Risk Assessment and Cloud Strategy Development:

Getting it Right this Time!

Barbara Endicott-Popovsky, PhD
University of Washington
Center of Information Assurance and Cybersecurity

Kirsten Ferguson-Boucher
Aberyswyth University, Wales
Dept of Information Studies

"If the Internet were a street, I wouldn't walk it in daytime…"

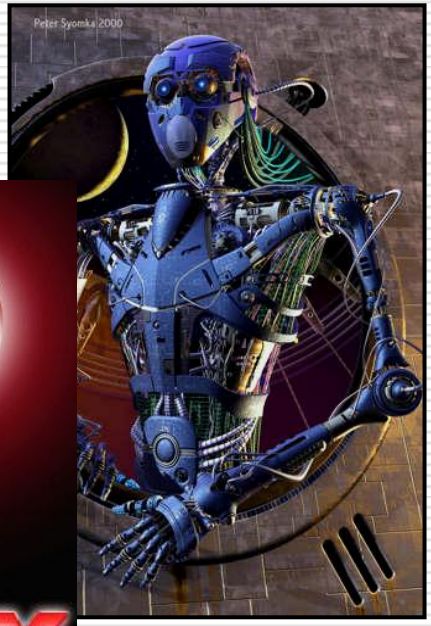
- 90% of email traffic is spam
  http://news.cnet.com/8301-1009_3-10249172-83.html
- 1-3% of all traffic is malicious
  http://www.csoonline.com/article/326013/up-to-three-percent-of-internet-traffic-is-malicious-researcher-says
- Unprotected PC infected in minutes
  http://iggyz.com/?p=1329
- Organized crime makes more on the Internet than drugs
  http://www.google.com/hostednews/afp/article/ALeqM5ikPuK5Ri0UnDW2IXwJnA5-fDA7HA?docId=CNG.a00f68010092a06189a0276c763e93a4.131
- 'Take' from Internet >doubles e-commerce

Courtesy: FBI, LE

It is not pretty out there…

CYBER-CRIME

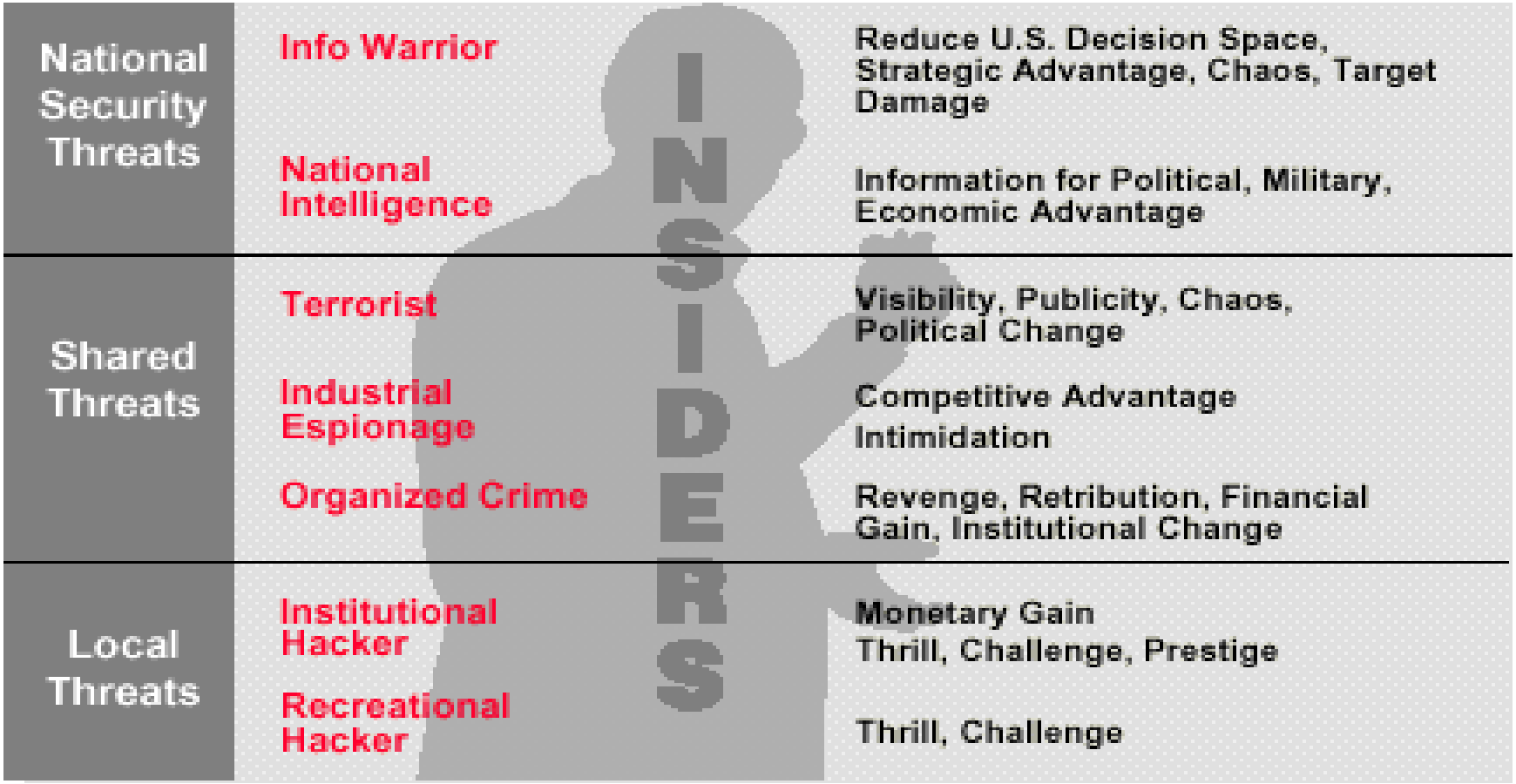
PC zombies and bot armies



Courtesy: K. Bailey/E. Hayden, CISOs

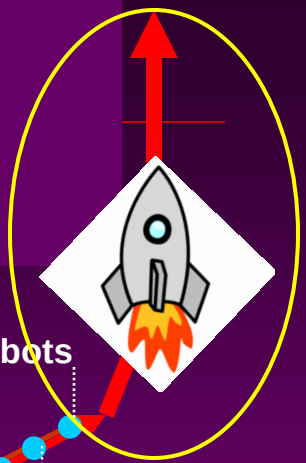
*"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks."—**Foreign Government Newspaper***

