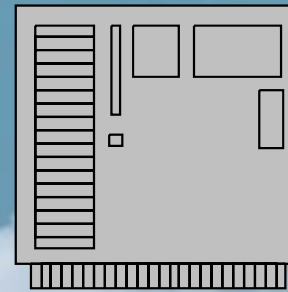
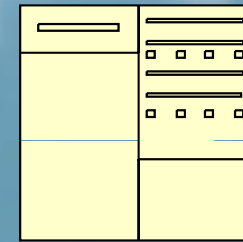
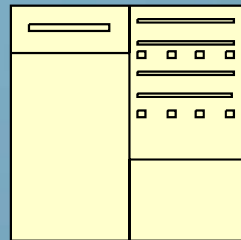
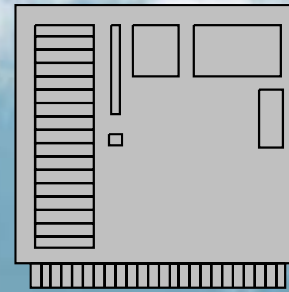
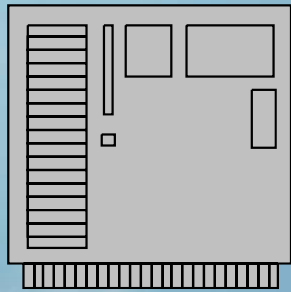


"I think there is a world market for about five computers" —
Remark attributed to Thomas J. Watson (Chairman of the Board
of International Business Machines) – 1943



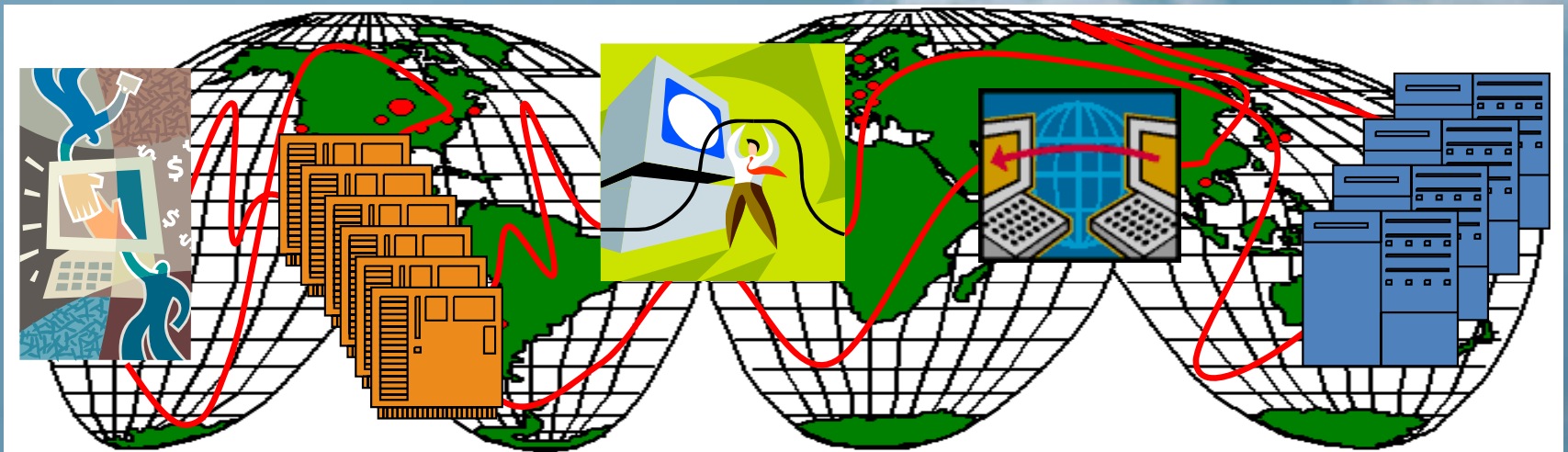
Cloudy, with a chance of rain...

Bruce Healton

So... Five computers!

- *"I think there is a world market for about five computers" — Remark attributed to Thomas J. Watson (Chairman of the Board of International Business Machines) – 1943*
- *"... In a sense, says Yahoo Research Chief Prabhakar Raghavan, there are only five computers on earth. He lists Google, Yahoo, Microsoft, IBM, and Amazon. Few others, he says, can turn electricity into computing power with comparable efficiency ..."*

From [Google and the wisdom of clouds](#), by Steven Baker - BusinessWeek.com



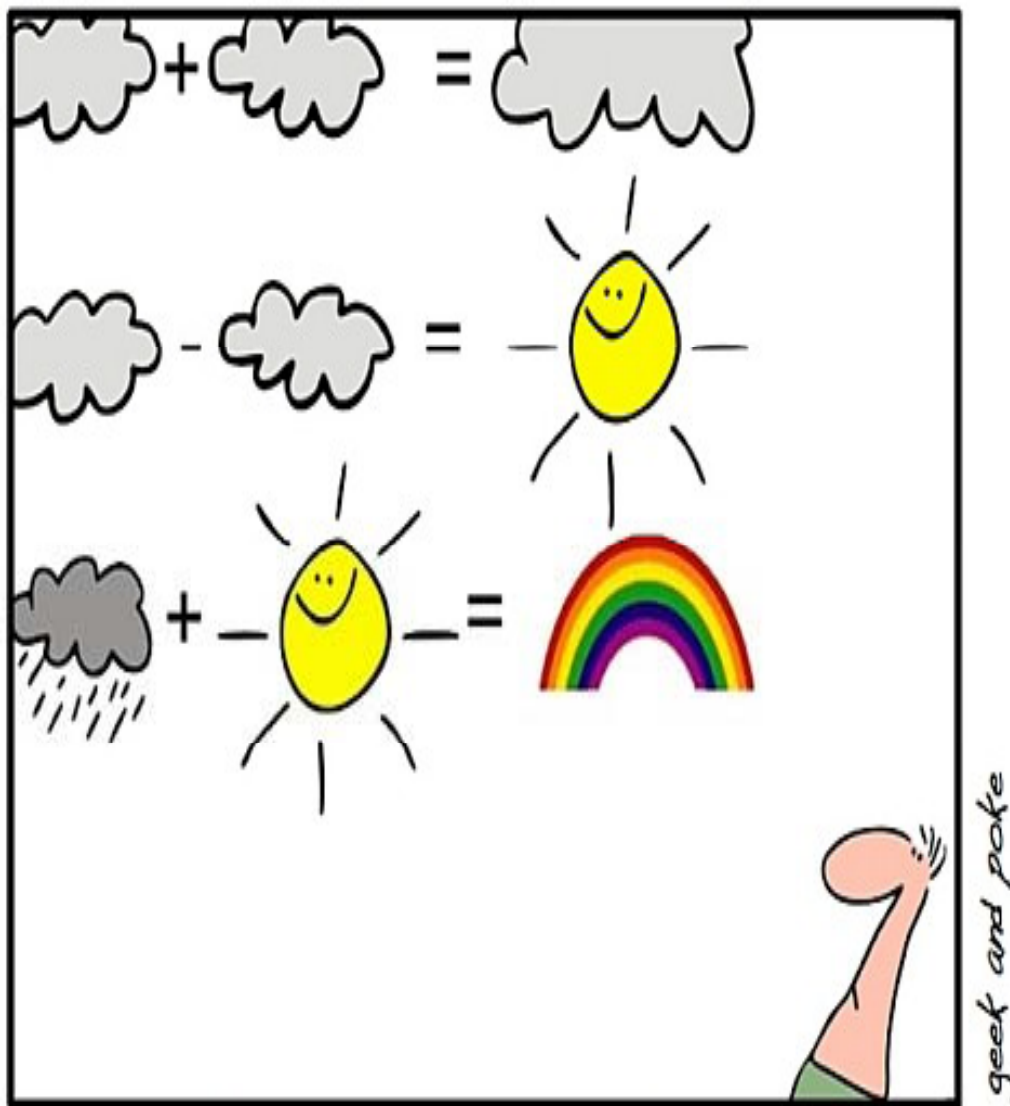
Who We Are

- 30+ years of experience with technology
- Consultants experience:
 - Financial (Banks, Brokerage, Insurance, Accounting), Personnel / HR Services, Manufacturing, Security, Technology and Service Providers
 - Worked for multinational, national, regional, and local concerns
 - Process & Methodology Development
 - Business & Practice Development
 - Technology Selection & Implementation
 - Published Privacy & Security researchers

Theoretical Practice

- *"Java, Agents, and Chronic Infections"*,
IEEE Aerospace Conference 1998, Healton, Kwong, and Lancaster
- *"Web Infections and Protections"*,
IEEE Aerospace Conference 1998, Healton, et al.
- *"Protecting against Internet Threats"*,
IEEE COMPSAC 1999, Healton, et al
- *"Web Infections and Protections 2000: The E-Commerce Perspective"*,
IEEE COMPSAC 2000, Kwong
- *"Measure and Countermeasure: Information Security in an Infowar"*,
IEEE COMPSAC 2001, Kwong
- *"The Dark Side of the Internet"*,
Cyber Crime Fighters Forum 2002, Healton
- *"E-Commerce Gone Bad: What to do after it passes"*,
MnIPS 2003, Kwong
- *"Protecting Your e-Commerce Website"*,
MnIPS 2003, Healton

