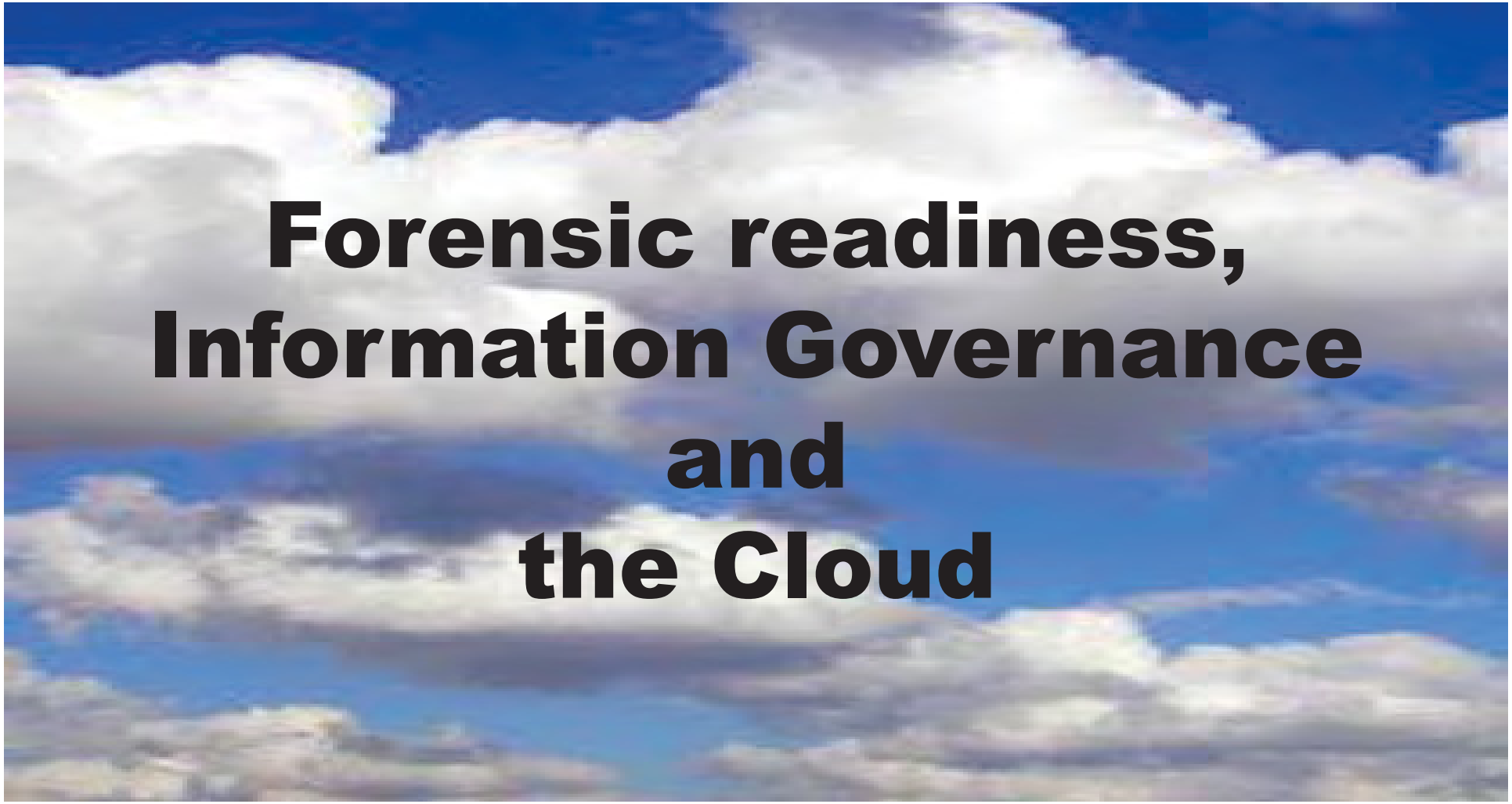


Forensic readiness, Information Governance and the Cloud

Dr. Barbara Endicott-Popovsky and Kirsten Ferguson-Boucher
University of Washington and Aberystwyth University

PRIFYSGOL ABERYSTWYTH UNIVERSITY

UNIVERSITY OF WASHINGTON

What do we mean by the Cloud?

PRIVACY IN THE CLOUD

The Tradeoff

- Benefits
  - flexibility
  - scalability
  - cost savings
- Potential challenges
  - diminished control over data
  - diminished control over the infrastructure that houses and processes that data

Incremental Risks to Privacy and Security

- Legal implications of moving certain data to a specific cloud services provider (CSP) in a specific geographic location.
  - Clarify rights and data ownership
- Long-term viability of the CSP.
  - Impacts of rehosting
- Reasonable level of transparency from the CSP with regard to what security, privacy, and compliance protections are in place.
  - Documentation
  - Third-party certifications, about protective measures effectiveness and verification.
- Diagram data flows to understand the security, privacy, and compliance risks.
  - Identify threats and residual risks in specific data
  - Used to improve protections and manage risks.

