Clouds Forecast

Doing business beyond the perimeter

- **Andrew Yeomans**
  Jericho Forum Board

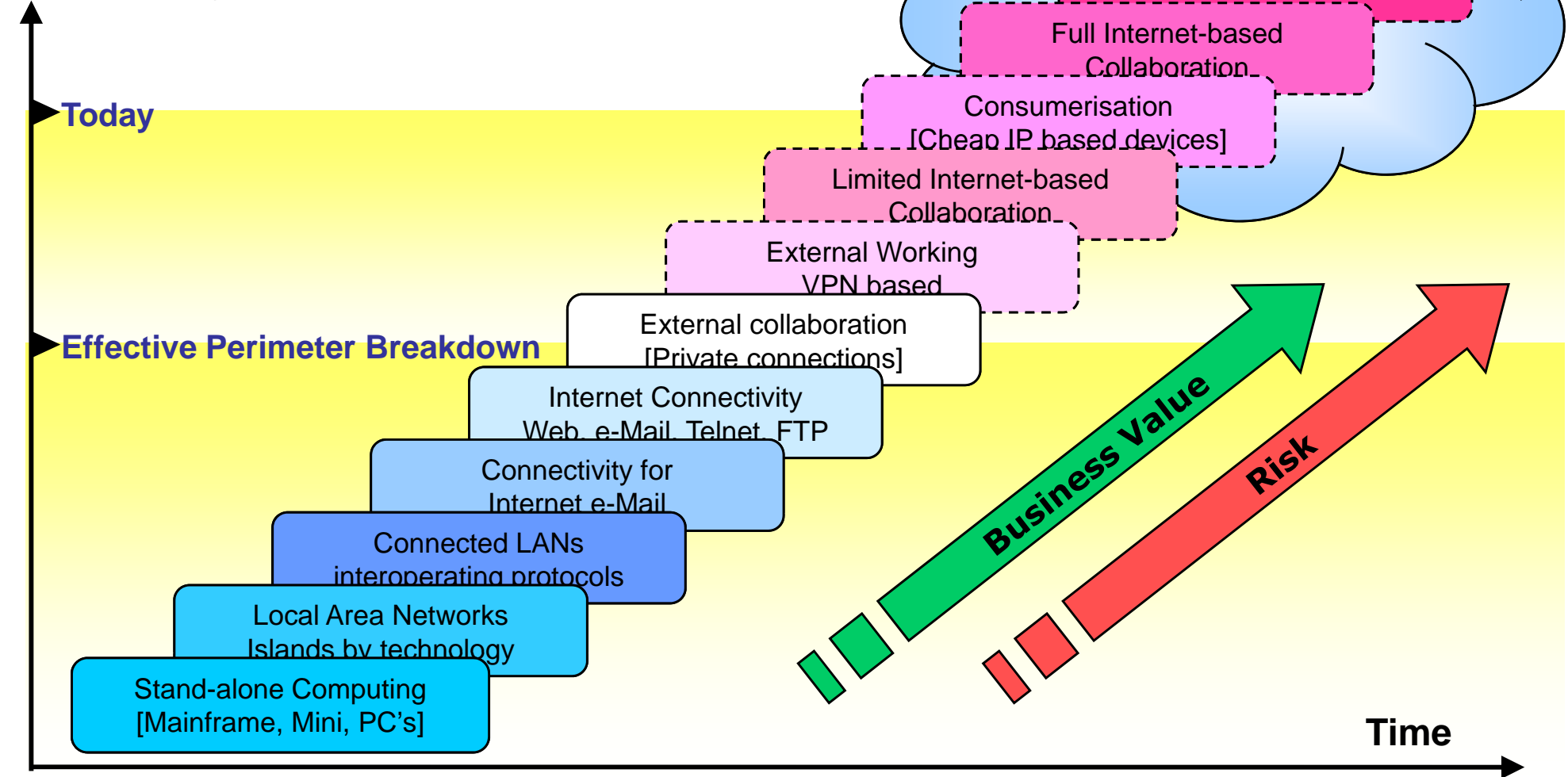# A brief introduction to the Jericho Forum

- The Jericho Forum aims to drive and influence development of security standards that will meet future business needs
- These standards will:
  - Facilitate the secure interoperation, collaboration and commerce over open networks
  - Be based on Collaboration Oriented Architectures (COA) and design approach entitled "de-perimeterization".
- Globally, more than fifty blue-chip user organisations, from all sectors, are working together to solve the problems posed by de-perimeterization
- The Open Group hosts the Jericho Forum
- Everything published is free and open-source.

Some of our members

From Connectivity to Collaboration

Connectivity

Today

Effective Perimeter Breakdown

Full de-perimeterized working

Full Internet-based Collaboration

Consumerisation
[Cheap IP based devices]

Limited Internet-based Collaboration

External Working
VPN based

External collaboration
[Private connections]

Internet Connectivity
Web, e-Mail, Telnet, FTP

Connectivity for
Internet e-Mail

Connected LANs
interoperating protocols

Local Area Networks
Islands by technology

Stand-alone Computing
[Mainframe, Mini, PC's]

Business Value

Risk

Time

Clouds – cheaper?

1400 users	Google	Exchange
Hardware	0	$20,000
Software	0	$138,314
Labour	$3,842	$119,130
Up-front total	$3,842	$277,444
Licences	$70,000	0
Maintenance	0	$37,578
Labour	$23,142	$78,744
Annual cost	$93,142	$116,322
3-year cost	$283,268	$626,411

Caution – figures from Google!

