Protecting Data and Privacy in a World of Clouds and Third Parties

Vincent Campitelli

Vice President, IT Risk Management

McKesson Corporation

What is Your Business Model? Economic Moats

"…In business, I look for economic castles protected by unbreachable 'moats' "

- Warren Buffett

The Rest of the World ……
Outsourcing /CloudSourcing !

Protecting Data and Privacy in a World of Clouds and Third Parties

WHY

Bother ?

Protecting Data and Privacy in a World of Clouds and Third Parties

Why Bother ?

It may be Required!

Protecting Data and Privacy in a World of Clouds and Third Parties

Why Bother ?

It may be Required!

Consumer Financial Protection Bureau regulations

PCI Security Standards Council

OCC Third Party Risk Guidance

NIST Cyber security Framework

HIPAA

ISO 27001/2

CUSTOMERS

Protecting Data and Privacy in a World of Clouds and Third Parties

Why Bother ?

It may cost you $$$$$

21 % of Breaches > 500 (HHS site)

TARGET

Tricare

NYC Health and Hospitals Corp

Utah Dept of Health

The Threat Landscape

Threats Causing Companies Most Concern

Risk and Controllability Ratings by Information Security Executives

n = 55.

Source: CEB 2012 Information Security Threat Landscape Survey.

More advanced attacks such as social engineering and state sponsored attacks are top concerns for information security executives.

Abbreviations Definitions

BYOD—Bring your own device

IaaS—Infrastructure as a service

SaaS – Software as a service

SCADA—Supervisory control and data acquisition

Do You Have a Program?

Do You Have a Program?

- Program Governance
- Policies, Standards, Procedures
- Contracts
- Vendor Risk Identification and Analysis
- Skills & Expertise
- Communication and Information Sharing
- Tools, Measurement and Analysis
- Monitoring and Review

Source: Shared Assessments Program, Vendor Risk Management Maturity Model (VRMMM)

A Process View

IT Vendors serving McKesson

2. Analyze

Determine the level of risk posed by each third party relationship using a risk model.

3. Evaluate

Implement due diligence activities commensurate with the risk rating.

4. Mitigate

Design appropriate risk mitigation plans to manage the residual risk of the relationship.

5. Monitor

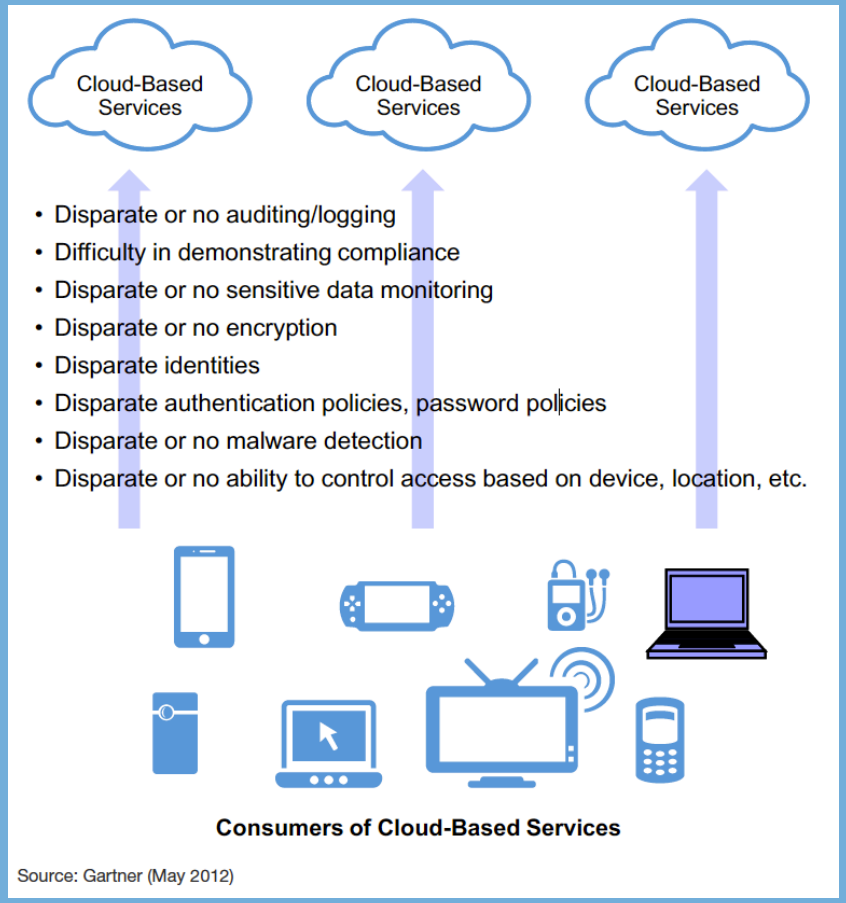
Design ongoing monitoring programs to identify events/ activities that alter risk profile.