The Cloud: What is it?

- Several different services, some not so new
- Differing opinions about what it is
- NIST offers definition

National Institute of Standards and Technology (NIST)

- **Software as a Service** (SaaS), software applications are provided and managed in the cloud by a Cloud Service Provider (CSP)
  - Example: Microsoft® Online Services: hosted versions of Microsoft Exchange and Microsoft SharePoint®
- **Platform as a Service** (PaaS), CSP delivers the underlying infrastructure, including OS and storage, allows organizations to build and run applications using languages and tools provided and supported by the CSP
  - Example: Microsoft's Windows Azure™ platform
- **Infrastructure as a Service** (IaaS), in which a CSP gives an organization access to basic IT infrastructure (network, hardware, core operating system, and virtualization software) on which the organization can deploy its own applications and data in a virtualized environment, applications that were developed using languages and tools not provided or supported by the CSP.
  - Examples: Amazon's EC2 and Rackspace's Cloud Servers

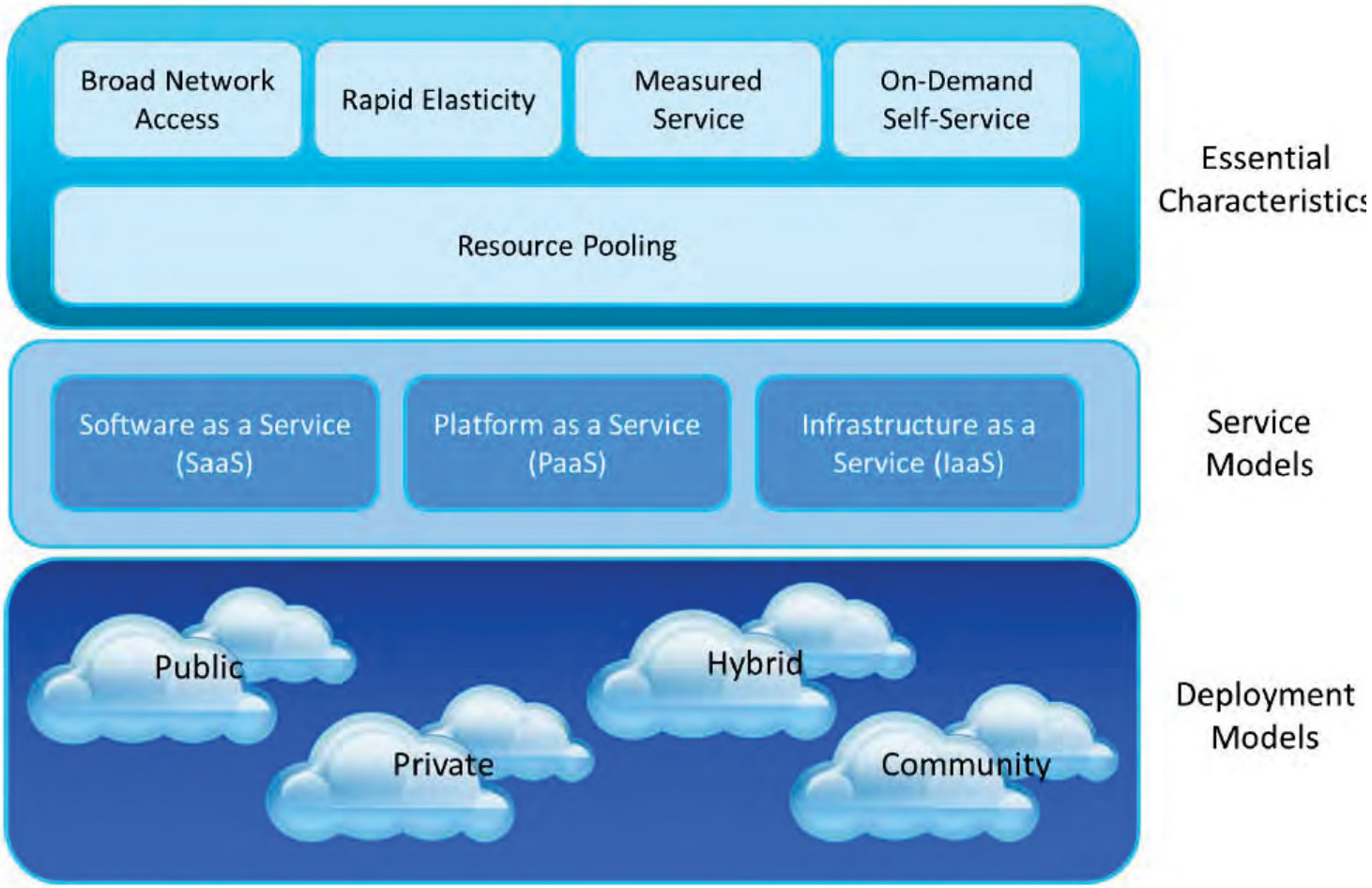
Key Characteristics of All Three Models

- Benefits: convenience, cost effectiveness, flexibility, and elasticity
- Sharing of resources by multiple tenants
- Rapid provisioning through self-service
  - Adding processing power & storage as needed.
- Information storage and processing not limited by space or geography
  - Unknown number of “virtual filing boxes”
  - Storage and processing scales to meet needs