Information Age Threat Spectrum



National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

Cyber Attack Sophistication Continues To Evolve



Source: CERT 2004

High

Intruder Knowledge

Attack Sophistication

Low

Tools

Attackers Technical Skills

password guessing

self-replicating code

password cracking

exploiting known vulnerabilities

burglaries

hijacking sessions

disabling audits

back doors

sweepers

sniffers

packet spoofing

network mgmt. diagnostics

GUI

automated probes/scans

www attacks

distributed attack tools

denial of service

"stealth" / advanced scanning techniques

Staged attack

bots

Cross site scripting

1980

1985

1990

1995

2000+

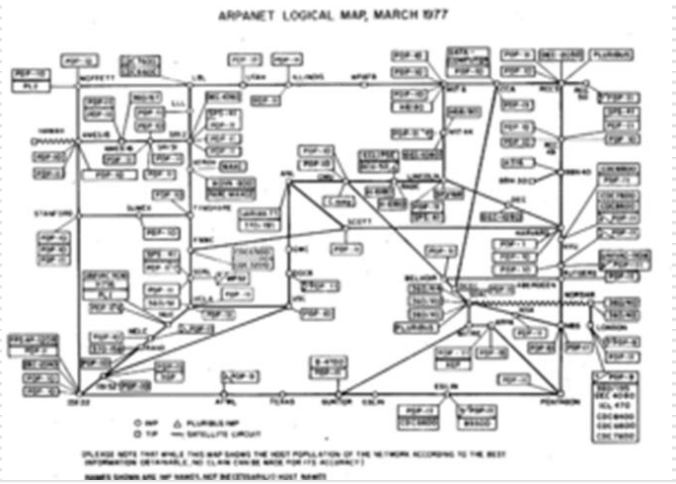
Courtesy: K. Bailey/E. Hayden, CISOs

What have we learned from our experiences with the Internet?

DESIGN IN CYBER SECURITY!!

Internet Conceptual Design

- Requirements:
  - Connect limited number of trusted researchers
  - Permit sharing of limited computer resources
  - Survive subordinate-network losses
- Purpose:
  - Share research data
  - Two communications



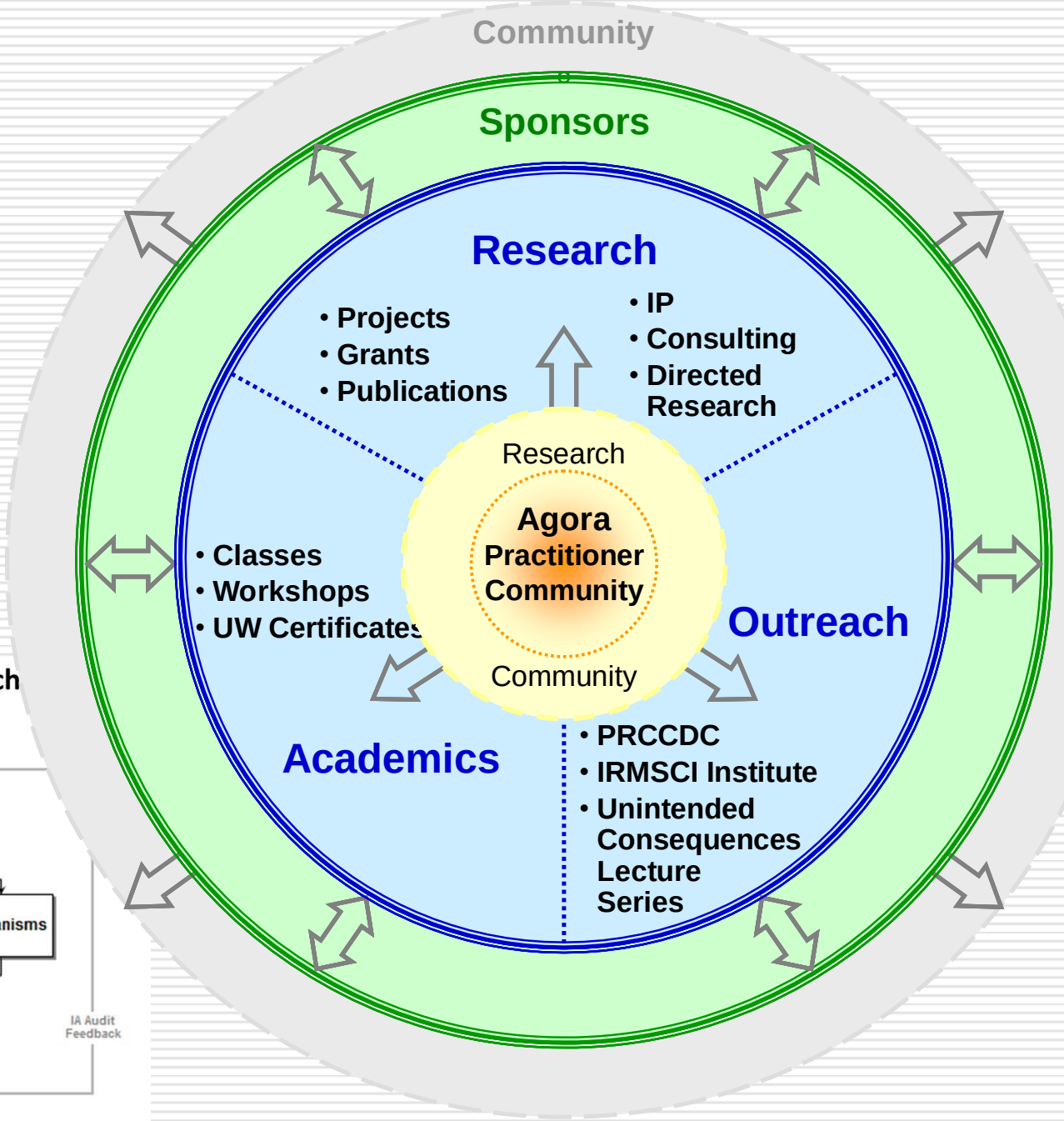
- Not considered: CYBER SECURITY!

What lessons can users transfer to the Cloud?

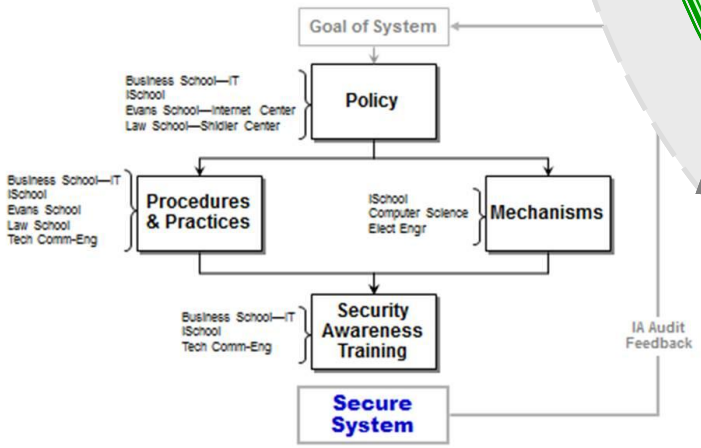
DESIGN IN CYBER SECURITY!!