How are They Identified?

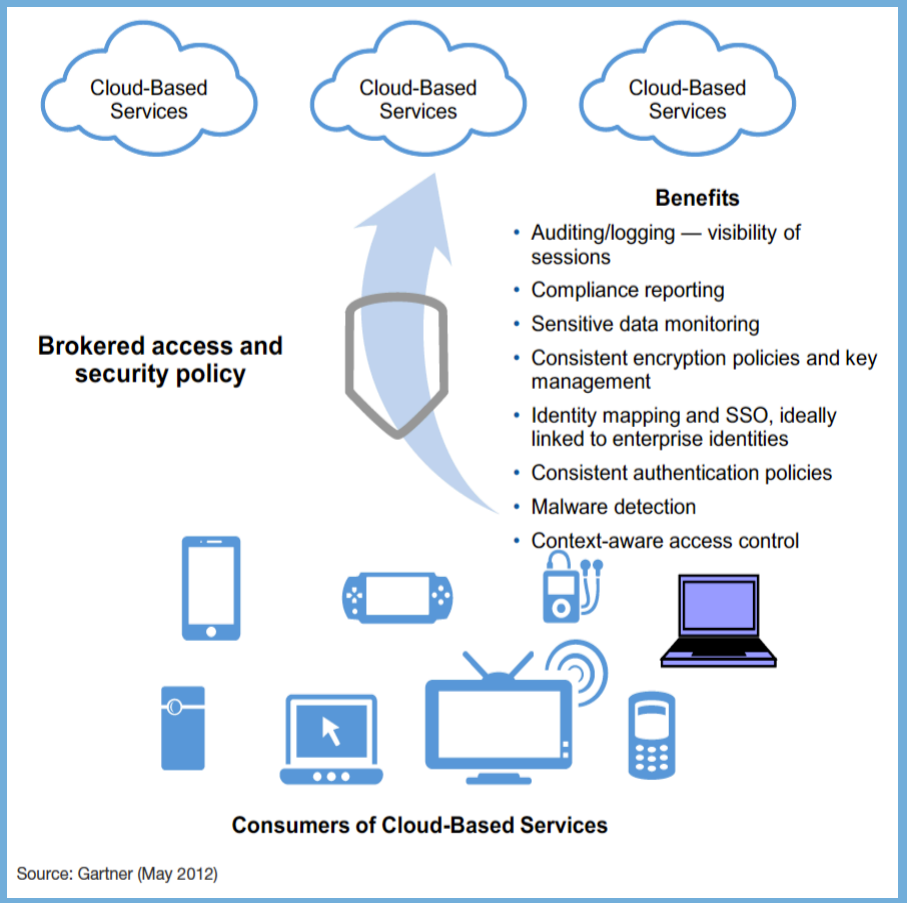
- Spend Analysis
- Corporate Procurement
- IT Procurement
- Legal /contracting
- Compliance Officers
- 3rd party cloud access security brokers?

What is a Cloud Access Security Broker?

Unbrokered Cloud Access



With Cloud Access Security Broker



Assess *Inherent* Risk

- Service description
- Contract Review
- R. A. questionnaire
- Risk Rating

Conduct Due Diligence

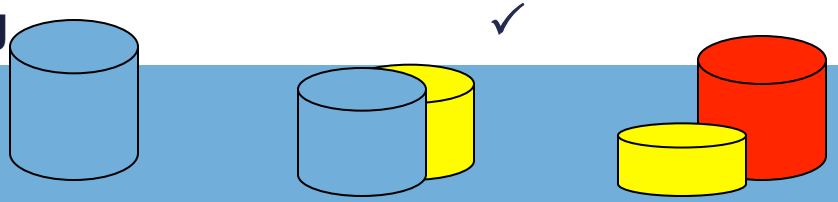
THE 3 BIG QUESTIONS ??

- WHAT IS DUE DILIGENCE?
- WHY DO I NEED IT?
- HOW DO I GO ABOUT IT?

Inherent Risk

- **Contract** ✓ ✓ ✓
- **Security Exhibits** ✓ ✓ ✓
- **BAA(PHI)** ✓ ✓ ✓
- **Validation procedures** ✓ ✓
- **On-going monitoring** ✓ ✓

Residual Risk



Cloud Service Providers – What's Different?

