



# DISRUPTIVE INNOVATION AND SECURITY IMPLICATIONS OF CLOUD COMPUTING

---

MULTIMEDIA USER BRIEFING  
February 2009

Chris Hoff  
*IANS Faculty*

**Chris Hoff**  
*IANS Faculty*

Christopher Hoff has over 15 years of experience in network and information security architecture, engineering, and operations. Hoff's expertise is focused on developing strategies for innovation and solving problems in the area of information assurance, rational risk management, virtualization and cloud computing security.

He is presently chief security architect for a global integrator, previously served as Crossbeam Systems' chief security strategist and was CISO and Director of Enterprise Security Services for a \$25 Billion financial services firm. Hoff has founded two startups and served as CTO of a national security consulting company that provided services to Fortune 500 and service provider customers globally.

**Context**

Chris Hoff provided a definition for cloud computing, laid out a taxonomy for it, discussed the security benefits and challenges, and offered suggestions for how information security professionals and organizations should deal with the cloud.

**Quick Read**

- The definition of cloud computing includes abstraction of infrastructure, resource democratization, services oriented, elasticity of use, and a utility model.
- Cloud computing is not one thing. It encompasses infrastructure, platform, and software as a service, each of which have multiple layers.
- A visual taxonomy of cloud computing is helpful in illustrating the layers and pieces of services available in the cloud.
- There are many similarities between cloud computing and virtualization.
- Ironically, most organizations haven't fully addressed problems associated with virtualization, where they have control. Yet they are rushing into cloud computing where they have less control.
- Security is the #1 challenge seen related to cloud computing.
- The main security concerns include confidentiality, privacy, trust, identity, reliability compliance, interoperability, and visibility.
- The good news: since security is seen as such a major issue, it is getting much attention. This attention is resulting in security-related benefits such as greater segmentation and better logging.
- The steps that practitioners should take to decrease the security risks associated with cloud computing are common sense. Practitioners should do a gap analysis and should focus on the basics like classification of data and assets, risk assessment, and thorough evaluation of vendors.

**Overview**

As with virtualization, organizations are flocking to cloud computing for the allure of lower costs. Instead of investing to purchase infrastructure and software, organizations are attracted by the idea of getting infrastructure, platforms, and software as a "pay per use" service.

But along with lower fixed costs, use of cloud computing brings with it a loss of control and an exposure to various risks, particularly security risks. Practitioners are advised to:

- Understand exactly what cloud computing means, which includes understanding the taxonomy and layers.
- Assess where cloud computing might make sense.
- Understand the risks faced, conduct a gap analysis, and develop plans to address the risks. Often these plans entail focusing on the basics by matching the business and security requirements against the most appropriate cloud models.
- Take actions such as classifying data and assets, conducting a risk assessment, evaluating vendors, educating their organization, and participating in the evolution of cloud computing.

## Key Points

- **While the term “cloud computing” means different things to different people, the concept of cloud computing has certain key ingredients.**

These key ingredients are:

- **Abstraction of infrastructure.** Where infrastructure is separated from other resources.
- **Resource democratization.** Resources become a pool which can be combined and mashed up in various ways.
- **Services oriented.** With cloud computing, everything is a service, including software, platform, and infrastructure.
- **Elasticity/dynamism.** Use of resources in the cloud can be scaled up or down as necessary based on an organization’s needs.
- **Utility model of consumption and billing.** Users of cloud computing pay only for the services they use, as with a utility.

Some things are good candidates for using cloud computing, while other things are not.

Good Candidates for the Cloud*	Not a Good Fit for the Cloud*
<ul style="list-style-type: none"> <li>• When processes, applications, and data are largely independent</li> <li>• When integration points are well defined</li> <li>• When a low level of security will work</li> <li>• When the core internal enterprise architecture and processes are healthy</li> <li>• When the web is the desired platform</li> <li>• When cost is an issue</li> <li>• When the applications are new</li> </ul>	<ul style="list-style-type: none"> <li>• When processes, applications, and data are largely bound and coupled</li> <li>• When integration points are not well defined</li> <li>• When a high level of security is needed</li> <li>• When the core internal enterprise architecture needs work</li> <li>• When the applications are legacy</li> <li>• When cost is an issue</li> </ul>

