Making Cloud Computing Safe
Trust, security, resiliency, availability and complexity

Stuart McIrvine
Cloud portfolio strategy
IBM Enterprise Initiatives
May 19, 2010
Concerns about data security and privacy are the primary – but not the only - barriers to public cloud adoption

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percent Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/privacy of company data</td>
<td>69%</td>
</tr>
<tr>
<td>Service quality</td>
<td>54%</td>
</tr>
<tr>
<td>Doubts about true cost savings</td>
<td>53%</td>
</tr>
<tr>
<td>Performance / Insufficient responsiveness over network</td>
<td>52%</td>
</tr>
<tr>
<td>Difficulty integrating with in-house IT</td>
<td>47%</td>
</tr>
</tbody>
</table>

Respondents could select multiple items

Source: IBM Market Insights, Cloud Computing Research, July 2009. n=1,090
### Specific customer concerns related to security and cloud

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of intellectual property and data</td>
<td>30%</td>
</tr>
<tr>
<td>Ability to enforce regulatory or contractual obligations</td>
<td>21%</td>
</tr>
<tr>
<td>Unauthorized use of data</td>
<td>15%</td>
</tr>
<tr>
<td>Confidentiality of data</td>
<td>12%</td>
</tr>
<tr>
<td>Availability of data</td>
<td>9%</td>
</tr>
<tr>
<td>Integrity of data</td>
<td>8%</td>
</tr>
<tr>
<td>Ability to test or audit a provider’s environment</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey
Cloud attributes that greatly affect information security:

- **INTERNAL DELIVERY** ➔ **EXTERNAL DELIVERY**
- **SINGLE-TENANCY** ➔ **MULTI-TENANCY**
- **IT-SERVICE** ➔ **SELF-SERVICE**
- **SLOW PROVISIONING** ➔ **RAPID PROVISIONING**
Security complexities raised by virtualization

- **New complexities**
  - Dynamic relocation of VMs
  - Increased infrastructure layers to manage and protect
  - Multiple operating systems and applications per server
  - Elimination of physical boundaries between systems
  - Manually tracking software and configurations of VMs

### Before Virtualization
- 1:1 ratio of OSs and applications per server

### After Virtualization
- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure
Cloud Security: Simple Example

**Today’s Data Center**

*We Have Control*
- It’s located at X.
- It’s stored in server’s Y, Z.
- We have backups in place.
- Our admins control access.
- Our uptime is sufficient.
- The auditors are happy.
- Our security team is engaged.

**Tomorrow’s Cloud**

*Who Has Control?*
- Where is it located?
- Where is it stored?
- Who backs it up?
- Who has access?
- How resilient is it?
- How do auditors observe?
- How does our security team engage?

© 2010 IBM Corporation
Categories of Cloud Risks

Less Control
Many companies and governments are uncomfortable with the idea of their information located on systems they do not control. Providers must offer a high degree of security transparency to help put customers at ease.

Data Security
Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure. Authentication and access technologies become increasingly important.

Reliability
High availability will be a key concern. IT departments will worry about a loss of service should outages occur. Mission critical applications may not run in the cloud without strong availability guarantees.

Compliance
Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications. Comprehensive auditing capabilities are essential.

Security Management
Providers must supply easy controls to manage firewall and security settings for applications and runtime environments in the cloud.
One-size does not fit-all:

Different cloud workloads have different risk profiles

- **Today's clouds are primarily here:**
  - Lower risk workloads
  - One-size-fits-all approach to data protection
  - No significant assurance
  - Price is key

- **Tomorrow’s high value / high risk workloads need:**
  - Quality of protection adapted to risk
  - Direct visibility and control
  - Significant level of assurance

**Need for Security Assurance**

- Low
- High

**Mission-critical workloads, personal information**

- Analysis & simulation with public data
- Training, testing with non-sensitive data

**Business Risk**

- Low-risk
- Mid-risk
- High-risk
One-size **does not** fit-all:

*Different cloud types have different security responsibilities*
Gartner’s security risks of Cloud
…map directly to the IBM Security Framework.