Deployment Models

- **Private clouds**: operated by or for a single organization
- **Community clouds**: operated for groups of organizations with similar service requirements
- **Public clouds**: one general SLA for all; data resides on shared resources.
- **Hybrid clouds**: connect public and private clouds sharing services and data among them.

NIST Working Definition of Cloud Computing



Off-premises Cloud Model

- Offers potential advantages:
  - Security improvements
  - Flexible scaling
  - Reduced or no capital spending on IT
- Inevitable tradeoffs
  - Consider these in risk management planning.

On-premises Cloud Model

Organization responsible for all aspects of IT—people, processes, and technology:

- Buys the hardware
- Licenses the software
- Secures the datacenters
- Defines processes and procedures
- Hires the people who run everything

Organization Responsible for/Controls Security and Privacy

- Physical location of the datacenter
  - Determines which country's laws apply
- Security of the datacenter
- How employee/customer PI is used/distributed
- Trustworthiness of system administrators
- Documented info. security program that provides the CIA of data and systems, i.e.:
  - Configuration
  - Patching
  - Incident response
  - Business continuity management

Legal, Operational, and Security-related Complexities Unique to the Cloud

- Hardware is often shared among customers
- Security boundary between may be virtual rather than physical
- On-the-fly allocation: geographic location depends on scalability/availability not security/jurisdiction
  - uncertainty about which laws apply to the data

Adapting to the Cloud

- Must address:
  - Compliance and risk management
  - Identity and access management
  - Service and endpoint integrity
  - Information protection

- Data management regime not under direct control
  - Extended security processes encompass multiple providers
  - Risk management, privacy, security
    - remain the organization's responsibility
    - must include the CSP

Cloud Computing: Legal Implications

Source: World Privacy Forum, 2009

•Significant implications for the privacy of PI as well as for the confidentiality of business and governmental information.

• Risks vary significantly with terms of service and privacy policy established of the CSP.

• For some types of info. and some categories of users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a CSP.

• Disclosure and remote storage may have adverse consequences for legal status of information

• Location of info. may have significant effects on the privacy and confidentiality protections and on the privacy obligations of those who process or store the information

• Info. may have more than one legal location at the same time, with differing legal consequences.

• Laws could oblige a CSP to examine user records for evidence of criminal activity , etc.

• Legal uncertainties make it difficult to assess the status of info. as well as privacy and confidentiality protections available

• Responses to privacy and confidentiality risks include better policies and practices by CSPs, changes to laws, and more vigilance by users.

Information Protection: Responsibilities of the Cloud Client

- **Data classification**
- **Data quality**
  - consistent data definitions to maintain QOS
  - limit costs
    - data cleansing
    - cloud resource consumption
    - facilitate data classification
  - synchronization with on-premises copies of data
- **Protective measures**
  - who controls the identity and authorization system for access
  - where backup data is stored
  - whether data encryption is supported
  - costs associated with encryption (e.g., feature loss), etc.

Information Protection: Responsibilities of the Cloud Client (Cont'd.)

- **Data partitioning and processing**
  - Who has access to data?
  - Is risk is acceptable?
  - Understand CSP architecture
  - Assurance that shared VMs are secure against attacks from other VMs on same physical hardware
  - Legal aspects of the CSP agreement
    - How access to data will be granted if there is a dispute
    - Can the CSP guarantee it will not retain data if service canceled?

Compliance and Risk Management

- Delegation does not discharge responsibility for compliance
  - Skilled team—both places
  - Process transparency; but limited for security
- Resulting agreement includes
  - Contractual commitments
  - Agreed-upon level of visibility into the CSP's control framework
  - Third-party verified certifications and attestations
  - Elements the customers can integrate into its own data governance program