\* Use with permission from David Linthicum

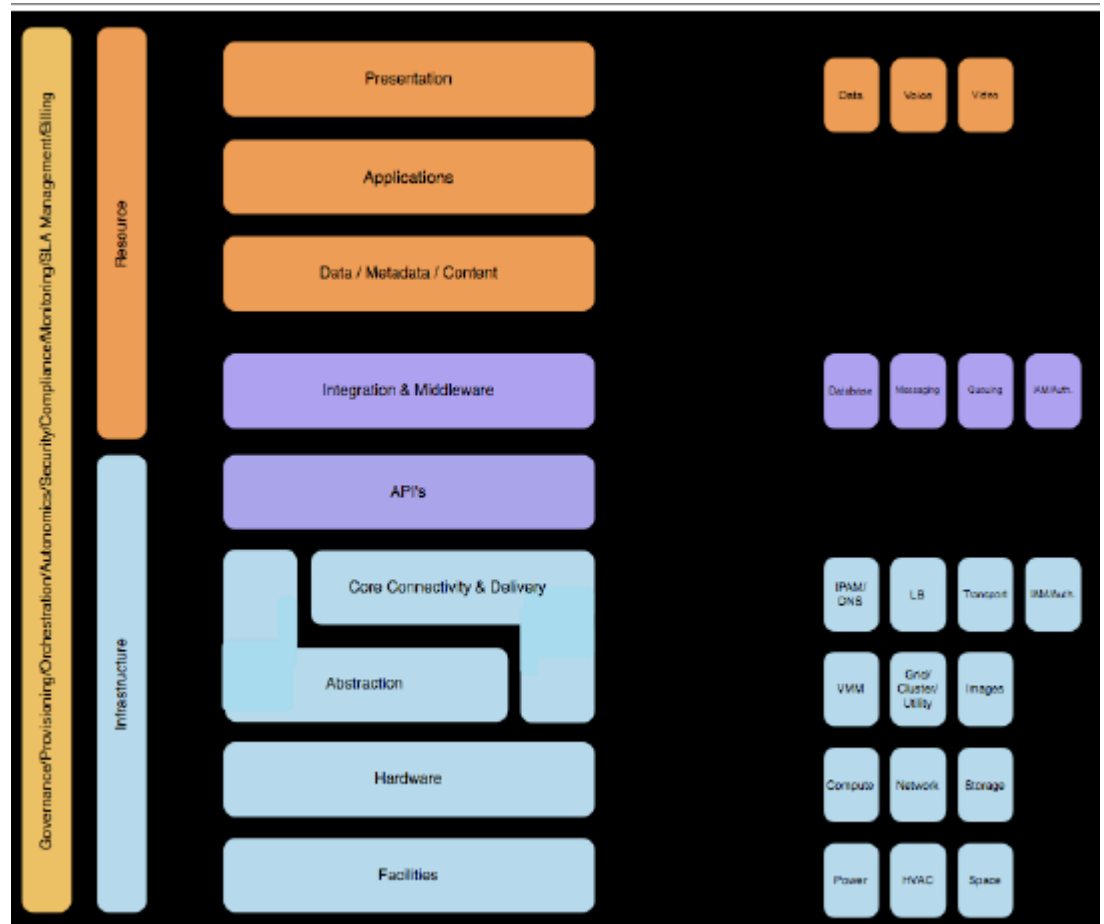
- **“The cloud” is not one thing. It is a series of layers and pieces, which can be understood through the following taxonomy.**

When people refer to “the cloud” they are typically talking about the SPI model which includes software (S), platform (P), and infrastructure (I) as service. The taxonomy below illustrates the components and layers of these services.

- **Infrastructure as a service.** This includes the physical facilities, the hardware, an abstraction layer, a core connectivity and delivery layer, and APIs. Vendors in this space include Amazon EC2, GoGrid, and FlexiScale.
- **Platform as a service.** This is the middleware that integrates the infrastructure and the resources that sit on top of it. It can include identity and access management, databases, and authentication. PaaS vendors are Force.com, Google AppEngine, and Coghead.

- **Software as a service.** This is the data and the applications. Examples of SaaS vendors are Salesforce.com, GoogleApps, and Oracle on Demand.

These different services and their many layers mean that organizations can pick and choose the different pieces of the SPI model that meet their needs.



“When a vendor says they do ‘cloud computing’ you can use this taxonomy to ask exactly what they do.”

- **There are many similarities between cloud computing and virtualization.**

Virtualization is an enabler of cloud computing, as the new de facto atomic unit of the digital infrastructure is now a virtual machine.

A reality of virtualization is that organizations have rushed to adopt it without solving many of its attendant security, privacy, and management challenges. And now, without having solved the problems associated with virtualization—problems that are within an organization’s own control—organizations are moving to the cloud, where they have even less control.

- **The rush to the cloud is raising concerns about security, but there are also many security benefits of the movement to the cloud.**

Practitioners see security as the key challenge/issue related to cloud computing. A study by IDC ranks security as the #1 issue with the cloud model, cited by 75% of survey respondents.

“What we care about [with cloud computing] is that the assets we care about are at least as well cared for outside our walls as they are inside.”

*“Abstraction of infrastructure is really driving the need for information centricity.”*

Ultimately, what security practitioners want is to ensure that the assets they care about are at least as well cared for outside their walls as they are inside (which in many instances isn't saying much).

The security problems that organizations face related to cloud computing are the same as those related to virtualization—but even more so. The abstraction of infrastructure points to the need for information centricity.