Center for Information Assurance and Cybersecurity

NSA-CAE-R



Multi-Disciplinary Approach
Cloud Focus



The Ponemon Institute, April 2011

SECURITY OF CLOUD COMPUTING PROVIDERS STUDY

http://www.ponemon.org/blog/post/ponemon-releases-cloud-server-provider-study

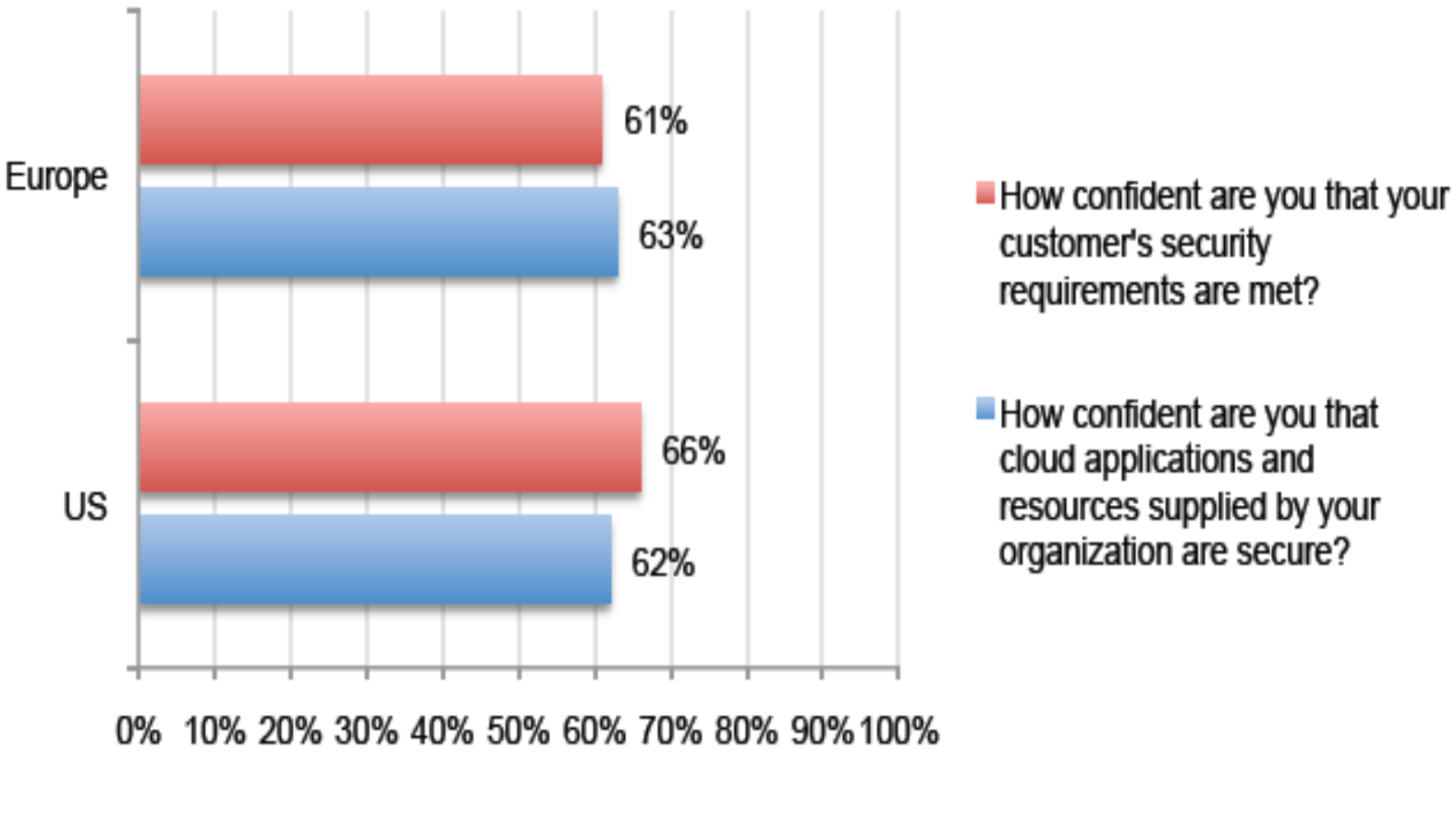
Summary Findings

"These findings indicate that respondents overwhelmingly believe it is the responsibility of users of cloud computing to ensure the security of cloud resources they provide. The majority does not believe their cloud services include the protection of sensitive data. Further, only 19 percent of US cloud providers and 18 percent of European cloud providers strongly agree or agree that their organization perceives security as a competitive advantage in the cloud marketplace."

