

iSOA Cloud Computing

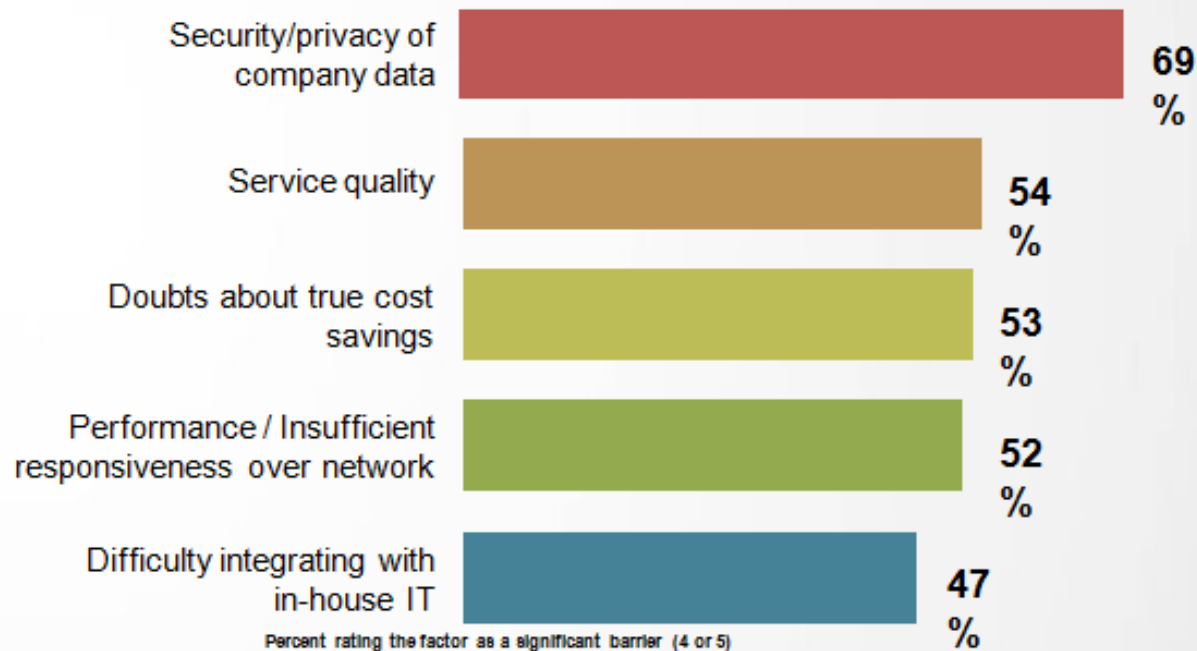
Cloud Security

Bryon Kataoka

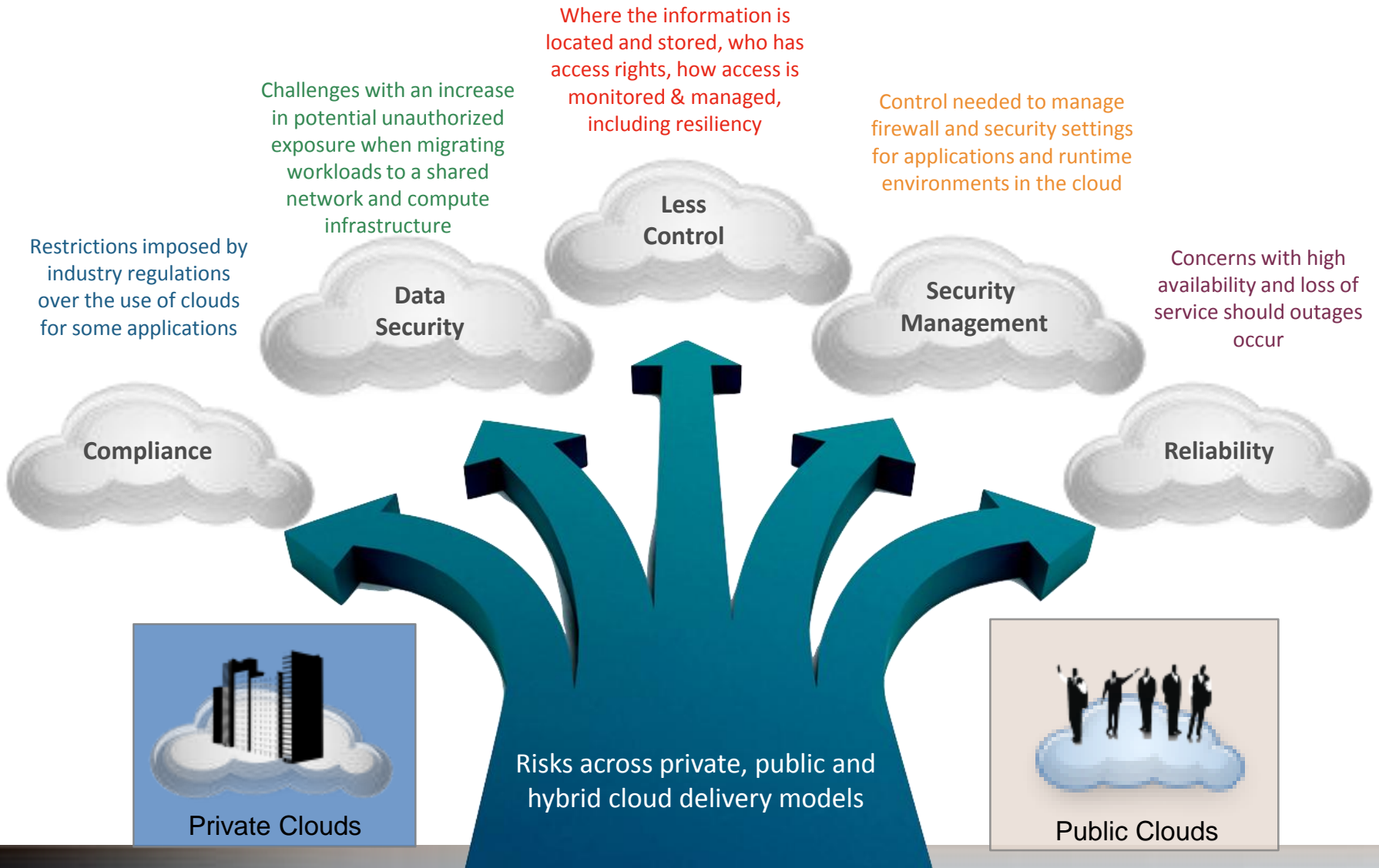
iSOA Group CTO and Trusted Advisor

Security is a top concern with cloud computing...

What, if anything, do you perceive as actual or potential barriers to acquiring public cloud services?



Source: IBM Market Insights, Cloud Computing Research, July 2009. n=1,090



“Cloud-computing environments have IT risks in common with any externally provided service. There are also some unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing.”

[Source Gartner August 31, 2011](#)