ITPRO
FIT FOR BUSINESS

Home | Security | Mobile & Telecoms | Internet | Server | Netw

In this channel: News Features Reviews How Tos & Tutorials

Home : Client : News

Telegraph swaps Microsoft Office for Google Apps

The newspaper publisher is moving 1,400 seats away from Microsoft Office in favour of Google's web-based application suite.
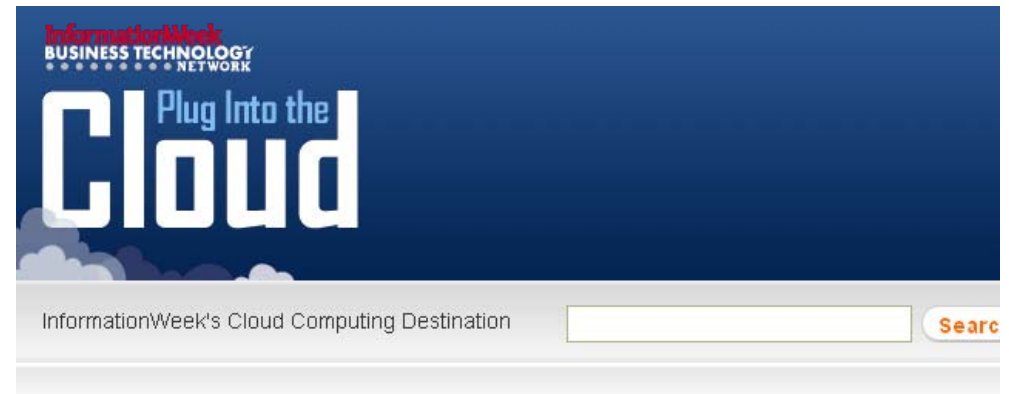By Miya Knights, 16 Jul 2008 at 17:53

The **Telegraph Media Group** (TMG) has become the latest corporate customer for Google's hosted office suite **Google Apps Premier Edition**.

The publisher of *The Daily Telegraph* will migrate 1,400 seats over to Google's enterprise version of its business productivity software before the end of this year, after successfully completing a trial with 10 per cent of its users during May and June.

Clouds – faster?

- "a new server can be up and running in three minutes (it used to take Eli Lilly seven and a half weeks to deploy a server internally) and a 64-node Linux cluster can be online in five minutes (compared with three months internally)"

Clouds – inside your data centre?

Technology	Cost in Medium-sized DC	Cost in Very Large DC	Ratio
Network	$95 per Mbit/ sec/ month	$13 per Mbit/ sec/ month	7.1
Storage	$2.20 per GByte / month	$0.40 per GByte / month	5.7
Administra-tion	140 Servers / Admin	>1000 Servers / Admin	7.1

Clouds – greener?

Price per KWH	Where	Possible reasons why
3.6¢	Idaho	Hydroelectric power; not sent long distance
10.0¢	California	Electricity transmitted long distance over the grid; limited transmission lines in Bay Area; no coal fired electricity allowed in California.
18.0¢	Hawaii	Must ship fuel to generate electricity

http://www.eia.doe.gov/neic/rankings/stateelectricityprice.htm

Cloud future – design your network
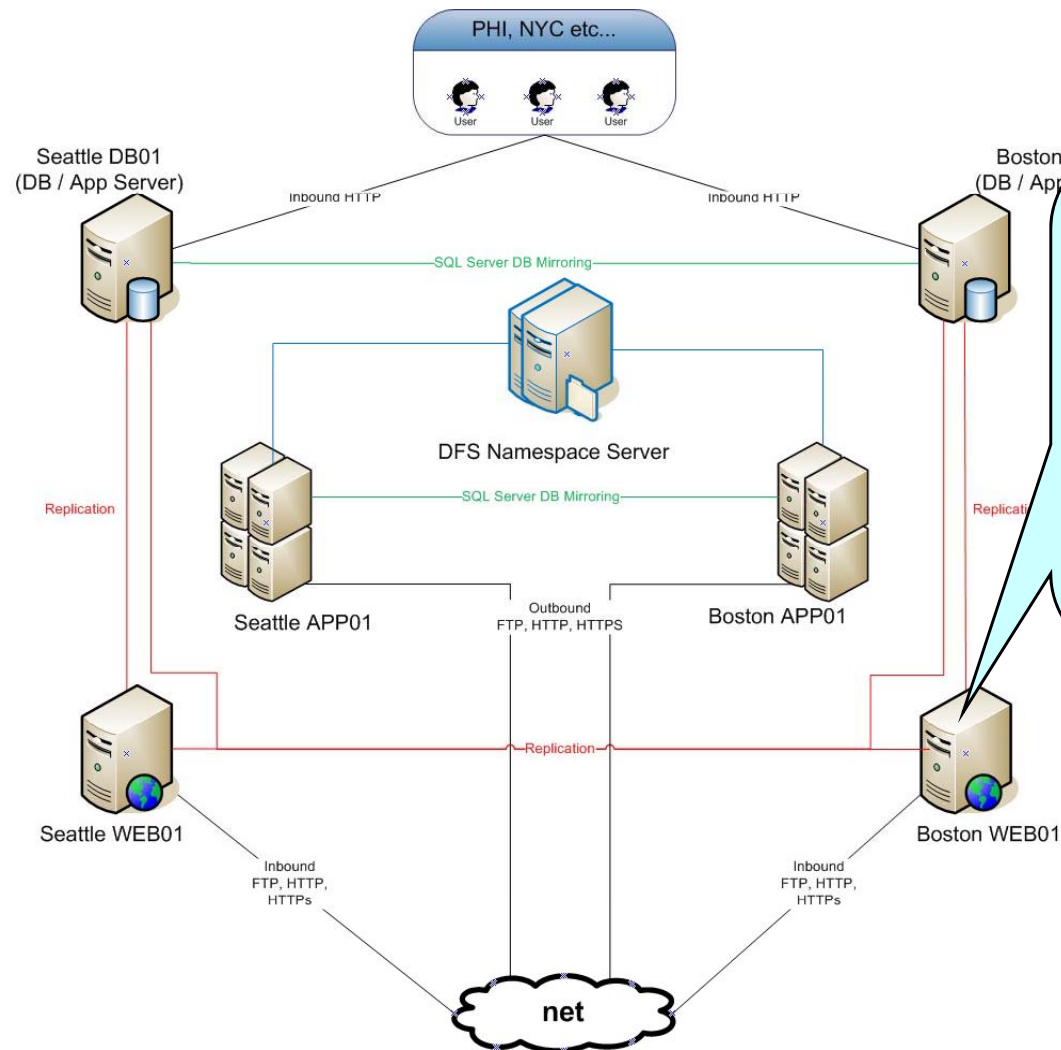
Clouds for risk mitigation