Practical, Not Just Theory

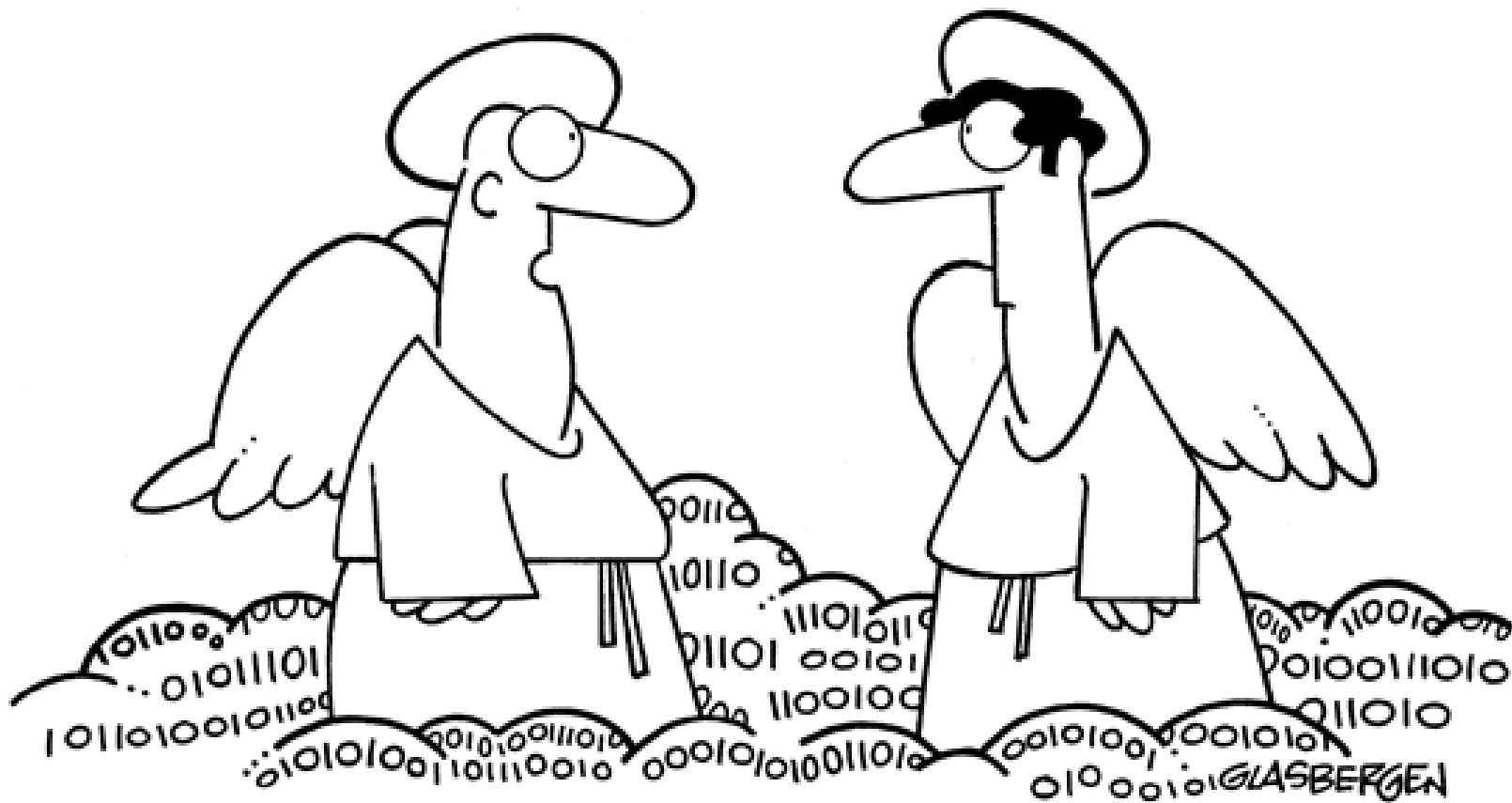


**SIMPLY EXPLAINED - PART 17:
CLOUD COMPUTING**

- Front-line support of SMB technology for numerous organizations
- Design, develop, and audit organizational security plans and implementations for SMB to international concerns
- Front-line support of SMB web-presence
- Developed a organizational security standards compliance application as a SaaS product offering
- Audit and critic 3rd-party SaaS applications

Living in the Illusion of Virtual

© Randy Glasbergen
www.glasbergen.com



“You should have been here back in the old days before cloud computing.”

Currently Available Applications



Cloud Computing

Having secure access to all your applications and data from any network device

Applications coming soon?

- **Coming Soon**

- Picasa/Flickr/Photos/Photoshop (Splashup, Pixlr, etc.)
- Project Management (lots of choices) / project support (basecamp, git)
- Common Bill Pay (Mint.com)
- More than a blackboard (MITOpenCourseWare (MIT), Open Learning Initiative (Carnegie Mellon University), Open Yale Courses (Yale University), Stanford Engineering Everywhere (Stanford University), UOnline (University of Utah))

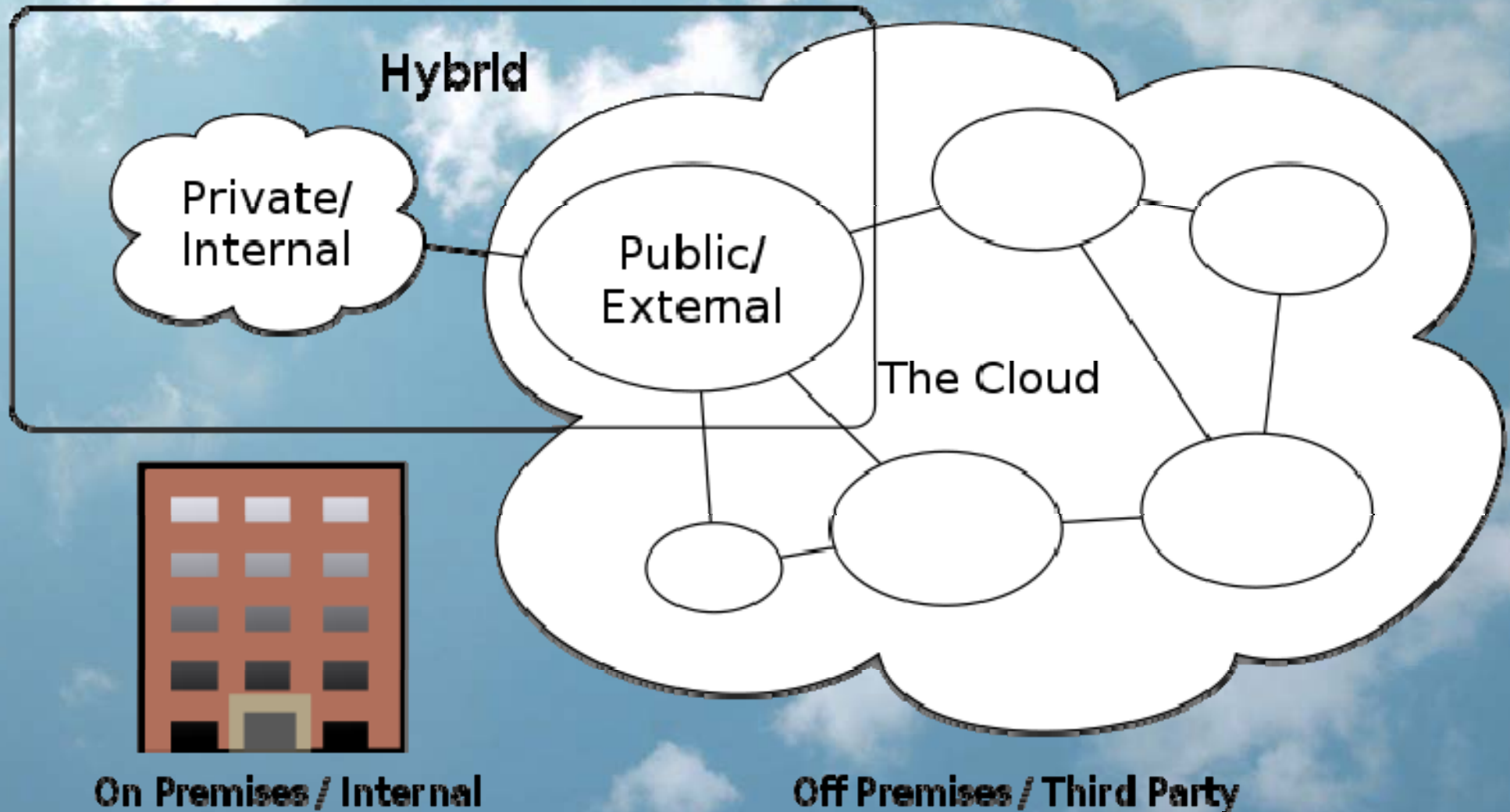
- **Almost there**

- Ticketing / TicketMaster / Live Entertainment/AEG
- OpenTable
- Intuit
- Governments

- **Already There**

- Travel – Travelocity, Orbitz, Expedia, TripAdvisor
- Shopping – amazon, ebay, yahoo, buy.com, real estate
- Online suites - zoho, google, microsoft
- Mapquest / Google Maps / SmartPhone GPS
- eBooks / eMags / ePodCasts
- Payroll / Personnel / Personal Finance

