East African Information Conference 13-14th August, 2013, Kampala, Uganda

Security and Privacy: Can we trust the cloud?

By Dr. David Turahi
Director, Information Technology and Information Management Services
Ministry of Information and Communications Technology (ICT)

What is a Cloud Computing ?

- NIST defines cloud computing by:
  - 5 essential characteristics
  - 3 cloud service models
  - 4 cloud deployment models

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Essential Characteristics

- On-demand service
  - Consumer can unilaterally provision computing capabilities (e.g. server time &network storage) as needed automatically without human interaction with each service provider
- Broad Network Access
  - Services available over the net and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. workstations, tablets, laptop, mobile phones)

Essential Characteristics

- Resource pooling
  - Provider's computing resources pooled to serve multiple clients using a multi-tenant model
  - Different physical and virtual resources dynamically assigned and reassigned according to client demand
- Rapid Elasticity
  - Unlimited capabilities (from a clients view) can be elastically provisioned and released to scale rapidly outward and inward according to demand, in any quantity and at any time
- Measured service
  - Automatic control and optimization of resource use by leveraging a metering capability (e.g. storage, bandwidth and active user accounts

Cloud Service Models

- **Software as a Service (SaaS)**
  - We use the provider apps
  - User doesn’t manage or control the network, servers, OS, storage or applications
- **Platform as a Service (PaaS)**
  - User deploys their apps on the cloud
  - Controls their apps
  - User doesn’t manage servers, IS, storage

Cloud Service Models

- **Infrastructure as a Service (IaaS)**
  - Consumers gets access to the infrastructure to deploy their stuff
  - Doesn’t manage or control the infrastructure
  - Does manage or control the OS, storage, apps, selected network components