- "Black Swan" events
- BCP too expensive?
- Off-site backup
- Pay as you go

Relative Impact

Pandemic Influenza

Coastal Flooding

Major Industrial Accidents

Inland Flooding

Attacks on Crowded Places

Attacks on Critical Infrastructure

Attacks on Transport

Major Transport Accidents

Non-conventional Attacks*

Severe Weather

Animal Disease

Electronic Attacks

Relative Likelihood
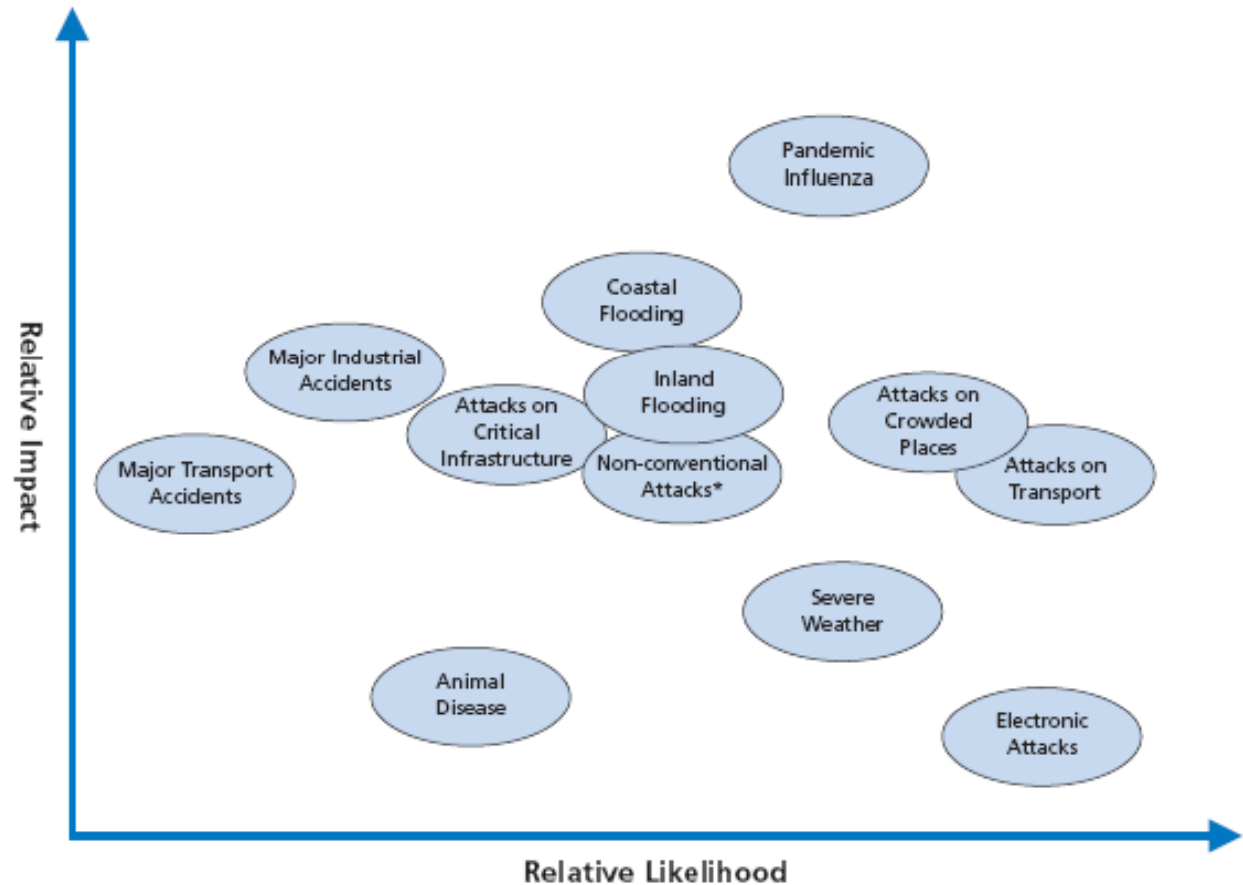
UK Cabinet Office – National Risk Register