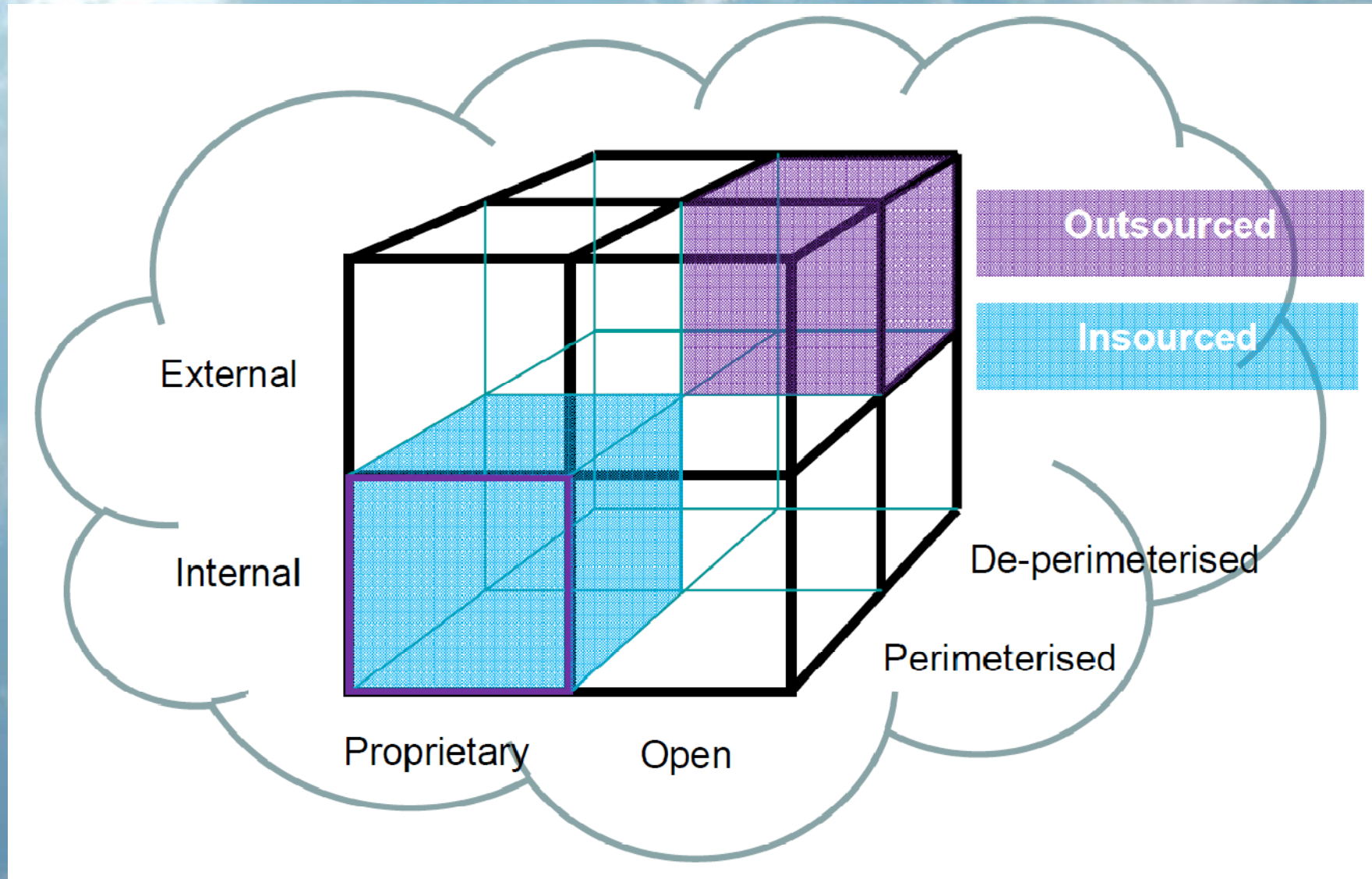
Types of Clouds



Cloud Computing Types

What is Cloud Computing?

- Jericho Forum - Cloud Cube Model




*The Open Group: Jericho Forum : <http://www.opengroup.org/jericho/publications.htm>


IBM System View of Clouds

Service Portals

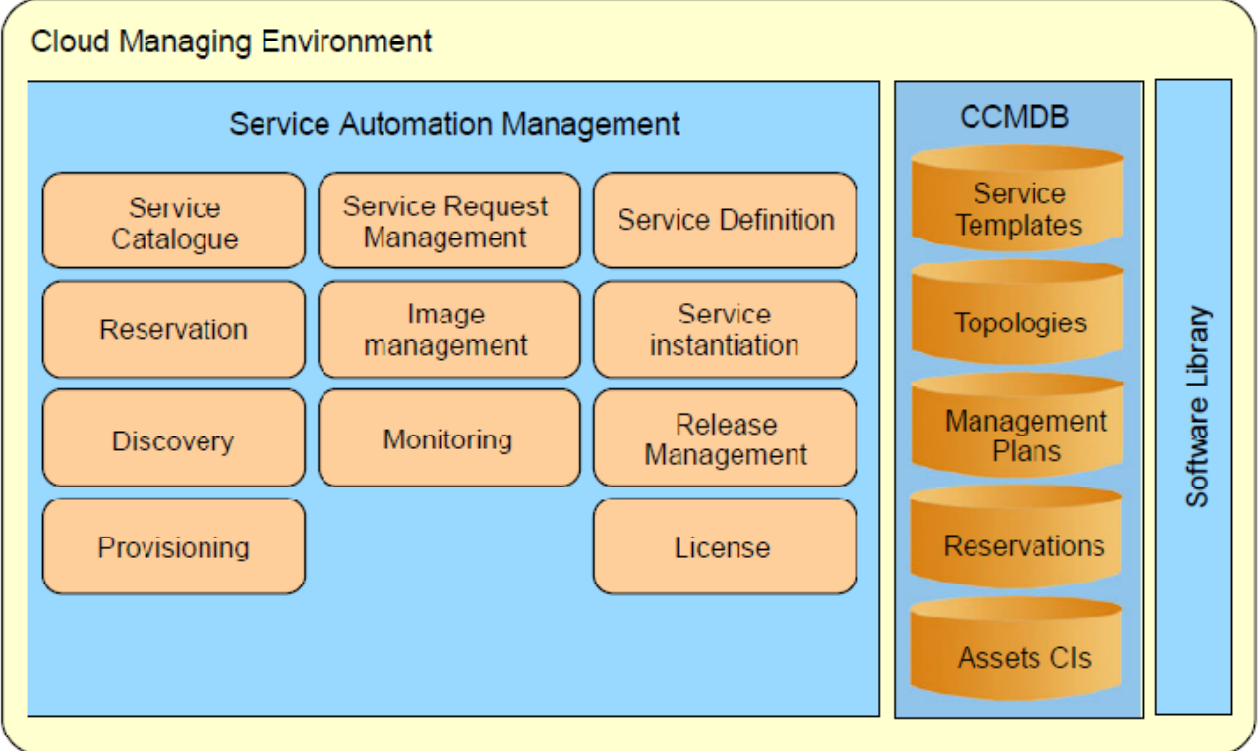
Cloud Service Customer



Cloud Service Provider

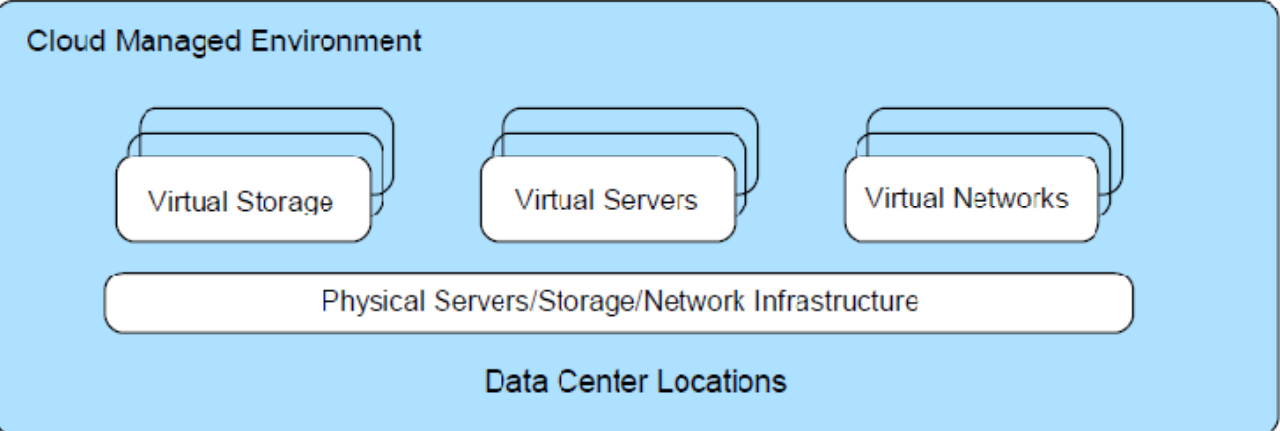


Service Request and Operations



Operations

Infrastructure (MW, Platform, DB, Software) for Service Products



External Systems

- Change Management
- Problem Management
- Configuration Management
- Metering
- Chargeback
- Storage Management