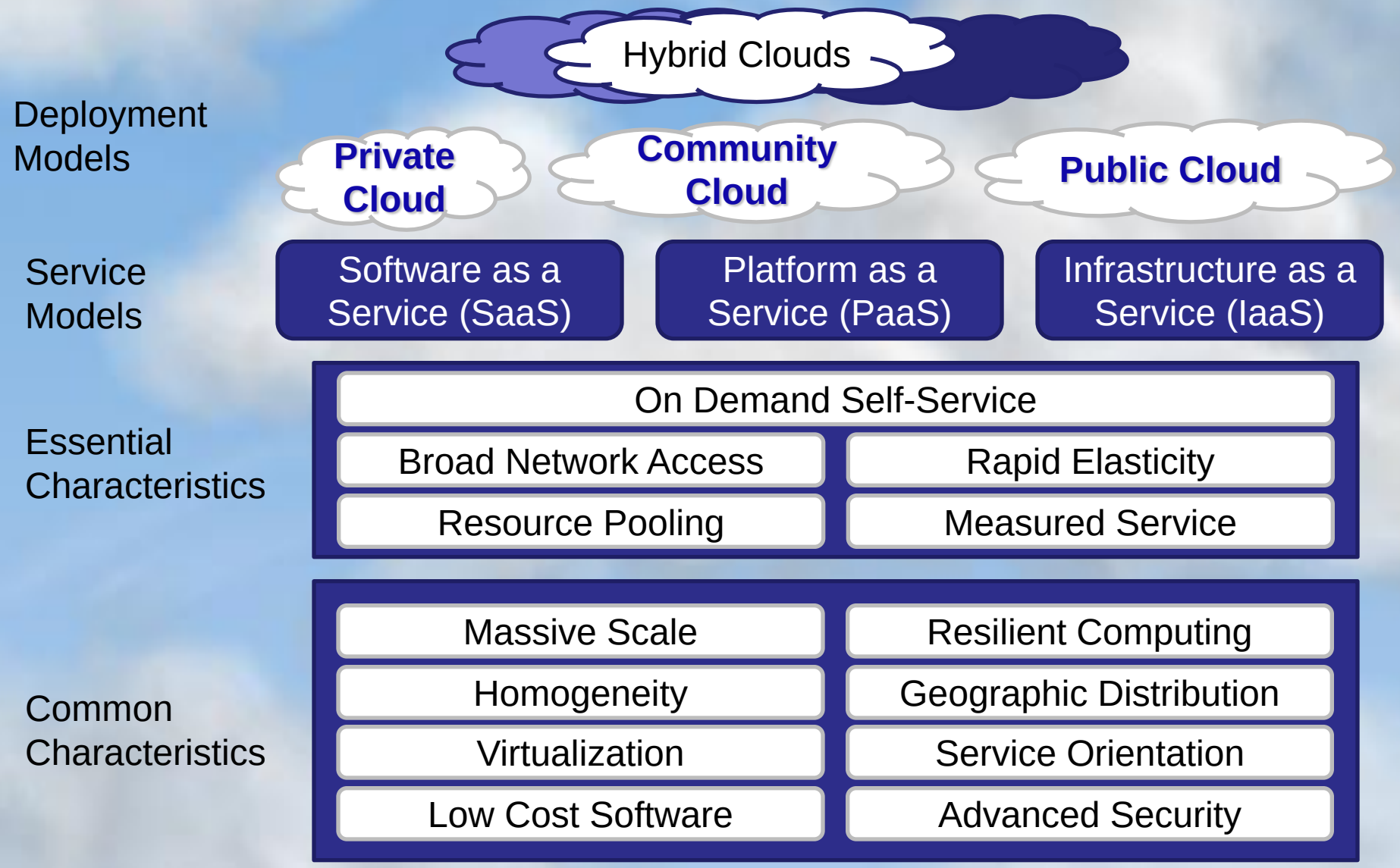
Deployment Models

- Public
  - Cloud infrastructure is available to the general public, owned by org selling cloud services
- Private
  - Cloud infrastructure for single org only, may be managed by the org or a 3rd party, on or off premise

Deployment Models

- Community
  - Cloud infrastructure shared by several orgs that have shared concerns, managed by org or 3rd party
- Hybrid
  - Combination of 2 or more clouds bound by standard or proprietary technology

The US National Institute of Standards and Technology (NIST) Cloud Definition Framework