Thunder clouds – the problems

- Inertia – why change?
- Availability – outages?
- Lock-in – how to get my data out again?
- Confidentiality – who else can see it?
- Auditability – and can you prove that?
- Jurisdiction – who can get to the data?
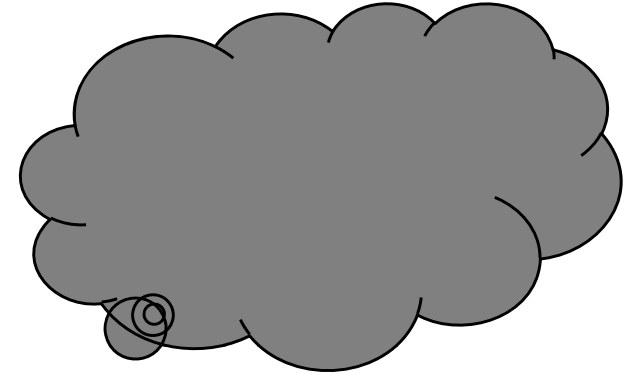
Confidentiality in clouds

Risk Control Acceptance Curve

Risk Control Levels

<1%

14%

85%

Ratios closer to data volumes

JERiCHO
FORUM
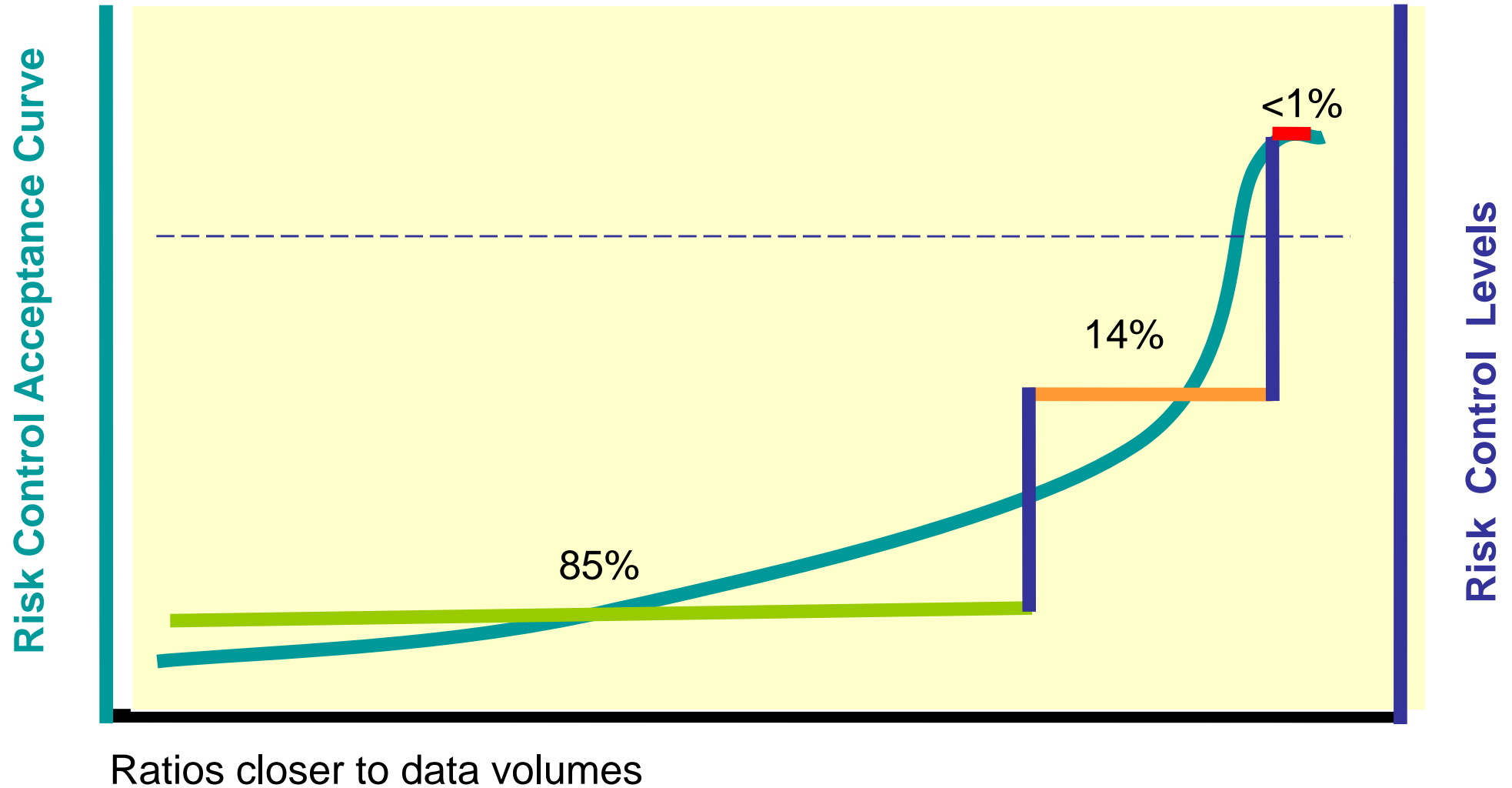
Data protection choice is easy!

- In IT systems we have two main protection methods:
  - Encryption (or not)
  - Access controlled (or not)

Encrypted Uncontrolled	Encrypted Controlled access
Unencrypted Uncontrolled	Unencrypted Controlled access

JERiCHO FORUM

Three Laws of Data Encryption

- Based on Rich Mogull:

- 1. External loss - Encryption for media protection – if the data moves, physically or virtually. Simple key management.