An IBM publication featuring analysis by Gartner

Dynamic Infrastructure

Delivering Superior Business and IT Services with Agility and Speed

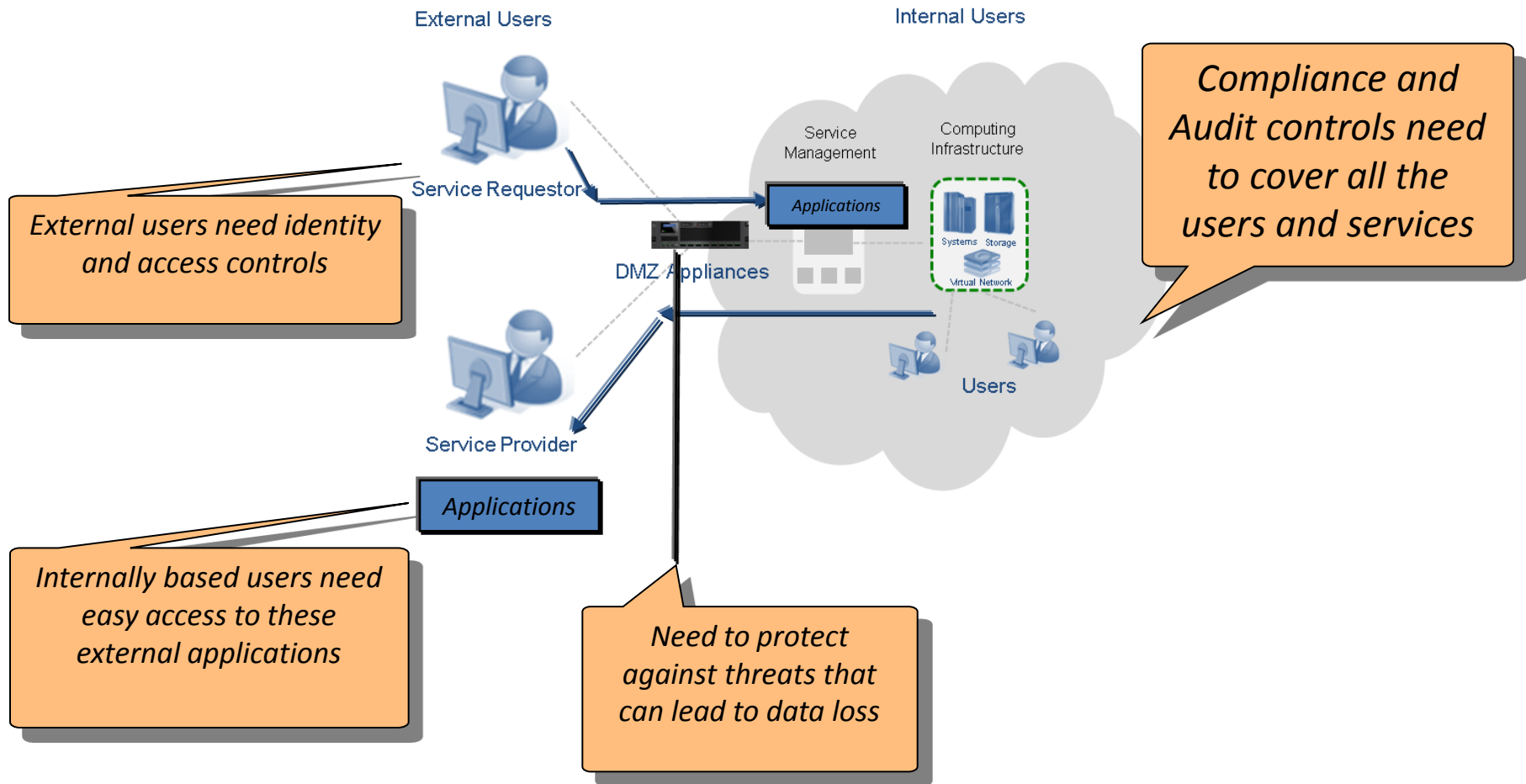


Assessing the Security Risks of Cloud Computing

- Often use 3rd party services (lost cost to vendor, higher risk for consumer)
- Access to key risk areas
 - Data segregation
 - Privacy
 - Access control
 - Availability
 - Recovery
- Consider the above just like any internal project
- Location independent service providers could use sub-vendors. (Possible legal and compliance issue that are unique to cloud)
- Business executives making un-authorized use of external services can circumvent corporate security practices and create unrecognized and unmanaged information related risks.



What does this mean for Your Company's Security?



Cloud deployments need the same or better security versus traditional deployments.

