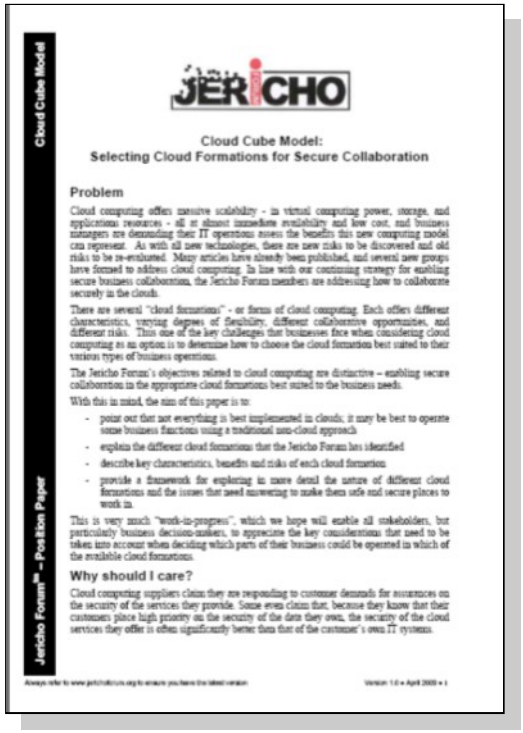
de-risking the cloud through effective risk management

Paul Simmonds, Jericho Forum co-founder & Board Member

JERICHO FORUM

Key Publications


Cloud Cube Model

JERICHO

Cloud Cube Model:
Selecting Cloud Formations for Secure Collaboration

Problem

Cloud computing offers massive scalability - in virtual computing power, storage, and applications resources - all at almost immediate availability and low cost, and business managers are demanding their IT operations assess the benefits this new computing model can represent. As with all new technologies, there are new risks to be discovered and old risks to be re-evaluated. Many articles have already been published, and several new groups have formed to address cloud computing. In line with our continuing strategy for enabling secure business collaboration, the Jericho Forum members are addressing how to collaborate securely in the clouds.

There are several "cloud formations" - or forms of cloud computing. Each offers different characteristics, varying degrees of flexibility, different collaborative opportunities, and different risks. This one of the key challenges that businesses face when considering cloud computing as an option is to determine how to choose the cloud formation best suited to their various types of business operations.

The Jericho Forum's objectives related to cloud computing are distinctive – enabling secure collaboration in the appropriate cloud formations best suited to the business needs.

With this in mind, the aim of this paper is to:

- point out that not everything is best implemented in clouds; it may be best to operate some business functions using a traditional non-cloud approach
- explain the different cloud formations that the Jericho Forum has identified
- describe key characteristics, benefits and risks of each cloud formation
- provide a framework for exploring in more detail the nature of different cloud formations and the issues that need answering to make them safe and secure places to work in.

This is very much "work-in-progress", which we hope will enable all stakeholders, but particularly business decision-makers, to appreciate the key considerations that need to be taken into account when deciding which parts of their business could be operated in which of the available cloud formations.

Why should I care?

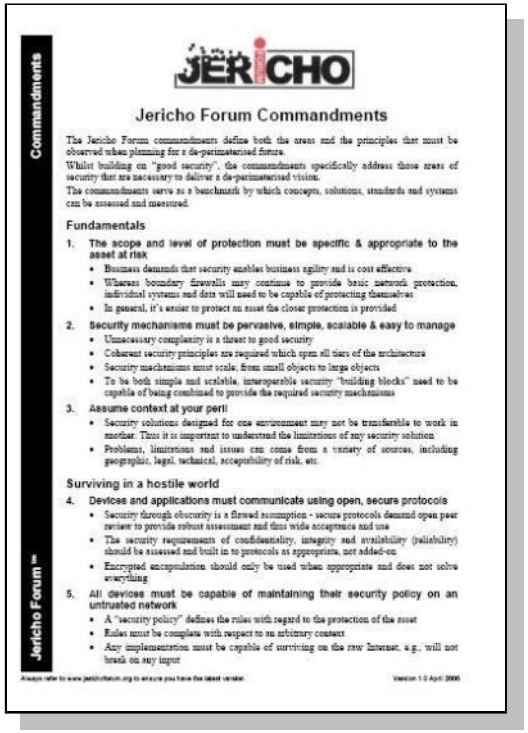
Cloud computing suppliers claim they are responding to customer demands for assurances on the security of the services they provide. Some even claim that, because they know that their customers place high priority on the security of the data they own, the security of the cloud services they offer is often significantly better than that of the customer's own IT systems.