The latest research from the UK

ADOPTION OF 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

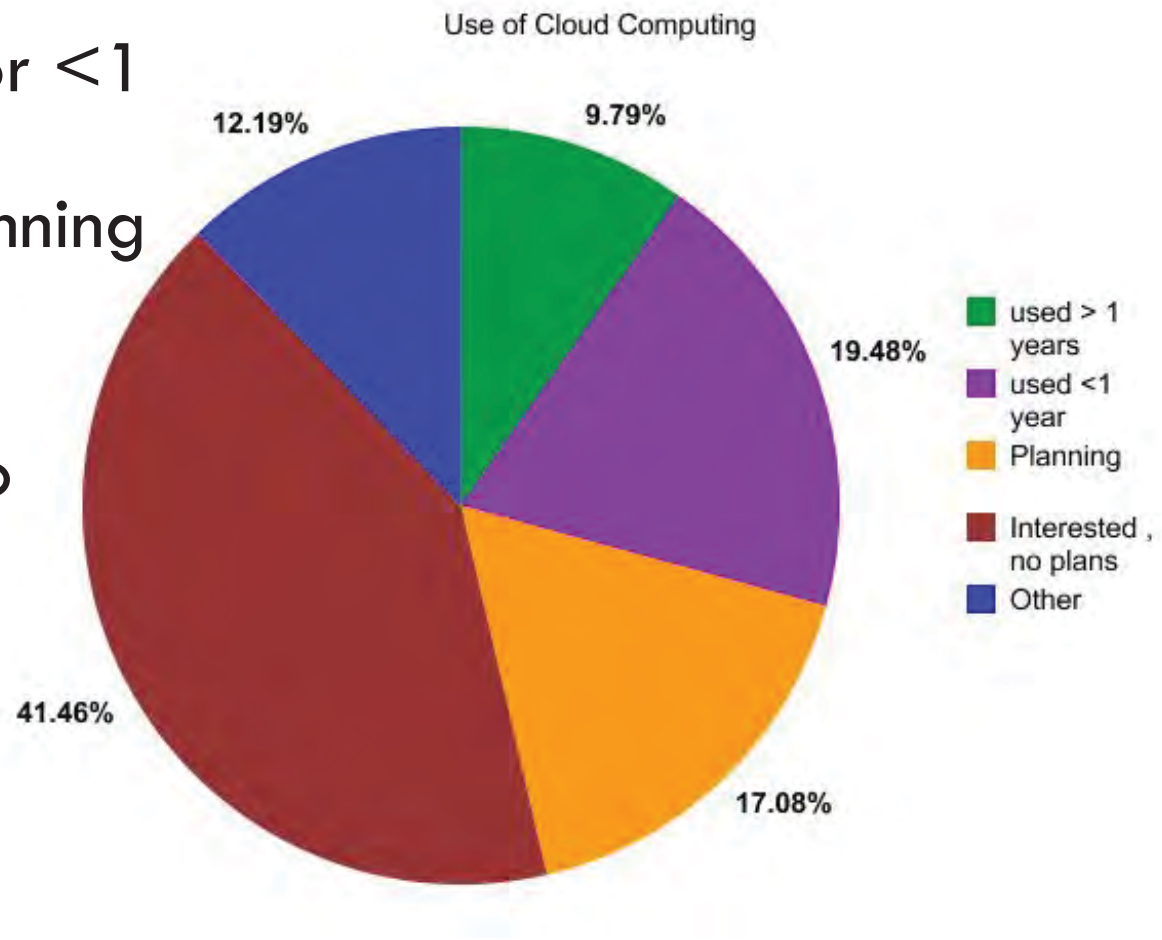
- Literature Review on CC and Information Governance and Assurance
  - Evidence still in early adoption stage in which technical concerns and product reviews dominate
- Consultations:
  - Online questionnaire (further evidence of embryonic stage – still to gain ground with information professionals in 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 http://vimeo.com/disaberystwyth

