CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

The Upside and Downside of Security in the Cloud

Key Message: When considering cloud services, business leaders need to weigh the economic benefits against the security and privacy risks.

Executive Summary

Using cloud computing services (Infrastructure- , Platform- , and Software as a Service) can be very enticing given the potential cost savings. Business leaders need to make sure they (1) evaluate the benefits of these savings against security and privacy risks that can arise when co-mingling their data with other, unknown organizations; (2) demonstrate that they meet their compliance requirements; and (3) attempt to hold providers accountable.

In this podcast, Tim Mather, Vice President and Chief Security Strategist for RSA Security Conference, describes what cloud computing is and highlights some of the risks and opportunities it presents when it comes to security and privacy.

PART 1: CLOUD SERVICES; SECURITY RISKS

Traction for Cloud Computing

Cloud computing is gaining momentum as companies are lured by promises of significant cost savings. In the current economy, anything that will drive costs down is very attractive.

What Is Cloud Computing Exactly?

Cloud computing includes 3 services:

- Infrastructure as a Service (IaaS): Amazon web services and storage in the cloud are prominent examples. IaaS provides all infrastructure services including networks and servers. You provide your own applications. Using IaaS allows you to turn capital expenditures into operational expenditures.
- Platform as a Service (Paas): This involves renting a third-party application that has been developed on an open platform by one of the cloud service providers. Google’s app engine and salesforce.com are two prominent examples.
- Software as a Service (Saas): This involves renting a specific application such as salesforce.com. The underlying platform and infrastructure are provided as part of SaaS.

There are also management services that aid in facilitating the three types of services described above.

SaaS, in particular, can be accessed fairly seamlessly, as though the service was provided internally.

Security: The Number One Concern

Security is the number one concern of IT professionals and business unit executives when using cloud computing.

Distinguishing Public Clouds and Private Clouds

A private cloud infrastructure, which can be provided by both internal and external providers, is dedicated to a specific organization. In other words, your operational services and applications are not mixed in with those of other organizations.

Most references to cloud computing refer to public clouds where services are shared by many organizations. This is where the cost savings accrue as well as where the security concerns arise.

Co-mingled Resources

Of course, with sharing comes the potential of co-mingling your data with customers and competitors, and the possibility of inappropriate access and sharing of this data.

This raises the following questions:

- Where are the trust boundaries between organizations and how are they enforced?
- What is under your control vs. the control of a third party?
- What is the third party doing with your assets? Do you trust them to do what they say they will (and won't)?
- What assurance do you and your auditors have that security measures are being carried out?

This likely requires a redefinition of traditional controls as well as determining who's responsible for controls and what assurance means with respect to controls.

Security Incidents in the Cloud

At least two cases of security incidents involving cloud service providers and their customers have been publicly reported:

- The Washington Post reported that customers of Amazon Web Services had been attacked by other customers with malicious intent beyond spam.
- Some customers of Google Apps were subject to inappropriate sharing of their information.

PART 2: TO CLOUD OR NOT TO CLOUD

Implications for Legal, Audit, Security, and Privacy Compliance

Cloud service users need to consider how using such services affects their ability to meet their compliance requirements.

One example is Amazon Web Services. Their web site implies that these services are "HIPAA-compliant." But this is not totally accurate; the users of the service need to take action to meet HIPAA requirements. Any provider of IaaS has this issue.

The lesson is that cloud service users and owners of data retain the responsibility for ensuring that they are compliant when using these services.

Jim Dempsey of The Center of Democracy and Technology reports the loss of fourth amendment protection for US entities that use cloud services. Legal orders for data need not be served on the data owner and can be served on the cloud service provider.

As a result, data owners may not be aware that their data has been provided to a government agency or court.

There are currently no audit frameworks specific to cloud computing. Some are using a SAS 70 Type 2 audit but the applicability of this method for cloud computing is questionable.

Making an Informed Decision

Leaders considering the use of cloud services need to ask if the data that they are thinking of putting into the cloud is sensitive or regulated. If the answer is no, they can go ahead and explore the range of services.

Most leaders do not believe that the protection of sensitive or regulated data in the cloud will stand up to an audit.

Most large organizations find that the security capabilities of cloud providers are not sufficient to meet the requirements of their information security programs.

That said, many small and medium businesses (SMBs) don't have the resources of larger organizations. They may find that the security and privacy controls offered by cloud providers are better than what they currently have in house.

When making a decision to use or not use cloud services, leaders need to consider:

- the availability of resources
- staff competencies
- the involvement of sensitive or regulated vs. non-sensitive, non-regulated data
- the size and scope of the organization's security program (large enterprise vs. SMBs)

Difficult to Hold Cloud Service Providers Accountable

Most providers do not offer or use service level agreements. In addition to the points made above, leaders need to also consider these issues:

- the use of private vs. public cloud services
- the services they intend to use (IaaS, PaaS, SaaS)

The lower you are in the stack (IaaS being the lowest), the more responsible you are for security. As you move up the stack (to PaaS, then SaaS), more security controls are included with the service.

You need to have a checklist of security capabilities you are expecting before you engage with a provider.

PART 3: TEMPERING THE BUSINESS RUSH TO "JUST USE IT"

Who Is Involved?

Business unit leaders tend to be first to suggest cloud services due to the anticipated cost savings.

Security staff is typically playing catch-up, trying to understand what services and features are provided. The questions they tend to ask are:

- Where are the trust boundaries?
- Who is responsible for providing what?
- What is the level of assurance we can expect?
- What audit logs and audit results can we rely upon?
- How do we know if the provider is doing what they say they are?

Security and privacy staff are often involved in the decision surrounding the use of cloud services, based on CIO involvement and concerns about data security.

While availability and service and infrastructure interoperability may be higher priorities, security is on the list.

Resources

Open Security Architecture

Cloud Security Alliance

Tim Mather and Eric Olden podcasts: Extending Security from the Enterprise across the Cloud. May 2009.

Condon, Stephanie. “FTC questions cloud-computing security.” cnet.news, March 17, 2009.

Condon, Stephanie. “Experts: Federal policies could make, break cloud computing.” cnet.news, March 20, 2009.

Golden, Bernard. “The Case Against Cloud Computing.” CIO.com. Five parts from January 2009 through March 2009.

Jackson, Kevin. “Cloud Computing in the Obama Administration.” Web2.0 Journal, March 4, 2009.

Twentyman, Jessica. “Security Concerns for Cloud Computing.” ComputerWeekly.com, 27 March 2009.