October 29, 2010

Q&A: Demystifying Cloud Security

An *Empowered* Report: Getting Past Cloud Security Fear Mongering

by Chenxi Wang, Ph.D.
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

At Forrester's Security Forum 2010 in Boston, Eran Feigenbaum, director of security, Google Apps; and Archie Reed, chief technologist for cloud security at HP, joined me on stage for a keynote panel on cloud security. We explored topics such as private clouds versus public ones, cloud security standards, and emerging trends. This document captures the essence of the questions and answers between the audience and the panel.

QUESTIONS

1. Is cloud necessarily less secure than my own IT infrastructure, or can it be more secure?
2. What are the most significant security concerns?
3. How do I go about assessing a cloud security provider?
4. What are some of the key trends in cloud services today?
5. Are there standards bodies that are working on a common set of security-related standards for cloud services?

CLOUD ADOPTION IS ON THE RISE DESPITE SECURITY CONCERNS

The industry has been buzzing with talks about the cloud for quite some time. Security and risk professionals remain skeptical that cloud providers can manage the responsibility to protect users, their data, and their privacy. Despite these concerns, according to Forrester surveys of multiple IT roles, cloud adoption is on the rise. Here are some of our findings:

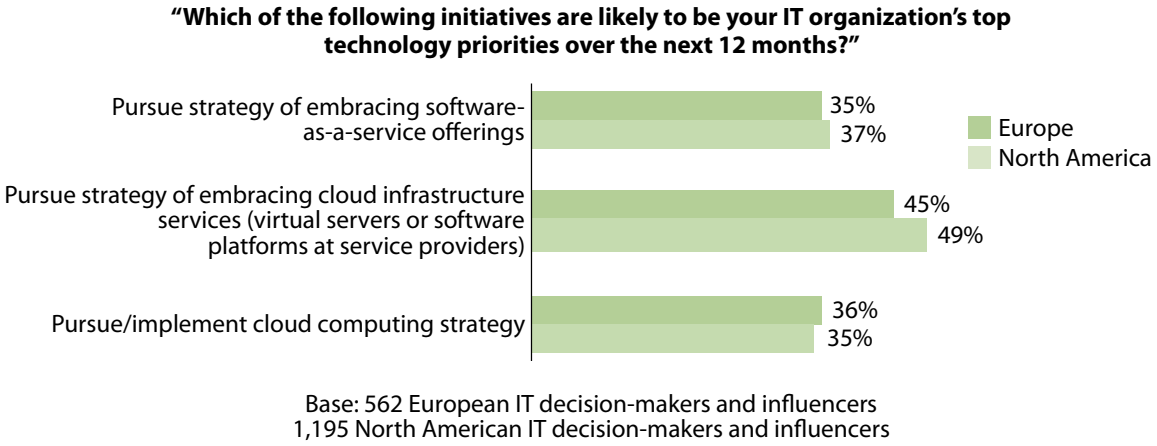
- **IT decision-makers and influencers say that cloud is a critical or high priority.** In a recent Forrester survey of 2,803 IT decision-makers, 49% of North American companies and 45% of European companies report that pursuing a strategy of embracing cloud infrastructure services is a high or critical priority during the next 12 months (see Figure 1).[1] Another Forrester survey reports that one in four companies is already using some form of cloud computing.[2]

- **Security no longer has the power to veto.** Whether it's cloud, mobile, social, or videoconferencing, security professionals no longer have the power to block access or use of these technologies. At Forrester's Security Forum 2010, we surveyed 85 security professionals in attendance to find out

how they're supporting today's empowered employees.[3] Of the 85 respondents, only 28 reported that their company was not using or piloting some form of cloud computing. In addition, only 12 of the 85 reported that security still had veto power over empowered technologies.

Since business and IT leaders are moving full steam ahead with cloud services, and since you no longer have the power to stop them, it's probably best to stop dwelling on cloud security and to start preparing for the move to the cloud.

Figure 1 Cloud Services Are A Priority In Both North America And Europe



Source: Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010

56689 Source: Forrester Research, Inc.

1. Is cloud necessarily less secure than my own IT infrastructure, or can it be more secure?

It's important not to dismiss cloud services outright because of security concerns — the benefits of cloud, including efficiency and economics, are compelling enough that you should do a deeper cost/benefit analysis. In addition, a cloud provider may have IT security capabilities that meet or exceed your own internal capabilities. Moving to a cloud service may actually improve your security posture. Think about it: Is it more secure to store sensitive corporate information on end user laptops and USBs rather than in a central repository with a cloud provider that you have thoroughly vetted?