Jericho Forum™ – Position Paper

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 • April 2009 • 1

Cloud Cube


Commandments

JERICHO

Jericho Forum Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterised future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterised vision.

The commandments serve as a benchmark by which concepts, solutions, standards and systems can be assessed and measured.

Fundamentals

1. **The scope and level of protection must be specific & appropriate to the asset at risk**
   - Business demands that security enables business agility and is cost effective
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
   - In general, it's easier to protect an asset the closer protection is provided
2. **Security mechanisms must be pervasive, simple, scalable & easy to manage**
   - Unnecessary complexity is a threat to good security
   - Coherent security principles are required which span all tiers of the architecture
   - Security mechanisms must scale; from small objects to large objects
   - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms
3. **Assume context at your peril**
   - Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution
   - Problems, limitations and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a hostile world

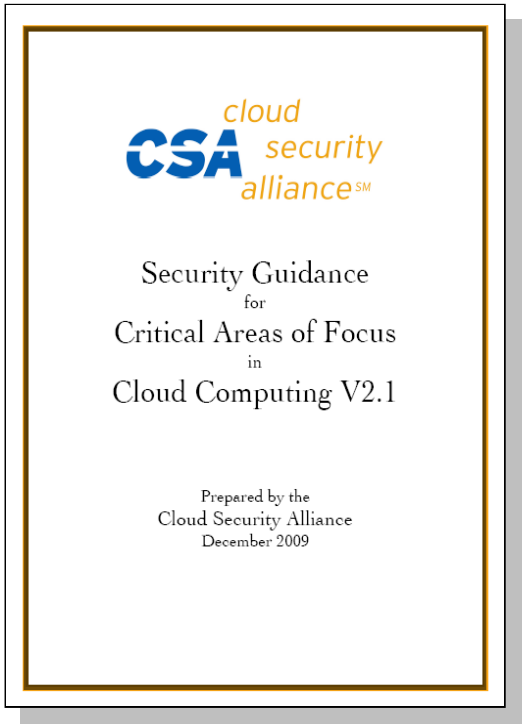
4. **Devices and applications must communicate using open, secure protocols**
   - Security through obscurity is a flawed assumption - secure protocols demand open peer review to provide robust assessment and then wide acceptance and use
   - The security requirements of confidentiality, integrity and availability (reliability) should be assessed and built in to protocols as appropriate, not added-on
   - Encrypted encapsulation should only be used when appropriate and does not solve everything
5. **All devices must be capable of maintaining their security policy on an untrusted network**
   - A "security policy" defines the rules with regard to the protection of the asset
   - Rules must be complete with respect to an arbitrary context
   - Any implementation must be capable of surviving on the raw Internet, e.g., will not break on any input

