cloud security alliance SM

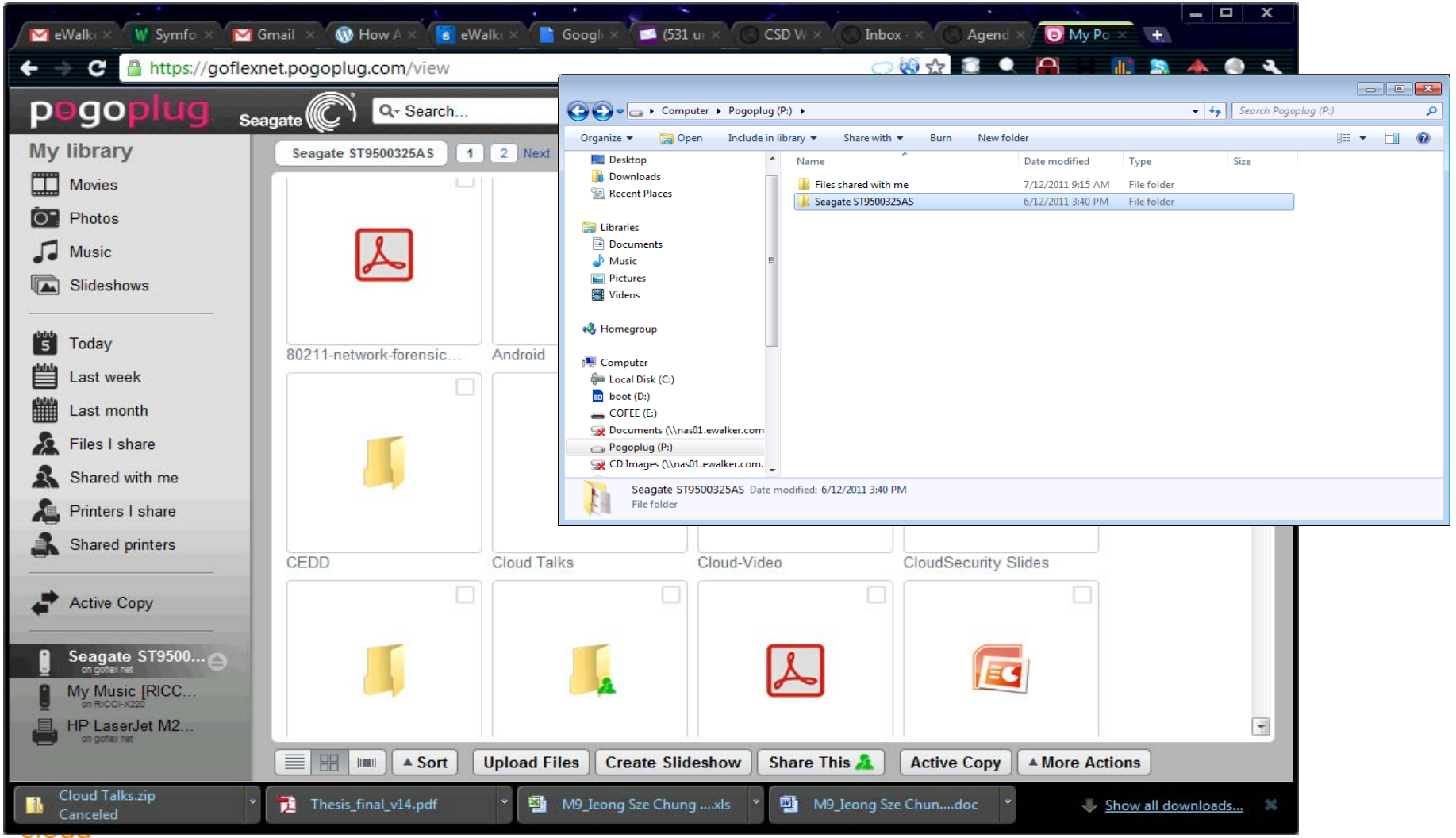
Cloud Security – considerations for business adoption

Ricci IEONG
CSA-HK&M Chapter

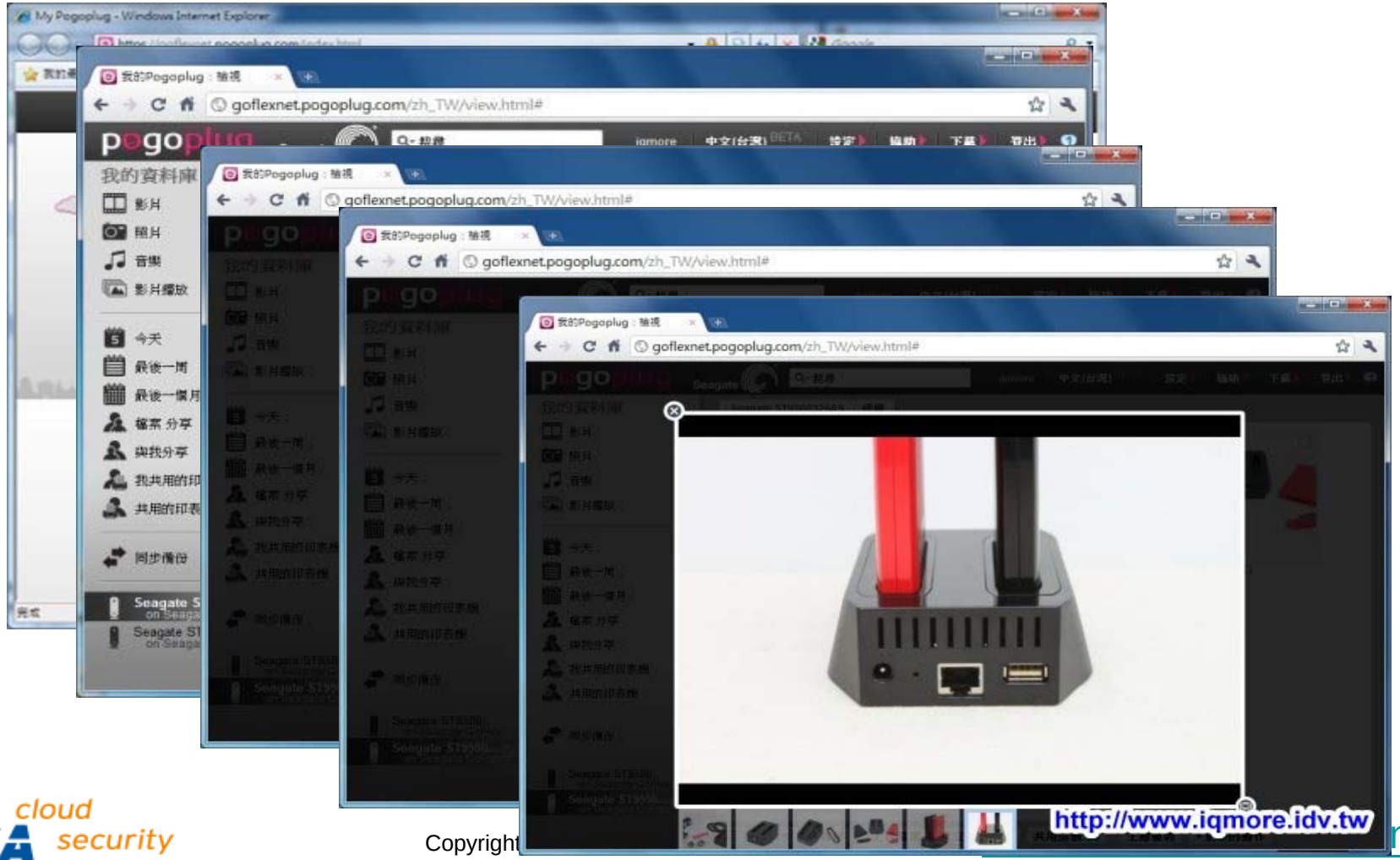
What is Cloud Computing?

What is Cloud Computing?