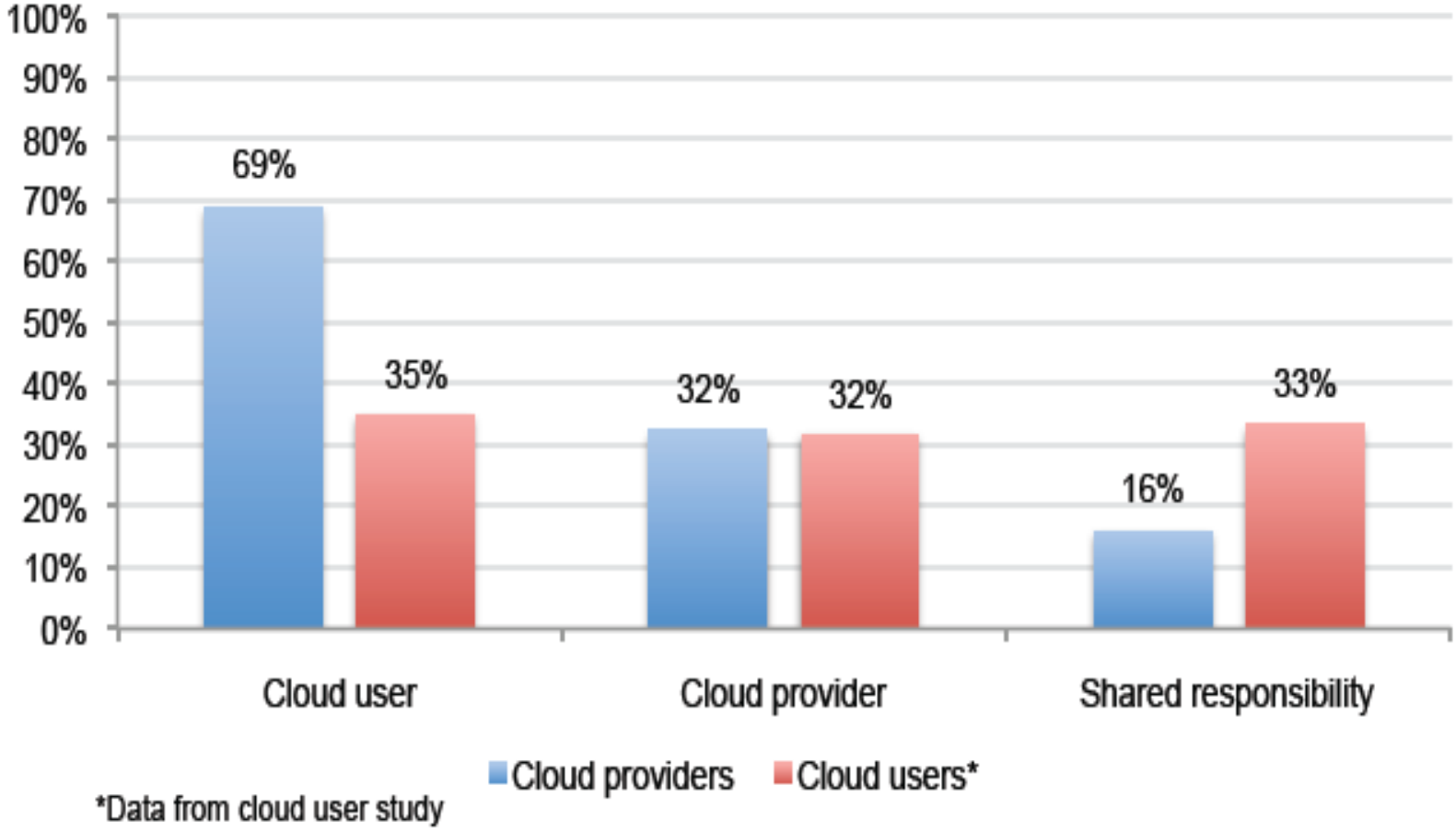
Cloud Provider Sample Size

Table 3: Sample response	US	Europe
Organizations	1,180	263
Contacts made (by phone)	879	240
Returned surveys	130	32
Rejections for reliability	27	8
Final sample	103	24

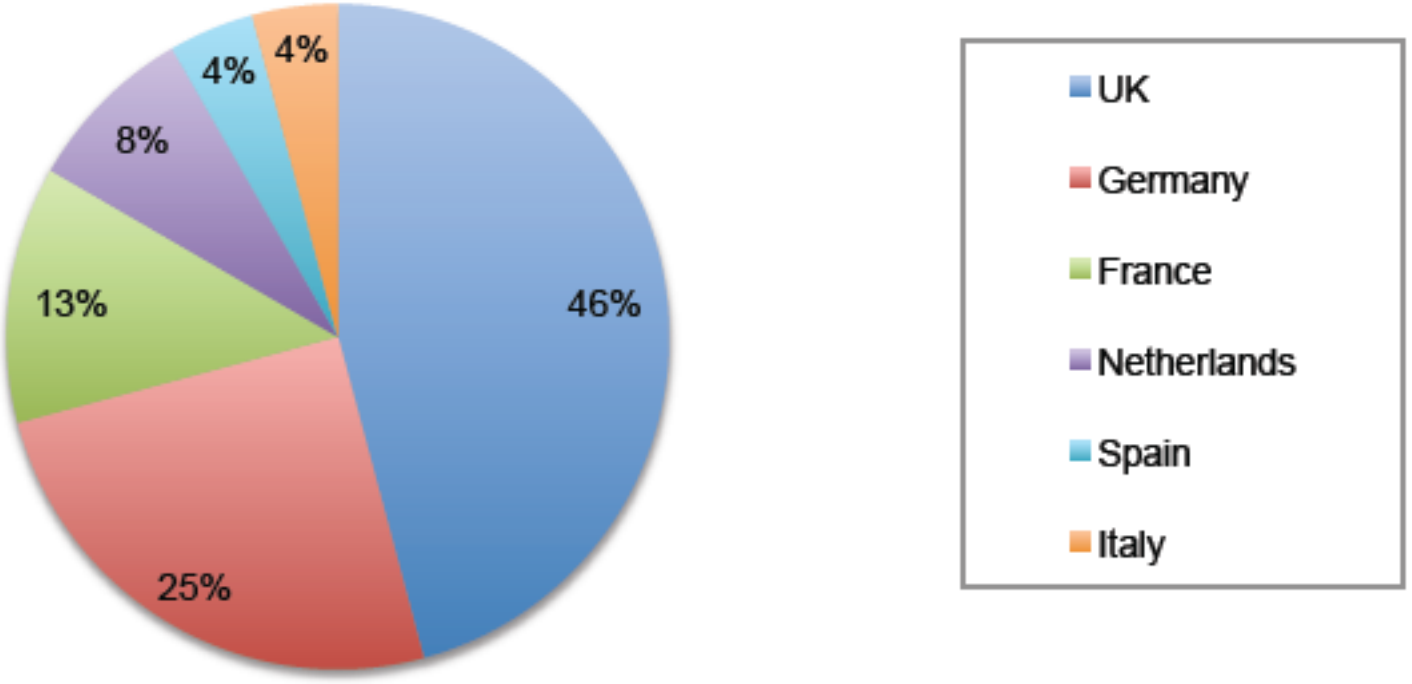
Lack of Confidence in Security of Cloud Resources



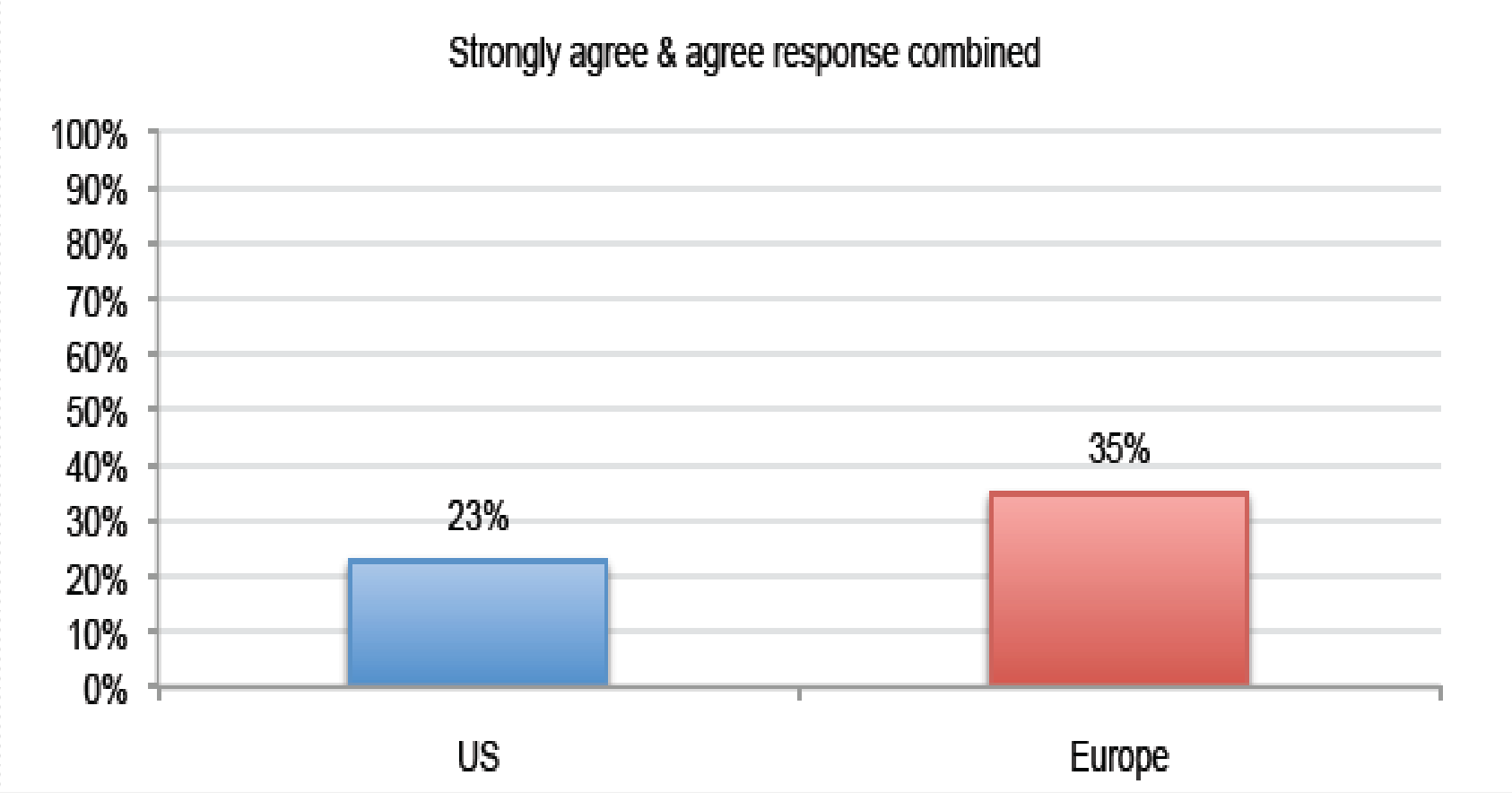
Who is Most Responsible for Ensuring Security of Cloud Resources?



