THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Defending the Fortress:
New Threats Meet New Defenses

Assessing Security in the Cloud

C. Warren Axelrod, Ph.D.

Senior Consultant, Delta Risk, LLC

Research Director, U.S. Cyber Consequences Unit

Agenda

- What are Cloud Computing Services?
- Economics of Cloud Computing Services
- Risks Categories of Cloud Computing
- Assessing Security for Cloud Services
- Mitigating Security Risks of Cloud Computing
- Takeaways

Opening Statement

- Security requirements in the cloud are generally similar to those for internal computing and IT outsourcing
- However, certain characteristics of the cloud suggest modification of security technologies and management to address security risks with more impact in cloud-computing environments

Cloud Computing Services

- **Software as a Service** – use of providers' applications
- **Platform as a Service** – clients' applications run on providers' platforms
- **Infrastructure as a Service** – clients receive access to equipment only, and must supply own platforms and applications

Economics of Cloud Computing

Costs (Negatives)

- Loss of control (security/privacy measures, costs of compliance)
- Costs of restructuring systems, e.g., application changes, increased communications costs
- Lack of interoperability and portability, i.e., termination and transition costs

Benefits (Positives)

- Relatively low costs for resources, i.e., computing, storage, etc.
- Flexibility, scalability, redundancy, rapid implementation
- Metered use, i.e., pay only for resources used

Security Risks of Cloud Computing

(Source: F. Farahmand, "Risk Perception and Trust in the Cloud," **ISACA Journal**, Volume 4, 2010, pages 41- 48, referencing J.Heiser & M. Nicolett, "Assessing the Security Risks of Cloud Computing," **Gartner Group**, June 2008)

- **Privileged user access** to in-house programs
- **Regulatory compliance** – customers responsible for data
- **Data location** – not knowing where data stored
- **Data segregation** – shared environments among customers
- **Recovery** – ability to restore within required time
- **Investigative support** of inappropriate/illegal activities
- **Long-term viability** – data availability following changes in cloud environment

Risk Perception of Cloud Users

(Adapted from F. Farahmand, "Risk Perception and Trust in the Cloud," **ISACA Journal**, Vol. 4, 2010, pages 41-48, referencing B. Fischoff *et al*, "How Safe is Safe Enough?" **Policy Sciences**, Vol. 9, No. 2, 1978, pages 127-152)

- **Voluntariness** of user involvement
- **Immediacy and severity of effect** of risk consequences
- **Knowledge about risk** – extent and precision of known risks
- **Control over risk** – ability to avoid consequences of activity
- **Chronic or catastrophic** – individual versus group impact
- **Newness** – degree to which risks are new
- **Common dread** – rationality of user attitude toward risks

Mitigating Cloud Security Risks

- Get business unit, IT and Infosec buy-in and ownership
- Review applications/data/services with Legal/Compliance
- Implement protection for sensitive information
- Implement effective identity & access management process
- Develop and test joint Business Continuity and DR Plans
- Ensure collection and protection of, and appropriate access to, forensic data
- Establish a formal exit strategy, including data destruction

Due Diligence for Cloud Services

- Involve all parties (business unit, IT, Infosec, Legal, Compliance) in the initial evaluation process
- Negotiate with appropriate decision-makers at CSP (Cloud Services Provider)
- Review CSP's information security capabilities and the costs/benefits of different security levels
- If data location and separation are important, arrange on-site inspections or get reports from trusted third parties
- Include all due-diligence items of regular IT outsourcing

IT Outsourcing Due Diligence Issues

(Source: C. W. Axelrod, **Outsourcing Information Security**, Artech House, 2004)

- Maintaining control over service provider
- Viability and commitment to business of service provider
- Relative size and negotiating power of customer vs. cloud services provider
- Quality (tangible/intangible) and service level measures (SLAs)
- Trust: security, privacy, safety, shared environments

Takeaways

- Make sure that moving applications/services to the cloud is appropriate
- Get buy-in from ALL parties, especially Legal/Compliance
- Do not be intimidated by CSP and don't accept the claim that "No one else has asked for this"
- Make sure that you (or someone else) has performed adequate due diligence and that you have evidence of it
- Ensure that there is a continuing CSP review program

Contact Information

- C. Warren Axelrod
- Email: waxelrod@delta-risk.net
- Phone: 917-670-1720