Privileged User Access
Data Segregation
Data Recovery
Investigative Support
Regulatory Compliance
Data Location
Disaster Recovery

IBM Cloud Security Guidance document

- Based on cross-IBM research and customer interaction on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:
  
  - Building a Security Program
  - Confidential Data Protection
  - Implementing Strong Access and Identity
  - Application Provisioning and De-provisioning
  - Governance Audit Management
  - Vulnerability Management
  - Testing and Validation

http://www.redbooks.ibm.com/abstracts/redp4614.html
IBM Security capabilities

= Services

= Products

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

= more info

Security Governance and Compliance Services

Identity and Access Mgmt. Services

Identity Management

Access Management

Data Security Services

Data Loss Prevention

Encryption and Key Lifecycle Mgmt.

Messaging Security

E-mail Security

Database Monitoring and Protection

Application Security Services

App Vulnerability Scanning

Web App Firewall

Web/URL Filtering

Vulnerability Assessment

Mainframe Security

Threat Assessment, Mitigation, and Mgmt. Services

App Source Code Scanning

Data Masking

Virtual System Security

Access and Entitlement Mgmt.

SOA Security

Physical Security Services

Security Events and Logs

IPS

SIEM and Log Mgmt

= more info

© 2010 IBM Corporation
IBM is a visionary in the field of IT Security
Enabling more advanced, yet secure services for the Smarter Planet

IBM Research Projects

Homomorphic Encryption

Enterprise Security Architecture

High Tech Risk Analytics

International Association of Privacy Professionals recognized IBM Research as one of the “Top Privacy Innovators” in 2009
IBM Cloud Security in Action - LotusLive

Security through the entire lifecycle and stack
IBM has established a more efficient and dynamic, cross-company approach for its IT security portfolio in which research, design, development, marketing, services and support for IT security solutions for IBM clients worldwide are consolidated and linked together.

- **IBM is the Trusted Partner** delivering products and services recognized for leadership in IT security

- **IBM’s philosophy of Secure By Design;** Factor Security and Privacy into the initial design, not bolted on after the fact

- **IBM security solutions allow customers to address the 3 Cs;** Complexity, Compliance and Cost

one coordinated voice for security.
Thank you!

For more information, please visit:
  w3.ibm.com/cloud
Customers require **visibility** into the security posture of their cloud.

**Implement a governance and audit management program**

- Establish 3rd-party audits (SAS 70, ISO27001, PCI)
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Support for forensics and e-Discovery

**Supporting IBM Products, Services and Solutions**

**IBM Information Security Assessment**

Assessing security to create a roadmap to reduced risk

A comprehensive evaluation of an organization's existing security policies, procedures, controls and mechanisms.

**IBM Resiliency Consulting Services**

Assessment and planning – resilient cloud validation

A comprehensive evaluation of an organization's existing disaster recovery plans and alignment to the environment.
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

**IBM Information Protection Services**
- **Continuous data protection**
  - Remote Data Protection Services
  - Email Management Express
  - Fastprotect Online
Customers require **secure cloud applications** and **provider processes**.

**Establish application and environment provisioning**

- Implement a program for application and image provisioning.
- A secure application testing program should be implemented.
- Ensure all changes to virtual images and applications are logged.
- Develop all Web based applications using secure coding guidelines.