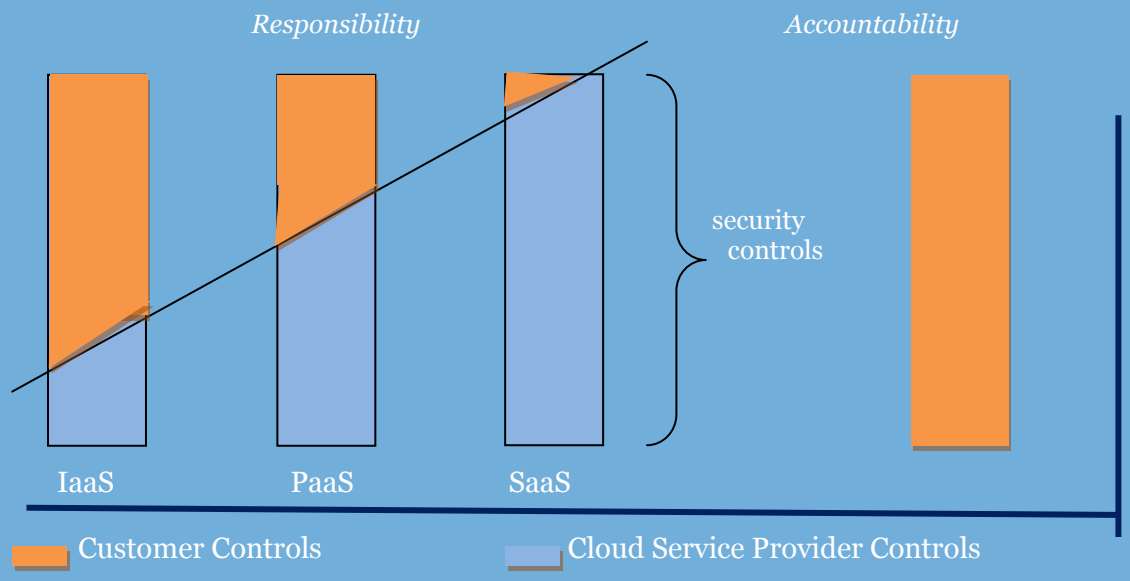
- Services based model
- Consumption based usage
- Multi-tenant
- Multi – modeled delivery
- Lack of transparency
- Indirect control/monitoring
- Data Retention/location/return/use
- Lack of maturity

Cloud Services – Responsibility/ Accountability

Responsibility and Accountability for Cloud Security Controls

As illustrated in Appendix C, in a private cloud owned and managed by McKesson, all of the security services and management thereof are the responsibility of the relevant McKesson IT organization. In public cloud settings, the division of security controls and management is a function of the cloud service model as shown below. A public cloud SaaS service places the least amount of control responsibility on McKesson. A current example of this is the cloud based CRM services provided by SalesForce.com. These responsibilities change significantly when PaaS or IaaS services are acquired. The gradation of additional security controls are detailed in Appendix C.

Division of Responsibility and Accountability for Security Controls
by Cloud Service Model



From a risk management perspective, it is important to understand that regardless of the cloud service model and the scope of security controls, McKesson is *accountable* for the effectiveness of the service provider's security controls. McKesson's approach to meeting this objective is detailed in the ISRM Vendor Assurance Program.

Control Responsibilities by Service Model

On-premise (Private)

On –Premise Service Stack	Customer Control Responsibilities	CSP Control Responsibilities	Audit and Compliance Responsibilities	Assurance Responsibilities
Applications	✓	N/A	Customer	Customer
Data	✓	N/A	Customer	Customer
Runtime	✓	N/A	Customer	Customer
Middleware	✓	N/A	Customer	Customer
O/S	✓	N/A	Customer	Customer
Security/Management	✓	N/A	Customer	Customer
Virtualization	✓	N/A	Customer	Customer
Servers	✓	N/A	Customer	Customert
Storage	✓	N/A	Customer	Customer
Networking	✓	N/A	Customer	Ciustomer
Facilities	✓	N/A	Customer	Customer

Legend:

- **Customer control responsibilities** – scope of security and related controls that are the responsibility of McKesson.
- **CSP Control responsibilities** - scope of security and related controls that are the responsibility of cloud service provider(s).
- **Audit and Compliance responsibilities** – scope of responsibilities to meet audit and relevant regulatory compliance requirements.
- **Assurance Responsibilities** – scope of responsibilities to monitor and review third party requirements.