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

Cloud Computing Security

Cloud Computing: A Massive Concentration of Resources

- Also a massive concentration of risk
  - expected loss from a single breach can be significantly larger
  - concentration of “users” represents a concentration of threats
- “Ultimately, you can outsource responsibility but you can’t outsource accountability.”

From John McDermott, ACSAC 09

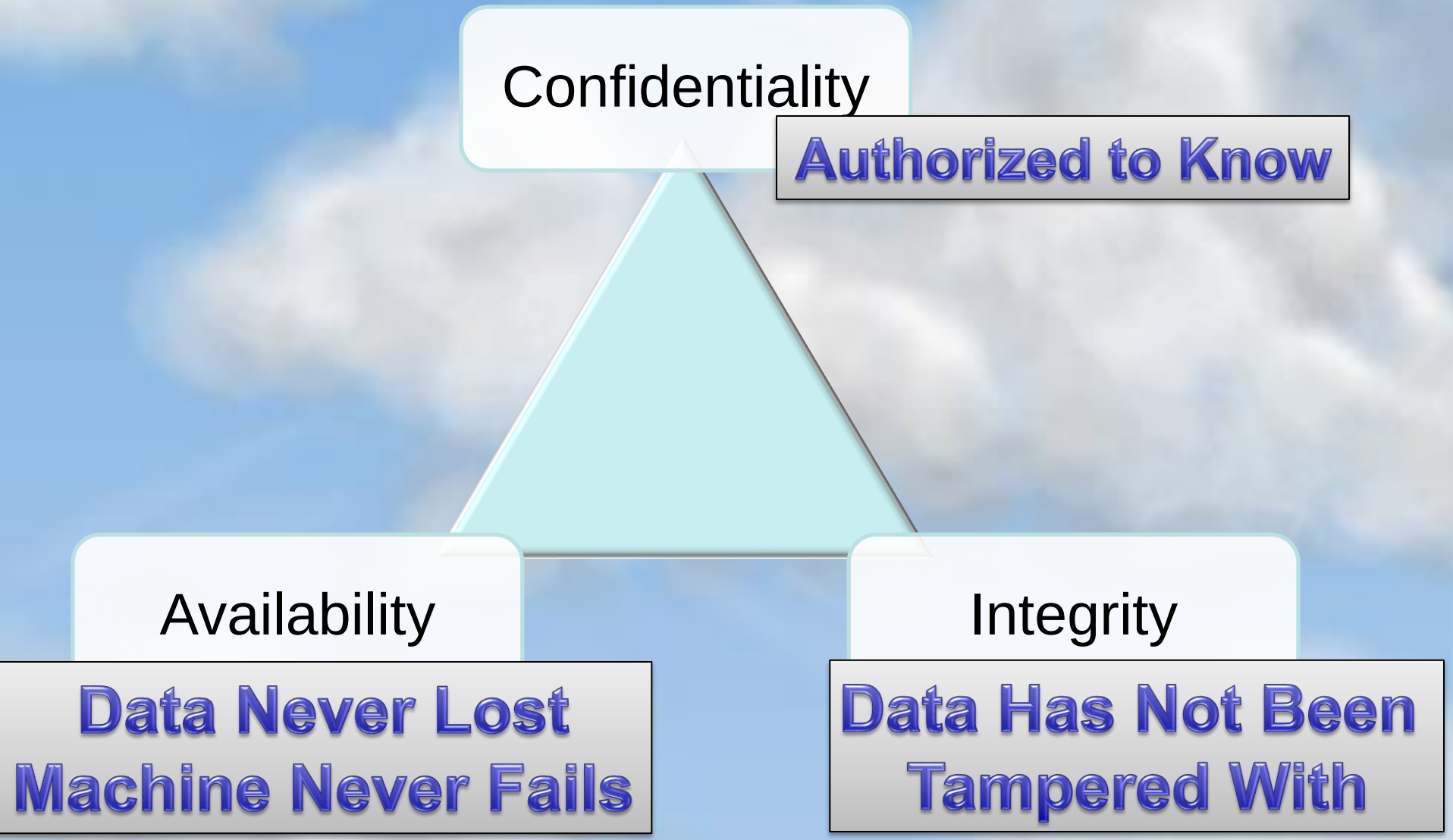
Cloud Computing: who should use it?