Country Locations of European Sample



Who is Most Concerned about Cloud Security



UK Perspective

STORING INFORMATION IN THE CLOUD

Research aim: UK context

- Investigate the management , operational and technical issues surrounding the storage of information in the cloud and provide an overview of Cloud Computing uses and challenges relating to common **records keeping practices**
- Develop a toolkit to assist **Information Professionals** in assessing the risks and benefits of outsourcing information storage and processing in the cloud

Research methodology

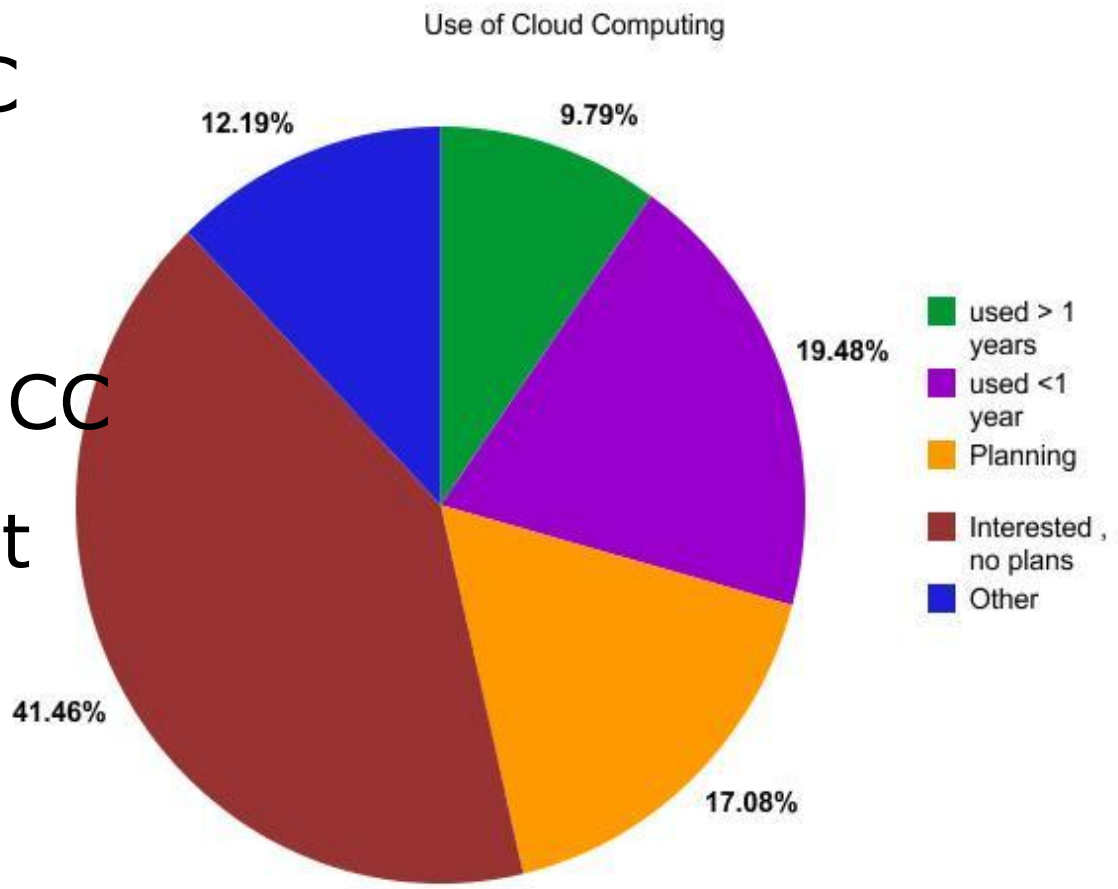
- Literature Review on CC and Information Governance and Assurance
  - Evidence still in early adoption stage in which technical concerns and product reviews dominate
- Consultations:
  - Online questionnaire (further evidence of embryonic stage – still to gain ground with information professionals in the UK)
  - Interviews (3 case studies – Guardian Media Group, Melrose Resources and the Cabinet Office, UK government)
  - Event – "Storing Information in the Cloud Unconference: Manchester, England