Jericho Forum™

Always refer to www.jerichoforum.org to ensure you have the latest version

Version 1.0 April 2006

Jericho Forum Commandments


cloud security alliance℠

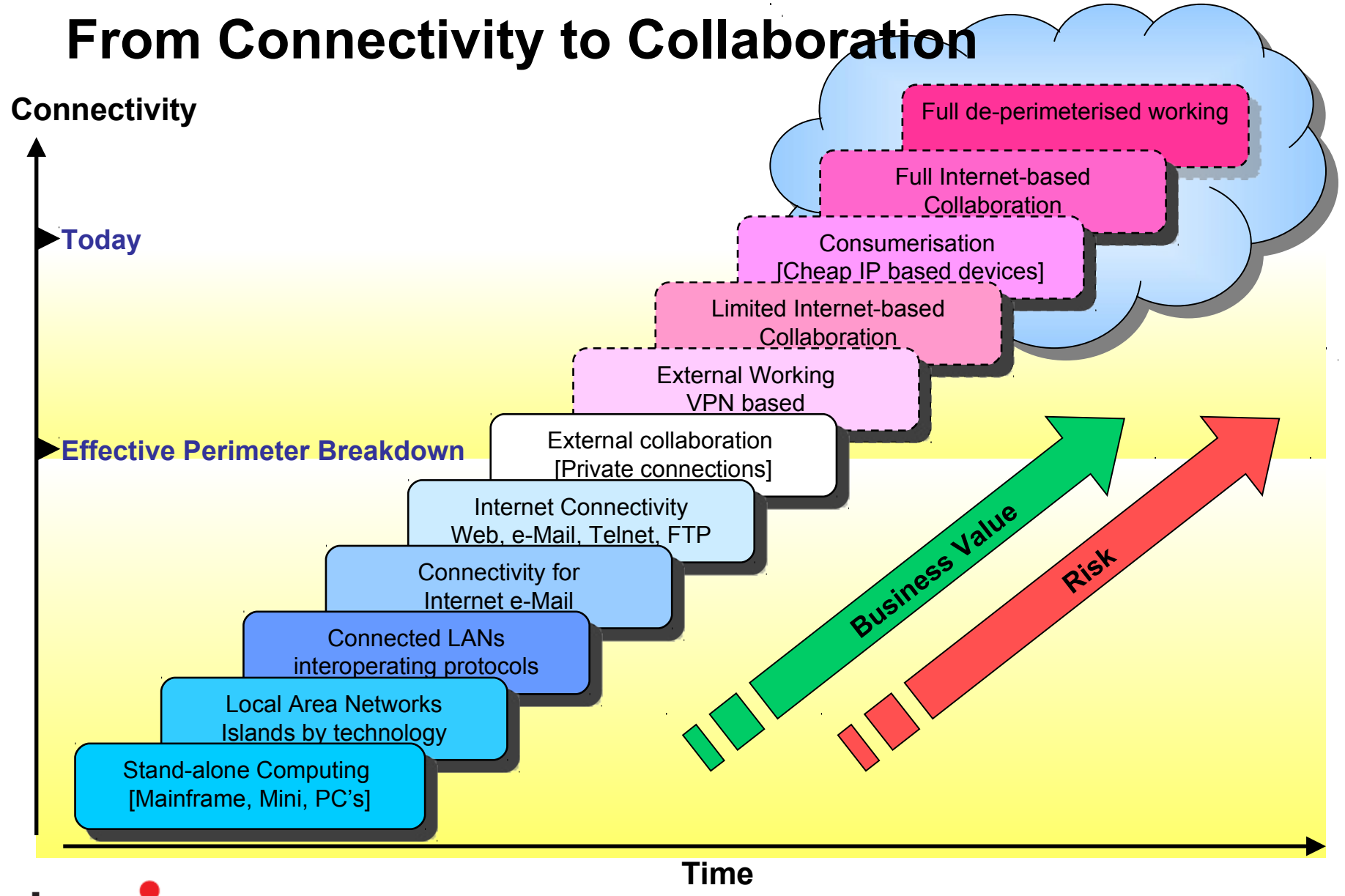
Security Guidance
for
Critical Areas of Focus
in
Cloud Computing V2.1