- 2. Internal access - Encryption to restrict privileged access (sometimes misnamed separation/segregation of duties). Complex key management if really works.

- 3. Mandated encryption (e.g. PCI)

Two other forms of protection

- **Protect by monitoring**
  - Can't always have technical controls
  - Monitor for policy violations
  - Advertise to reduce temptations
  - Results from "DLP" can steer Data Classification and create dialogue with business
- **Protect by destroying!**
  - The best form of confidentiality
  - Data Retention policies

But it must be manageable

- **Missing – an open format for data protection (c.f. DRM**
- **Key management standards**
- **Missing - Open authentication**
- **Data zones**
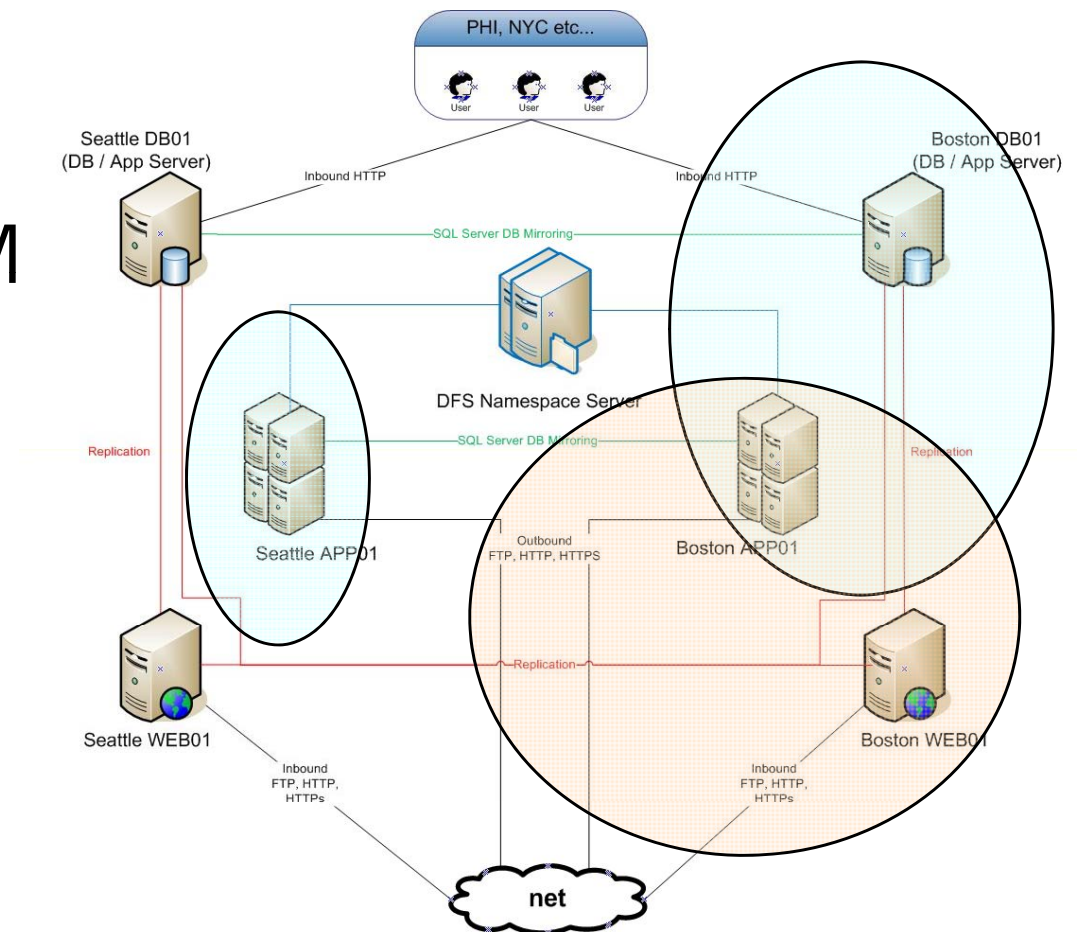
A look to the future - OpenEIPC

- Missing – an open format for data protection (c.f. DRM)

- Strawman – ZIP + XACML

- Also works for ODF and OOXML

- Scope and level appropriate to asset at risk

Mimetype
Pictures/1001.png
Pictures/1002.png
content.xml hCTqkH557Q6yeIh uz+kbOfADzas2om qWD3USq4HOjh/s yMeHVH
styles.xml
meta.xml
eipc.xml
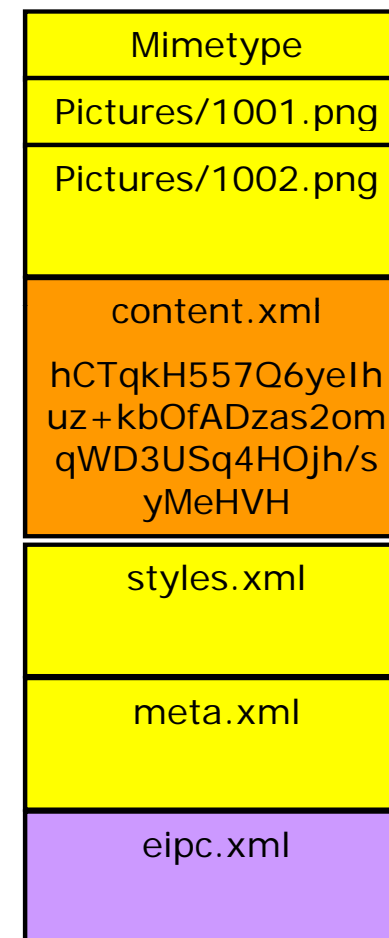
Are clouds the right shape?