In addition to other evaluation criteria, you should look for a provider that has:

- **Built homogeneous IT environments.** Most cloud providers don't have to deal with the complexity of legacy applications and infrastructure that exists in many enterprises. They typically use identical servers and system software across data centers, and they may maintain one application version globally. In such a homogeneous environment, it's easy to see when something is out of whack and to remediate immediately.

- **Adopted industry certifications to prove its security maturity.** Cloud service providers know that security-related concerns are one of the top barriers to accelerated adoption of cloud services. As a result, many providers are adopting widely recognized industry standards such as SAS 70 Type II, ISO 27001/2, and FISMA, in the hopes of addressing some of these concerns. These certifications alone aren't sufficient, but they should be a factor in your consideration.

- **Developed advanced threat intelligence and management capabilities.** Some cloud services, in particular security services, have a wide visibility of threats because they process so much traffic. You want to ensure that your provider capitalizes on that visibility to develop advanced threat intelligence and the ability to respond to those threats quickly.

- **Built a highly qualified security staff.** If you entrust a service provider with your data, you'd better be comfortable with the way the service provider is safeguarding it. This comes down to who the provider has on its security team and how competent they are. Google has approximately 175 highly qualified staff in the security group. Your own company may not be able to make that kind of investment.

In the final analysis, cloud computing in itself doesn't necessarily lead to more or less security. You need to evaluate the security maturity of the cloud provider, just as you would in a traditional outsourcing scenario.

2. What are the most significant security concerns?

While cloud service providers have taken steps to secure their core IT infrastructures — such as adopting mature security processes, guidelines, and standards and hiring qualified staff — there are still some IT security-related concerns. Forrester clients tell us that they are most often concerned with:

- **Ensuring data security in flight, at rest, in use, and at disposition.** Many providers offer secure data transfer in and out of their environment through HTTPs or other secure channels. A much smaller number provide data-at-rest protection (e.g., encryption). Still fewer have any form of protection for data-in-use (i.e., within the application) and assurance of secure data disposition. What we need are services capable of secure life-cycle management of data, from the data's first appearance in the cloud infrastructure to its permanent erasure. The cloud industry, as a whole, is still not at that level of maturity.

- **Maintaining identity and access control.** It's easy to manage single sign-on with a cloud or even with two different cloud services. What becomes challenging is when you have to do that with multiple cloud providers, managing diverse standards and handling third-party access to your data and applications within the cloud context. Maintaining identity and access control across an environment that includes private infrastructure, public clouds, and possibly, private clouds, is challenging.

3. How do I go about assessing a cloud security provider?

Just as with any other type of outsourcing service, security maturity will vary from vendor to vendor. It's ultimately incumbent on security and risk professionals, together with their counterparts in sourcing and vendor management, to assess each cloud provider against a list of security, compliance, privacy, and other legal and contractual requirements. When assessing a cloud service provider, SAS 70 II, ISO 27001/2, FISMA, and other certifications are useful because they tell you whether the provider has essential processes and controls in place. However, the certifications alone are not sufficient because they weren't developed specifically for cloud services. You will still need your own list of requirements.

You can start with your security and risk requirements for your internal IT systems and adjust these to account for cloud-specific issues and concerns. To help you in this process, Forrester has put together a checklist of key issues and concerns.[4] You should also plan to adjust requirements depending on:

- **The type of cloud service.** There are many types of cloud services, including software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS), each with different security requirements. For example, an IaaS deployment may give you, the user, complete control over a guest virtual machine (VM) OS all the way up to your applications. SaaS is a very different story. A SaaS user has little control over how the application operates in the cloud, let alone how it affects low-level infrastructure and operating systems. Based on the type of cloud services, you may have to adjust your assessment criteria from actual controls to monitoring key performance indexes.

- **The criticality of the data.** Your requirements will also change depending on the nature of your data. If it's regulated or highly sensitive and contains personally identifiable information, you need to impose more stringent security and privacy requirements. If your cloud provider doesn't offer a specific control, say, encryption-at-rest, either you work with your provider to implement that control, which may result in a higher fee, or you have to simply walk away. But a set of dealbreaker assessment criteria, like the ones based on protection of critical data, is exactly what you need to quickly eliminate services that aren't a good fit.

- **The location of the service.** Although the cloud service may be available wherever there is Internet access, the servers that host your applications and process your data must live somewhere. If you operate in countries that have restrictive data privacy laws, such as the EU or Japan, you need to scrutinize the service and ensure that it doesn't violate any privacy laws that restrict the movement of data across borders.