Among the key security concerns related to cloud computing are:

- **Confidentiality and segregation.** This is a concern anytime there is a shared infrastructure and is particularly a concern in the cloud.
- **Privacy.**
- **Trust.**
- **Identity.**
- **Compliance.**
- **Portability and interoperability.** There are issues and complexities associated with moving and sharing data.
- **Reliability and resiliency.** An organization loses control and is vulnerable if a vendor lacks resiliency and goes down.
- **Visibility and manageability.**

The significant focus on cloud computing is actually garnering attention for security. Enterprise architects and other really smart people are beginning to talk about security in ways they have never done before. Some of the security benefits that are coming from the adoption of cloud computing and the related focus on security include:

- **Centralized data.**
- **Greater segmentation of data/applications.** This makes an organization more “cloud ready.”
- **Better logging and accountability.**
- **Standardized images for asset deployment.**
- **Better resilience to attack and streamlined incident response.**
- **Earlier testing.**
- **More streamlined audit and compliance.**
- **Better visibility to process.**
- **Faster deployment.**
- **Innovative solutions.**

*“There are quite a few security benefits of moving to the cloud.”*

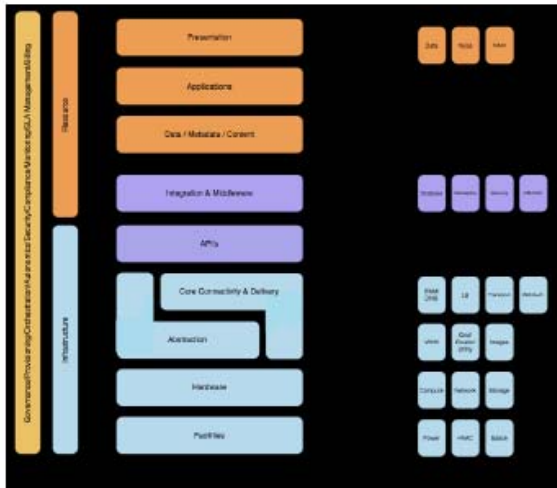
- **The steps that security practitioners should take to decrease the risks associated with cloud computing are common sense.**

*“In dealing with the cloud, it's back to common sense . . . you already have most of what you need.”*

Practitioners already have most of what is needed to make an informed set of decisions about cloud computing. The challenge is to match the organization's business and security requirements against the various cloud “service” (aaS) models. Among the requirements: not being a speed bump to the business and achieving and maintaining compliance.

Step that practitioners should engage in include conducting a cloud computing risk assessment and a gap analysis. An organization can assess security for each layer in the cloud and can identify any shortcomings. The visual below shows the types of security that can/should be in place for each layer of the cloud.

### Cloud Taxonomy



### Security Taxonomy

<b>Applications</b>	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Security
<b>Information</b>	DLP, CMF, DAM, Encryption
<b>Management</b>	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
<b>Network</b>	NIDS, NIPS, Firewalls, DPI, Anti-DDoS, QoS
<b>Storage</b>	Encryption, Masking
<b>Compute</b>	Firewalls, HIDS/HIPS, Integrity, File/Log Management
<b>Physical</b>	Physical Plant Security, CCTV, Guards

In addition, specific steps to provide greater security for cloud computing include:

- **Classify.** Assets and data.
- **Assess.** Conduct a risk assessment to understand what in your organization is appropriate for the cloud and what is not.
- **Evaluate.** Evaluate and interrogate potential vendors. Review their roadmap and understand critical upstream and downstream vendors.
- **Engage.** Don't ignore the cloud. It is not going away.
- **Educate.** Educate yourself and your organization on exactly what the cloud means, its layers, benefits, and risks.
- **Participate.** Be part of the evolution of the cloud. Get involved.

### Other Important Points

- **Public vs. private clouds.** People often describe a cloud as “internal or external.” This is a bad distinction. Where the cloud resides is less important than whether a cloud is public or private. This terminology isn't about where a resource is physically located; it focuses on who and from where resources can be accessed.

**Additional resources.** There are a wealth of good resources available with information on cloud computing, and multiple ways for practitioners to join in the conversation as cloud computing evolves. These resources include:

- **Cloud computing Google Groups.**
  - Cloud Computing: <http://groups.google.com/group/cloud-computing>

- Cloud computing Interoperability Forum  
<http://groups.google.com/group/cloudforum>
- Cloud Storage: <http://groups.google.com/group/cloudstorage>
- **Attend a local CloudCamp.**
- **Read Craig Balding's blog.** <http://www.cloudsecurity.org>
- **Read Chris Hoff's blog.** <http://rationalsecurity.typepad.com>

### **About IANS**

IANS is the premier membership organization for practicing information security professionals. IANS' mission is to provide key technical and business insights to help members solve their most pressing technical and professional challenges.

IANS achieves this mission through a broad offering of services—insightful events, thought-provoking publications, best-practice research, and unique networking opportunities.

IANS is committed to providing its members with unbiased, relevant insights to increase their productivity and effectiveness as emerging technical leaders in their organizations.