- Cloud computing definitely makes sense if your own security is weak, missing features, or below average.
- Ultimately, if
  - the cloud provider's security people are "better" than yours (and leveraged at least as efficiently),
  - the web-services interfaces don't introduce too many new vulnerabilities, and
  - the cloud provider aims at least as high as you do, at security goals,

  then cloud computing has better security.

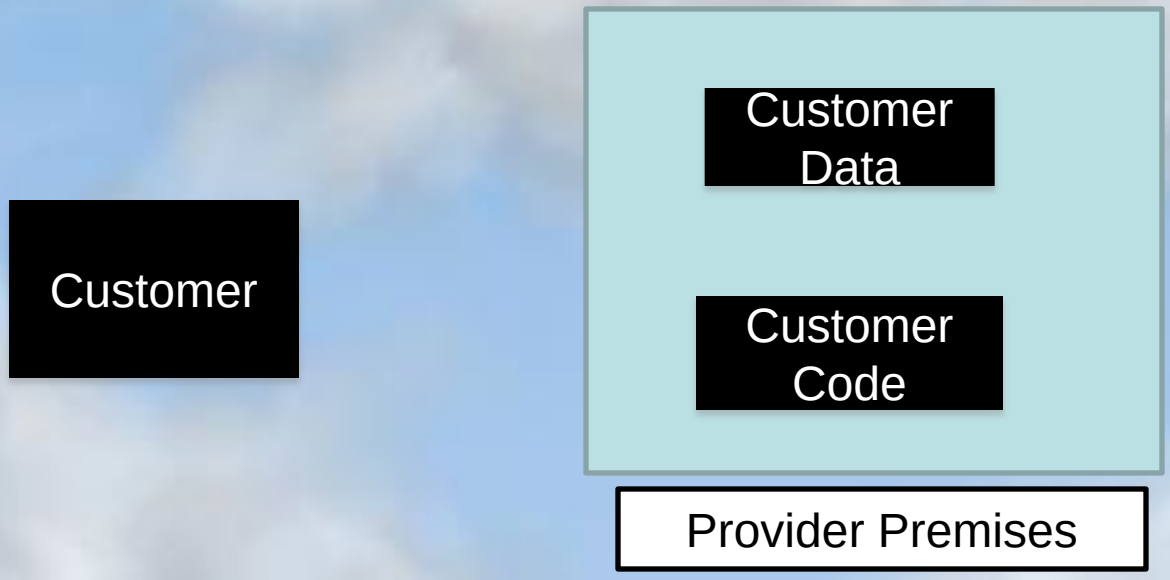
From John McDermott, ACSAC 09

Security Services

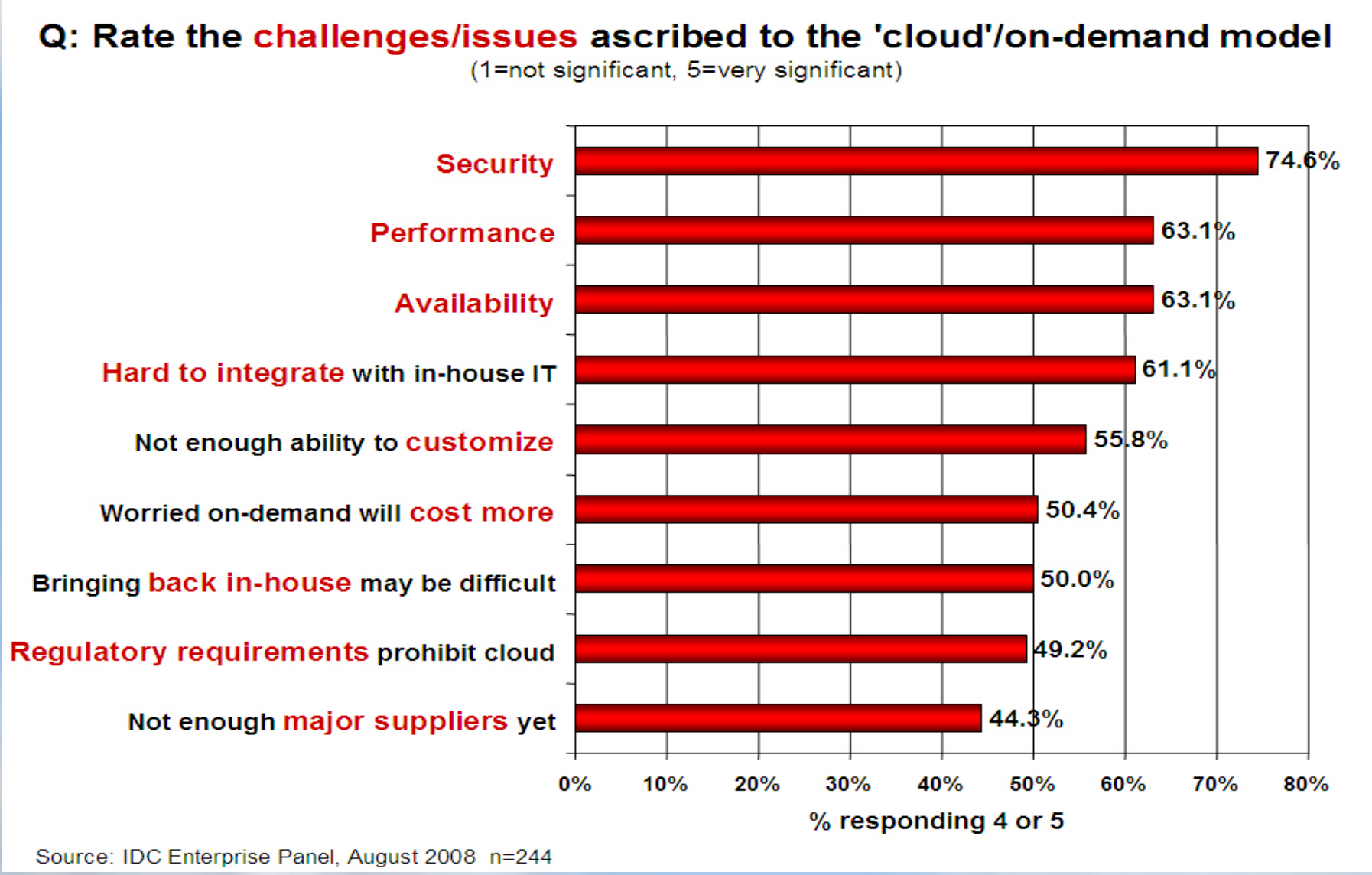


Cloud Security !! A major Concern

- Security concerns arising because both customer data and program are residing at Provider Premises.
- Security is always a major concern in Open System Architectures