Prepared by the
Cloud Security Alliance
December 2009

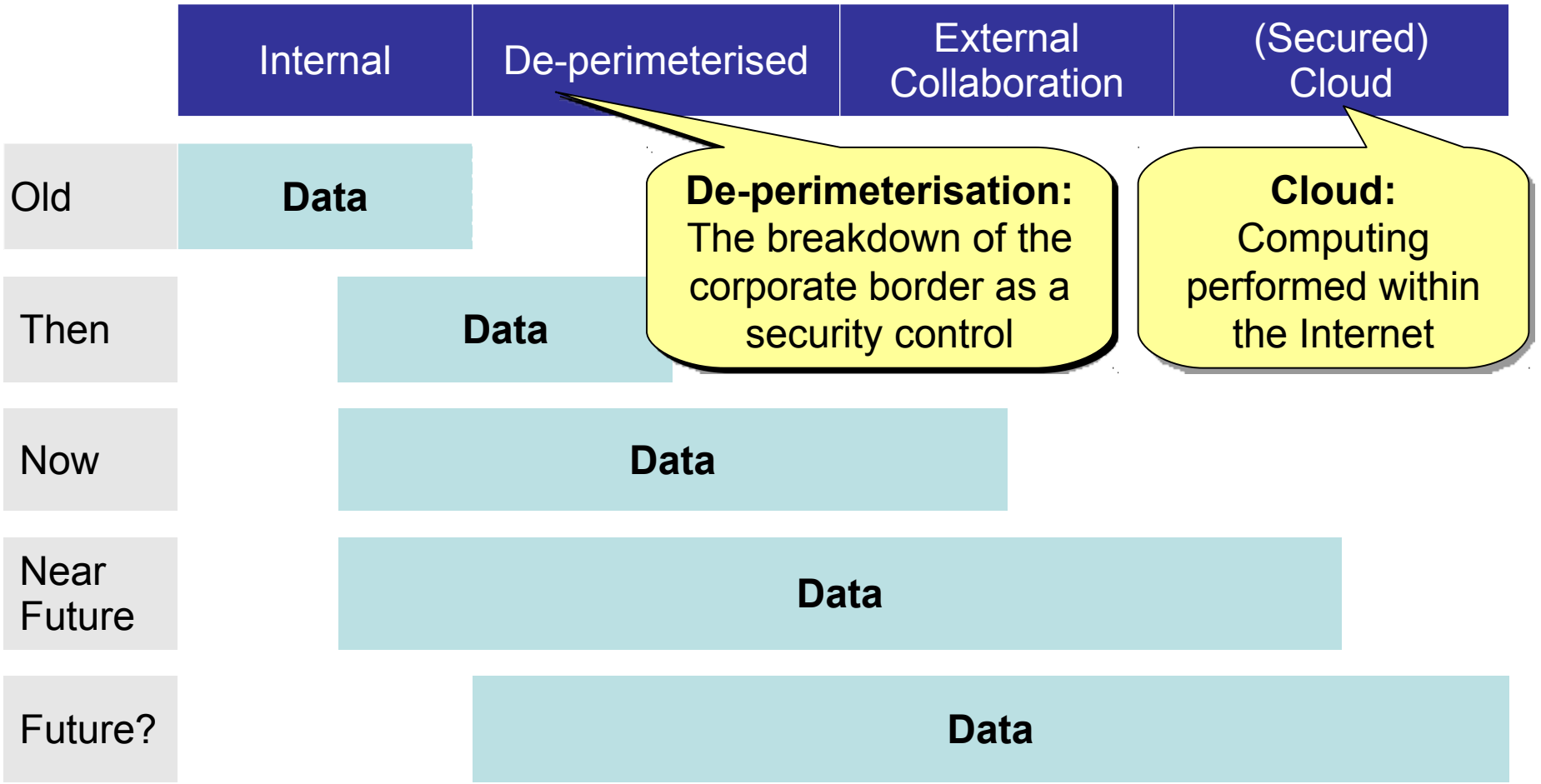
CSA Security Guidelines 2.1

JERICHO FORUM

From Connectivity to Collaboration



Understanding the externalisation of data



The security of the network becomes increasingly irrelevant, and the security and integrity of the data becomes everything.

JERICHO FORUM

"The perimeter going away?
That's baloney.....
The perimeter cannot go away and does not get less important in the future."

John Pescatore, Gartner, 2005[1]