Integration Points

Cloud Computing as a Service

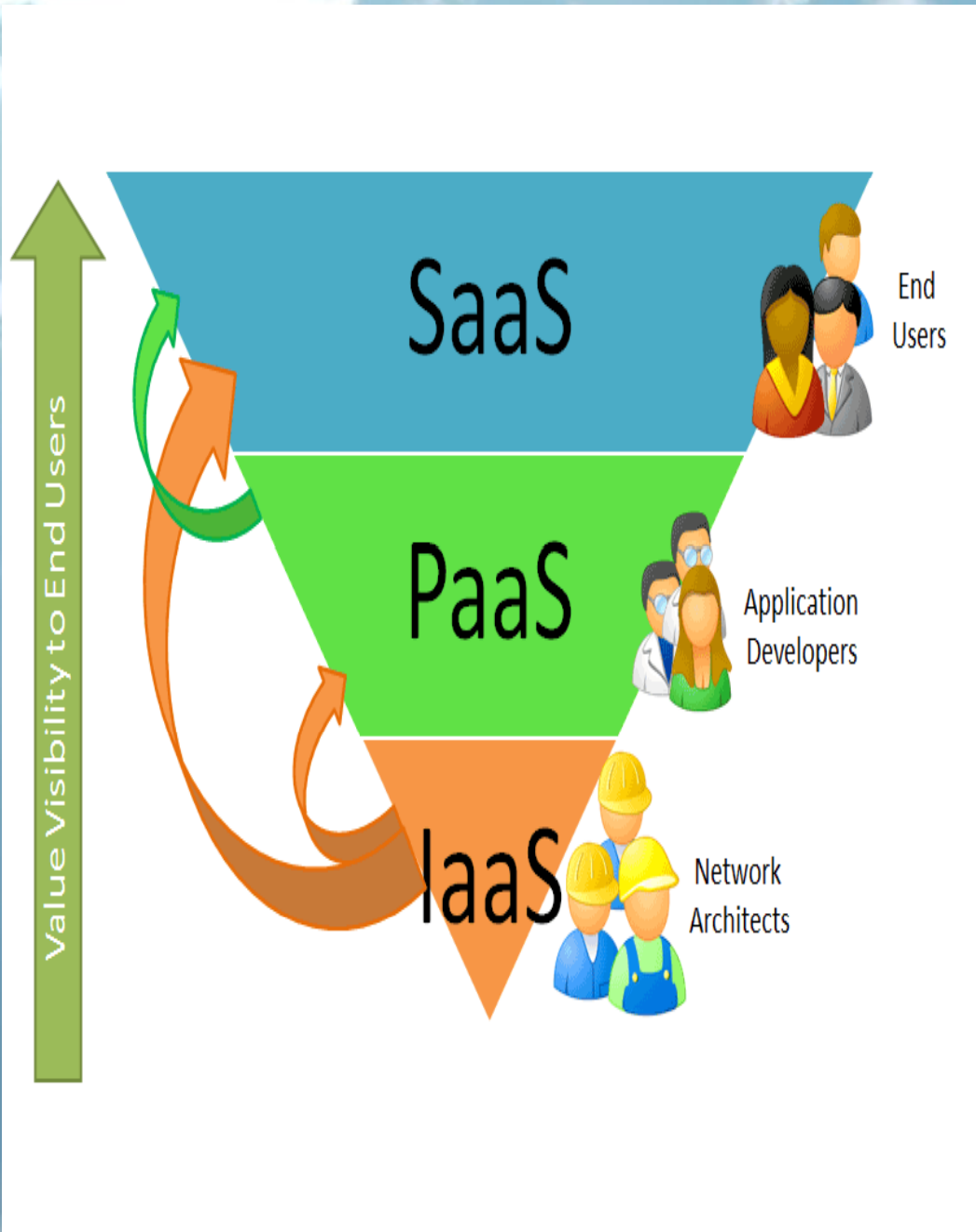
Pros and Cons



From <http://blogs.zdnet.com/Hinchcliffe>

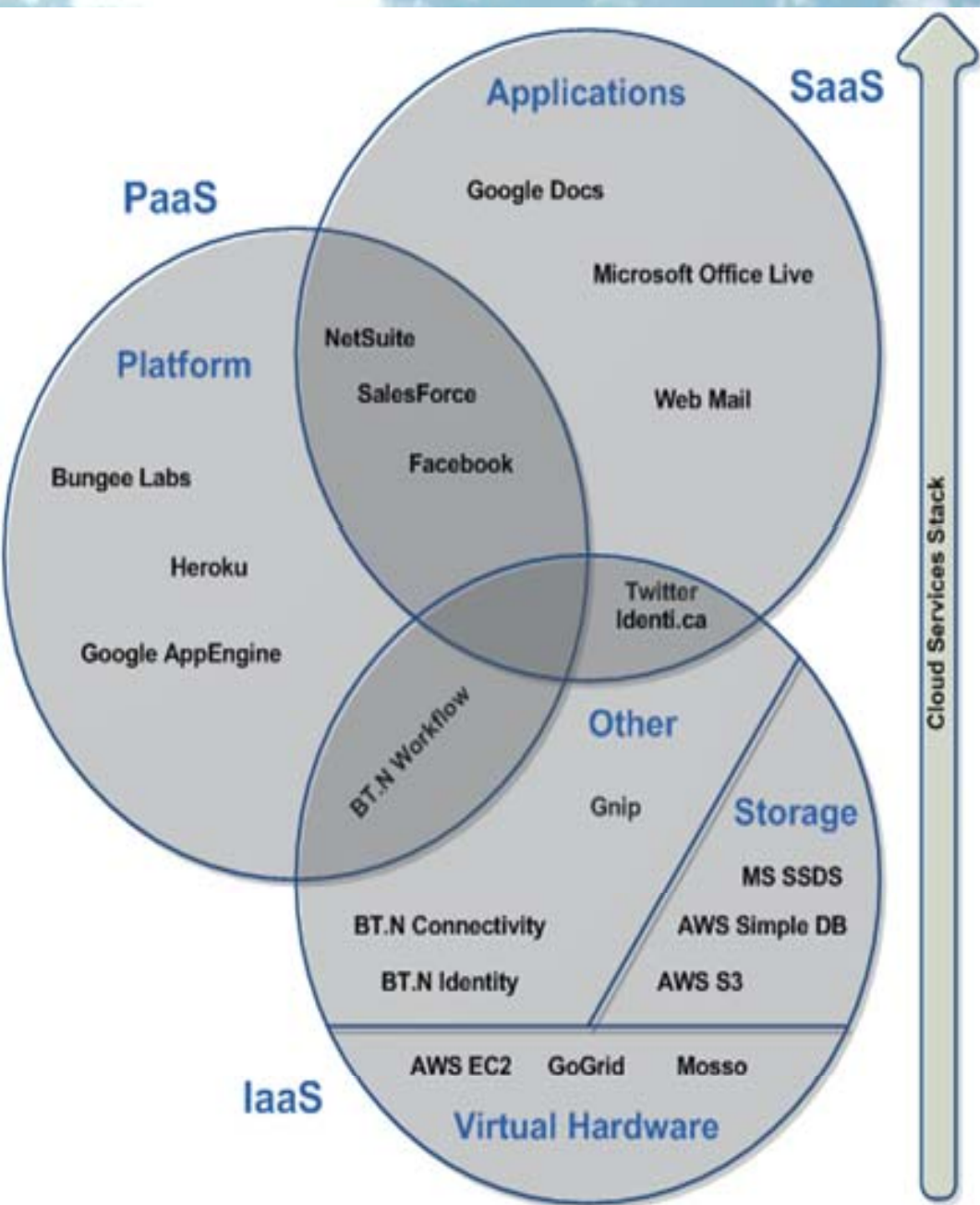
- Each layer encapsulates on-demand resources
- Each layer comes with its own application development model
- Three service layers:
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service (IaaS)

Software as a Service (SaaS)



- Cloud provider offers software services that are of potential interest to a wide variety of users
- Users (optionally) buy subscription to software products
- Software implemented by cloud provider on their own infrastructure
- Instances of the software run on cloud provider infrastructure and serve multiple client organizations
- Some or all of the data resides remotely
- Examples: [SalesForce.com](https://www.salesforce.com), [Google Mail](https://mail.google.com), [Google Docs](https://docs.google.com)

Platform as a Service (PaaS)



Cloud provider offers a platform upon which developers provide services that are of potential interest to a wide variety of users

Users (optionally) buy subscription to software products

Software implemented by developers to run on the cloud provider infrastructure

Instances of the software run on cloud provider infrastructure and serve multiple client organizations

Some or all of the data resides remotely

Examples: **Google Apps Engine, Amazon Web Services (w/ basic web stack)**

Infrastructure as a Service (IaaS)

IaaS - Infrastructure as a Service

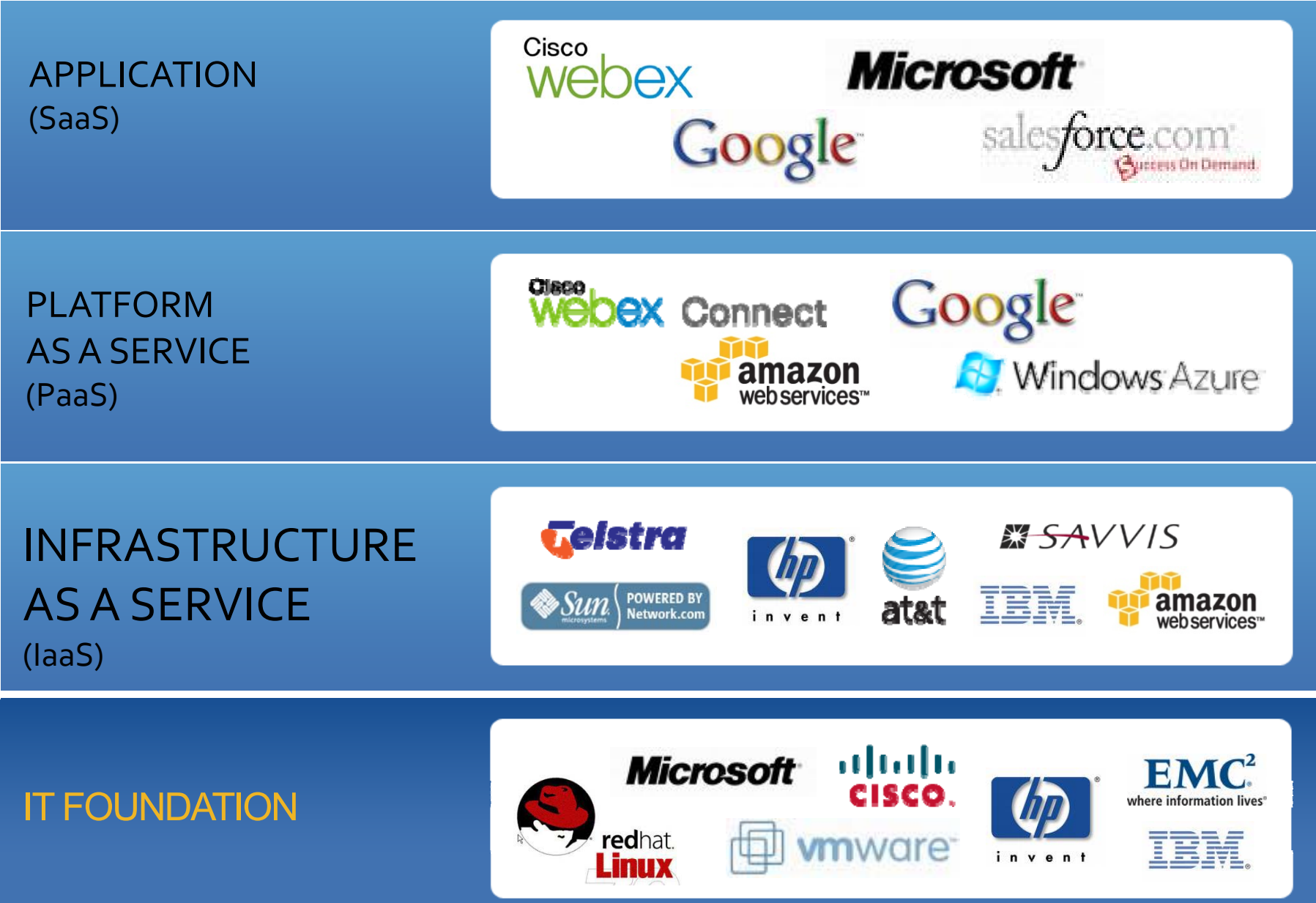
(Service Provided, SLA, Dynamic Licensing, Variable Expense, Speed to Market)