Cloud Computing: The Business View

Enable Value

Control Processes

Wiki's
Blogs
Readers
Collab eMail
Workflow
IM
+,more
COA
P
E
Enterprise
R
D
I
Devices
People
Risk
Information

Adrian Secombe
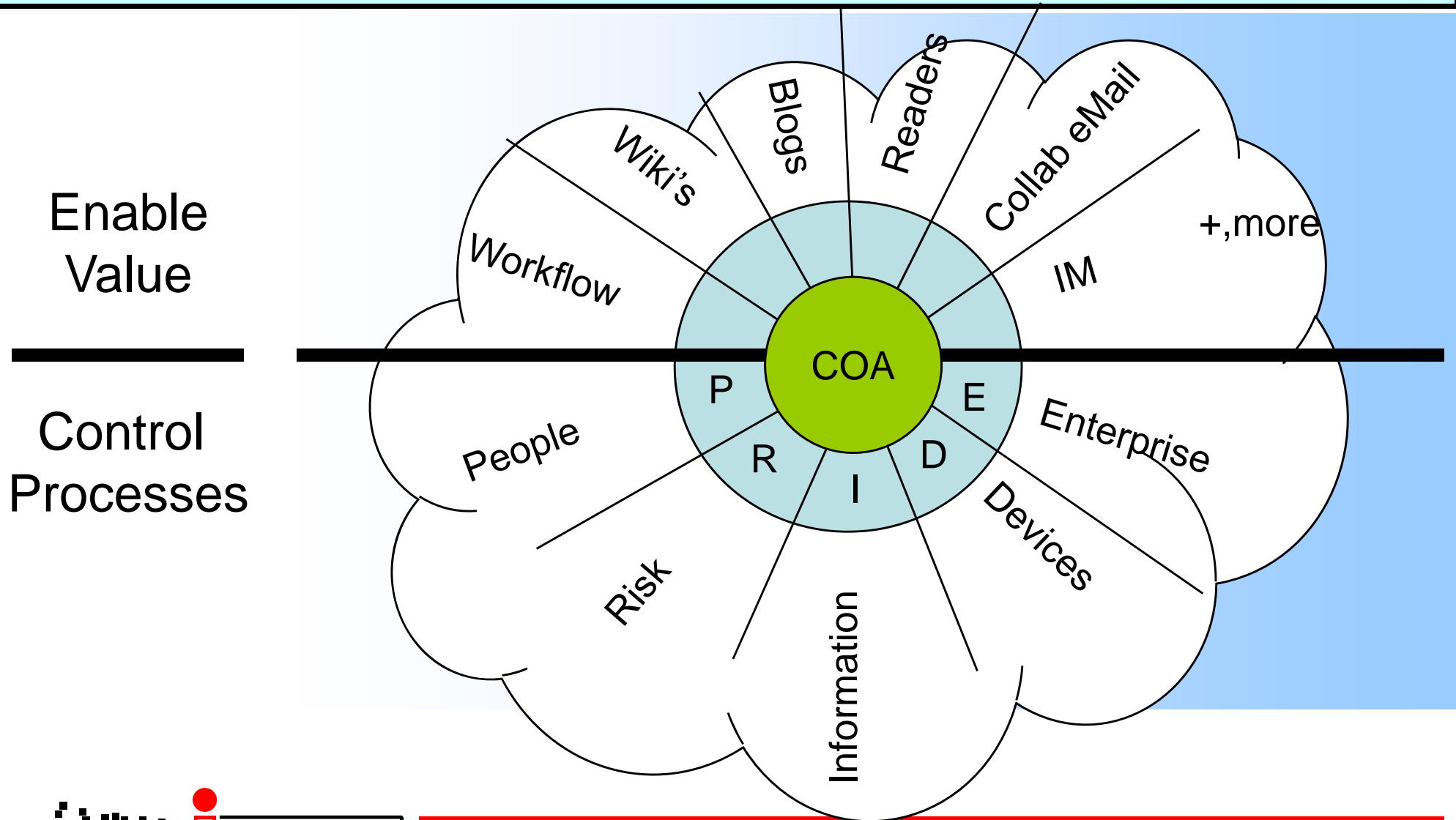
Cloud Computing: The Technical View

Enable Value

Control Processes

SLATES

- Authorship
- Links
- Tags
- Extensions
- Signalling
- Search
- S L A T E S
- COA
- IdAM
- Data Integration
- Orchestration
- Security
- Admin
- Information and Record Lifecycle
- Audit
- Device Trust