1. www.networkworld.com/news/2005/070405perimeter.html

Digital Natives

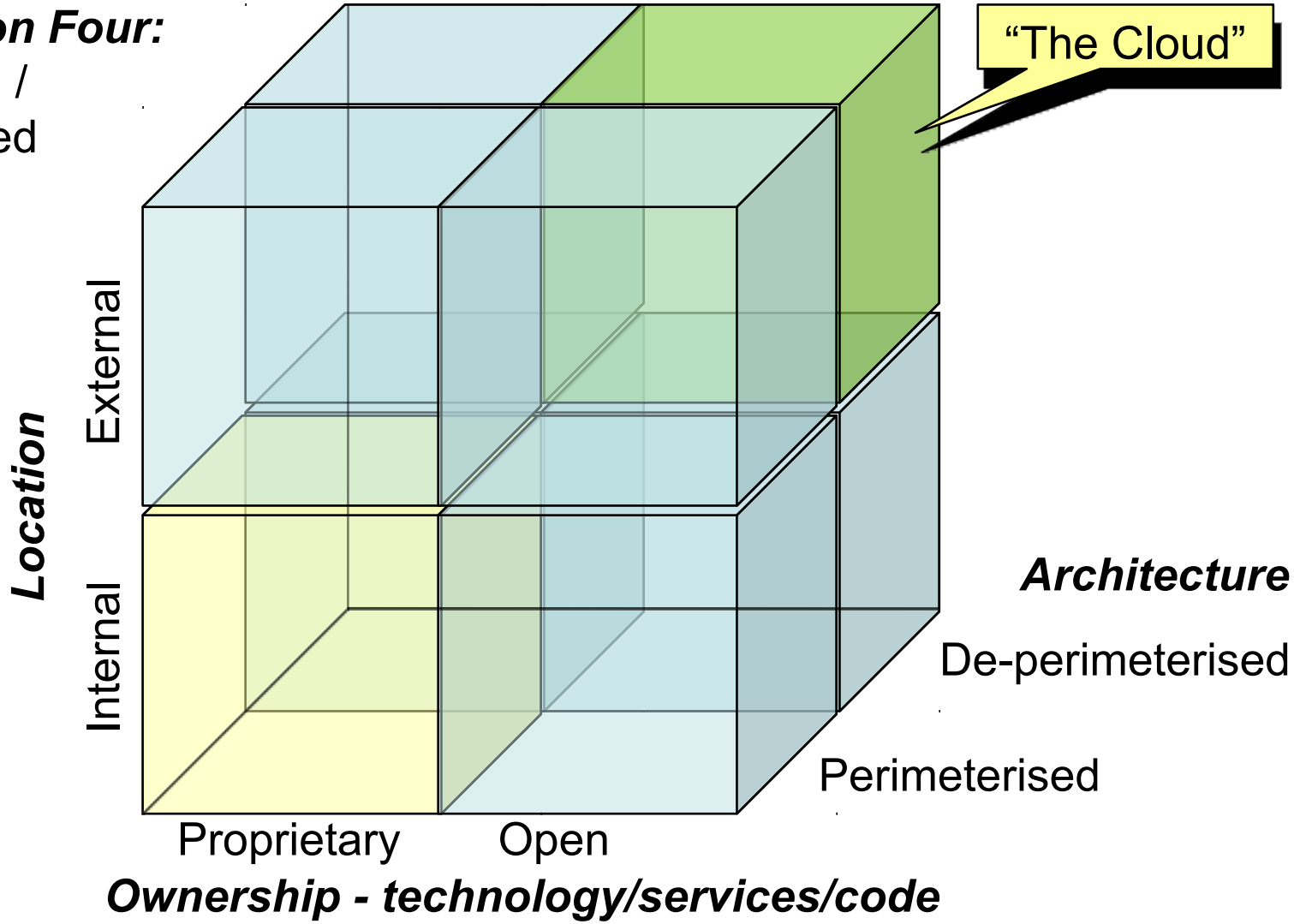
- New expectations from both employer and employee
- Charateristics for generation Y/M:
  - Individualists
  - Sceptic on authorities
  - Grown up with IT/Internet
  - IT is a social tool
- Collaboration is the norm
- Expectation of ”always-on”
- Just find it on the Web.
- More consumer software

Why Cloud?

- Logical conclusion of the business direction
- Cheap
- Fast to market
- Little capital investment (true cloud)
  - Start-ups
  - African virtual mobile operators
- Great for “off-load computing”

