Cloud Computing: Security Risks and Compliance Implications

Or, “Don’t Lose Your Security Head in the Cloud”
Security @ Brown

- Security evangelism
- Project support
- Audit support
- Compliance and legal standards
- Firewalls, IDS, IPS, VPN, sniffers, A/V, DNS, etc.
- Security audits and certifications

- Public Safety support
- Human Resources support
- Records Management
- Business Continuity
- Disaster Recovery
- Copyright / DMCA agent
- Discipline Committee
- Mandatory / elective training
- Awareness
Disclaimer

This will NOT be a technical discussion!
Agenda

• Defining the cloud
• What it is.....What it is not
• Uses and players
• CIO concerns, and myths
• Security & Compliance
• Recommendations and key points
• Q&A
What is cloud computing?

“attractive, seductive, and perhaps irresistible”

(Information Security Magazine, March 2009)
Defining the Cloud

A style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies

Gartner Feb. 2009
Defining the Cloud

• Simply put: Internet-based use of computing technology
• Not a real ‘thing’, but an extension of the network design metaphor
• A virtual network of both services and infrastructure
• Can be accessed from anywhere, to anywhere, at anytime
• An old idea who’s time has finally come(?)
What the cloud is....

- A time saver
- A money saver
- Potentially powerful
- Potentially unlimited scalability
- Potentially a game changer
- Ready for limited, though cautious, use
What the cloud is not....

- It is not grid computing or thin client
- It is not the end of localized IT
- It is not expensive
- It is not primetime (yet)
- It is not without concerns
Categories and Uses

• Two Broad Categories:
  • Infrastructure
  • Applications

• Popular Uses
  • SaaS, PaaS, IaaS
  • Sandboxes
  • BCP / DR
  • Market driven events
  • Rapid Prototype / Small Project
Cloud Vendors to Watch
(per Forrester Research, March 2009)

- Akamai
- Amazon
- Areti
- Enki
- Fortress
- Joyent
- Layered Technologies
- Rackspace
- Salesforce.com
- Terremark
- XCalibre

- Others in the space include: Dell, Flexi-Scale, IBM, Microsoft, Mosso, Slice-Host, and Sun
CIO: Obstacles and Concerns

- Availability of data
- Data Lock-in / Data bottlenecks
- Confidentiality and auditing
- Performance unpredictability
- Bugs in large scale environments
- Reputation Sharing
- Licensing
Myths of the cloud

- The business advantages outweigh the need for strong security measures
- You automatically forfeit security
- Your provider assumes all responsibility
- It’s “just like getting electricity”
- You should strongly consider the size of the vendor
Security & Compliance

- Think twice about what you put in the cloud
- Consider it no different than your data center
- Will it blur the auditors’ vision?
- International borders implications
- What happens if a firm gets bought?
- How can privacy be proven?
- Your can not turnover control!
Security in (for?) the cloud

Gartner’s Big Questions: ask your provider about:

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Availability
- Recovery
- Investigative support
- Viability of provider
- Support in reducing risk
Five reasons to embrace the cloud

1. Fast start-up
2. Scalability
3. Business agility
4. Faster product development
5. No capital expenditures
Five reasons to stay away

1. Bandwidth could bust your budget
2. Application performance could suffer
3. Your data is not cloud-worthy
4. You are too big already to scale
5. Your human capital is lacking
Five questions to ask yourself

1. Are your applications ready?
2. Where will your data be?
3. How is your data to be protected?
4. What will my customer service be like?
5. What is my exit strategy?
Recommendations

• The time is now to start experimenting with cloud based services
  • Begin to document both management and governance models for future cloud use
  • Be cautious, and only use low-risk, non-mission critical opportunities to take advantage of cloud-based evaluations

• Assess cloud providers on both traditional and non-traditional methods
  • Security and compliance....yes
  • But elasticity and adoption rate as well

• Keep up with the continuing maturation
  • www.cloudsecurityalliance.org
15 Strategic Cloud Domains

1. Information lifecycle mgmt
2. Governance & Enterprise Risk Mgmt
3. Compliance & Audit
4. General Legal
5. eDiscovery
6. Encryption & Key Management
7. Identity & Access Management
8. Storage
9. Virtualization
10. Application Security
11. Portability and Interoperability
12. Data Center Ops Management
13. Incident Response
14. “Traditional” security impact
15. Architectural Framework
Future: a perfect storm (cloud)

- Computing as a utility? Finally?
- The cloud could/will drive new technology trends and business models
- New application opportunities
- Will there be classes of utility computing?
- As with all technology, the market will dictate this
Clearing up the Cloudiness: Key Points

- Ascend in to the cloud with caution
- Do not even consider using for sensitive data
- Use initially to drive down cost
- Stick to your policies
- Demand transparency from your provider
- Include your audit and legal teams!
- Apply your initial internal risk assessment, and assess all legal/regulatory/audit areas
- Confirm with a certified third party assessor
Thanks for choosing my session…..!!!

Q & A

David Sherry  CISSP CISM
Chief Information Security Officer
Brown University
401-863-7266
david_sherry@brown.edu