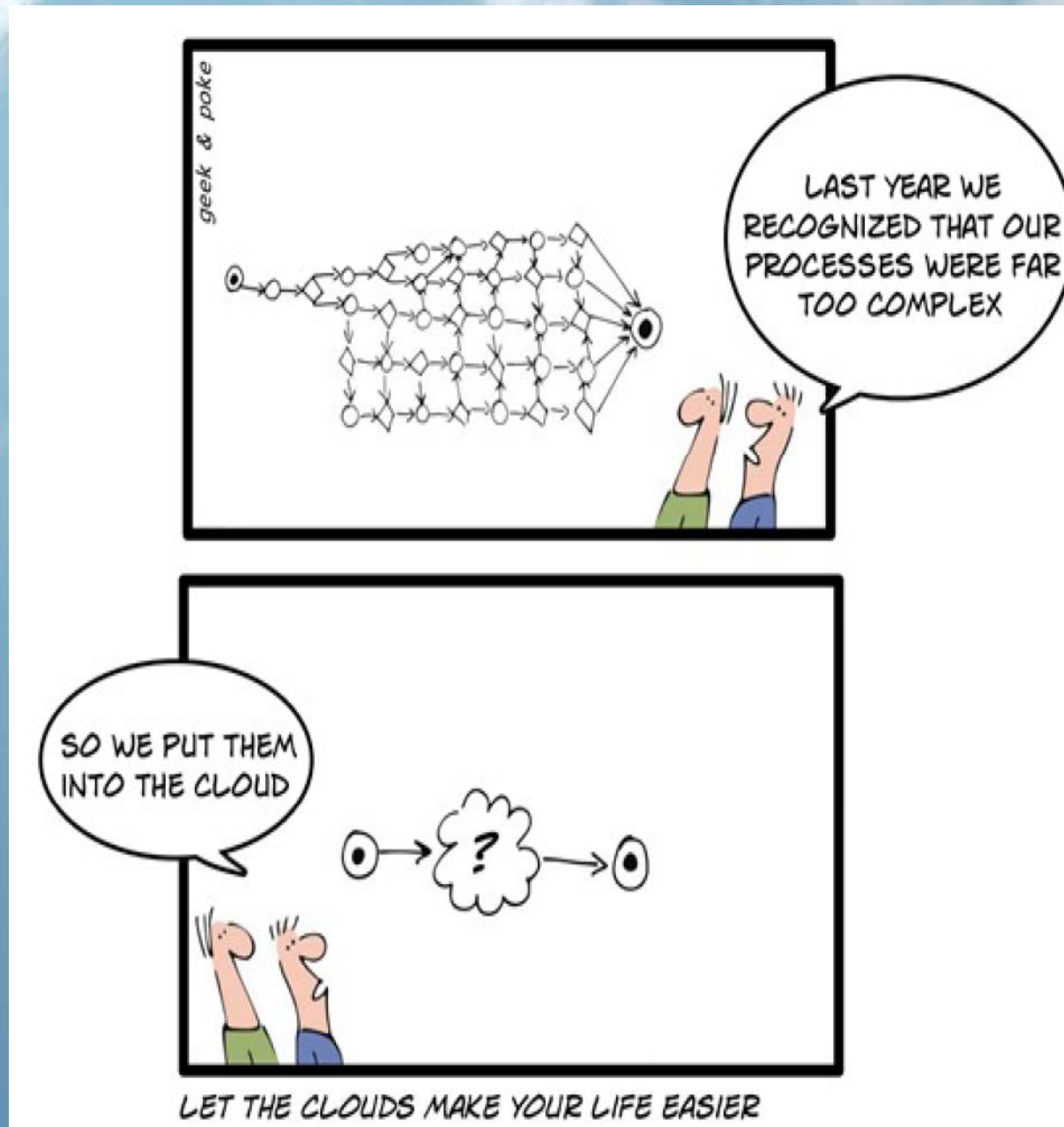
David Williams

- Cloud provider offers IT infrastructure (compute, storage, network, etc.) to customers
- Virtualization is leveraged to dynamically combine resources in order to build and deliver *ad hoc* systems to the customer
- Customers deploy their own software environment (i.e. virtual machine images) to run on these systems
- Resources used by customers can grow and shrink on demand
- Some or all of the data resides remotely Examples: **AWS (EC2 and S3)**

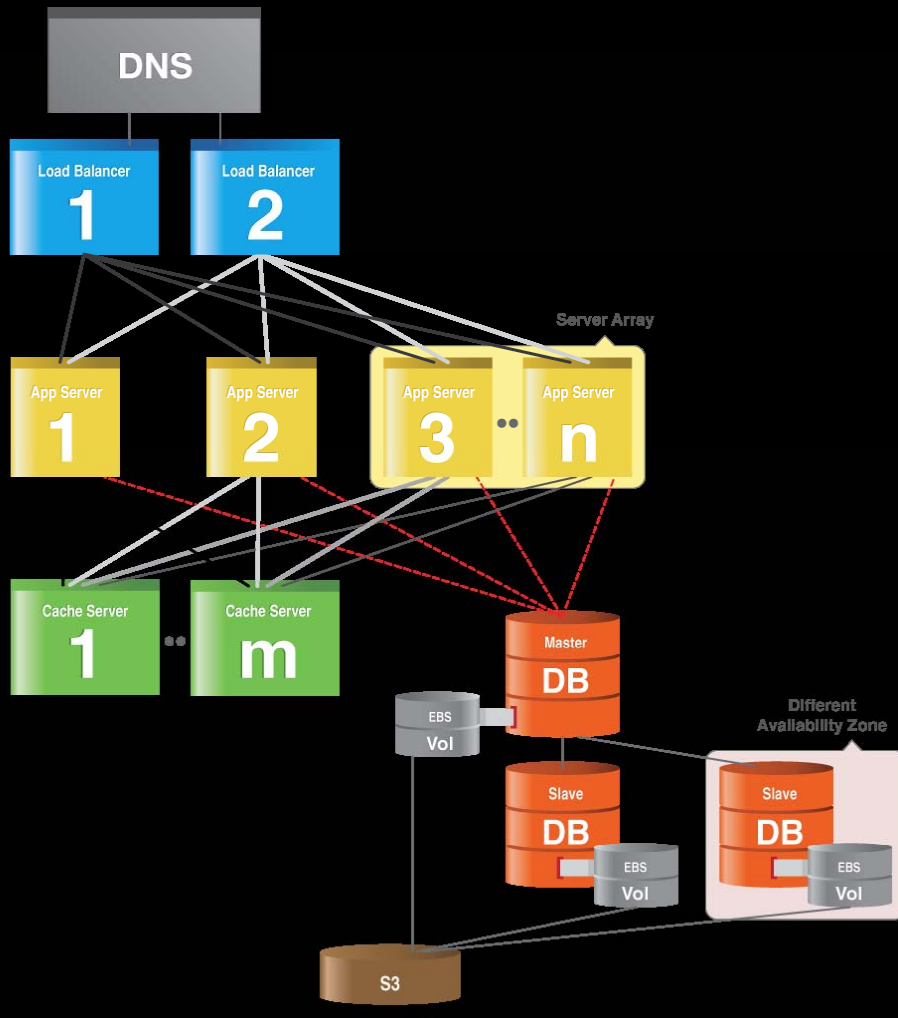
Who Are the Major Cloud Players?