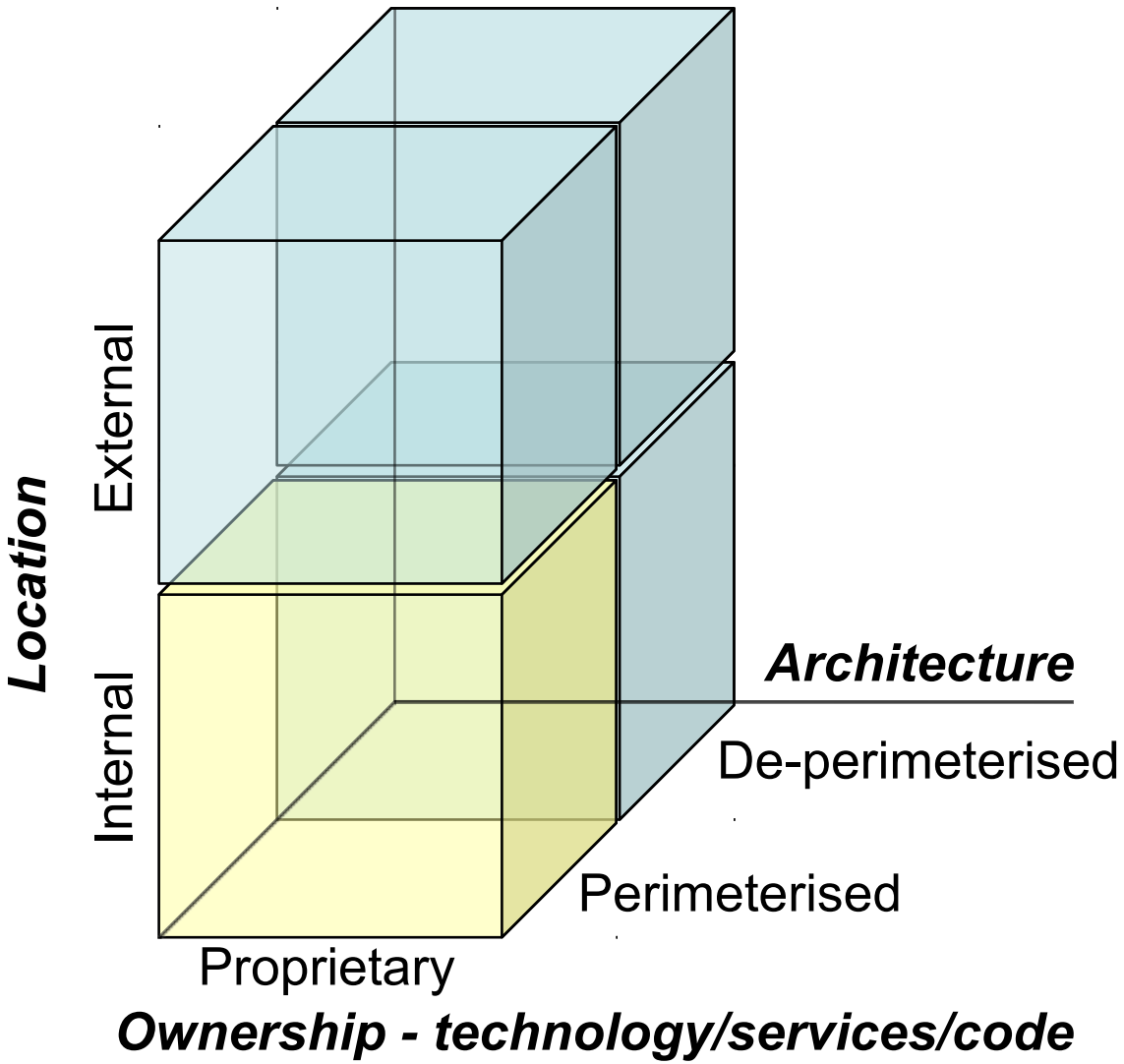
Jericho Forum Cloud Cube Model

Dimension Four:
Insourced /
Outsourced



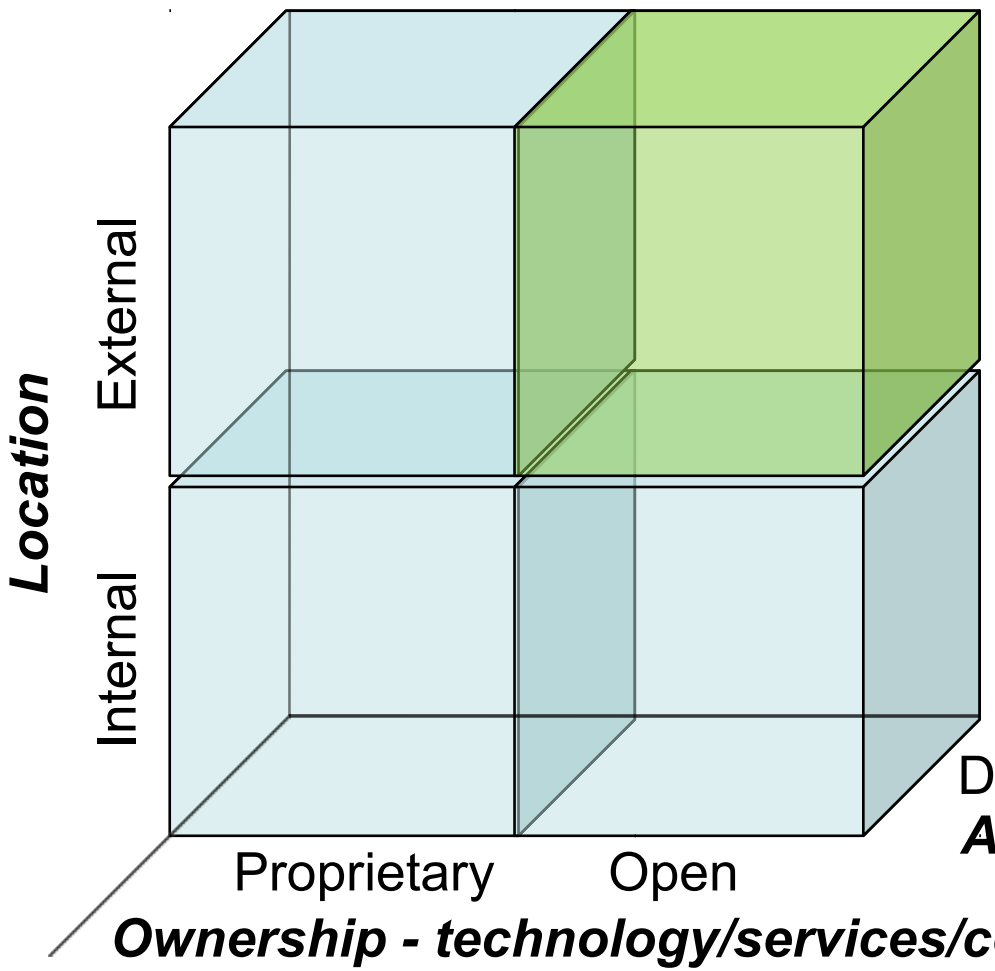
JERICHO FORUM

Cloud Cube – Proprietary Axis - Risks



- Vendor Lock-in
- Reliance on vendor APIs
- Difficulty in collaborating?
- Proprietary standards?
- Proprietary software?
- Process-as-a-Service Solutions
- SaaS Solutions

Cloud Cube – De-perimeterised Axis - Risks



- Lack of open & secure standards
- Reliance on vendor APIs
- Issues extending Identity into cloud
- Lack of shared identity standards

Clouds & the Cloud Cube model

- The ‘commandments’ still valid for the cloud

- Hybrid Computing will be the norm
  (a mix of traditional and various cloud computing)
  - Private Clouds are Perimeterised
  - Collaborative Clouds are best de-perimeterised

- Select one of the eight types with care!

The Cloud Identity Crisis

- The Cloud won't take off fully without appropriate Identity Management and Access Management
- Private Clouds will be able to take advantage of the old Perimeterised Identity and Entitlement & Access Management models
- Collaborative Clouds will need a significant shift from Enterprise Centric security to User Centric Security
- Clouds also will benefit greatly from the shift from;
  - Access by Lists (Role-based Access Control), to;
  - Access by Assertions [Claims] (Rules-based Access Control)

Future Research

- RSA 2010 Awards
  Excellence in the Field of Mathematics
- Dr. David Chaum developed a cryptography research group at the Center for Mathematics and Computer Science (CWI) in Amsterdam. During that time Dr. Chaum founded DigiCash, which pioneered electronic cash innovation.