SLATES are defined by Andrew McAfee

Adrian Secombe
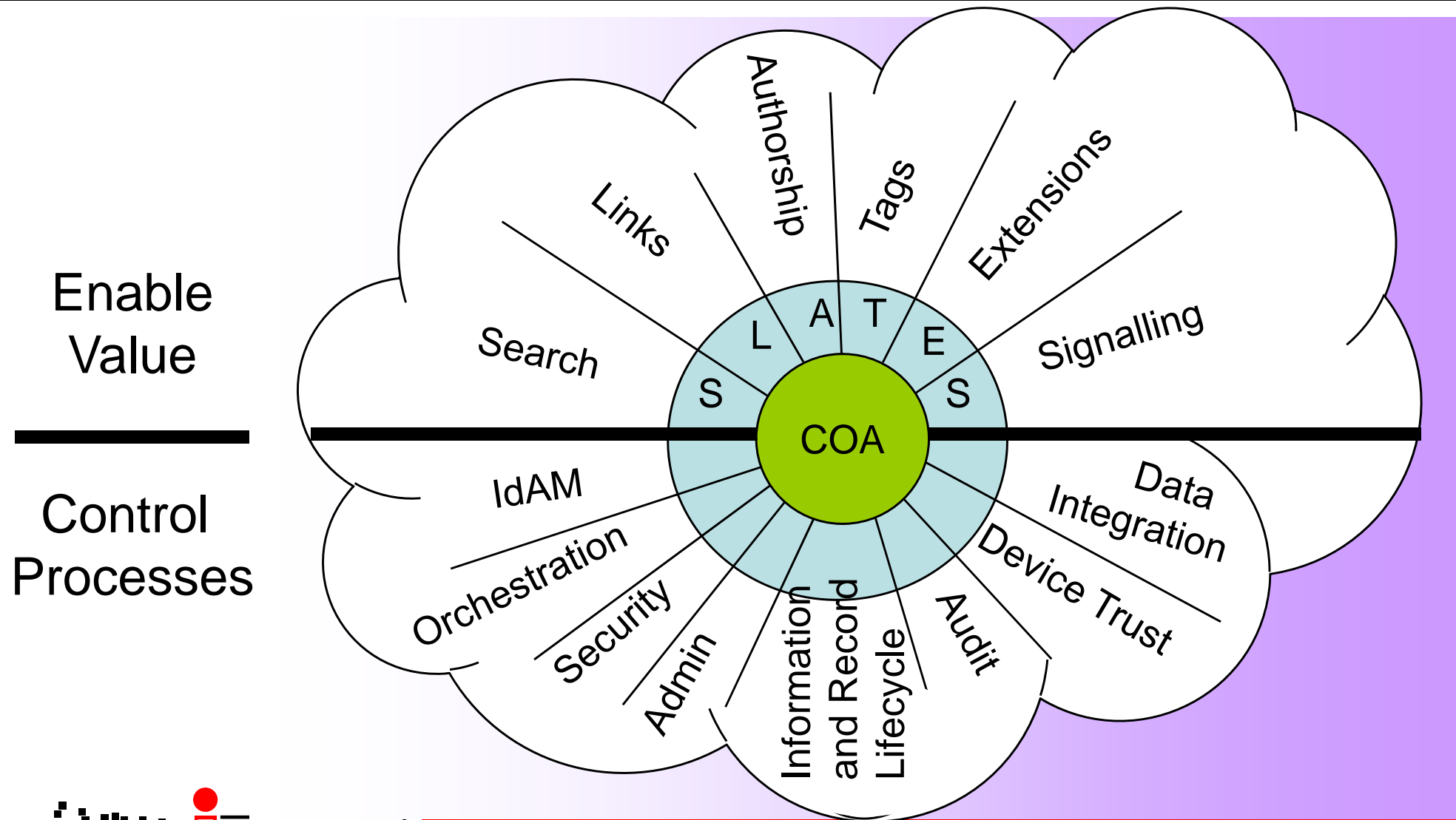
Components of Collaboration Oriented Architectures

Principles
- Known parties
- Assurance
- Trust
- Risk
- Compliance
- Legal, Regulatory, Contractual
- Privacy

Technologies
- End Point Security/Assurance
- Secure Communications
  - Secure Protocols
- Secure Data/Information
  - Content Monitoring
  - Content Protection

Processes

People
Risk
Information
Devices
Enterprise

Services
- Federated Identity
- Policy Management
- Data/Information Management
- Classification
- Audit

Solution Attributes
Usability/Manageability
Availability
Efficiency/Performance
Effectiveness
Agility

Security Questions

Where is my data?

What due diligence did my employees do prior to using the service?

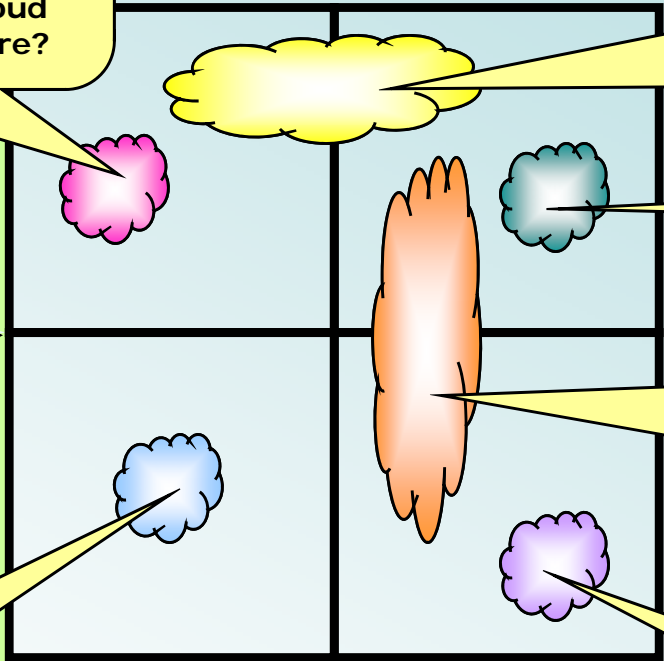**What leaks are there from the cloud service back into my infrastructure?**

Who is responsible if something goes wrong?

What about business continuity?

How does my data securely enter and exit the cloud?

External

How is my data protected in transit?

Distinction Fades as Virtualisation Increases

Internal

Who has access to my data?

What about export and Privacy laws?