Complexity is a BAD Thing



Complexity in the Cloud



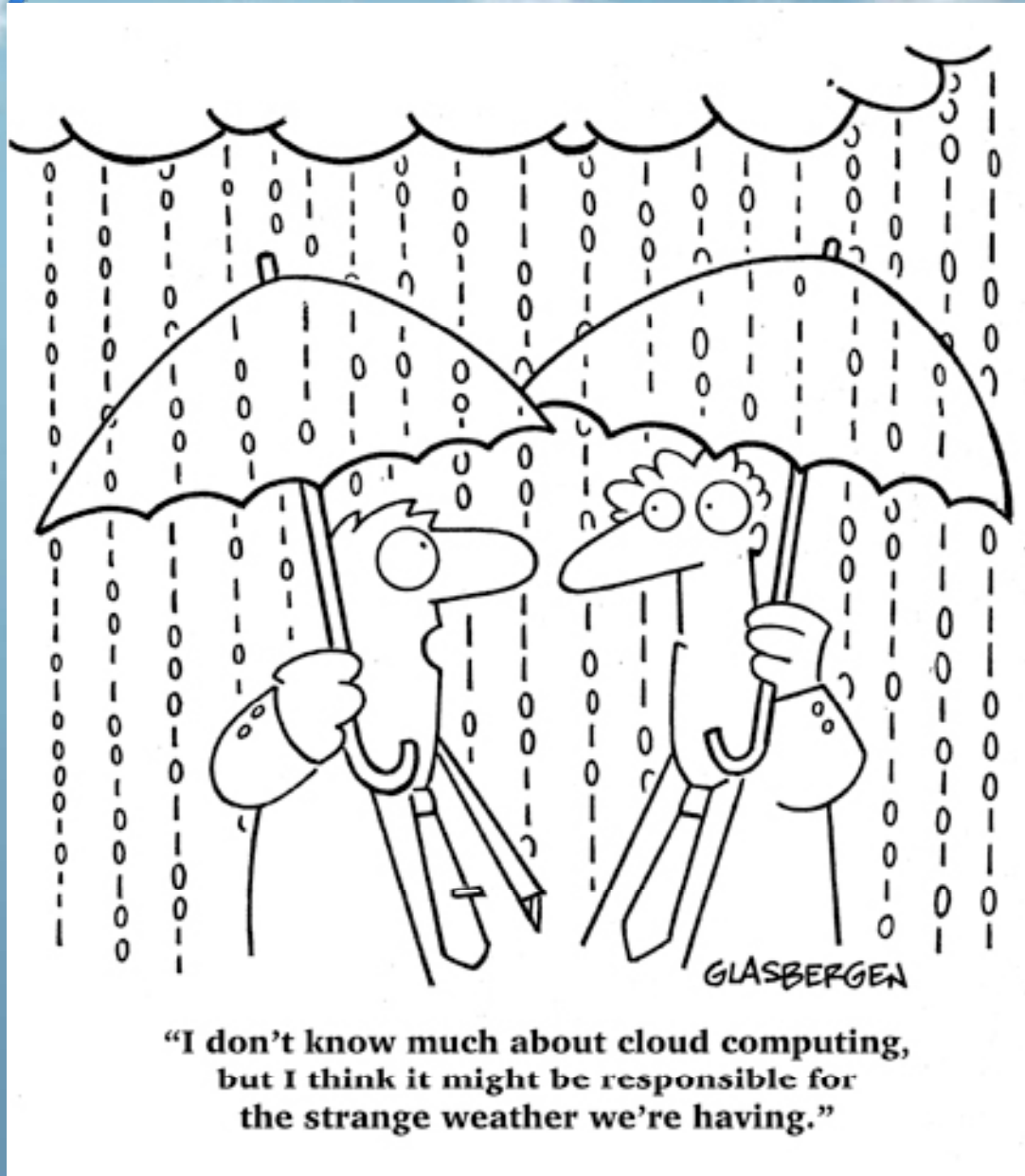
- Tiers
 - Domain Name Services (DNS)
 - Load Balancing
 - Application
 - Database
- Disaster Recovery
- Geographic Dispersal

Simplicity in the Cloud



- Data movement (Dropbox)
- Sales / shopping (eBay, Amazon)
- Virtual web servers
- Transcription / Data capture (Progressive, banks, LegalZoom)
- 1-n contacts (Twitter, blogging)

What you don't know...



6 Worst Cloud Security Mistakes

1. Assuming the cloud is less secure than your data center.
2. Not verifying, testing, or auditing the security of your cloud based service provider.
3. Failing to vet your cloud provider's viability as a business.
4. Assuming you're no longer responsible for securing data once it's in the cloud.
5. Putting insecure apps in the cloud and expecting that to make them more secure.
6. Having no clue that your business units are already using some cloud-based services.

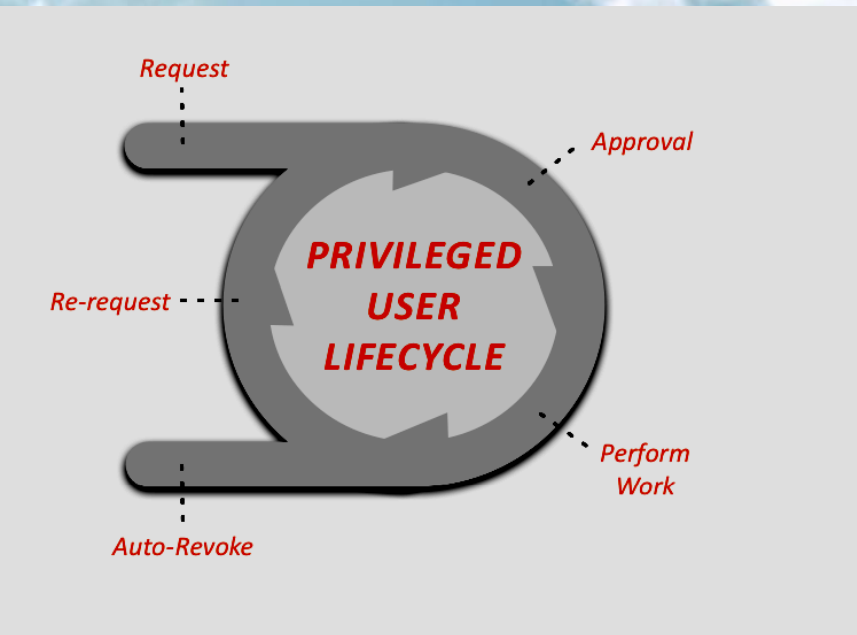
Source: Darkreading [5]

Risks in the Cloud



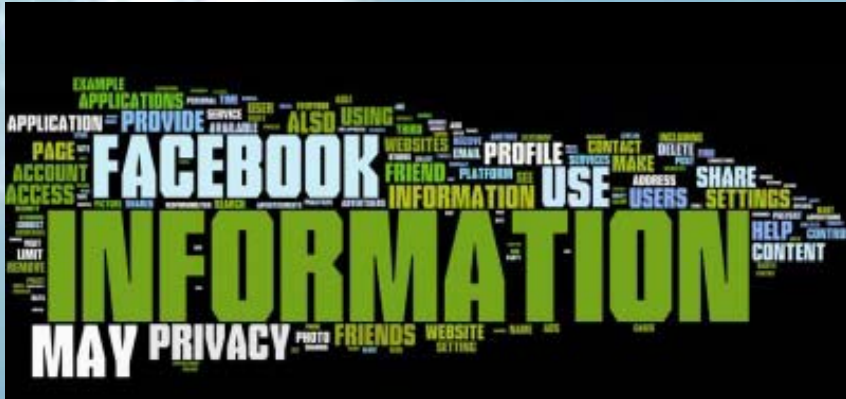
Clouding the Issue: Privileged User Access

- Does the sysadmin know your private Facebook secrets? Flickr? Google Docs?
- Are backups secure?
- Have you signed away your rights (TwitPic)?
- Can parents look at family pages?
- If you're working on a class project can people force you to share?
- If you're working for a company can your boss read all of your gmail?



Clouding the Issue: Data Segregation

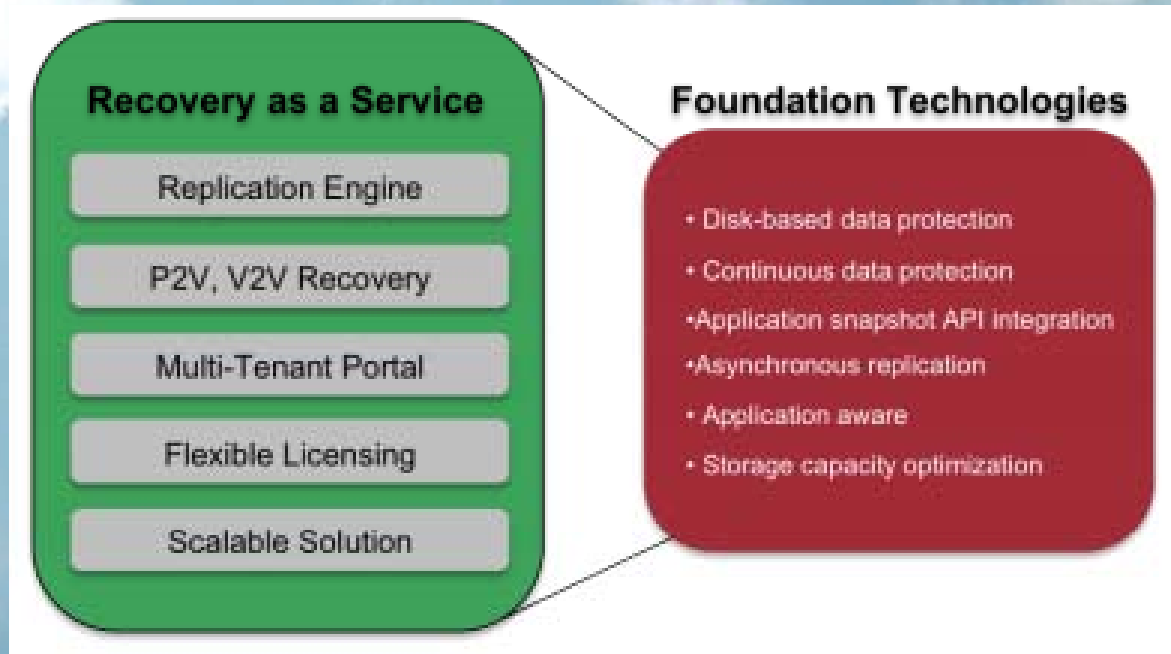
twitpic



- When do you own your content (video, pictures, music)? Licenses only?
- When do original works get protected? (Authors, musicians, photographers)
- Are corporate files private from competitors? Even when restored?
- Are my system images private on a cloud server?
- Who owns your crypto keys?

