Acting in my previous role as CTO for Security, IBM Corporation (but all opinions are just mine …)

Industry Perspective on Cloud Security
Outline

- Brief Introduction to Cloud Computing
- Security: Grand Challenge for the Adoption of Cloud Computing
- IBM and Cloud Security
Brief Introduction to Cloud Computing
“Cloud” is a new consumption and delivery model inspired by consumer Internet services.

Enabled by
- Ubiquitious network access
- Pooling and virtualization of resources
- Automation of service management
- Standardization of workloads

Cloud enables:
- Self-service
- Location independence
- Sourcing options
- Flexible payment models
- Economies-of-scale

“Cloud” represents:
- The industrialization of delivery for IT supported services
## IT Benefits from Cloud Computing are Real…

### Results from IBM cloud computing engagements

<table>
<thead>
<tr>
<th>Increasing speed and flexibility</th>
<th>Test provisioning</th>
<th>Change management</th>
<th>Release management</th>
<th>Service access</th>
<th>Standardization</th>
<th>Metering/billing</th>
<th>Payback period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Weeks</td>
<td>Months</td>
<td>Weeks</td>
<td>Administered</td>
<td>Complex</td>
<td>Fixed cost</td>
<td>Years</td>
</tr>
<tr>
<td></td>
<td>Minutes</td>
<td>Days/hours</td>
<td>Minutes</td>
<td>Self-service</td>
<td>Reuse/share</td>
<td>Variable cost</td>
<td>Months</td>
</tr>
<tr>
<td>Reducing costs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server/storage utilization</td>
<td>10–20%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>70–90%</td>
</tr>
<tr>
<td>Payback period</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Based on IBM and client experience.
Spectrum of Deployment Options for Cloud Computing

**Private**
IT capabilities are provided “as a service,” over an intranet, within the enterprise and behind the firewall

- Enterprise data center
  - Private cloud
  - Managed private cloud

- Third-party operated

**Public**
IT activities / functions are provided “as a service,” over the Internet

- Shared cloud services

**Hybrid**
Internal and external service delivery methods are integrated through hybrid cloud gateways

- Public cloud services

- Managed private cloud
  - Hosted private cloud
  - Third-party hosted and operated
Clients Interviewed Significantly Prefer Private over Public

Overall, how appealing are the public, private and hybrid delivery models for your company?

<table>
<thead>
<tr>
<th>Model</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>64%</td>
</tr>
<tr>
<td>Public</td>
<td>30%</td>
</tr>
<tr>
<td>Hybrid</td>
<td>38%</td>
</tr>
</tbody>
</table>

Public vs. Private trade-off considerations

**Benefits**
- Increased Speed
- Lower Cost

**Security**
- Insecure or incomplete data deletion
- Isolation failure
- Malicious Insiders
- Management infrastructure compromise

**Governance**
- Resiliency
- Level and source of support
- Architectural & management control
- Compliance

**Customization / specialization**

Source: IBM Market Insights, Cloud Computing Research, July 2009. n=1,090
Workloads may be at Different Levels of Cloud Readiness

- Ready for Cloud
- Analytics
- Infrastructure Storage
- Industry Applications
- Collaboration
- Medical Imaging
- Financial Risk
- Energy Management
- Workplace, Desktop & Devices
- Business Processes
- Disaster Recovery
- Development & Test
- Infrastructure Compute

- Information intensive
- Isolated workloads
- Mature workloads
- Pre-production systems
- Batch processing

- Ready for Cloud
- Sensitive Data
- Highly Customized
- Not yet virtualized 3rd party SW
- Complex processes & transactions
- Regulation sensitive

- New workloads made possible by clouds ...

- Market bias:
  - Private cloud
  - Public cloud

May not yet be ready for migration ...
Security – Grand Challenge for the Adoption of Cloud Computing
Where is the Data? – Moving from Private to Public Leads to a Real or Perceived Loss of Control

We Have Control

- It's located at X.
- We have backups.
- Our admins control access.
- Our uptime is sufficient.
- The auditors are happy.
- Our security team is engaged.

Who Has Control?

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

33% Of respondents are concerned with cloud interfering with their ability to comply with regulations

80% Of enterprises consider security #1 inhibitor to cloud adoptions

48% Of enterprises are concerned about the reliability of clouds

Source: Driving Profitable Growth Through Cloud Computing, IBM Study, 2008 (conducted by Oliver Wyman)
### Specific Customer Concerns Related to Security

<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, 2007
One-size does not fit-all:
Different cloud workloads have different risk profiles

- **Low-risk workloads**: Training, testing with non-sensitive data
- **Mid-risk workloads**: Analysis & simulation with public data
- **Mission-critical workloads, personal information**: High-risk workloads

**Need for Security Assurance**

**Low**
- **Training, testing with non-sensitive data**

**High**
- **Mission-critical workloads, personal information**

**Business Risk**

- **Low-risk**
- **Mid-risk**
- **High-risk**

**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

One-size does not fit-all: Different cloud workloads have different risk profiles
What is Cloud Security?