Survey results

30% have used CC for <1

17% are actively planning to use CC

41% interested but no active plans



Main concerns

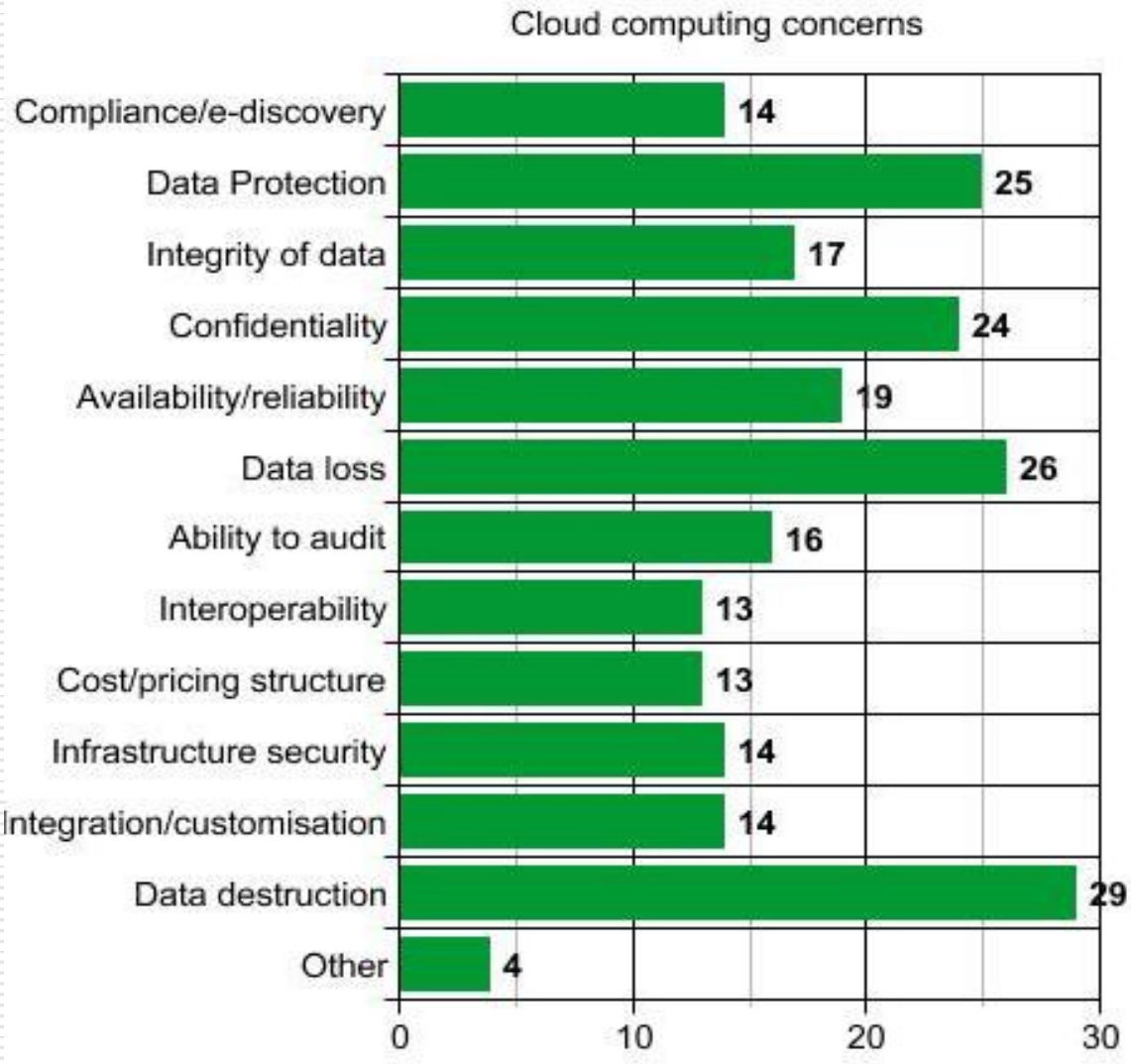
Destruction of data

Loss of control over data

Data protection

Confidentiality

Availability of service



What are the issues?

Governance:

- Privacy/Data protection
- Compliance and e-discovery
- Integrity of data
- Confidentiality of data/unauthorised access
- Ability to audit service
- Loss of control over data and services

Unconference outcomes: RISK to the organisation

"Cloud computing is based on risk-assessment and establishing a trust relationship with providers –

Know the risks and make a choice!"

PRIFYSGOL ABERYSTWYTH UNIVERSITY

Toolkit for outsourcing to the cloud

Top ten questions

1. *Which process, application and information* can be moved to the cloud to gain efficiency and cost benefits while satisfying the organisation's security and compliance requirements?
2. *How can the organisation be harmed* if systems, applications, services or information are accessed by unauthorised people and information is being made available to the public?
3. *How are information and systems protected* against unauthorised access (e.g. hacking, interception, user misuse) by the cloud service provider?
4. *How can the organisation ensure the integrity, authenticity and reliability* of information stored in the cloud?
5. *What are the organisation's responsibilities* regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?

Toolkit for outsourcing to the cloud

Top ten questions continued

- How can the organisation apply its *records and information management programmes* (e.g. classification, retention) to the cloud environment?
- What is the impact of outsourcing services and information to the cloud on the *legislative and regulatory requirements* of the organisation (e.g. DP, FOI, SOX, e-discovery, copyright, licensing etc.)?
- *How should the organisation audit and monitor* cloud services and establish relevant service level agreements?
- Will the organisation be able to *negotiate contracts and agreements* that fit their risk assessment and compliance environment?
- *What are the total costs* of setting up and managing the cloud services?

Top 10 of Cloud Computing Concerns

- these cluster loosely into those attendant with **performance**, specifically efficiency and cost, monitoring and total costs;
- those relating to **alignment** with organisational objectives i.e. organisational responsibility and impact of outsourcing;
- those associated with ensuring **information assurance and value** through information governance and assurance programmes and the protection of systems;
- the perceived **risk** to the organisation and the robustness of the contracts and outsourcing procedures figured highly in ranking.

Top 10 of Cloud Computing Concerns

- It is clear from the findings that many of the concerns associated with cloud computing relate to specifically to information governance and assurance, i.e. the handling of data in the cloud.
- Decisions must be taken after consideration of the wider context of organisational strategy.

Information Governance and Assurance

- They form part of a complex structure of assessments regarding information *value, alignment, performance* and *assurance.* All of these operate within an overreaching risk framework.
- VAAPR: pronounced Vapour:

  Value; Alignment, Assurance in

  Performance and Risk framework
- Holistic approach to information governance and assurance

Information Governance and Assurance

- Take advantage of changes in user practice for the organisational objectives
- Work in conjunction with existing processes and procedures
- Add value, but ensure assured and operating within performance and risk framework
- There are different concerns when *preparing* to use cloud computing services, to those most relevant when *managing* and ultimately *operating* in the cloud

Guide to data governance for privacy, confidentiality and compliance

- Data classification and quality; protective measures, data partitioning and processing; compliance and risk management, identity and access management; service integrity, endpoint integrity
- Moving into the cloud: viability, transparency, compliance
- Secure infrastructure, identity and access control, information protection, auditing and reporting
- Data privacy principles
- Risk/gap analysis

PRIFYSGOL ABERYSTWYTH UNIVERSITY

Toolkit for outsourcing to the cloud

- Preparing for the cloud
  - Information classification
  - Risk assessment
- Managing the cloud
  - Information management
  - Compliance
  - Contract and cost
  - Monitoring, auditing and reporting
- Operating in the cloud
  - Security
  - Availability
  - Identity and access management

Preparing for the Cloud

initial deliberations focus on alignment with business objectives:

- the legal framework in which organisations operate,
- the existing internal systems for staff and other resources,
- the IT infrastructure and
- central business drivers and current initiatives.

different for each organisation , effective anticipation of the related risks and the identification of mitigation strategies.

value added elements that information can bring to the organisation: identification of the information to be serviced in the cloud and some form of ***classification*** to enable its retrieval and effective usage.