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

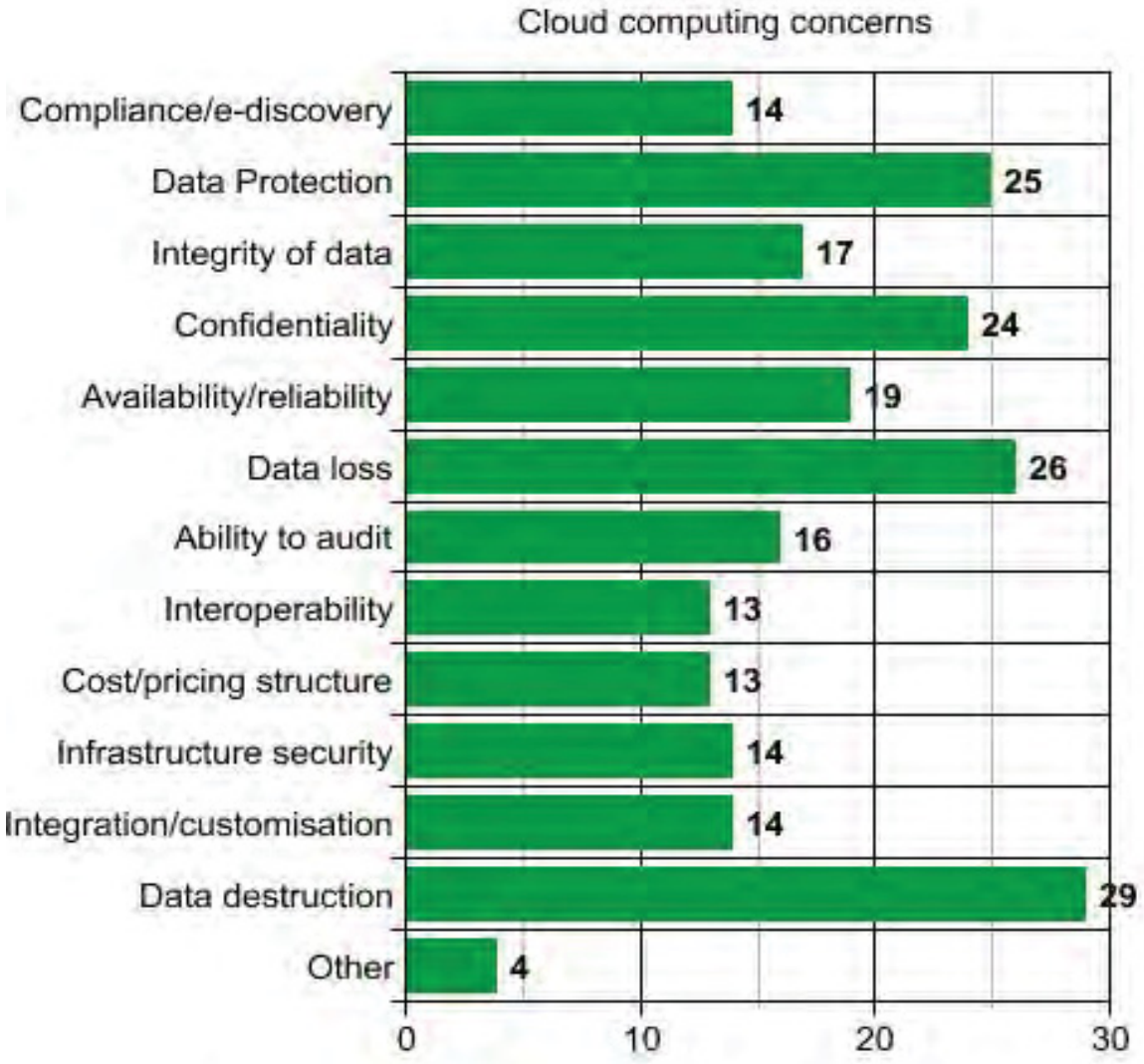
Loss of control over data

Data protection

Confidentiality

Availability of service

Integrity/security?



Research findings

- The integrity, authenticity, reliability and confidentiality of information rests on the ability to demonstrate that it has not been tampered with or been accessed by unauthorised persons. In the cloud environment, information is additionally at risk of being compromised by

Compromised:

- unauthorised access by malicious insider at the cloud provider
- interception while in transit over an unsecured network
- being accessed while processed in unencrypted state
- being commingled with information of other customers in a multi-tenant environment
- remanence when it has only nominally been removed from hard drives

Research findings

- **Availability and reliability of services:** Cloud providers are -due to the nature of their business- a much higher target for hackers or malicious insiders. Even though they might invest much more in security and incident response procedures, they have to be able to prevent or react to DDoS or malware attacks, hacking, port scanning and other potential security threats.

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

What are the issues?

Technological/operational:

- Availability and reliability of services
- Portability and interoperability of cloud services
- Unknown cost due to variable pricing structure
- Infrastructure and network security
- Lack of customisation/integration with existing systems
- Retrieval and/or destruction of data when service terminated

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!"

Toolkit for outsourcing to the cloud

- **Incident response**

- *Consideration:* Define acceptable incident response and patch management procedures.

Toolkit for outsourcing to the cloud

- *Rationale*: A main threat to the availability and security of cloud services is the ability for hackers and malware to exploit systems and infrastructure vulnerabilities in order to gain access to services and information in the cloud. While it would be ideal to prevent attacks to systems and networks in the first place, not all security incidents can be prevented.

Toolkit for outsourcing to the cloud

- The cloud provider should have procedures in place to
- detect incidents rapidly
- minimize the impact of the incident
- restore systems and networks rapidly
- analyse how the incident happen and
- identify weaknesses of systems and networks

Questions in the ToolKit :

- **Preparation**
- Does the provider have policies and procedures in place to assess the risk of vulnerabilities?
- Does the provider have formal policies and processes in place for detecting, identifying, analysing and responding to incidents?
- Is this process rehearsed to check that incident handling processes are effective?

Questions in the ToolKit:

- How are incidents reported to the customers (e.g. periodical reports, dashboards, emails)?
- Are procedures in place to prioritise incidents based on the criticality of the affected system?