**Supporting IBM Products, Services and Solutions**

**IBM Rational AppScan**
Secure testing for web application vulnerability
Solution features a scalable enterprise architecture that enables centralized scanning of multiple applications simultaneously

**IBM WebSphere DataPower XML Security Gateway XS40**
Secure web facing applications vulnerability at the code level
Solution features an integrated appliance that provides ongoing security protection, policy management, and governance for securing web facing applications
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**

- **IBM Virtual Server Security for VMware**
  Protection of cloud-based infrastructure
  Provides market-leading intrusion prevention, firewall and visible security for virtual environments

- **IBM Endpoint Data Protection**
  Remote protection of sensitive data
  - Prevent data access when a device is lost or stolen
  - Protect sensitive data when stored, accessed, transmitted or shared
  - Monitor usage of sensitive data
  - Enforce policies at the end-user level
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.
Recent accolades

“Taking a strategic, comprehensive and systematic approach to security is not something an organization can achieve overnight... This can only be done in collaboration with trusted partners, armed with the most current and objective knowledge of what works and what doesn’t in planning for both today’s and tomorrow’s risks.

In light of IBM’s growing presence in security and compliance, and the weight of its impact on the larger issues of business risk control, these factors should make IBM a primary partner to consider in shaping strategy and evaluating technologies and services that make a difference. Few others have the range of capabilities of today’s IBM for addressing the challenge—fewer still have the resources of an IBM for understanding the nature of business risks and emerging threats, and how best to address them going forward.”

Enterprise Management Associates® (EMA™), Dec 2009

“... there is a profound transition in the way organizations assess security needs, acquire security technologies, measure risk, and conduct security operations. All of these trends shift the balance of power from security point tool vendors to larger firms with broad security services and product offerings.

IBM’s combination of products, services, customer reach, and rich resources give it a unique position in the security industry. IBM and a few others can help any sized customer with security, regardless of whether they need help securing their business, implementing an enterprise security initiative, or fixing a big security problem.”

Enterprise Strategy Group, Nov 2008

“Security has become a C-level conversation, and enterprises are looking for reputable vendors with the capability to help customers manage risks and reduce complexity. IDC believes IBM has recognized this trend and has created comprehensive security packages that leverage various products to provide for multiple layers of security to customers.”

IDC, IBM Security Summit, Doc # 215370, Nov 2008

IBM was named the “Best Security Company”
By SC Magazine
## IBM Security: Sum is greater than its parts

<table>
<thead>
<tr>
<th>Brand</th>
<th>Marketshare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forrester</td>
<td>Wave: User Account Provisioning (TIM)</td>
</tr>
<tr>
<td></td>
<td>Wave: Enterprise Security Information Management</td>
</tr>
<tr>
<td>Gartner</td>
<td>MQ: User Provisioning (TIM)</td>
</tr>
<tr>
<td></td>
<td>MQ: Web Access Management (TAM)</td>
</tr>
<tr>
<td></td>
<td>MQ: Security Information &amp; Event Management (TSOM)</td>
</tr>
<tr>
<td>Gartner</td>
<td>ISS Network Security, Firewalls and Managed Services</td>
</tr>
<tr>
<td>Gartner</td>
<td>Marketshare: Application Security Vulnerability Scanning, 2006 (Rational AppScan)</td>
</tr>
<tr>
<td>Gartner</td>
<td>Identity Management (TIM, TAM, FIM, TDI, TDS)</td>
</tr>
<tr>
<td>Frost &amp; Sullivan</td>
<td>Marketshare: Managed Security Services</td>
</tr>
<tr>
<td>Frost &amp; Sullivan</td>
<td>Marketshare: Identity and Access Management</td>
</tr>
<tr>
<td>IDC</td>
<td>Marketshare: Application Vulnerability Assessment (Rational AppScan, Ounce Labs)</td>
</tr>
</tbody>
</table>

**Leadership Titles**

- Leader
- Ranked #1
IBM is working with clients worldwide to implement the new Enterprise Security Architecture

- Combines:
  - IBM Methodology for Architecting Secure Solutions
  - Enterprise architecture framework of IBM Global Services Method

- The new architecture is defined around the concept of six security zones of control
  *Boundary control, authentication, authorization, integrity services, audit/monitoring, and cryptographic services*