce.com's AppExchange is just one example of such an ecosystem. The down side is that, at least initially, the cost of due diligence will be high, because you have had to assess the risk of engaging with multiple third-party service providers to meet that initial business need.

A quick look at the applications in Salesforce.com's AppExchange reminds us that the cloud is an excellent place for mobile and social applications, or any application that requires collaboration and information exchange with parties outside the enterprise. Without the cloud, you have to build an extranet to exchange information with others, leaving your enterprise to solve some of the same security architecture problems faced by cloud providers, e.g., the source IP address filtering challenges described previously. As an information security and risk management professional, the ability to easily support collaboration is one of the most compelling reasons to prefer a cloud-based solution. And, to the degree that complexity is the enemy of security, cloud solutions reduce the complexity of collaboration (or at least spread that complexity out over a wider field of resources and specialists).

And so, it is no surprise that collaboration is a key component of each of the cloud-based solutions of which I have been a part. X.509 certificate authorities need to be hosted by trusted third parties to achieve the segregation of duties central to the registration model and also must make submission of certificate requests and distribution of revocation information easier. Customer communications are pushing to mobile and social platforms. And, vendor risk management requires collaboration and information exchange between enterprises and their third parties for assessments and audits. For these activities, the cloud simply makes sense.

Just as cloud providers use their ability to specialize and their economies of scale to perfect the business solutions they provide, so too can they leverage these differentiators to secure and govern their solutions. Enterprise architects have to build computing environments that support the general-use case of multiple, disparate business applications. Each application presents unique challenges to use, operate, secure and govern. For on-premises solutions, this either leads to great expense and complexity as you customize, or it leads to increased risk acceptance as you generalize. By contrast, a security architect of cloud solutions can specialize. By securing instance after instance of a single solution, the security architect can drive a security and risk management program closer to perfection than in any other environment. That this is possible makes cloud solutions an attractive option for risk professionals. But, unfortunately, not all cloud providers make this investment. As risk professionals, our duty, as always, is clear: to understand and make transparent the unknown, thereby replacing the irrationality of fear with risk-based decisions that allow the business to correctly capitalize on good opportunities.

ENDNOTES

[1] Open Systems Interconnection (OSI) model is developed and maintained by the International Organization for Standardization (ISO); see ISO/IEC 7498-1.