Questions in the ToolKit:

- **Detection and Analysis**
- Does the provider have automated detection capabilities in place such as intrusion detection systems, anti-virus software and log analysers?
- Is there real time security monitoring in place?
- How can the customer report anomalies to the provider?

Questions in the ToolKit :

- How are incidents documented and is evidence collected, especially when logging and data is co-located for multiple customers?
- How much access does the customer have to these logs??
- What controls are in place to prevent malicious activities by insiders?

Questions in the ToolKit:

- **Containment, eradication and recovery**
- What mechanisms are in place to contain the incidents (e.g. shutting down the system, disconnect from network, disabling systems functions, isolation parts of the infrastructure)?
- How are components of the incident eradicated (deleting malicious code, disabling breached accounts)?

Questions in the ToolKit:

- How are systems recovered and hardened to prevent similar incidents (restoration from clean backup, rebuilding system from scratch, changing passwords)?
- How does eradication and recovery impact on the customers' services and stored information?

Open issues in the new ecosystem

- Enforcement in the cloud challenging
- Difficult to determine exact location
- Difficult to determine processors of data
- Difficult to anticipate future usage of the service
  - Pearson, HP laboratories

Some approaches

Internally	◻ Risk assessment – how could we be harmed? ◻ Policy and processes (working groups)
With provider	◻ SLAs ◻ Audits
Externally	◻ Certification to standards ◻ Interoperability (API/open source) ◻ Security as a service

Some solutions?

Compliance gateways (Jesse Wilkins)

- Facetime: Security, Management & Compliance for Unified Communications, Web 2.0 and Social Networks
- Finra: social media compliance & Litigation protection
- Socialware: move from social silos to integrated social business processes

Virtual management layer (Steve Bailey)

- MCIS: Management Control & Information System

Research Questions?

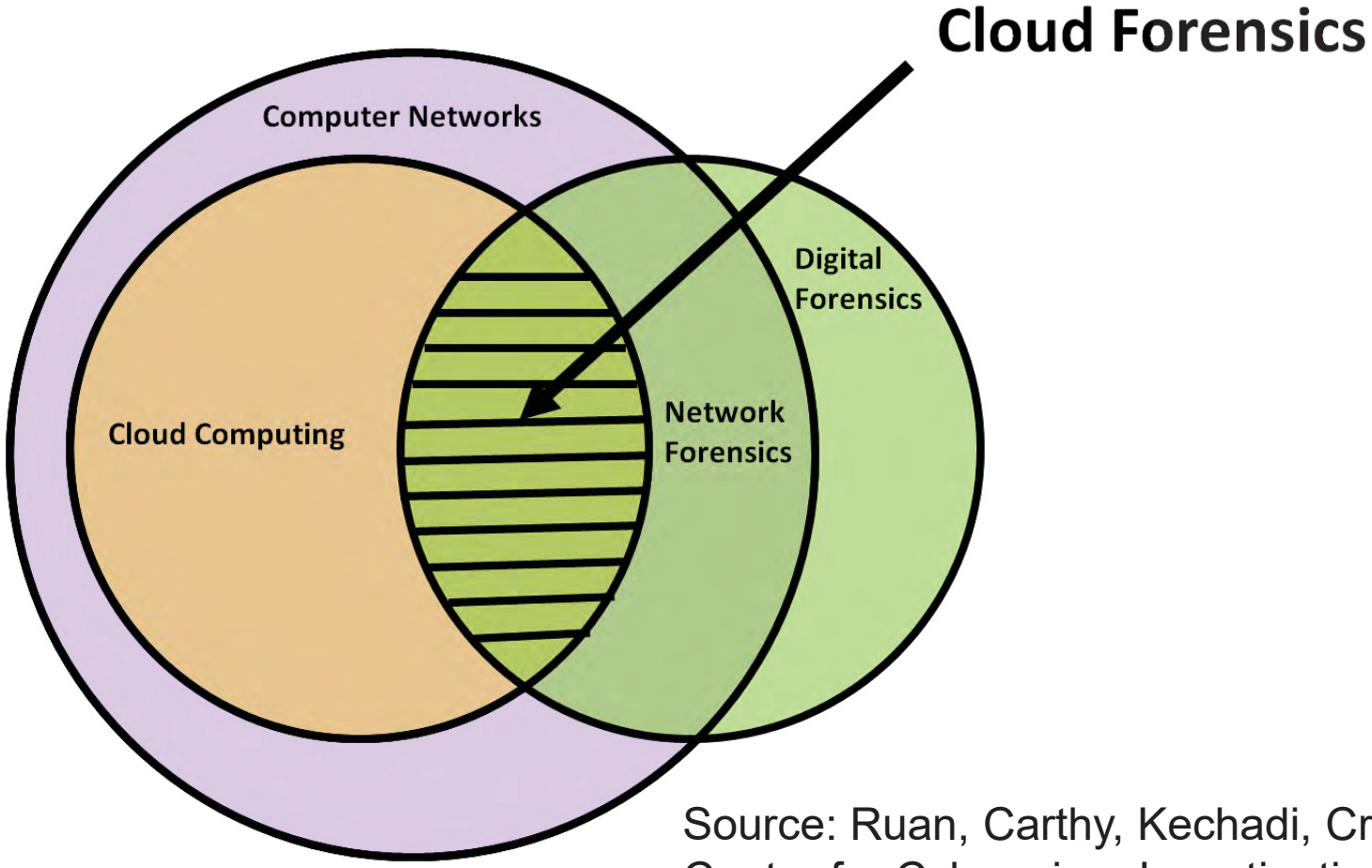
- Which tools are most appropriate for providing "broad dispersal of embedded forensic capability in the cloud, considering the path of an intruder is unpredictable".
- How can managing records systematically assist with "providing documentation of due care".
- On what basis would an organisation undertake the application of risk strategies for cloud systems?