Confidentiality, integrity, availability of business-critical IT assets
Stored or processed on a cloud computing platform

There is nothing new under the sun but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary
Cloud Security = SOA Security + Secure Virtualized Runtime

Service-oriented Architecture
- SOA Security model and protocols apply
- Technical challenges: multi-tenancy, across trust domain, REST-based, new protocols (e.g., OpenID)
- Definitional challenges: profiles and security SLAs for cloud

Virtualized Runtime

Top Threats and Risks in Cloud Computing
- Process/VM Isolation, data segregation, multi-tenancy
- Malicious insiders (co-tenants, cloud provider)
- Management (incl. self-service) interface compromise
- Insecure interfaces and APIs
- Uncertainty over data location
- Data protection and security
- Data recovery, resiliency
- Insecure or incomplete data deletion
- Account or service hijacking
- Abuse of cloud services (extrusion)
- Compliance risks

IBM and Cloud Security
IBM's Strategy for Cloud Security

IBM Security Framework: Risk management-based approach to security

Provider of Security Products for Clouds

Provider of Cloud-based Security Services

Provider of Secure Clouds
IBM Cloud Security Guidance

Based on cross-IBM research and customer interaction on cloud security

Highlights a series of generic best practice controls, which can be further refined by workload

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
Applying Security to Software as a Service

- Governance & Compliance
  - Policy Management
  - Security Information
  - Event Management
  - Directory Integration
  - Usage and Accounting

- People & Identity
  - Access Management
  - Application Gateway
  - User Management
  - Directory Services
  - Federated Identity

- Data & Information
  - Data Protection
  - Data Encryption
  - E-Discovery
  - Data Redaction
  - Resiliency Services

- Application & Process
  - Vulnerability Scanning
  - Anti-Spam
  - Anti-Virus
  - Application Acceleration and analysis

- Network, Server & Endpoint
  - Intrusion Prevention
  - Firewalls
  - Network Isolation/routing
  - VPN connectivity
  - Data Leakage Prevention
Applying Security to Infrastructure as a Service

Governance & Compliance
- Security Event Information Management
- Security Policy Management
- Directory Integration
- Virtual Image Management
- Utilization Monitoring
- Integration API's
- Image Migration Utilities

People & Identity
- Federated Identity
- Directory Services
- Access Management

Data & Information
- Encryption Technologies
- Data Protection Services*
- E-Discovery Support
- Image Destruction
- Resiliency Services

Application & Process
- Vulnerability Scanning

Network, Server & Endpoint
- Intrusion Prevention
- Data Leakage Prevention
- Virtual Image Protection
- Firewalls
- Network Isolation/Routing
- VPN Connectivity
- Traffic Analytics

* optional based on virtual guest
Hybrid as a Service and Security

- Security Event Information Management
- Security Policy Management
- Directory Integration
- Virtual Image Management
- Utilization Monitoring
- Integration API's
- Image Migration Utilities

- Federated Identity
- Directory Services
- Access Management

- Encryption Technologies
- Data Protection Services*
- E-Discovery Support
- Image Destruction
- Resiliency Services
- Key Management

- Vulnerability Scanning
- Asset management
- License Management

- Intrusion Prevention
- Data Leakage Prevention
- Virtual Image Protection
- Firewalls
- Network Isolation/Routing
- VPN Connectivity
- Traffic Analytics

* optional based on virtual guest
Cloud Service Model Suggests Split of Responsibilities between Provider and Subscriber

Who is responsible for security at the … level?

<table>
<thead>
<tr>
<th>Datacenter</th>
<th>Infrastructure</th>
<th>Middleware</th>
<th>Application</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
<td>Subscriber</td>
<td>Provider</td>
<td>Subscriber</td>
<td>Subscriber</td>
</tr>
<tr>
<td>Provider</td>
<td>Subscriber</td>
<td>Provider</td>
<td>Subscriber</td>
<td>Subscriber</td>
</tr>
<tr>
<td>Provider</td>
<td>Subscriber</td>
<td>Provider</td>
<td>Subscriber</td>
<td>Subscriber</td>
</tr>
</tbody>
</table>

Provider/Subscriber service agreement determines actual responsibilities.
IBM's Approach to Providing Secure Clouds

Client Services
(Customized by Client)

- Client's responsibility
- IBM does not touch client resources
- IBM provides guidance for customization and management of client services

Base Services
(Offered by IBM)

- IBM's responsibility
- IBM provides tested base services

IBM Cloud Computing Platform
IBM Global Cloud Data Centers

- Hardened management interfaces and cloud service management
- State-of-the-art data center service management
- Cloud subscriber management based on IBM Web Identity
- State-of-the-art data-center security (physical, organizational, system, network)
- Strict policies and extensive monitoring to control privileged users

- IBM's responsibility
- Base operated and managed according to IBM's internal technical and organizational security standards
- Extensive regular internal legal, geo-specific, data privacy, technical reviews
- Regular ethical hacking/security testing
- Based on IBM's strategic outsourcing practices and the IBM Common Cloud Reference Architecture
Thank you!

For more information, please visit:
ibm.com/cloud
ibm.com/security