Unfortunately for many small and medium-size enterprises, you may not have the clout to insist on an internal audit of every cloud service provider. For example, Google Apps sees more than 3,000 businesses sign up every day. Given this scale, Google can't support every audit request. In fact, if

just 1% of those businesses wanted to perform an audit, Google would have to respond to more than 30 audits every day! In lieu of an audit, you must rely on a set of detailed evaluation criteria to determine vendor suitability.

4. What are some of the key trends in cloud services today?

One of the most prominent trends is that cloud users are becoming more sophisticated in choosing the right type of cloud for their needs. People are investigating options across public, private, and hosted private clouds to balance their functional, security, and cost requirements.[5] Here are just a few of the cloud options to be aware of:

- **You can build your own private cloud.** A private cloud is a virtualized infrastructure with automatic workload distribution that sits entirely behind an organization's firewall. A private cloud certainly affords you the most control while allowing your business groups to benefit from some of the elasticity and scalability features of the cloud. However, you won't be able to leverage the pay-as-you-go cloud economics, as your organization will need to make an upfront investment to build the private cloud infrastructure. Moreover, if the infrastructure is sitting at 40% load, there's no one else to share that idle overhead with.

- **You could ask a provider to host a private cloud for you.** A hosted private cloud is a dedicated infrastructure hosted by a cloud provider. It's similar to a private cloud in that no one else will have access to this infrastructure, but since it's hosted, your ongoing administrative and operational overhead is significantly less than running a private cloud. Because the infrastructure is dedicated, it's possible that you can impose specific security controls (e.g., PCI controls) across the infrastructure and applications. Some enterprises have found hosted private clouds to be a good compromise between cloud economics and security.

- **You could build or host a cloud with your friends.** Community cloud is another interesting microtrend. A community cloud is designed for different entities or companies that have similar needs. For instance, the Department of Defense (DoD) built a community cloud for different organizations within the department. The cloud infrastructure is divided into two parts, with confidential data living in one and public data in another. Any agency within DoD can use the cloud and leverage the unique protection features afforded by the two-part infrastructure.[6]

  A community cloud is intriguing because you can build it once and have it satisfy the requirements of many in a particular industry or with similar requirements. Perhaps we will see community clouds built for PCI, HIPAA, and other standards or regulations. One of the compelling features of a community cloud is that if the regulation changes, the cloud provider only has to update the infrastructure or practices once, and all users will instantly benefit.

5. Are there standards bodies that are working on a common set of security-related standards for cloud services?

There are more than 78 industry groups working on cloud-related standards, and more than 48 of them claim to have a security-related piece. For example, the Storage Network Industry Association (SNIA) is working on security standards related to data and storage management. The National Institute of Standards and Technology (NIST), an influential government standards body in the US, has a few special cloud working groups and publications, but nothing definitive yet. Of these different groups, Forrester believes that the Cloud Security Alliance (CSA) is the most comprehensive to date because it takes a more holistic view of cloud security. In addition, CSA has the widest participation from users as well as cloud vendors. Security and risk professionals should participate in industry efforts such as the CSA to influence emerging standards and to make your voice heard.

Nonetheless, we don't expect to see one single cloud security standard. It's impossible to define one all-encompassing standard that will apply to different types of clouds. We might see industry-specific standards, however, or standards that emerge to govern specific types of clouds such as IaaS and SaaS.

ENDNOTES

[1] Source: Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010.

[2] Source: Enterprise And SMB Networks And Telecommunications Survey, North America And Europe, Q1, 2010.

[3] Source: Josh Bernoff and Ted Schadler, *Empowered: Unleash Your Employees, Energize Your Customers, Transform Your Business,* Harvard Business Review Press, 2010 (http://www.forrester.com/empowered).

[4] If your organization is interested in cloud computing, there are some key security and privacy, compliance, and legal issues that you need to broach with the service provider. To help with this process, we've put together a checklist of key issues and concerns. See the October 30, 2009, "Cloud Computing Checklist: How Secure Is Your Cloud?" report.

[5] Cloud computing platforms are more than just shared, multitenant infrastructures on the public Internet. There are actually three infrastructure-as-a-service cloud deployment options available to enterprises today, each with unique characteristics and economics that can help optimize application and service deployment objectives. See the April 13, 2009, "Which Cloud Computing Platform Is Right For You?" report.

[6] Cloud computing allows organizations to save money and increase flexibility by using shared IT resources, such as applications, storage devices, and servers. The DoD wants to tap into those benefits. Source: "Head in the Clouds: DoD Turns to Cloud Computing," *Defense Industry Daily,* May 25, 2010 (http://www.defenseindustrydaily.com/defense-cloud-computing-06387/).