Are we really ready?

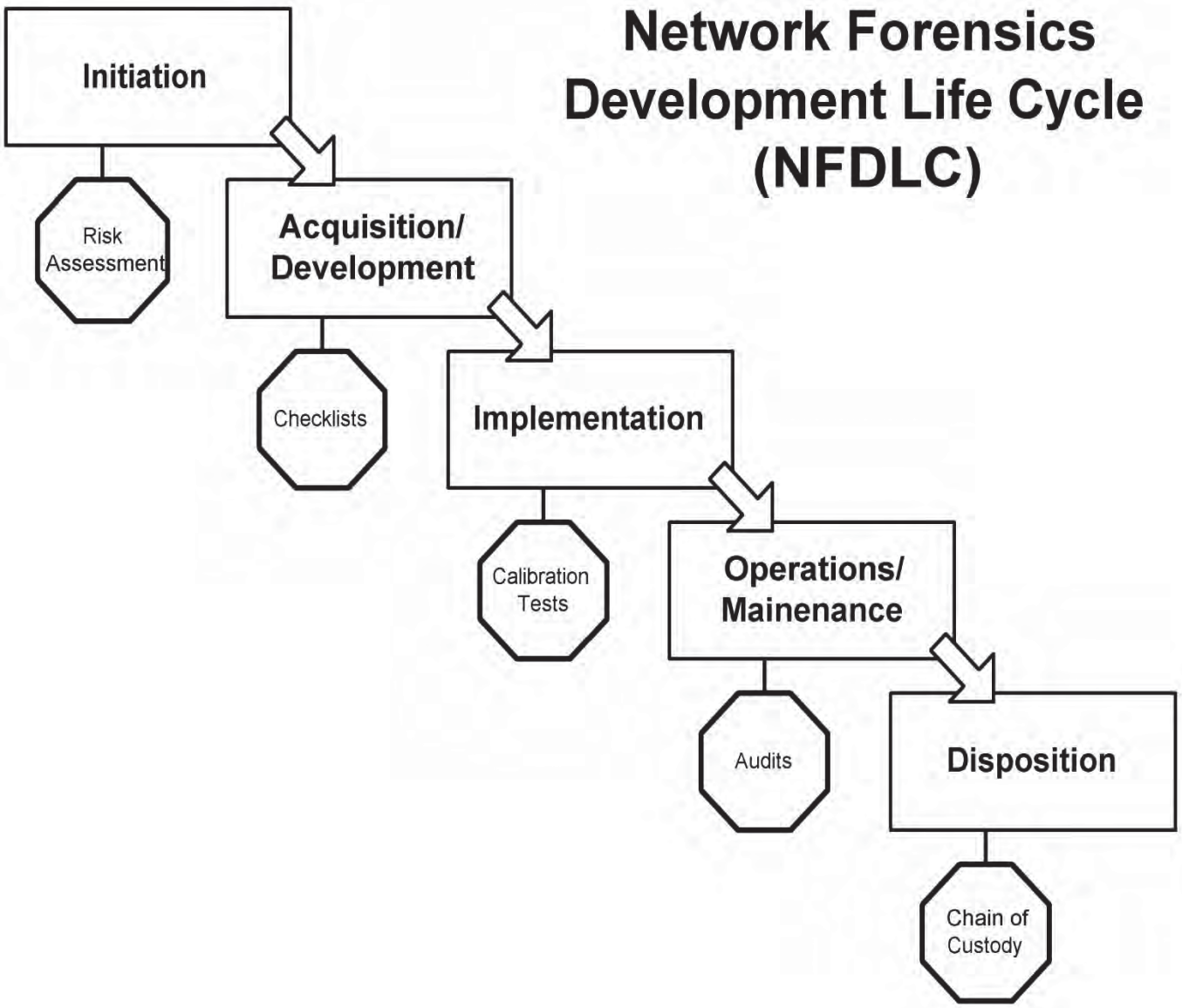
FORENSIC READINESS IN THE CLOUD

Definition of Cloud Forensics

The application of digital forensics in cloud computing as a subset of network forensics



Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin


Network Forensics Development Life Cycle (NFDLC)
Initiation
Risk Assessment
Acquisition/ Development
Checklists
Implementation
Calibration Tests
Operations/ Mainenance
Audits
Disposition
Chain of Custody

FRDLC additions

Information Systems Development Life Cycle Phases	Forensic Readiness DLC (Additional Procedures)	Forensic Readiness and the Cloud
Initiation Phase: preliminary risk assessment	Determine what aspects warrant digital forensic protection	*Risk management: Preparation for the cloud*
Acquisition/ Development Phase	Adhere to Rules of Evidence in system requirements	*Detailed Forensic requirements*
Implementation Phase	Perform baseline testing Perform mechanism verification/calibration tests	*Identify issues arising in systems as implemented and consider alternative solutions. Document the process*
Operation/ Maintenance Phase	Conduct verification/calibration audits	*Audit and change control procedures*
Disposition Phase	Incorporate chain of custody/ evidence preservation procedures	*Ensure secure deletion and disposal personal data*

Challenges

- **No.1 Access to forensic data**
  - Lack of customer control/knowledge of physical location of data
  - Data is mirrored during transitions
  - Lack of appropriate SLA terms of use to enable forensic readiness in the Cloud

Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin

Challenges

- **No.2 Identity management policies**
  - Strict access control but simple roles
  - Weak registration system facilitates anonymity

- **No.3 Recovery of deleted data**
  - Removal of mapping within domains starts immediately, and generally completes in seconds
  - Some data could remain present in the EBS (Elastic Block Storage) snapshot after deletion

Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin

Challenges

- **No.4 Encryption/Decryption**
  - Sensitive data most likely encrypted before uploading
  - Key retrieval issues

- **No.5 Segregation of forensic data**
  - Cloud infrastructure not designed for strong compartmentalization in a multi-tenant architecture
  - Tenants logically isolated; physically share infrastructure

Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin

Challenges

- **No. 6 Location/jurisdiction of forensic data**
  - Which country's laws preside?
  - Who owns the data?

- **No. 7 Lack of tools for large scale forensics**
  - Hypervisor layer tools

- **No.8 Chain of dependencies**
  - Chain of CSPs/customers highly dynamic
  - Interruption/corruption of chain challenges evidence

Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin

Challenges

- **No.9 Hypervisor investigation**
  - Attacks on hypervisor compromises all residents
  - No tools/procedures for investigating hypervisor
- **No.10 Synchronization of timestamps**
  - Across time zones, servers, servers on-the-fly
- **No.11 Unification of log formats**
  - Exacerbated in the cloud
- **No. 12 Proliferation of endpoints**
  - Exacerbated in the cloud

Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin

Challenges

- **No. 13 T&Cs in SLA regarding investigation**
- **No. 14 Legislation to facilitate collaboration and evidence retrieval**
- **No. 15 Access for civil litigation**
- **No. 16 General awareness and knowledge**

Source: Ruan, Carthy, Kechadi, Crosbie
Centre for Cybercrime Investigation,
University College Dublin

Conclusions

Cloud Computing:

- Provides huge benefits
- New opportunities for cyber crime
- Presents challenges for digital forensics readiness
- Requires new investigative approaches

References

- Extensive cloud computing and RM literature review https://docs.google.com/Doc?docid=0AUMD4SCCg7uaZGRxczNybndfMTZjODM4bXhmNw&hl=en
- Online resources have been bookmarked in Delicious and are available at http://www.delicious.com/nicoleschu/soacloud
- Toolkit available on the ARA website http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit.pdf
- Convery, Nicole and Kirsten Ferguson-Boucher, Storing Information in the Cloud – A Research Project. *Journal of the Society of Archivists in process for 2011.*

References (Cont'd.)

- J.Foley, "Federal Agencies Shift Into Cloud Adoption", InformationWeek, June 14, 2010
- Federal Bureau of Investigation, Regional Computer Forensics Laboratory (RCFL) Program Annual Report for Fiscal Year 2007, Washington, DC, 2008
- V.Roussev, L.Wang, G.Richard and L.Marziale, A Cloud Computing Platform for Large-Scale Forensic Computing, Advances in Digital Forensics V, Springer, 2009, pp201-215
- P.Mell, T.Grance, The NIST Definition of Cloud Computing Version 15, NIST, October 2009

References (Cont'd.)

- Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009
- Cloud Computing: Benefits, risks and recommendations for information security, European Network and Information Security Agency(ENISA), November 2009
- J.Oberheide, E.Cooke, F.Jahanian, "CloudAV:N-Version Antivirus in the Network Cloud", Proceedings of USENIX Security 2008, San Jose, California, July 2008, pp.91-106