= customer responsibilities
= CSP responsibility
= shared responsibility

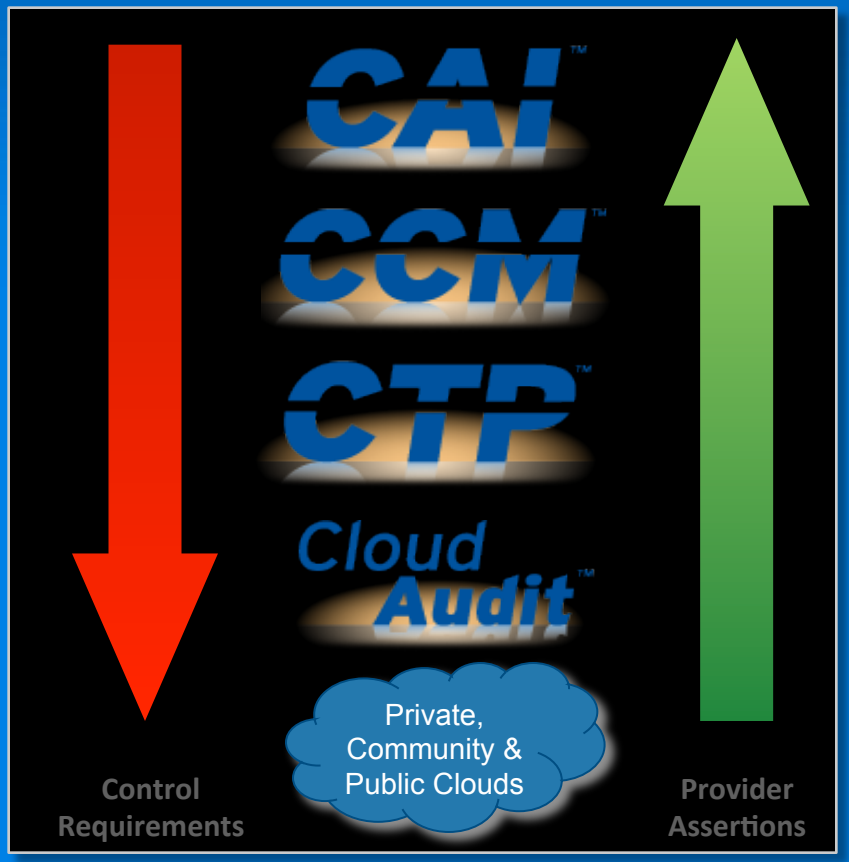
An Approach for Cloud

Assessment Resources

- ✓ NIST / FISMA
- ✓ HiTech
- ✓ Cloud Security Alliance
- ✓ ISO 27001

CLOUD Security Alliance

- *GRC - Toolkit*
  - *Family of 4 research projects*
    - *Cloud Controls Matrix (CCM)*
    - *Consensus Assessments Initiative (CAI)*
    - *Cloud Audit*
    - *Cloud Trust Protocol (CTP)*



CSA CCM controls – Key Controls

Domain Name	Control Type[1]	No of Controls	No of Key[2] Controls
1. Application and Interface Security	Specific	4	0
2. Audit Assurance & Compliance	Common	3	1
3. Business Continuity Mgmt and Operational Resilience	Common	12	4
4. Change Control & Configuration Management	Specific	5	4
5. Data Security & Information Lifecycle Management	Specific	8	4
6. Datacenter security	Common	9	8
7. Encryption and Key Management	Specific	4	4
8. Governance and Risk Management	Common	12	5
9. Human Resources	Common	12	5
10. Identity and Access Management	Specific	13	13
11. Infrastructure & Virtualization Security	Specific	12	12
12. Interoperability & Portability	Common	5	1
13. Mobile Security	Specific	20	8
14. Security, Incident Management, E-discovery & Cloud Forensics	Common	5	4
15. Supply Chain Management, Transparency and Accountability	Common	9	4
16. Threat and Vulnerability Management	Specific	3	3
		-----	------
		133	80

Risk Game Changers

Mitigation Options	Non-cloud	Cloud
Right to Audit	↑	↓
Contract terms	↑	
SLA's	↓	↓
Security SLA's	↓	↑
Conditional Acceptance		↑
3rd party reviews • annual requirement • Scope adjustments • Corrective action plans		↑ ↑ ↑ ↑
Encryption / Key Management		↑
Multi-factor authentication		↑

CSP assessment

Domain	Control Objective	Relevance	Yes	No	Additional info Required (AIR)
AIS	1	✓	✓		
	2			✓	
	3	✓			✓
	4				
AAC	1				
Totals	133	R(sum)	X(sum)	Y(sum)	Z(sum)
Index		R/133	X/133	Y/133	Z/133
		.56	.60	.15	.24

CSP Comparison

Vendors	Relevant Index	Yes Index	No Index	AIR Index
Vendor 1	.70	.85	.15	.05
Vendor 2	.70	.80	.20	.00
Vendor n	.70	.65	.30	.05

Ongoing Monitoring

- Develop assurance plan
- Manage assurance schedule
- Track Open findings/issues
- Enterprise rating/ visibility
- Create Vendor Scorecard

Questions