How is the EXT/INT interface managed?

Perimeterised **De-perimeterised**

Will I be able to deliver?
Do I have the skills?
Do I have the resources?
Can do I recover costs?

Distinction Fades as Collaboration Increases

Can the Outsourcer integrate into my infrastructure?

JERICHO FORUM

Interoperability Questions

What if I need to switch vendors?

What if my collaboration partner uses a different vendor?

Do I have to implement proprietary interfaces to do business with the provider?

Is this where I want to be? Do I still need internal cloud services?

External

Distinction Fades as Virtualisation Increases

Internal

Will this allow me to leverage multiple cloud service providers to jointly perform a task?

Will it further enable collaboration among multiple partners?

Proprietary   **Open**

When I run out of resources can I engage an external cloud service provider?

Distinction Hinders Collaboration

What standards should be developed?

Who should control them?

JERiCHO

Cloud Shape Architecture Model

External

Where is your data ?

Internal

Is data collaboratively shared ?

De-perimeterised

Perimeterised

Proprietary   Open

Are the interfaces public ?

Adrian Secombe
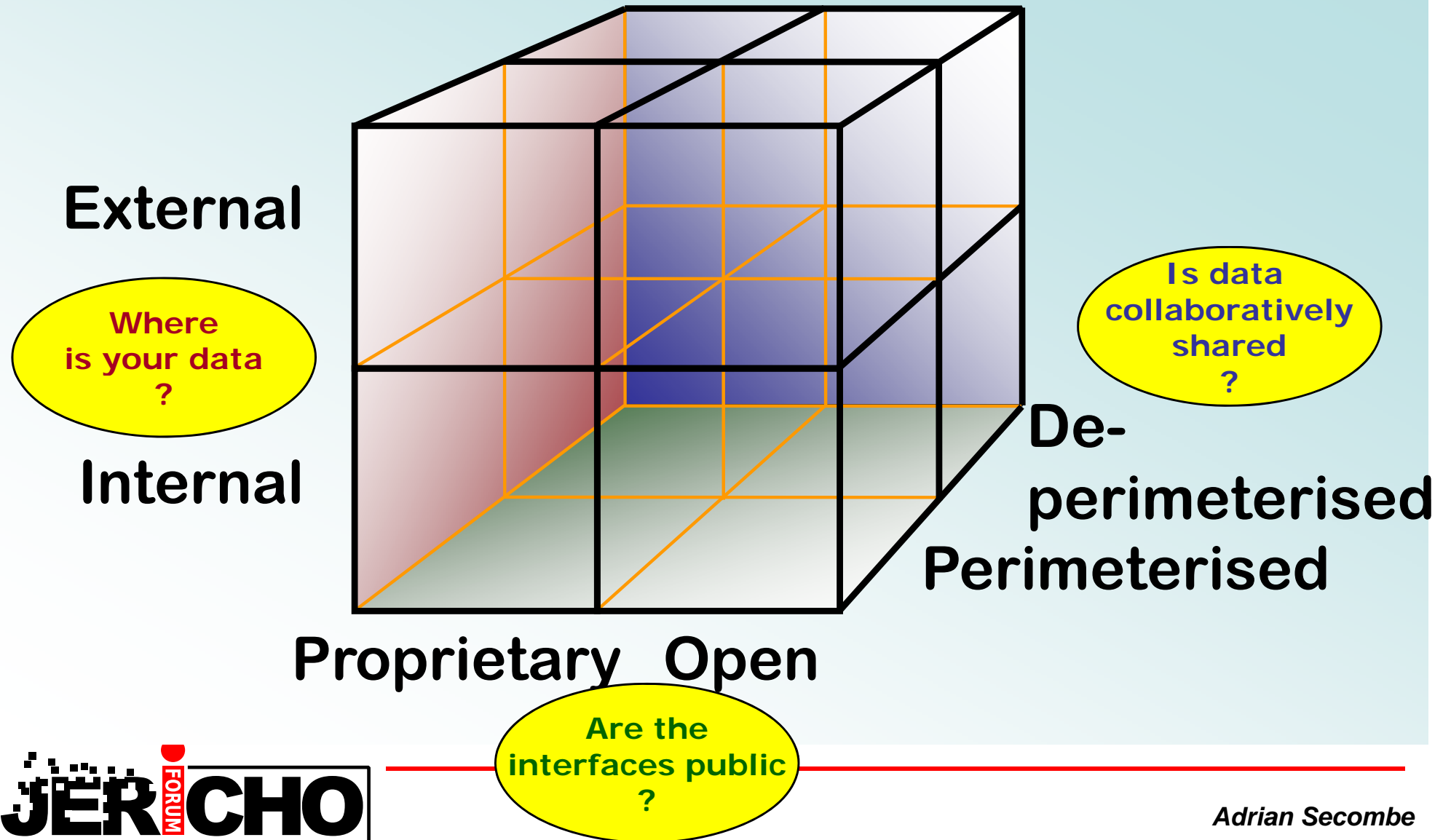
Jericho Forum Activity

- Like many others, we see huge potential and benefits for moving into "the cloud"
- But we advise not leaping in their before understanding the:
  - Risks
  - Security issues
  - Interoperability issues
  - Business rationale
- The Jericho Forum is taking a lead on:
  - Analyzing the issues
  - Raising awareness
  - Establishing clear requirements
- Goal: Make the cloud a safe place to collaborate

Thank You!

- **Andrew Yeomans**
  Jericho Forum Board

- *http://jerichoforum.org*