Managing the Cloud

- assurance and performance aspects of information governance and assurance
- guarantees relating to the continuing authenticity, reliability and integrity of the information
- contracts and service agreements are the documents which embody these understandings and support the specific nature of these arrangements.
- cost/benefit analyses and indeed the wider performance measurements which can be used to assess how effective, efficient, flexible and therefore sufficient the cloud solution is proving necessitate constant monitoring.
- clear exit strategy
- continually reassessing and reapplying the risk criteria, across the spectrum of information governance concerns, a balanced approach to cloud usage is achievable.

Operating in the Cloud

- information assurance and information value: assessing policies and procedures for physical, personnel, infrastructure, information and access security.
- availability of the service,
- appropriate provision of access to information,
- business continuity: continuing access to information despite interruptions and failures at any stage of the lifecycle,
- combined approaches to governance and assurance challenges should ensure robust and comprehensive solutions.

Information management

- Consideration: ensure that information stored in the cloud will be managed according to the organisations information management and compliance programmes in order to maintain authenticity, reliability and integrity of information over time and to ensure that information is accessible and retrievable for legal and regulatory compliance.

Managing in the cloud: Information Management

- Rationale: The organisation needs to ensure that policies and procedures surrounding the management of the whole life-cycle of information are administered and validated for information stored in the cloud in the same way they are administered onsite. The main aspects of managing records are the classification, appraisal and disposal of information in order to improve efficiency and facilitate compliance

Questions - general

- What impact will the management of information stored in the cloud have on existing information management policies and procedures
- Can cloud providers assure that their information security systems can support the authenticity and reliability of the organization's information, including metadata and log files
- Will it be possible to show that information is fully encrypted and protected against unauthorised disclosure

Questions – make and fix

- In what format is information created, transferred and stored in the cloud
- What implication does the format of information stored in the cloud have for access, retrieval and preservation
- What metadata can be applied to information stored in the cloud and can it be managed and searched
- Does the organisation need to apply additional metadata to information stored in the cloud than it would apply to information stored in-house? What kind of metadata would that be?

Questions – keep and seek

- classified (full classification) and supplied with relevant metadata to ensure efficient identification and retrieval
- provisioned access and usage rights to categories of information
- retention and disposal schedules – how are they applied and executed
- how will information be destroyed – overwritten timescales available, audit and certification of destruction
- preservation needs – permanent or long term retention – transferred to digital archive? place of legal deposit? remain in the cloud?

Define the risks

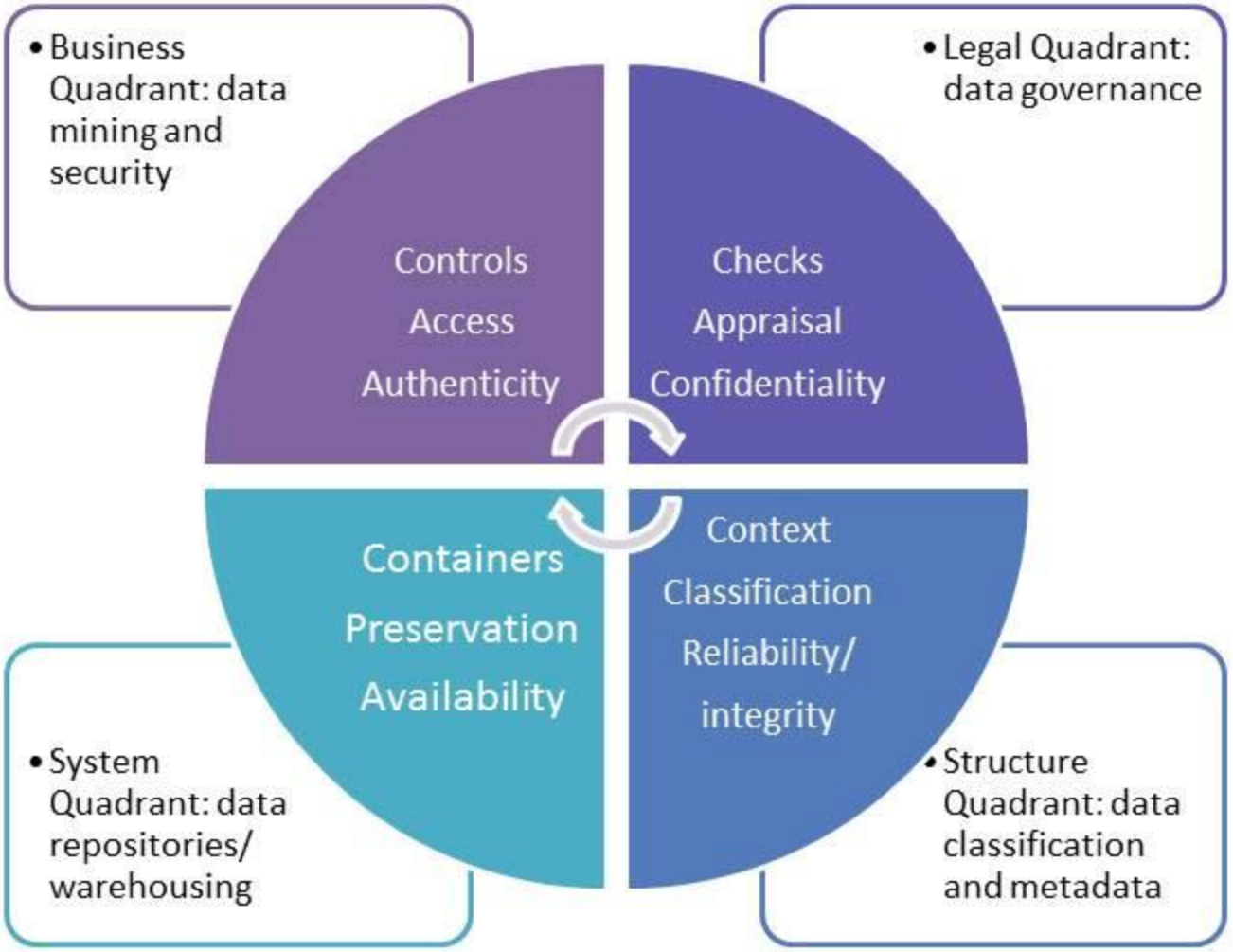
Legal Risk – we don't ensure that the "right stuff" including the content, context and structure is selected to meet legal requirements

Structural Risk – we don't design systems and architecture so that "the right stuff" is suitably managed through out the lifecycle