Security is the Major Issue



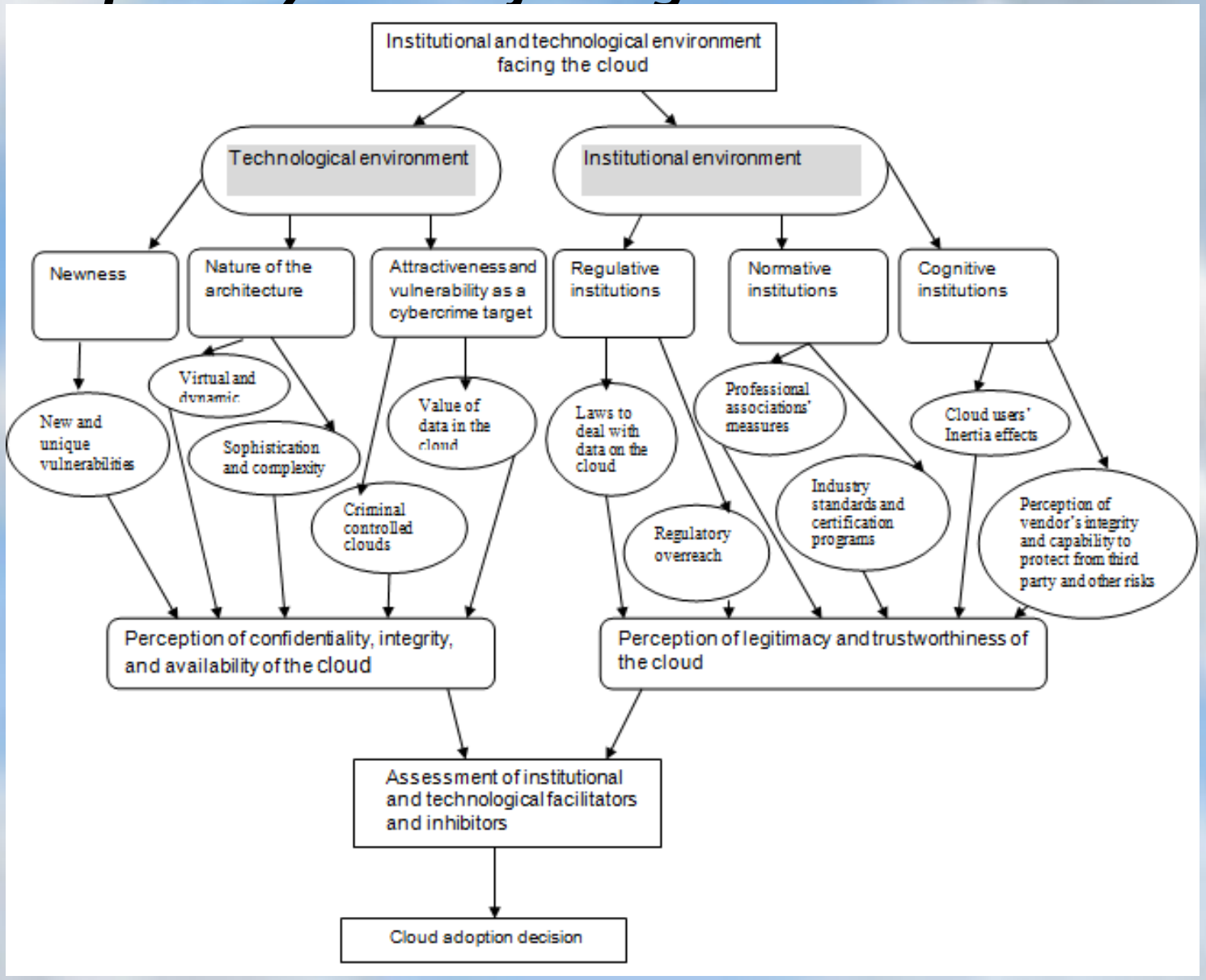
General Security Advantages

- Shifting public data to an external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

General Security Challenges

- Trusting vendor’s security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can’t be examined
- Loss of physical control

A framework for understanding security and privacy issues facing the cloud



Source: Addressing security challenges on a global scale, ITU

Why Cloud Computing brings new threats?

Traditional system security mostly means keeping bad guys out

The attacker needs to either compromise the authentication/access control system, or impersonate existing users

Why Cloud Computing brings new threats?

- Cloud Security problems are coming from :
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

Why Cloud Computing brings new threats?

Consumer's loss of control

- Data, applications, resources are located with provider
- User identity management is handled by the cloud
- User access control rules, security policies and enforcement are managed by the cloud provider
- Consumer relies on provider to ensure
  - Data security and privacy
  - Resource availability
  - Monitoring and repairing of services/resources

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?
- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

What are the concerns?

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

What are the concerns?

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?
  - Often-voiced concern
    - Although cloud providers argue their downtime compares well with cloud user's own data centers

What are the concerns?

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

What are the concerns?

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- The cloud acts as a big black box, nothing inside the cloud is visible to the clients; Clients have no idea or control over what happens inside a cloud
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

Thank You