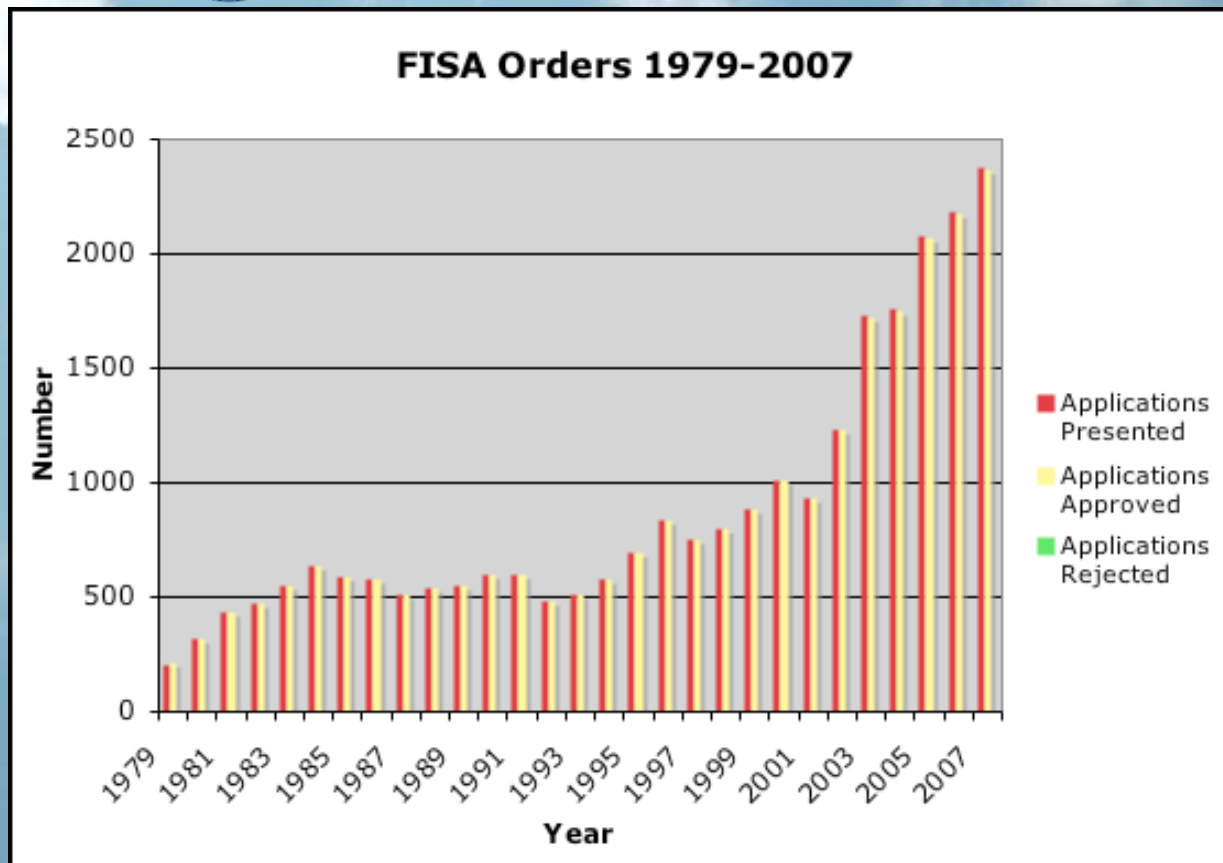


Clouding the Issue: Data Recovery



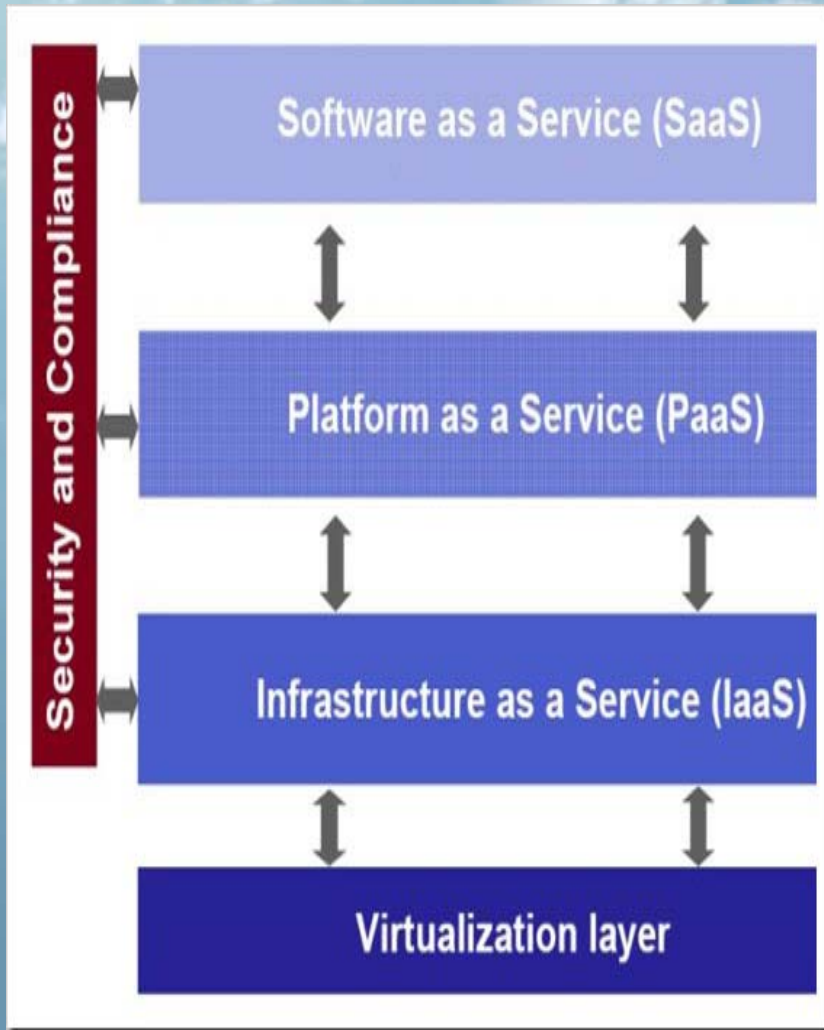
- See Disaster Recovery (for Recovery of the *as a Service)
- Data Recovery – when you make an application mistake (“I didn’t want to delete 10 years of pictures!”)
- Data Recovery – when malicious events happen to your configuration or data
- Data Recovery – for auditors, taxes, or separated entities (like couples)

Clouding the Issue: Investigation



- Something changed in your DropBox folder, do you know who, what, how, when?
- When things go wrong, can you determine what happened? (Sony)
- “The Feds” have subpoenaed information from/about your provider. Will you know? (Patriot Act, FISA, FCPA, HSA, ...)

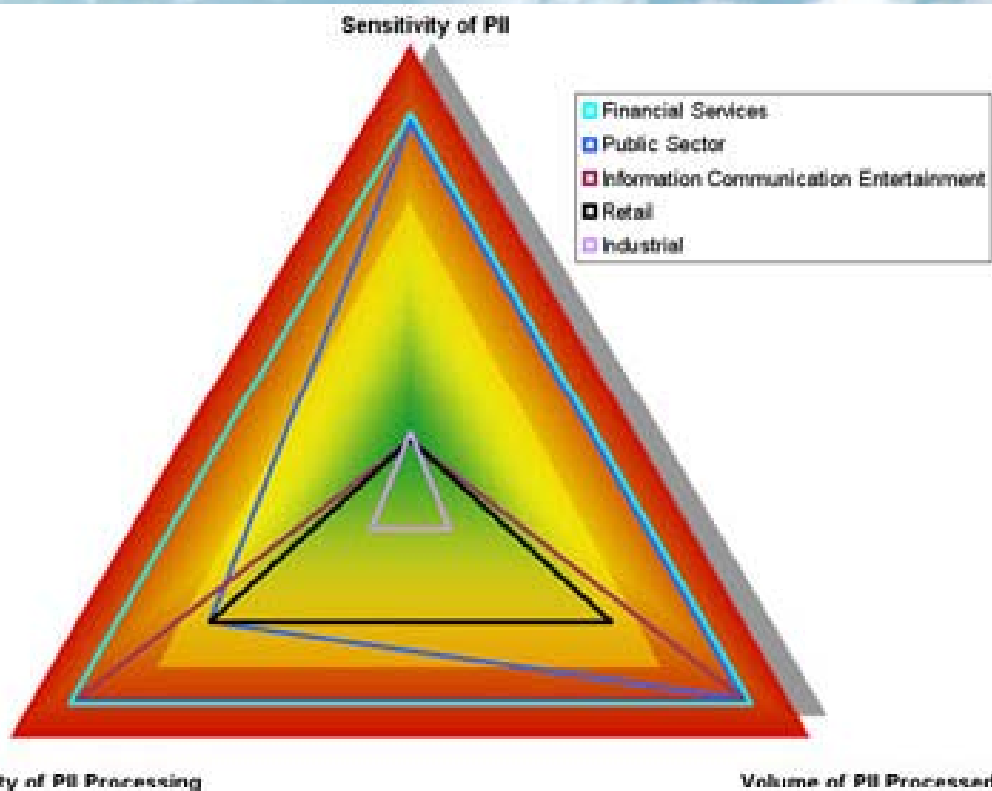
Clouding the Issue: Compliance



- Credit card transactions require compliance with Payment Card Industry (PCI) standards
 - Business processes and procedures
 - IT processes, procedures, standards compliance
 - Authentication
 - Encryption
 - Data Transmission
 - "Data at rest"
 - Development, testing, and installation processes, procedures, safeguards
- PCI has recently announced clouds can be certified as compliant in an overall PCI-app