Why DataPower & iSOA Group for Security

- DataPower



- Cast Iron







Go To IBM Partner for
DataPower
Numerous integrations in
multiple industries

- Financial
- Retails
- Energy
- Government
- Telecommunications
- Healthcare



Smarter Business Agility with WebSphere DataPower Appliances

-  **SECURE** your SOA, Web 2.0, B2B, and Cloud environments
-  **SIMPLIFY** your connectivity infrastructure
-  **ACCELERATE** your time to value
-  **GOVERN** your evolving IT architecture



WebSphere DataPower Appliances provide a low startup cost, helping clients **increase ROI** and **reduce TCO** with specialized, consumable, dedicated appliances that combine **superior performance** and **hardened security**.

Integration Appliance **XI52**

- Consumable hardware ESB
- Any-to-any conversion at wire-speed
- Intelligent Load Distribution and Dynamic Routing
- Web services security
- Rich authentication and authorization
- Centralized policy management

B2B Appliance **XB62**

- Unparalleled B2B performance
- Secure B2B messaging (EDIINT AS1, AS2, AS3)
- Trading Partner Profile management
- Transaction viewing and resending
- EDI and ebXML Support
- Native MQ FTE Integration

Edge Appliance **XE82**

- WebSphere Application Accelerator
- Designed for web applications over Public Networks and SaaS applications over Hybrid Networks
- Web Application Gateway
- Web Services Proxy
- Intelligent Workload Management



DataPower

- Agility
- B2B integration
- Web Services integration
 - Using WS standards
- Authentication/Authorization
 - LDAP, SAML
- Application Integration
- Trusted Security



Cast Iron

- Public Cloud Integration
 - Salesforce
 - Many more
- Private Cloud Integration
 - Siebel
 - PeopleSoft
 - And more
- Legacy integration
 - Direct to DB
 - CSV conversions
 - FTP integrations



Marriage

- DataPower



- Cast Iron





Backup



Customers require proper authentication of cloud users.

Implement strong identity and access management

- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems
- A standards-based, single sign-on capability can help simplify user logons for both internally hosted applications and the cloud

Supporting IBM Products, Services and Solutions

IBM Tivoli Federated Identity Manager

Securely manage cloud identities

Employ user-centric federated identity management to increase customer satisfaction and collaboration

IBM Tivoli Security Information and Event Manager

Optimize security & compliance efforts

Monitor user activity for accidental or malicious activity that could put information at risk

Customers cite data protection as their most important concern.

Ensure confidential data protection

- Use a secure network protocol when connecting to a secure information store.
- Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.
- Sensitive information not essential to the business should be securely destroyed.

Supporting IBM Products, Services and Solutions

IBM Data Security Services

Protect data and enable business innovation

Solutions for network data loss prevention, endpoint encryption, endpoint data loss prevention, and log analysis



Enhanced

IBM Tivoli Key Lifecycle Manager

Manage the encryption key lifecycle

Simplify, centralize, automate and strengthen key lifecycle processes.

Enhance data security and reduce risk of data breaches.

Customers expect a secure cloud operating environment.

Maintain environment testing and vulnerability/intrusion management

- Isolation between tenant domains
- Trusted virtual domains: policy-based security zones
- Built-in intrusion detection and prevention
- Vulnerability Management
- Protect machine images from corruption and abuse

Supporting IBM Products, Services and Solutions

 NEW

Managed Security Services – hosted
vulnerability management

Identify vulnerabilities and manage risk to
reduce cost

Cloud-based security service to identify
vulnerabilities across network devices,
servers, databases and web applications

IBM Security Network IPS Server Protection
Network layer protection with IBM Security
Intrusion Prevention System

Protect users and applications from threat
Preserve the integrity of cloud-deployed
assets.

Customers expect cloud data centers to be physically secure.

Implement a physical environment security plan

- Ensure the facility has appropriate controls to monitor access.
- Prevent unauthorized entrance to critical areas within facilities.
- Ensure that all employees with direct access to systems have full background checks.
- Provide adequate protection against natural disasters.

Supporting IBM Products, Services and Solutions

IBM Physical Security Services

Defend and help secure physical environments

A full suite of digital security solutions and site assessments that can be integrated with your network and IT systems