My Cloud @ Internet

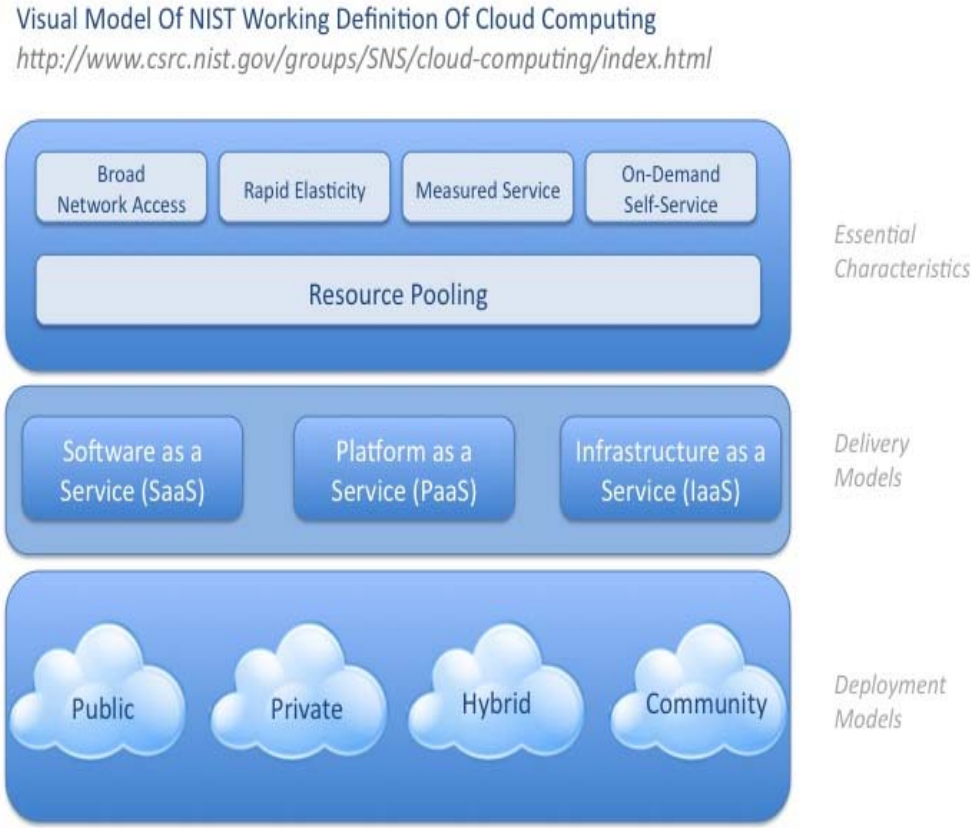


Pogoplug

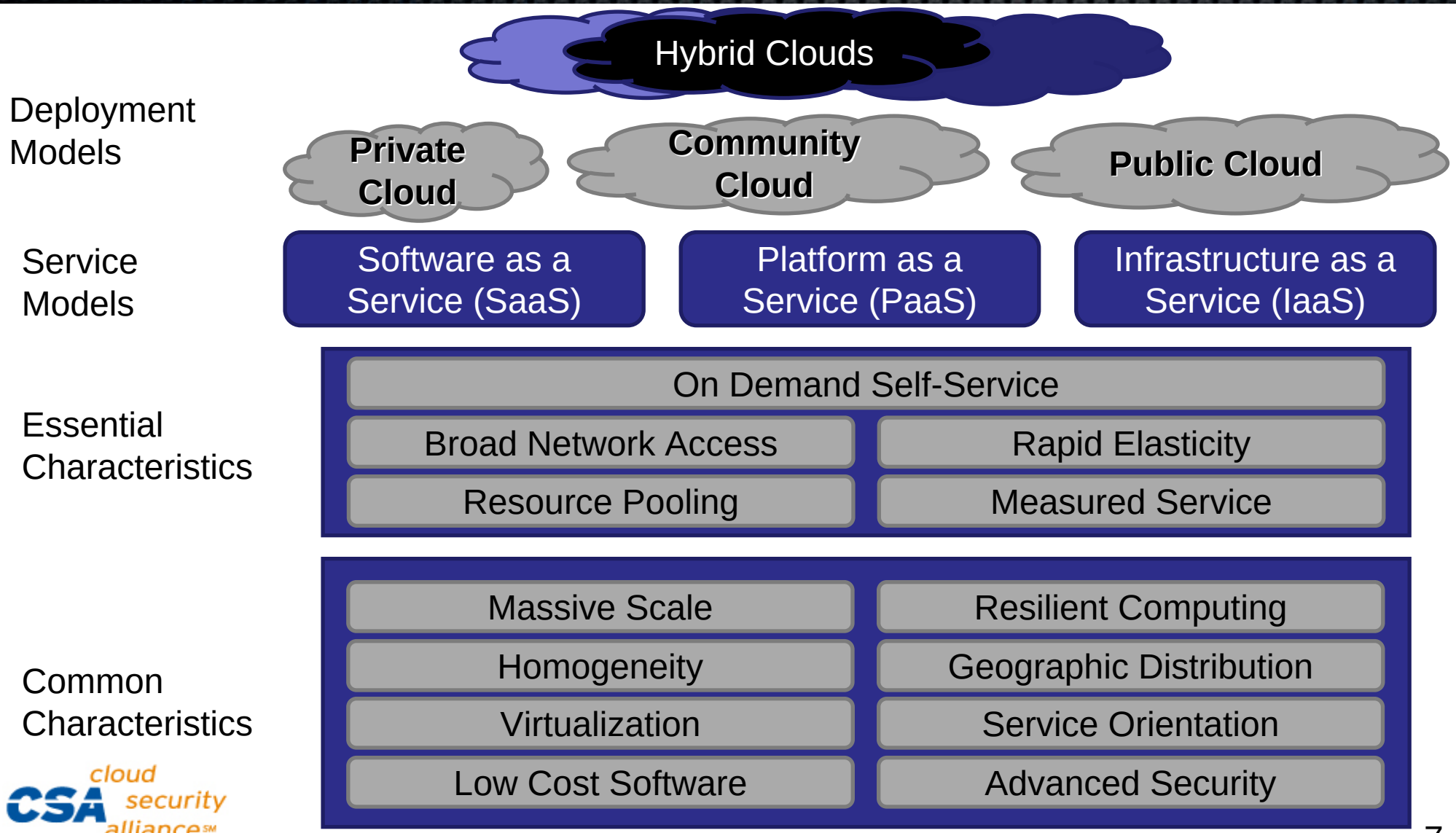


What is Cloud Computing?

- Compute as a utility: third major era of computing
- Cloud enabled by
  - Moore's Law
  - Hyperconnectivity
  - SOA
  - Provider scale
- Key characteristics
  - Elastic & on-demand
  - Multi-tenancy
  - Metered service
- IaaS may track energy costs



The NIST Cloud Definition Framework



cloud security alliance℠

Based upon original chart created by Alex Dowbor - http://ornot.wordpress.com

Cloud Business?

Cloud Business

(Process-as-a-Service)

Cloud Applications

(Apps-as-a-Service)

App Dev/Test App Deploy

Cloud (Application) Platforms

(Platform-as-a-Service)

Cloud Infrastructure

(Infrastructure-as-a-Service)

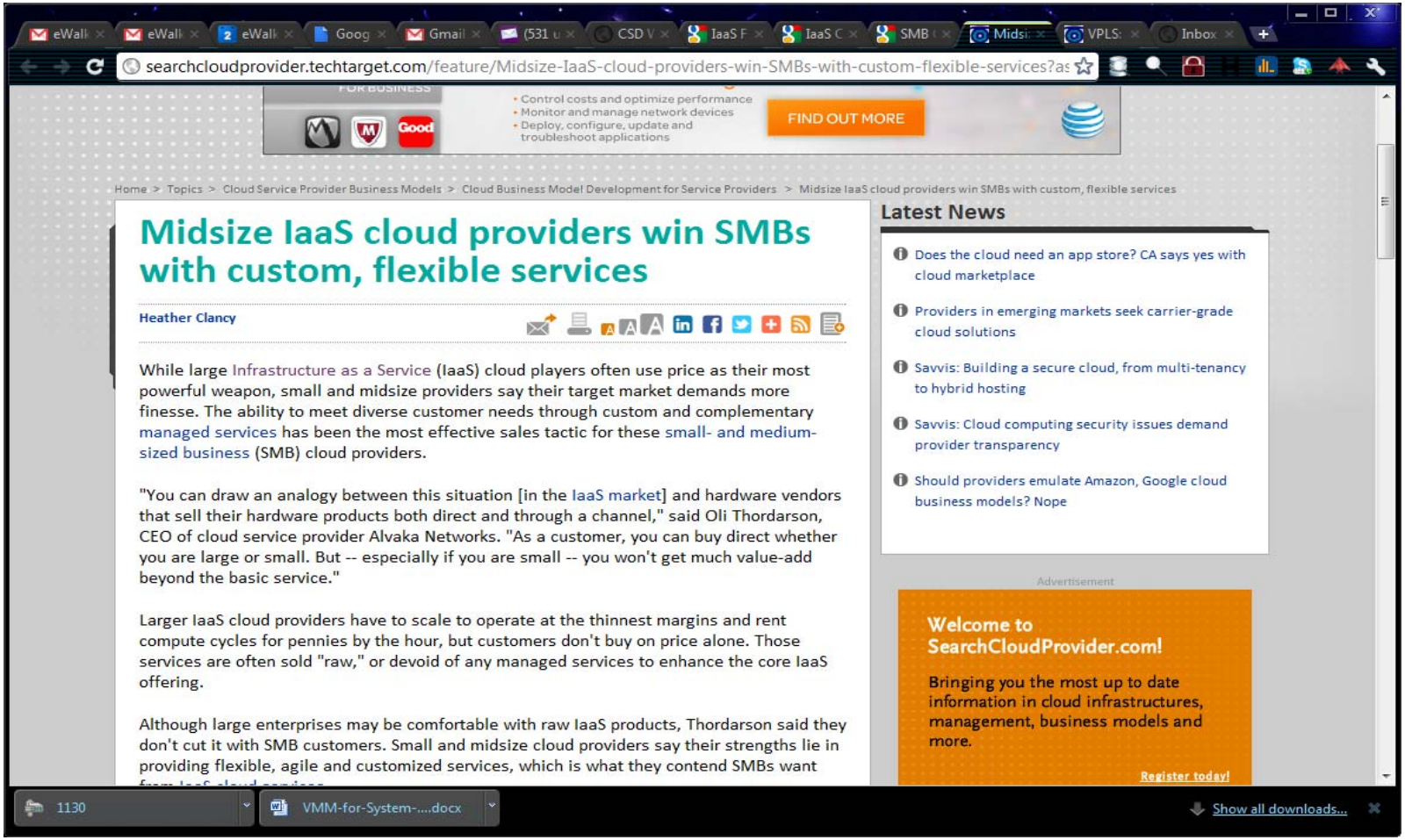
SME in the Cloud

- Growth is expected in all public cloud service segments
- In-Stat's latest market study includes the following insights:
  - SaaS (software as a service) is poised to grow 142 percent between 2010 and 2015.
  - Overall public cloud computing (IaaS, SaaS, and PaaS) is set to grow 153 percent from 2010 to 2015.
  - Small business (5 to 99 employees) is the fastest growing size segment growing from $2.5 billion by 2010 to $6.6 billion by 2015.
  - Small business account for over half of the market in SaaS and IaaS.

SME in the Cloud

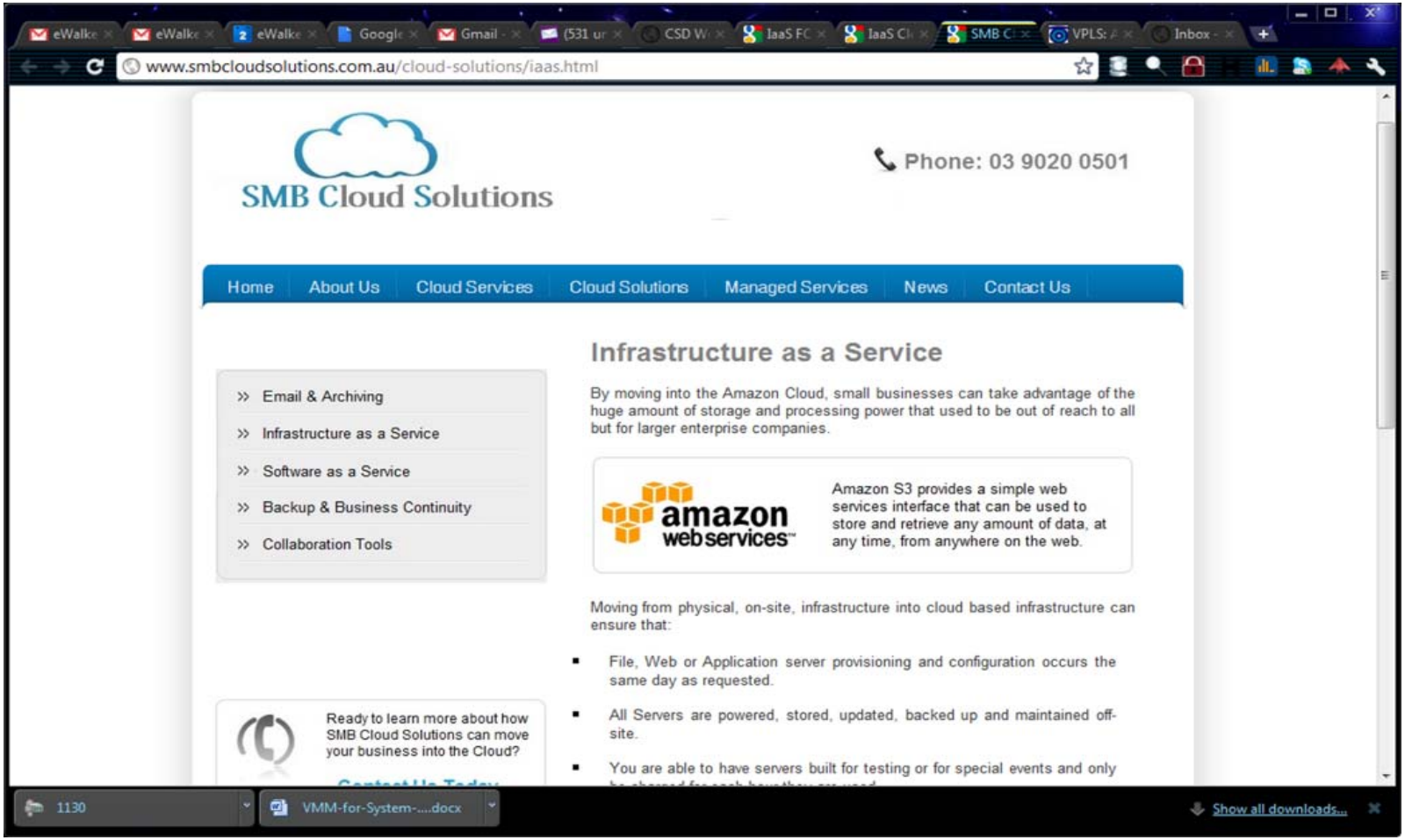
- In-Stat assessment, the top five vertical markets for IaaS offerings, in terms of 2011 market revenue,
  - Hospitality
  - Food
  - Healthcare
  - Social services
  - Retail trade

SME in the Cloud



http://searchcloudprovider.techtarget.com/feature/Midsize-IaaS-cloud-providers-win-SMBs-with-custom-flexible-services?asrc=EM_NLT_15575681&track=NL-544&ad=855887

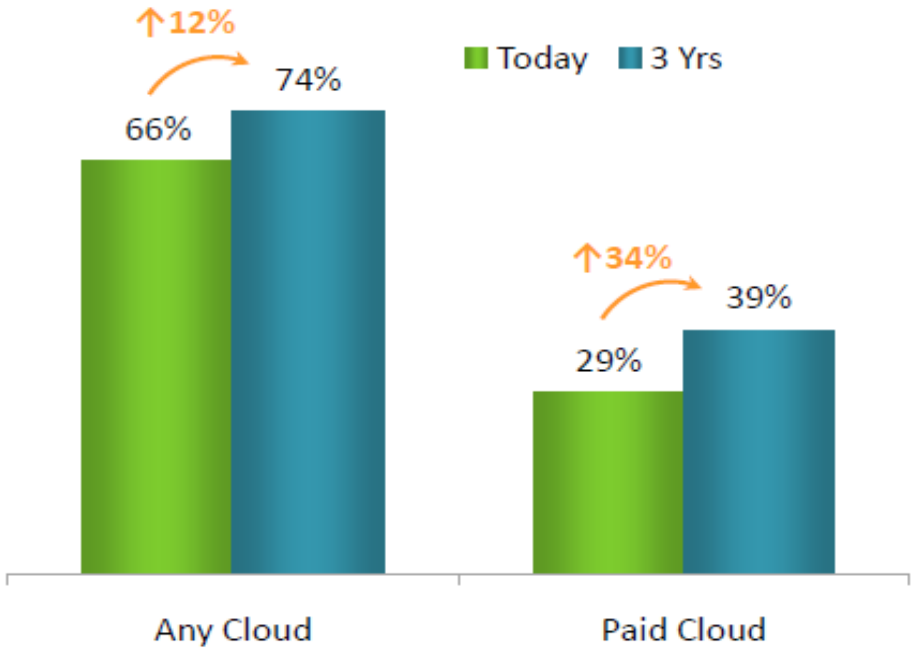
SME in the Cloud



SME Cloud Adoption Study by Microsoft 2011

Use of Cloud Services Today and Planned Use in 3 Years – Both Paid and Unpaid

All companies, N=3258



- 74% of SMBs plan to use at least one cloud service (paid or free) in 3 years
- 39% expect to be paying for cloud services

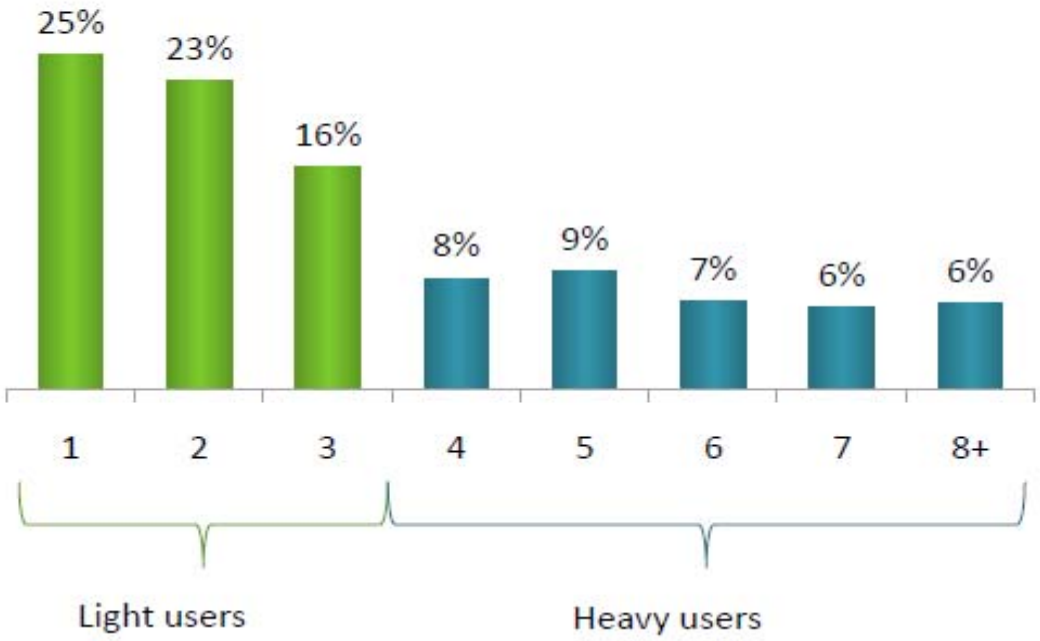
	Number of employees		
	2-10 *N=1180*	11-50 *N=1033*	51-250 *N=1045*
Any cloud, 3yrs	73% (↑12%)	78% (↑13%)	81% (↑13%)
Paid cloud, 3yrs	37% (↑38%)	45% (↑25%)	56% (↑27%)

www.cloudsecurityalliance.org

SME Cloud Adoption Study by Microsoft 2011

Number of paid services to be used

Companies planning to use at least paid app, N=1519

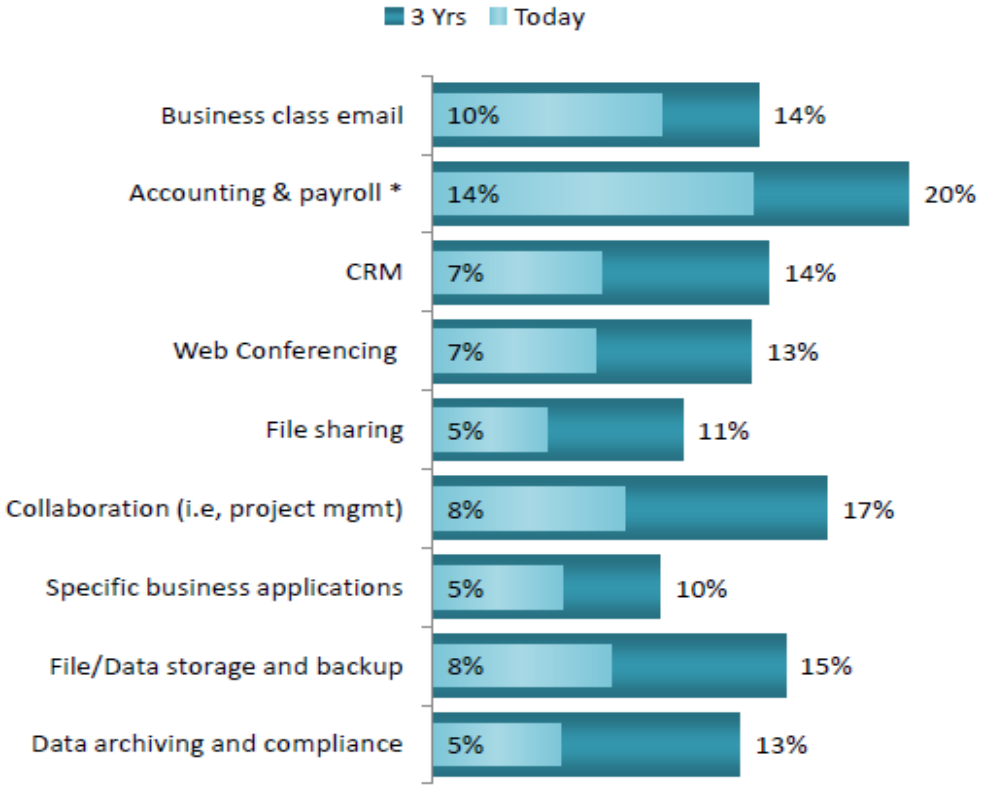


Mean number of paid services that will be used	
All companies *(N=1519)*	3.3
2-10 emp *(N=416)*	3.3
11-50 emp *(N=492)*	3.5
51-250 emp *(N=610)*	3.7

SME Cloud Adoption Study by Microsoft 2011

Workloads Addressed by Paid Cloud Services today and in 3yrs

All companies, N=3258



Number of employees (Today → 3 yrs.)

2-10 *N=1180*	11-50 *N=1033*	51-250 *N=1045*
9% → 13%	12% → 16%	15% → 21%
12% → 18%	18% → 25%	24% → 32%
6% → 13%	11% → 17%	15% → 24%
6% → 13%	8% → 15%	11% → 20%
4% → 10%	7% → 13%	11% → 20%
7% → 16%	11% → 18%	18% → 29%
6% → 9%	5% → 11%	7% → 13%
7% → 14%	10% → 18%	12% → 24%
4% → 12%	11% → 17%	11% → 22%

** Reflects companies using hosted service for Payroll*

cloud security alliance℠

www.cloudsecurityalliance.org

Benefit (extracted from AWS)

- Moving from physical, on-site, infrastructure into cloud based infrastructure can ensure that:
  - File, Web or Application server provisioning and configuration occurs the same day as requested.
  - All Servers are powered, stored, updated, backed up and maintained off-site.
  - You are able to have servers built for testing or for special events and only be charged for each hour they are used.
  - Compute and storage capacity ranging from Enterprise class to micro-instances.
  - Enterprise class, Virtual Server technology can grant 99.9% server uptime.
  - Virtual server instances can be accessed from anywhere at any time via Windows RDP or client end remote applications.

Other Benefits

appica.com/archives/tag/iaas-cloud-security

3 Reasons Server Administrators sleep better in the cloud.

Tuesday, September 13th, 2011

In the two years I've been reading, selling and writing about cloud virtualization, one of the concerns I always hear is that virtualization will devore the need for server administrators.

At Profitability.Net we see completely the opposite! Over the last 18 months, we have seen an incredible increase in the need for talented server administrators.

Now don't get me wrong, the days of only understanding the server operating system are gone. A talented server administrator must be proficient in all the hypervisors on the market as well as Windows and Linux operating systems. An IT Professional that has a solid understanding of mission critical applications like, management and monitoring software, ERP, CRM and BI will set themselves apart from the competition too.

So rest easy my server hugging friends, the need for quality server administrators is going to explode!

Here are 3 great reasons server administrators will be in high demand in the coming years;

1. Virtual servers are steadily increasing. In fact, 57% of companies are currently using some form of virtualization. So instead of managing 15-20 physical servers, it is feasible to manage serveral 100.
2. Having a virtualized environment gives great flexibility.The ability to monitor and put safeguards in place such as HA , allows IT professionals to focus on projects and moving their company forward.
3. Specialization. In today's world the application is king, gone are the days of the need for just file & print, mail and web servers. Now we see virtual private, public cloud, grid, cluster, blade, database, media, private cloud and energy efficient servers in our data center. Specialize in an area and develop much needed expertise.

In contrast to the past when IT was viewed as a "cost" of doing business, most IT leaders find themselves managing departments that are strategically planning the future of the company. When CIO's are building

1130 VMM-for-System-....docx Show all downloads...

One comprehensive solution for business

http://www.winweb.com/winweb-business-cloud-framework/

Comparison of various service model for SME

Service Model	Benefit	Applicability
SaaS	• Securer than in-house • Less expensive • Low development cost • Short development time • Easy operation • Scalable	H
Public cloud PaaS/IaaS	• Specific use • Less expensive • Short deployment time • Easy operation	M
Community Cloud	• Advantage of SaaS • Safe and Secure • Flexible	H
Private Cloud PaaS/IaaS	• No advantage in cost	L
Proprietary System/Mission Specific	• Original model	NA

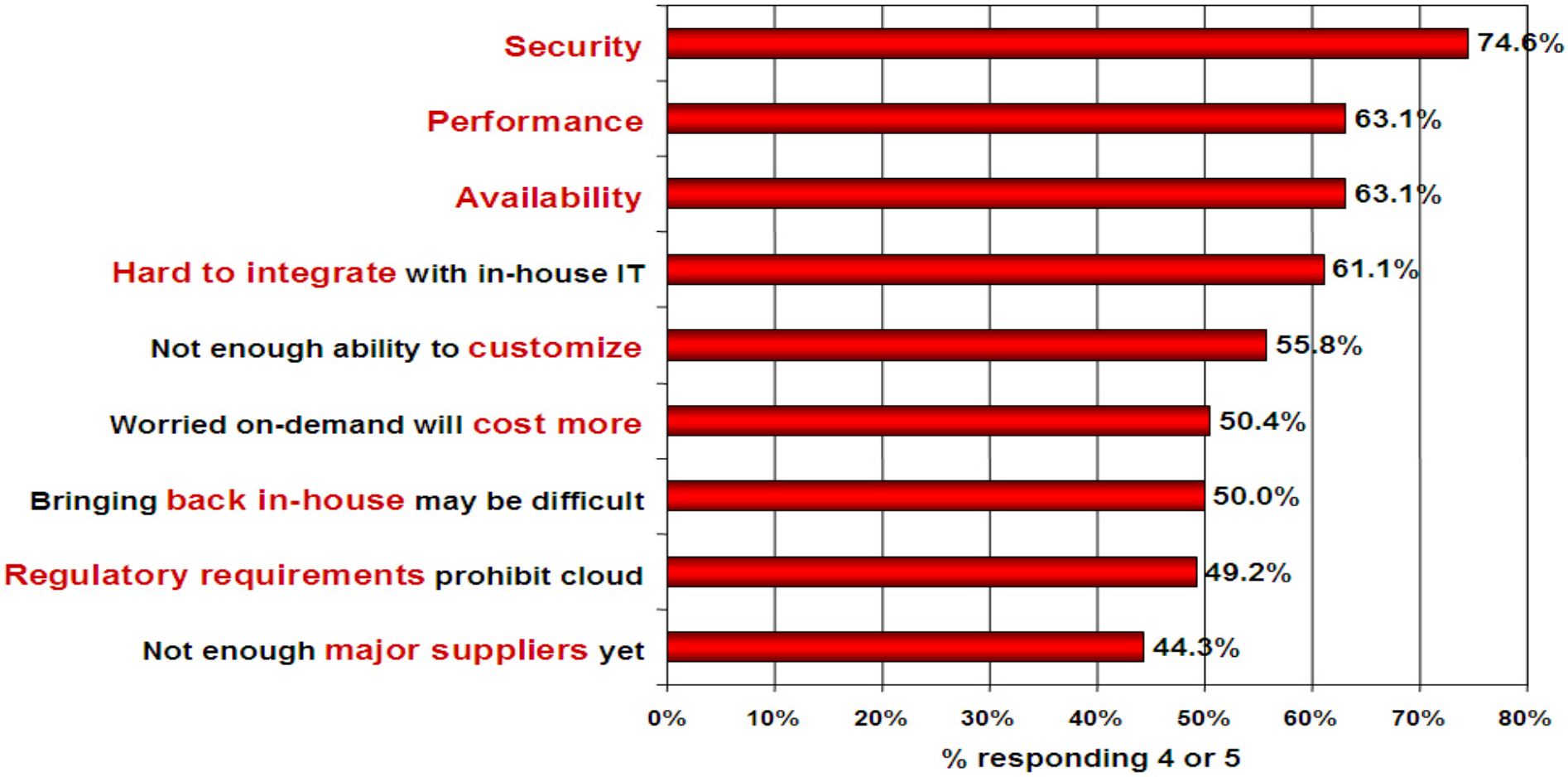
From IPA “SaaS and Cloud: Where applicable/suitable?” 16/03/2010

Dark side of using Cloud

Security is the Major Issue

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

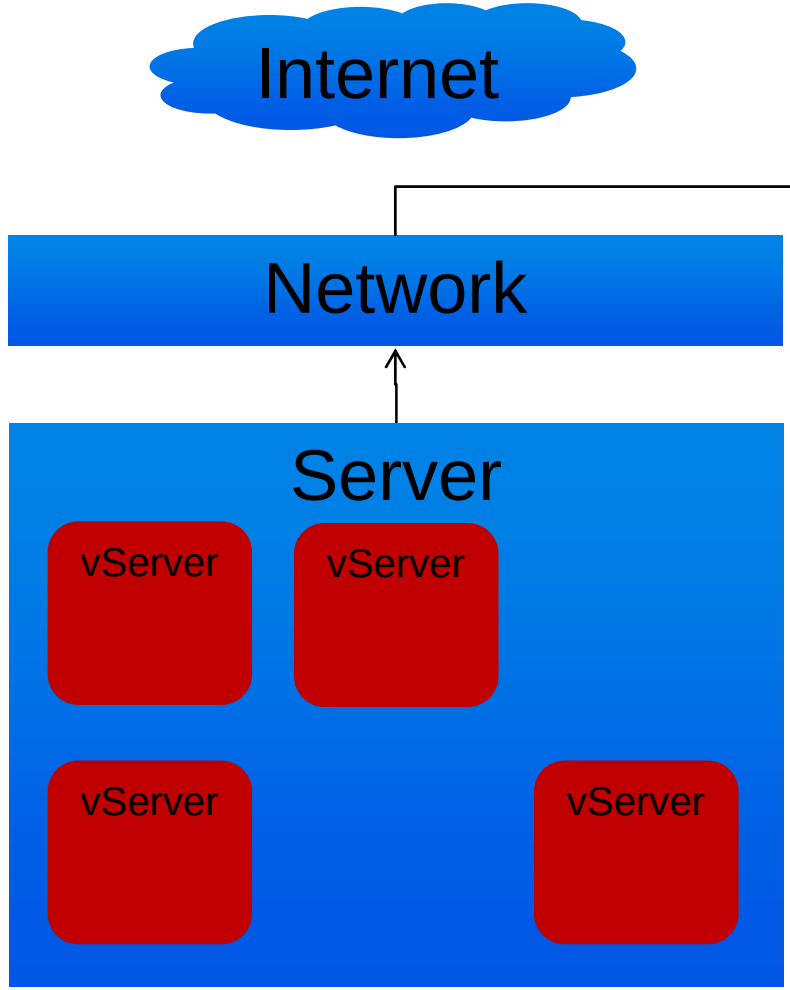
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

alliance℠

Cloud = 劏房??



Issue in Cloud = Issue in 劏房

Amazon

Zeus crimeware using Amazon's EC2 as command and control server

By Dancho Danchev | December 9, 2009, 8:13am PST

Summary

A recently intercepted variant of the most popular piece of crime, the Zeus bot, is using Amazon's EC2 service as a command and control server.

Topics

Amazon.com Inc., Social Networking, Cloud Computing, Network Technology, Security, Networking, Dancho Danchev

Blogger Info

Action	URL	Details
GET	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/config.bin	svchost.exe
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe

UPDATED: ScanSafe posted an update stating that "*In the past three years, ScanSafe has recorded 80 unique malware incidents involving amazonaws, 45 of which were in 2009, 13 in 2008, and 22 in 2007.*"

Security researchers have intercepted a new variant of the Zeus crimeware, which is using Amazon's EC2 services for command and control purposes of the botnet. The cybercriminals appear to be using Amazon's RDS managed database hosting service as a backend alternative in case they loose access to the original domain, which would result in the complete loss of access to the compromised financial data obtained from the infected hosts.

Would 2010 be the year when crimeware will dive deep into the cloud, in an attempt to undermine the security industry's take down operations?

Amazon

Spammers on Amazon EC2 starting to hammer Asterisk (VoIP) servers

April 13th, 2010 Posted in Uncategorized

Google

- Sep 2010:
- Google Engine
- Case

Google Engineer Allegedly Fired For Accessing Private User Information To Stalk Teens

Adrian Chen, Gawker | Sep. 14, 2010, 4:19 PM | 5,587 | 17

Recommend 134 Share Tweet 113 +1 0 Email A A A

We entrust Google with our most private communications because we assume the company takes every precaution to safeguard our data. It doesn't. A Google engineer spied on four underage teens for months before the company was notified of the abuses.

David Barksdale, a 27-year-old former Google engineer, repeatedly took advantage of his position as a member of an elite technical group at the company to access users' accounts, violating the privacy of at least four minors during his employment, we've learned. Barksdale met the kids through a technology group in the Seattle area while working as a Site Reliability Engineer at Google's Kirkland, Wash. office. He was fired in July 2010 after his actions were reported to the company.

It's unclear how widespread Barksdale's abuses were, but in at

Image: commons.wikimedia.org

GAWKER

- Egypt Fires Its Most Famous Government Huckster [Foreign Affairs]
- Here's the Outrageous Suicide Attempt Scene from ABC Family's Cyberbully [Video]
- A Week of Cooking Meth Can Make You Crazy Bored

DropBox

Dropbox Security Bug Made Passwords Optional For Four Hours

JASON KINCAID | Monday, June 20th, 2011 | 36 Comments

This morning a post on **Pastebin** outlined a serious security issue that was spotted at Dropbox: for a brief period of time, the service allowed users to log into accounts using any password. In other words, you could log into someone's account simply by typing in their email address. Given that many people entrust Dropbox with important data (one of the service's selling points is its security), that's a really big deal.

We've now confirmed with Dropbox that the service did have this issue yesterday — Dropbox says that it began after a code push at 1:54 PM PDT and was fixed at 5:46 PM PDT (they had the fix live five minutes after they discovered it). So, in total, the bug was live for around four hours.

The question now is how many people were affected. The company will be announcing that "much less than 1 percent" of users logged in during this time, and that all sessions have now been logged out as a security precaution. The team is now investigating if any accounts were improperly accessed, and says that anyone who was impacted will be notified.

Update: Here's the company's **blog post**, which just went live:

Security Considerations

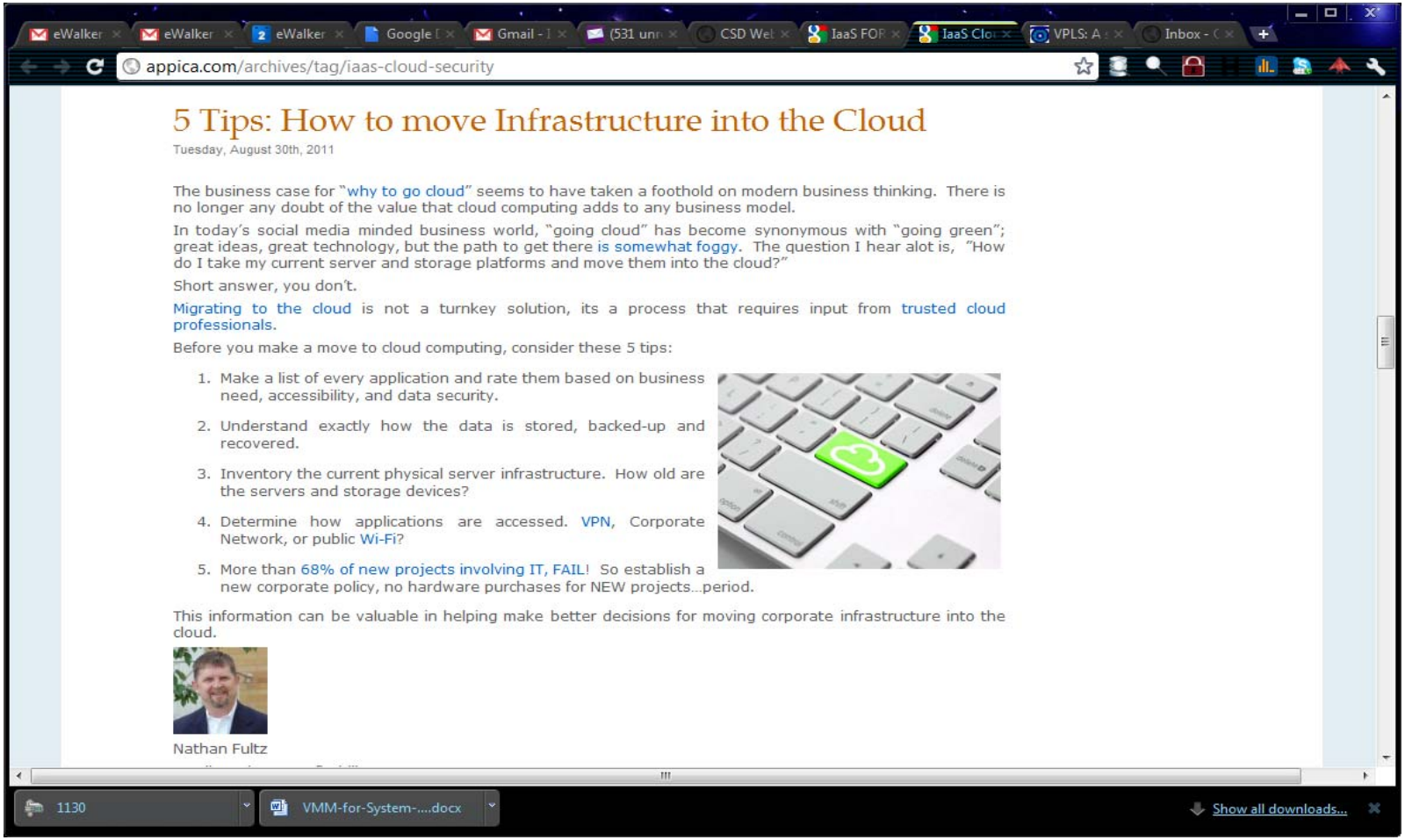
Cloud Security Challenges

- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees

Cloud Security Challenges

- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest
- Public cloud vs internal cloud security
- Lack of public SaaS version control

How to move forward



appica.com/archives/tag/iaas-cloud-security

5 Tips: How to move Infrastructure into the Cloud

Tuesday, August 30th, 2011

The business case for "why to go cloud" seems to have taken a foothold on modern business thinking. There is no longer any doubt of the value that cloud computing adds to any business model.

In today's social media minded business world, "going cloud" has become synonymous with "going green"; great ideas, great technology, but the path to get there is somewhat foggy. The question I hear alot is, "How do I take my current server and storage platforms and move them into the cloud?"

Short answer, you don't.

Migrating to the cloud is not a turnkey solution, its a process that requires input from trusted cloud professionals.

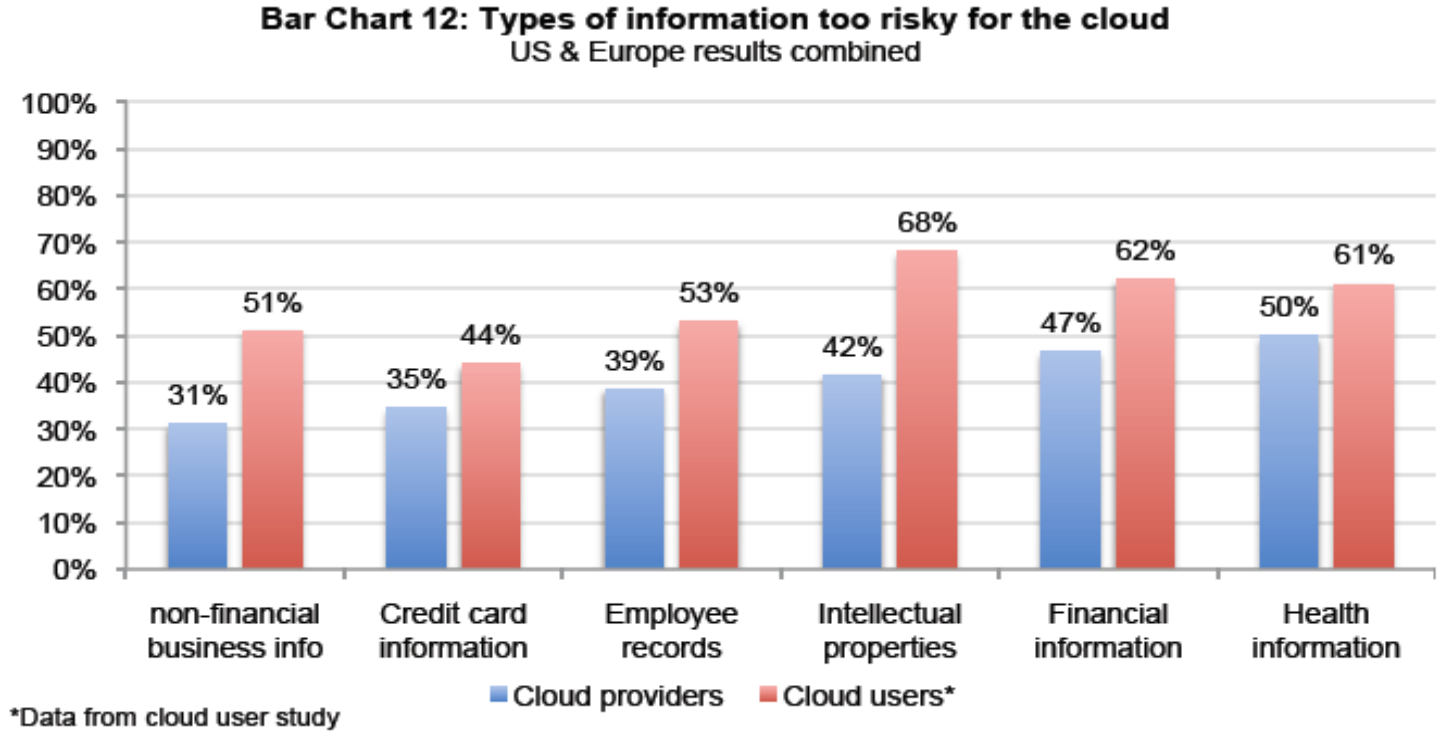
Before you make a move to cloud computing, consider these 5 tips:

1. Make a list of every application and rate them based on business need, accessibility, and data security.
2. Understand exactly how the data is stored, backed-up and recovered.
3. Inventory the current physical server infrastructure. How old are the servers and storage devices?
4. Determine how applications are accessed. VPN, Corporate Network, or public Wi-Fi?
5. More than 68% of new projects involving IT, FAIL! So establish a new corporate policy, no hardware purchases for NEW projects...period.

This information can be valuable in helping make better decisions for moving corporate infrastructure into the cloud.

Nathan Fultz

What Information are Too Risky for Cloud?



Source: Security of Cloud Computing Providers Study, Ponemon Institute

Self-assessment questions

- Evaluate what is critical to business?
- What's the purpose of cloud service?
- How to prepare for data protection?
- How to continuous monitor the incident?
- How to preserve evidence if any incident happened?

Security Checklists (Part 1)

Items	Criteria	Security requirement
Data Protection	• Data sensitivity (Confidentiality, Integrity & Availability) and privacy	• Make sure no company sensitive and no personal privacy related data are kept open in public cloud
	• Data ownership and data source	• SME is still the owner of the data • At least a backup copy of data should be kept locally by SME
	• Location of data	• Where will the cloud be? Is the data sensitive to different location?

Security Checklists (Part 2)

Items	Criteria	Security requirement
User Access Control	• Administration account?	• Administrator account and password should be securely kept • Only access to admin account from a restricted location. • Only admin account can upload information
	• Developer account?	• Normal user account • Cannot upload
	• User accounts?	• Enforce proper user account mgt scheme • Disable/suspend idle user account
	• Access management?	• Allow user with proper access to the accounts
	• Password management?	• Change password at least every 90 days • Use at least 8 character password

Security Checklists (Part 3)

Items	Criteria	Security requirement
Other Issues	• Physical access control • Fire and other natural disaster?	• Rely on vendor control through SLA
	• Backup arrangement	• Rely on vendor control through SLA
	• Monitoring	• Rely on vendor control through SLA

How do we build the "Trusted Cloud"?

About the Cloud Security Alliance

- Global, not-for-profit organization
- Over 23,000 individual members, 100 corporate members, 50 chapters
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation
  - Advocacy of prudent public policy

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

Here's How…

- Strategy
- Education
- Security Framework
- Assessment
- Build for the Future

Strategy

- IT Architecture supporting Hybrid enterprise
  - Federated IdM
  - Service Oriented Architecture “loose coupling” principles
- Consider cloud as an option to any new IT initiative
  - What are the cost differences?
  - What are the feature/functionality differences?
  - Does the application support different cloud deployments and multiple providers?
- Risk Management
  - Sensitivity of application and data, new risks introduced by cloud, risk tolerance levels

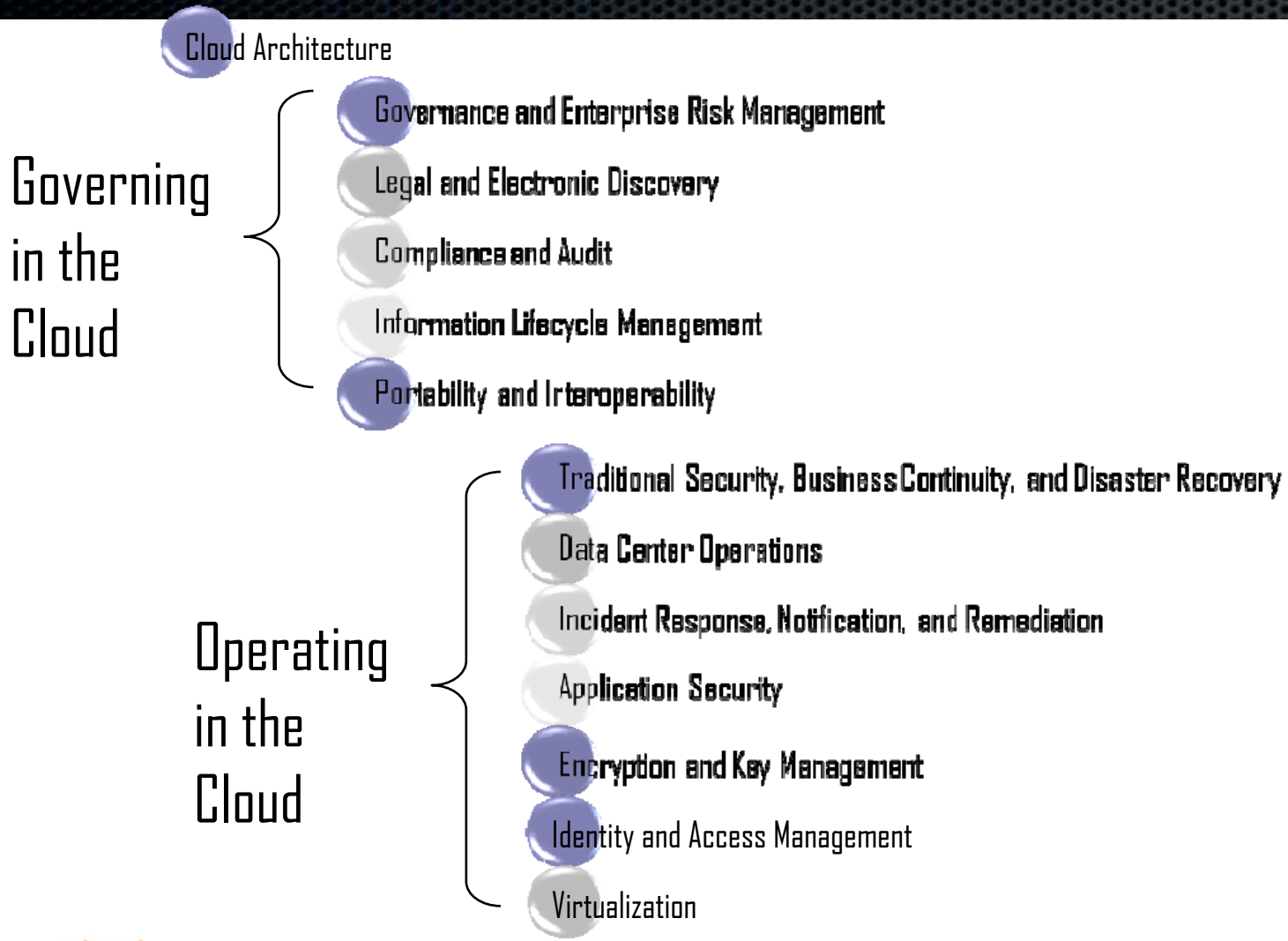
Education

CSA Guidance Research

- Popular best practices for securing cloud computing
- V2.1 released 12/2009
- V3 released 11/2011
- wiki.cloudsecurityalliance.org/guidance

Guidance > 100k downloads: cloudsecurityalliance.org/guidance

13 Domains of Concern by CSA



www.cloudsecurityalliance.org

CCSK – Certificate of Cloud Security Knowledge

- Benchmark of cloud security competency
- Measures mastery of CSA guidance and ENISA cloud risks whitepaper
- Understand cloud issues
- Look for the CCSKs at cloud providers, consulting partners
- Online web-based examination
- www.cloudsecurityalliance.org/certifyme

Training Courses

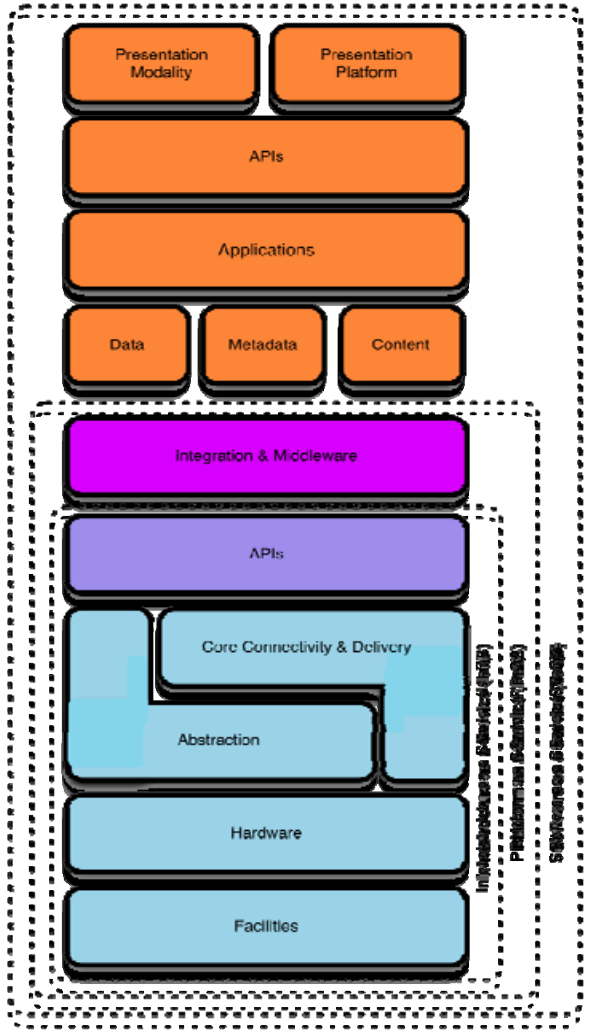
- CCSK Basic
  - One day course to enable student to pass CCSK
- CCSK Plus
  - Two day course includes practical cloud lab work
- GRC Stack Training
  - One day course to use GRC Stack components
- PCI/DSS In the Cloud
  - Achieving PCI compliance in cloud computing

https://cloudsecurityalliance.org/education/training/

Upcoming Conferences

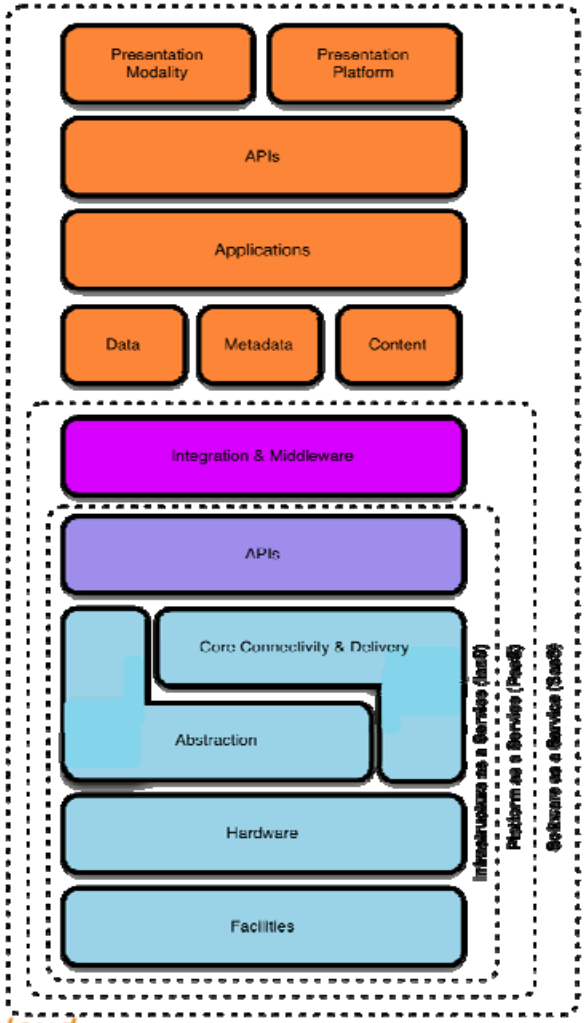
- CSA Summit RSA, Feb 27 2012, San Francisco
- SecureCloud 2012 (partnership with ENISA)

Security Framework



www.cloudsecurityalliance.org

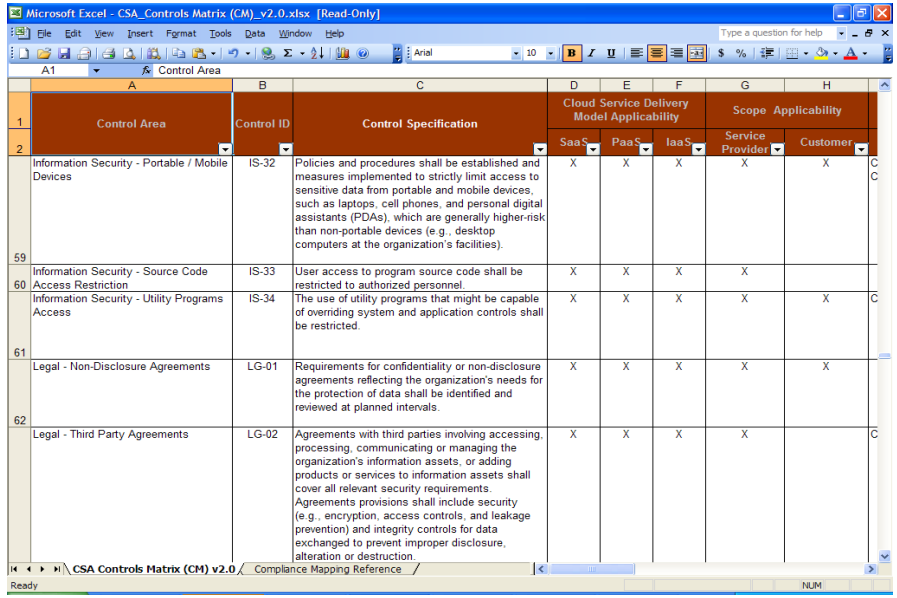
CSA Reference Model



- CSA Cloud Reference Model
  - IaaS (Compute & storage) is the foundation
  - PaaS (Rapid application dev) adds middleware to IaaS
  - SaaS represents complete applications on top of PaaS

Cloud Controls Matrix

- Controls derived from guidance
- Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA
- Rated as applicable to S-P-I
- Customer vs Provider role
- Help bridge the “cloud gap” for IT & IT auditors

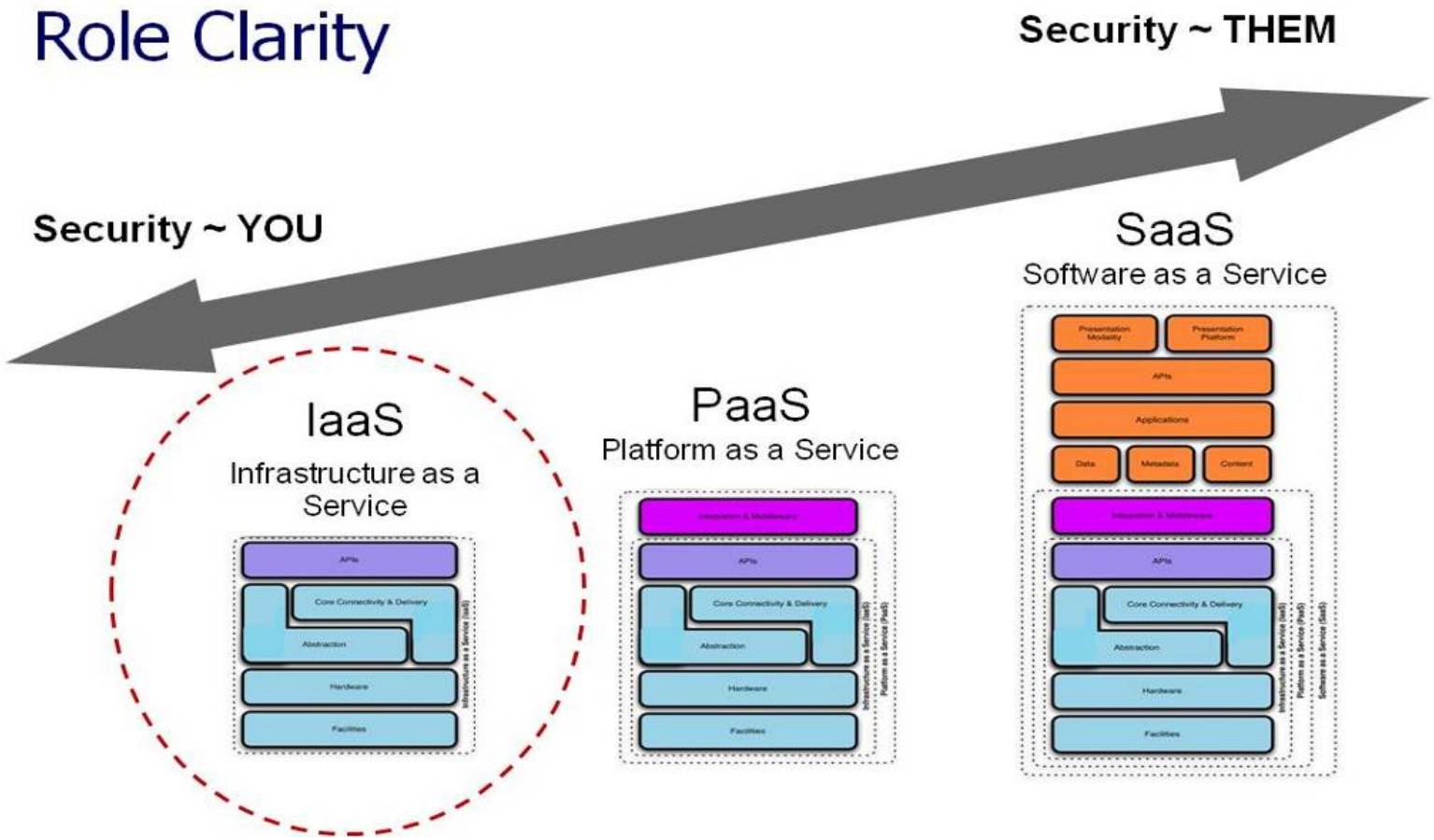


Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability	
			SaaS	PaaS	IaaS	Service Provider	Customer
Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X
Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X	
Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X
Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X
Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X	

- www.cloudsecurityalliance.org/cm.html

Assessment

Assessment responsibility



Consensus Assessment Initiative

- Research tools and processes to perform shared assessments of cloud providers
- Integrated with Controls Matrix
- V1.1 CAI Questionnaire released Sep 2011, approx 140 provider questions to identify presence of security controls or practices
- Use to assess cloud providers today, procurement negotiation, contract inclusion, quantify SLAs
- www.cloudsecurityalliance.org/cai.html

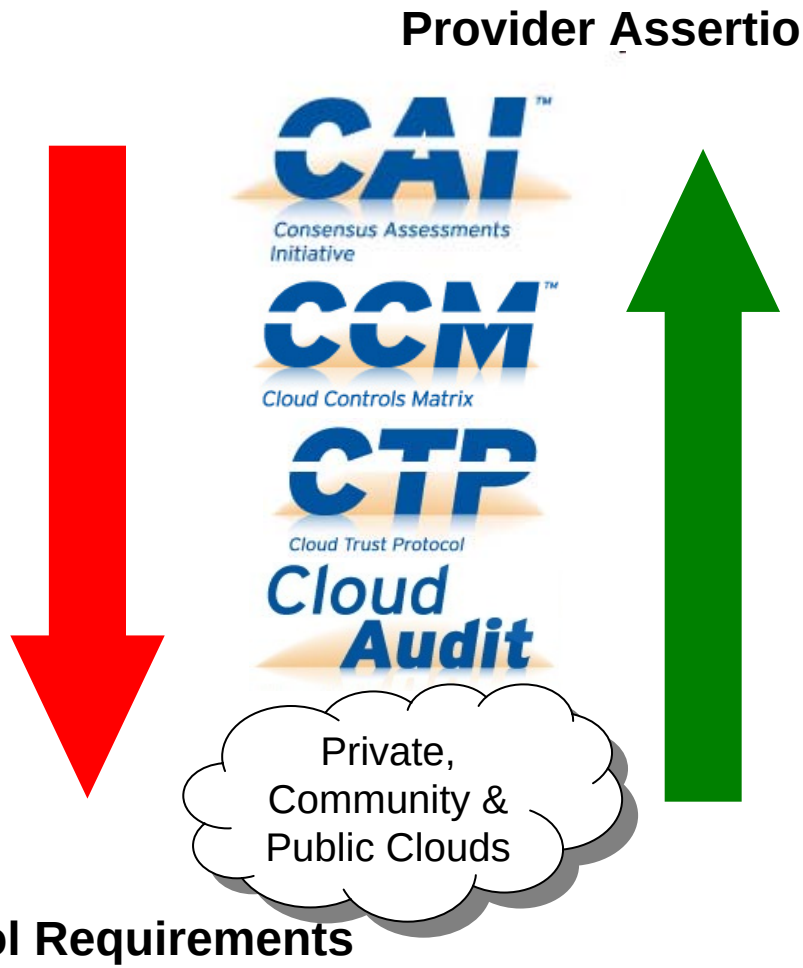
CSA STAR Registry

- CSA STAR (Security, Trust and Assurance Registry)
- Public Registry of Cloud Provider self assessments
- Based on Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
  - Provider may elect to provide assessments from third parties
- Available October 2011

Build for the future

CSA GRC Stack

- Family of 4 research projects
  - Cloud Controls Matrix
  - Consensus Assessments Initiative
  - Cloud Audit
  - Cloud Trust Protocol
- Tools for governance, risk and compliance mgt
- Enabling automation and continuous monitoring of GRC



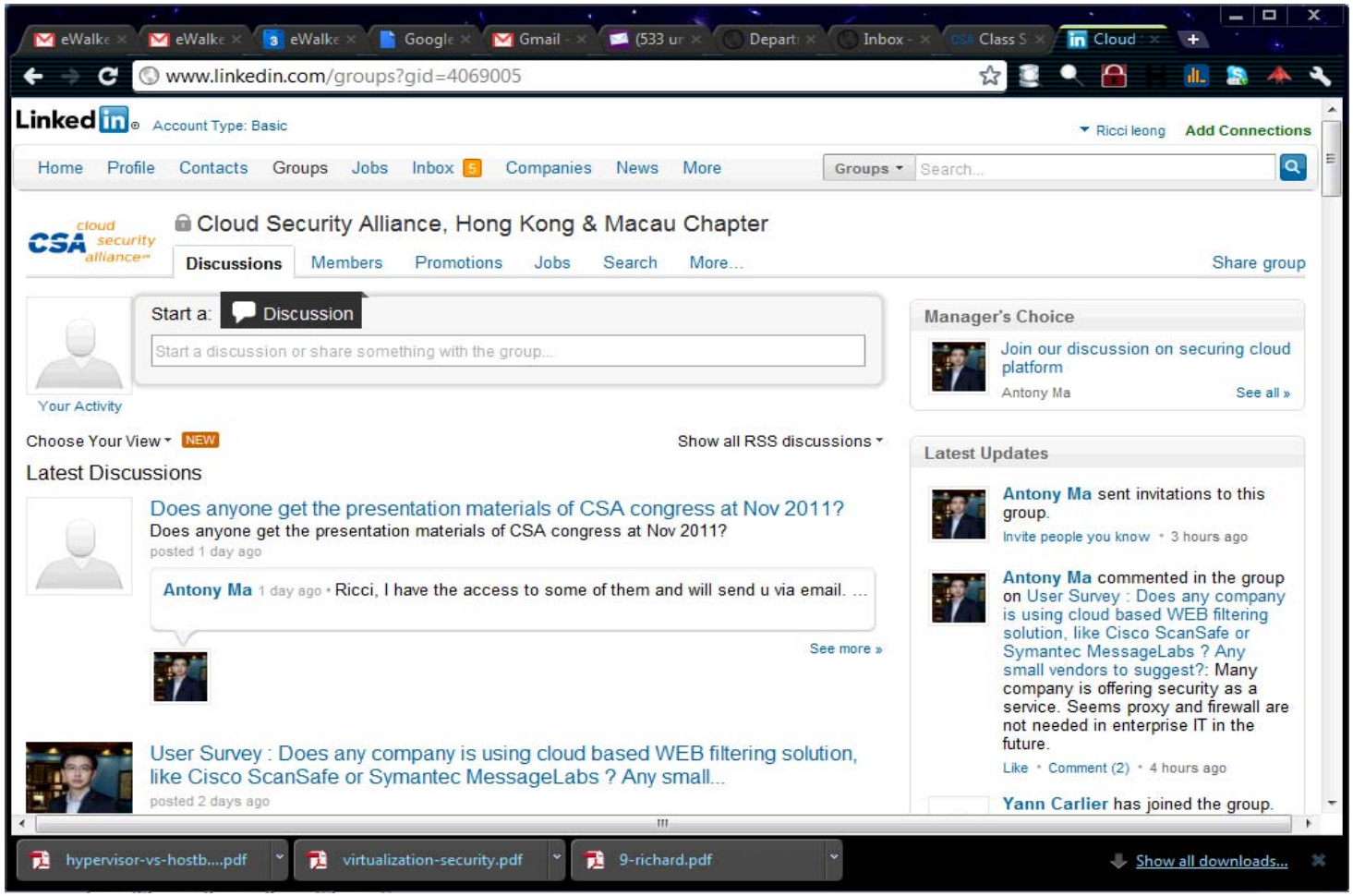
CloudAudit

- Open standard and API to automate provider audit assertions
- Change audit from data gathering to data analysis
- Necessary to provide audit & assurance at the scale demanded by cloud providers
- Uses Cloud Controls Matrix as controls nar
- Use to instrument cloud for continuous controls monitoring

CloudSIRT

- Consensus research for emergency response in Cloud
- Enhance community's ability to respond to incidents
- Standardized processes
- Supplemental best practices for SIRTs
- Hosted Community of Cloud SIRTs
- www.cloudsecurityalliance.org/cloudsirt.html

Cloud Security Alliance (HK&M)



www.cloudsecurityalliance.org

Contact

- Help us secure cloud computing
- www.cloudsecurityalliance.org
- LinkedIn: http://www.linkedin.com/groups?gid=4069005 (HK&M)
- LinkedIn: www.linkedin.com/groups?gid=1864210

Thank you!

cloud security alliance

www.cloudsecurityalliance.org