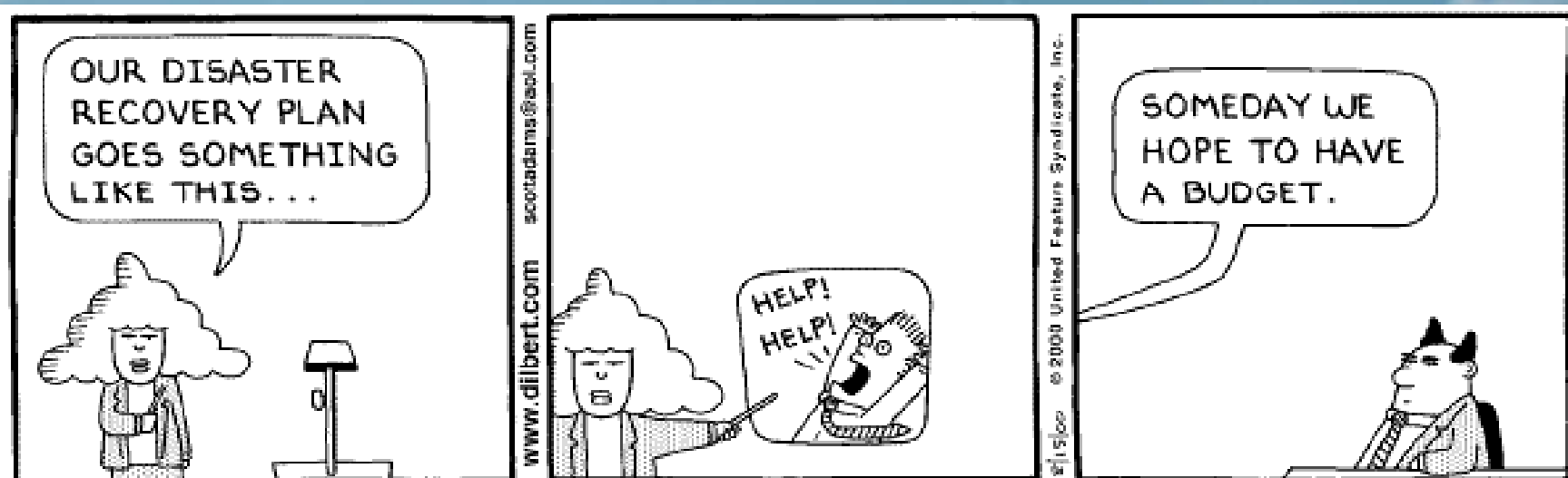
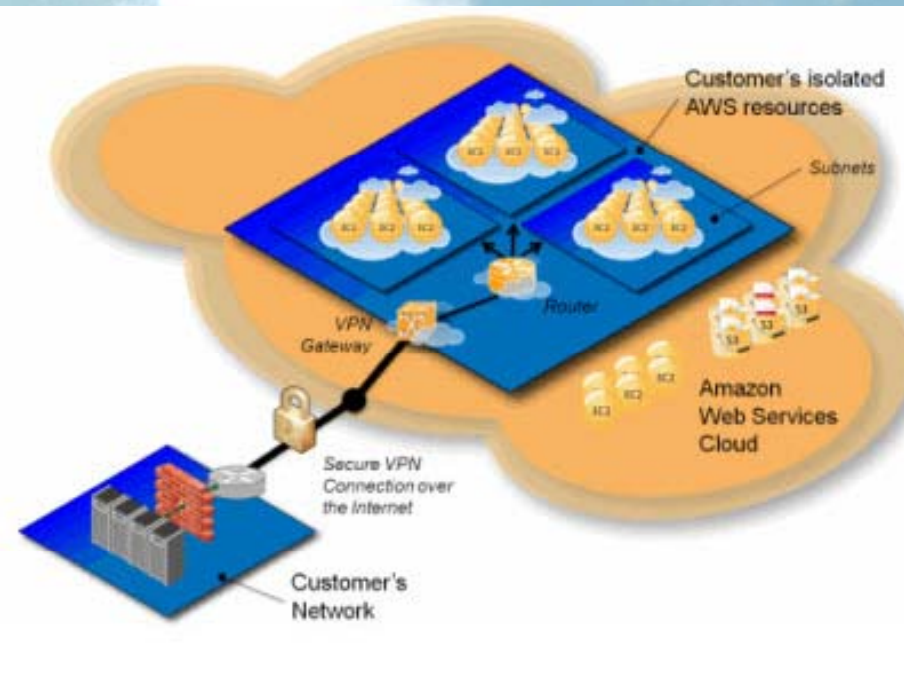
Clouding the Issue: Data Location

- Transborder dataflow rules in EU
- Legal/IP Protection Requirements
- National Laws for Data Location (US, Canada)
- Corporate IP Protections
- Access by citizens of restricted domiciles



Clouding the Issue: Disaster Recovery

- DR is not easy (Amazon, Microsoft, Google, and Salesforce know this now)
- DR in the cloud is unpredictable (non-dedicated resources, database engine problems, inability to control “partially up” environments)
- DR in the cloud requires resources (if your data is on a 50PB SAN is there a backup?)
- Fallback to local very difficult and complex



Clouding the Issue: Other Aggravation Examples & Issues



Spam and Phishing



- “The Classics”
- Targeted Attacks
 - Epsilon
 - Provider of Fortune 500 Opt-In mailing list data
 - Targeted for Phishing
 - Remote control software installed
 - Extracted 50 companies mailing lists
 - Sony
 - Shutdown PlayStation Network
 - Extracted credit card list for 77 Million users

RSA SecurID Token Source Code



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with
RSA SecurID software token

- RSA was targeted
- A sustained campaign
- “Undeleted” infected SPAM message opened by an internal user
- User’s machine “taken over”
- SecurID source extracted directly from RSA servers
- May have lead to other attacks against clients

SSL / Certificate Authority

Internet



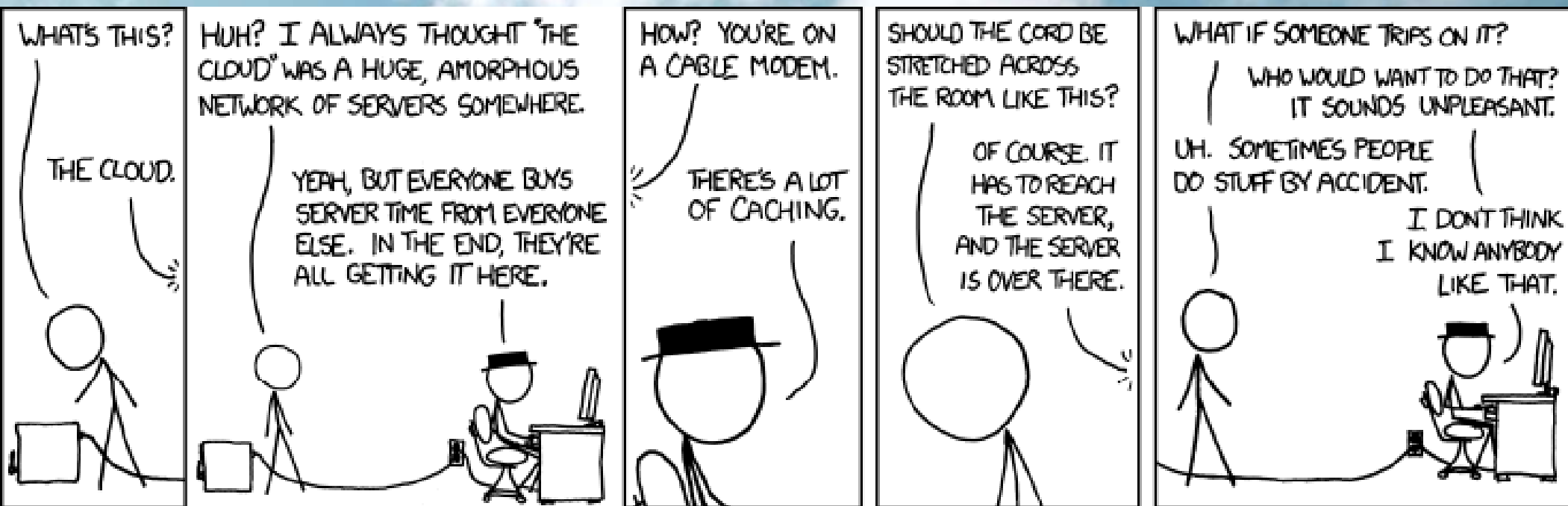
- SSL & Certificates
 - Weak hashes still accepted
 - “Public” CA procedures
 - Little public understanding
- CA compromised: Comodo
 - Multiple compromises
 - SQL Injection Attack
 - Issued 9 SSL certificates to an Iranian hacker via a “normal” un-audited request mechanism
- Browser Issues - certificates



TM

C·O·M·O·D·O
EV SSL SITE
AUTHENTIC & SECURE

Accidents Happen!



Partly Sunny, Partly Cloudy: Downtime

Provider	Duration	Cause
Amazon – EC2	Days	Failure in EBS (non-SLA)
Microsoft-Outlook	Hrs/Days	Multiple failures from cloud, DNS, and attacks
Google – Gmail	2.5-20 hours	Undisclosed (99.99% SLA)
Skype - VoiP	2 days	Microsoft code update
Vmware – Cloud Foundry	4-5 hours	Cascade error in cloud admin
Google - Blogger	20 hours	Data Corruption
Sony - PSN	3 weeks	Hack attack
Twitter	1-2 days	API failure to perform
Dig	Hrs-days	Migration from MySQL to Cassandra
Wordpress	1-6 hours	10 million blogs hit by configuration change
Facebook	2-4 hours	Configuration change

Conclusions



- **Constant Vigilance!!!**
- Clouds are not a panacea – just a logical extension
- Be paranoid
 - Analyze before
 - Implement carefully
 - Monitor continuously
 - Watch out for social engineering issues
- Be prepared for change – even after you “go live”

A Final Thought

- Just because you are paranoid, does not mean they aren't out to get you!



PARANOIA

Just a heightened state of awareness

(c)2007 Kellie & photoshoppix.com



PARANOIA

Security cameras packing heat. That's just what we need.

Contact Information

- Bruce Heaton
bheaton@extratelligence.com
- Arnold Kwong
akwong@extratelligence.com