  Dr. Chaum's contributions to cryptography include the invention of two anonymity networks – mix networks, the basis for virtually all modern anonymity networks and DC-Nets, including the invention of partial key techniques and the invention of cryptographic voting.

Risk Based Access

- Current access methods
  - Do not support business needs / granularity
  - Do not support “real” cloud working
  - Do not support the move the securing the data
- Trust but verify
  - Basic trust models for devices & users do exist

  But;
  - How do you verify environments you do not own?
  - How do you verify that environments you do not own are cleaned up after use?

Granular Access:
Access granted dependent on attributes and rules, not binary on Username

Martini model[1]: Any IP, any device, any time, anywhere

Risk Based Access

Logical / Data Access

Rules Based Access

Physical Access

Data and/or System

Data Attributes:
- Location?
- Classification
- AD Group
- etc.

Rules based access:
Using a mix of attributed, based on risk assessment

Device Attributes
- User Credentials
  - Classification of User
  - AD Group
  - Credential strength
- Location
  - IP-Address
  - Geo-location
  - GPS / GPRS
- Device Information
- Corporate Credentials
- Corp. Managed Device
- Functionality Required
- Functionality Offered
  - Sandbox
  - Secure container
- Cleanliness of device

1. Multiple Access Real Time IP Network Implementation

Conclusions

- De-perimeterisation still a relevant topic with plenty to be highlighted and addressed
- Commandments are both relevant and still relevant as we move to cloud issues
- There is a shift from
  Enterprise Centric to
  User Centric IAM
- Shift needed from
  RBAC & ACL's to
  Claims based access