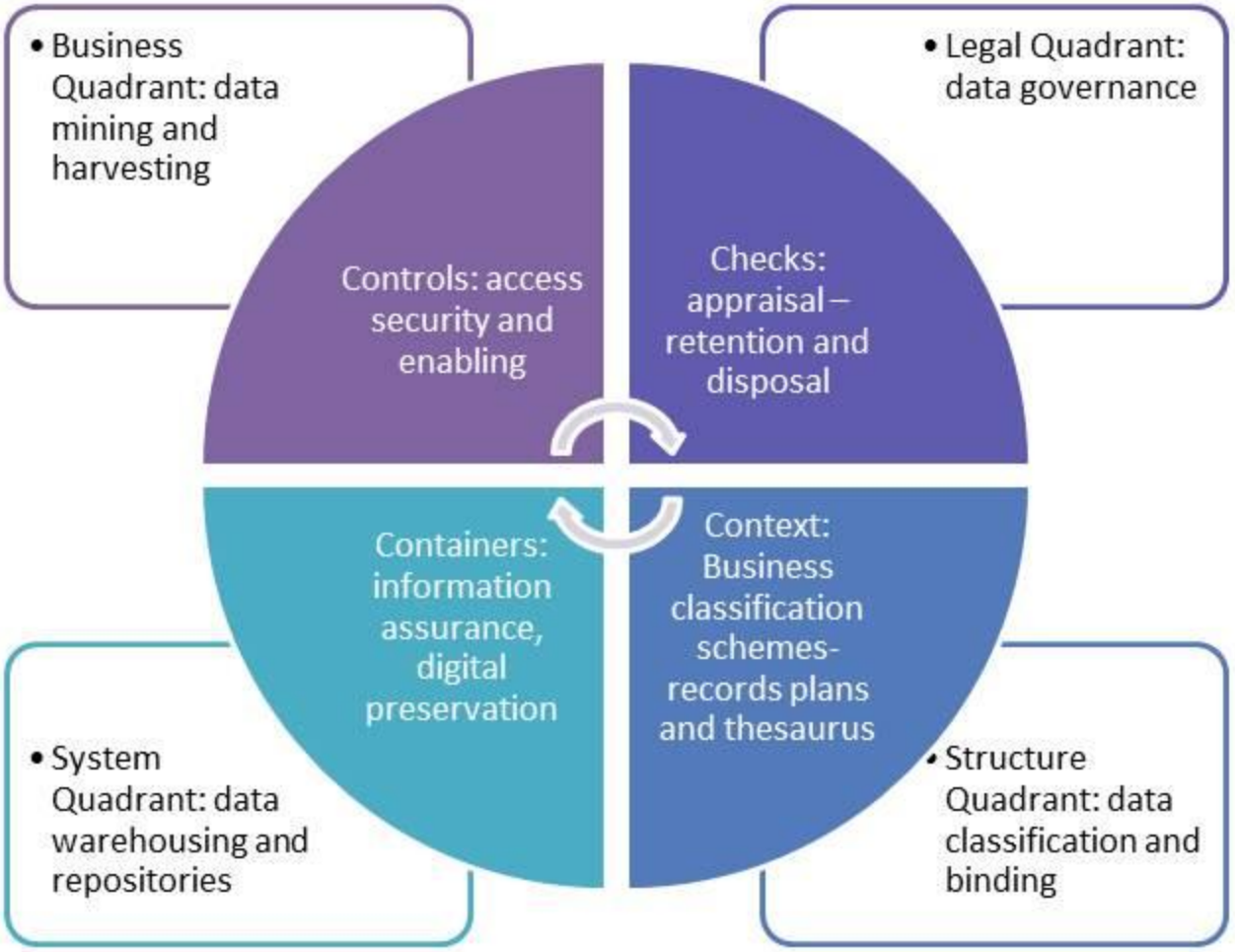
System Risk – we don't monitor the activities throughout the lifecycle of the digital object

Business Risk – we don't monitor the activities sufficiently to ensure that the creators, managers and users are adhering to the rules and regulations that have been put in place

Risk framework



Solutions


• Business Quadrant: data mining and harvesting
• Legal Quadrant: data governance
Controls: access security and enabling
Checks: appraisal – retention and disposal
Containers: information assurance, digital preservation
Context: Business classification schemes- records plans and thesaurus
• System Quadrant: data warehousing and repositories
• Structure Quadrant: data classification and binding

Future Research

- little actual research has been undertaken to formally assess the impact of Cloud Computing on professional information management practice. Many existing publications focus predominantly on the technical issues and many of the wider compliance and organisational issues are not fully addressed
- issues relating to trust and understanding, relating to the benefits and also the challenges to organisational governance provided by moving digital assets to the cloud
- benefits in broadening the Cloud Computing Toolkit to include wider Information Governance and Assurance dimensions, which are of concern for all organisations in making any cloud or technology implementation decisions and which impact directly on the confidence of decision makers regarding their strategies
- genericized to for all information, regardless of format, to include data held on mobile technologies, social media and technologies of the future

Contact Information

- Kirsten Ferguson-Boucher
  Aberyswyth University, Wales
  knb@aber.ak.uk

- Barbara Endicott-Popovsky
  University of Washington
  Center for Information Assurance and Cybersecurity
  endicott@uw.edu

Questions?

Security of Cloud Computing Providers Study

Ponemon Institute
April, 2011

- The majority of cloud computing providers surveyed do not believe their organization views the security of their cloud services as a competitive advantage. Further, they do not consider cloud computing security as one of their most important responsibilities and do not believe their products or services substantially protect and secure the confidential or sensitive information of their customers.
- The majority of cloud providers believe it is their customer's responsibility to secure the cloud and not their responsibility. They also say their systems and applications are not always evaluated for security threats prior to deployment to customers.
- Buyer beware – on average providers of cloud computing technologies allocate10 percent or less of their operational resources to security and most do not have confidence that customers' security requirements are being met.
- Cloud providers in our study say the primary reasons why customers purchase cloud resources are lower cost and faster deployment of applications. In contrast, improved security or compliance with regulations is viewed as an unlikely reason for choosing cloud services.

http://www.ponemon.org/blog/post/ponemon-releases-cloud-server-provider-study

Security of Cloud Computing Providers Study (Cont'd.)

Ponemon Institute
April, 2011

- The majority of cloud providers in our study admit they do not have dedicated security personnel to oversee the security of cloud applications, infrastructure or platforms.
- Providers of private cloud resources appear to attach more importance and have a higher level of confidence in their organization's ability to meet security objectives than providers of public and hybrid cloud solutions.
- While security as a "true" service from the cloud is rarely offered to customers today, about one-third of the cloud providers in our study are considering such solutions as a new source of revenue sometime in the next two years.

- A list of cloud computing resources relevant to the records and information management community has been made available on Google Docs and can be accessed at https://docs.google.com/Doc?docid=0AUMD4SCCg7uaZGRxczNybndfMTZjODM4bXhmNw&hl=en.

- Everyone can contribute further relevant resources to the Google document. Online resources have been bookmarked in Delicious and are available at http://www.delicious.com/nicoleschu/soacloud

- Outcomes of the unconference in the form of participants' concerns and suggestions widely inform the findings and recommendations of this report. Speaker sessions and participant feedback have been recorded and are available at http://vimeo.com/disaberystwyth

- The toolkit: http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf