Mitigating Risks in Cloud Environments

Wednesday, March 28

10:15 – 11:15 a.m.

Neopolitan II & III

Moderator

Don Douglas

President and CEO

Liquid Networx

Speakers

Jebb Dykstra

CEO

Meetrix Communications Inc.

Jim Lippard

Senior Product Manager for Security Products

EarthLink IT Services

Mitigating Risks in Cloud Environments

Presented by Jebb Dykstra, CEO
Meetrix Communications, Inc.

Type of Cloud Environments (as defined by NIST)

1) Public Cloud
2) On-Site Private Cloud
3) Out-Sourced Private Cloud
4) On-Site Community Cloud
5) Out-Sourced Community Cloud
6) Hybrid Cloud

Public Cloud

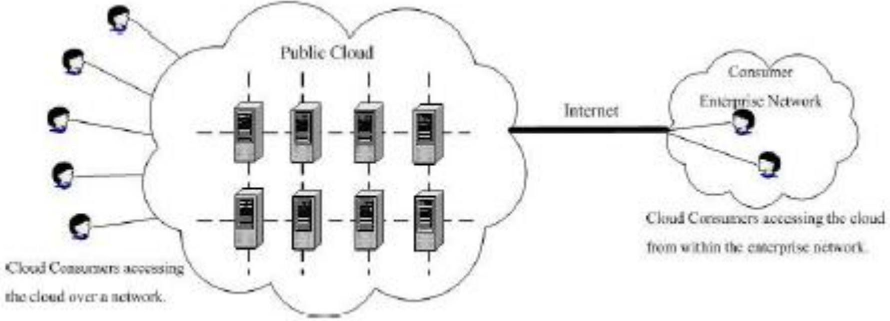

Public Cloud
Internet
Consumer Enterprise Network
Cloud Consumers accessing the cloud from within the enterprise network.
Cloud Consumers accessing the cloud over a network.

Figure 9: Public Cloud

On-Premises Private Cloud

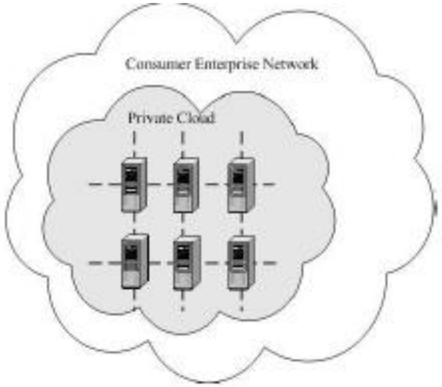


Figure 10: On-site Private Cloud

Hybrid Cloud

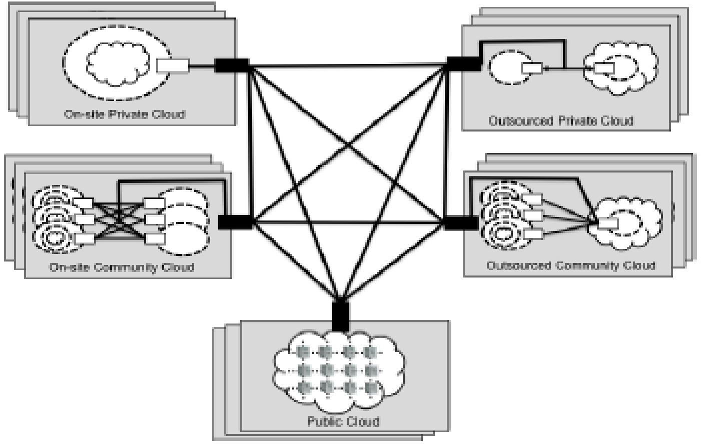


Figure 14: Hybrid Cloud

Cloud Risk Paradigms

Technical/Business

- Outages
- 3rd Party Control
- Cloud - not data center

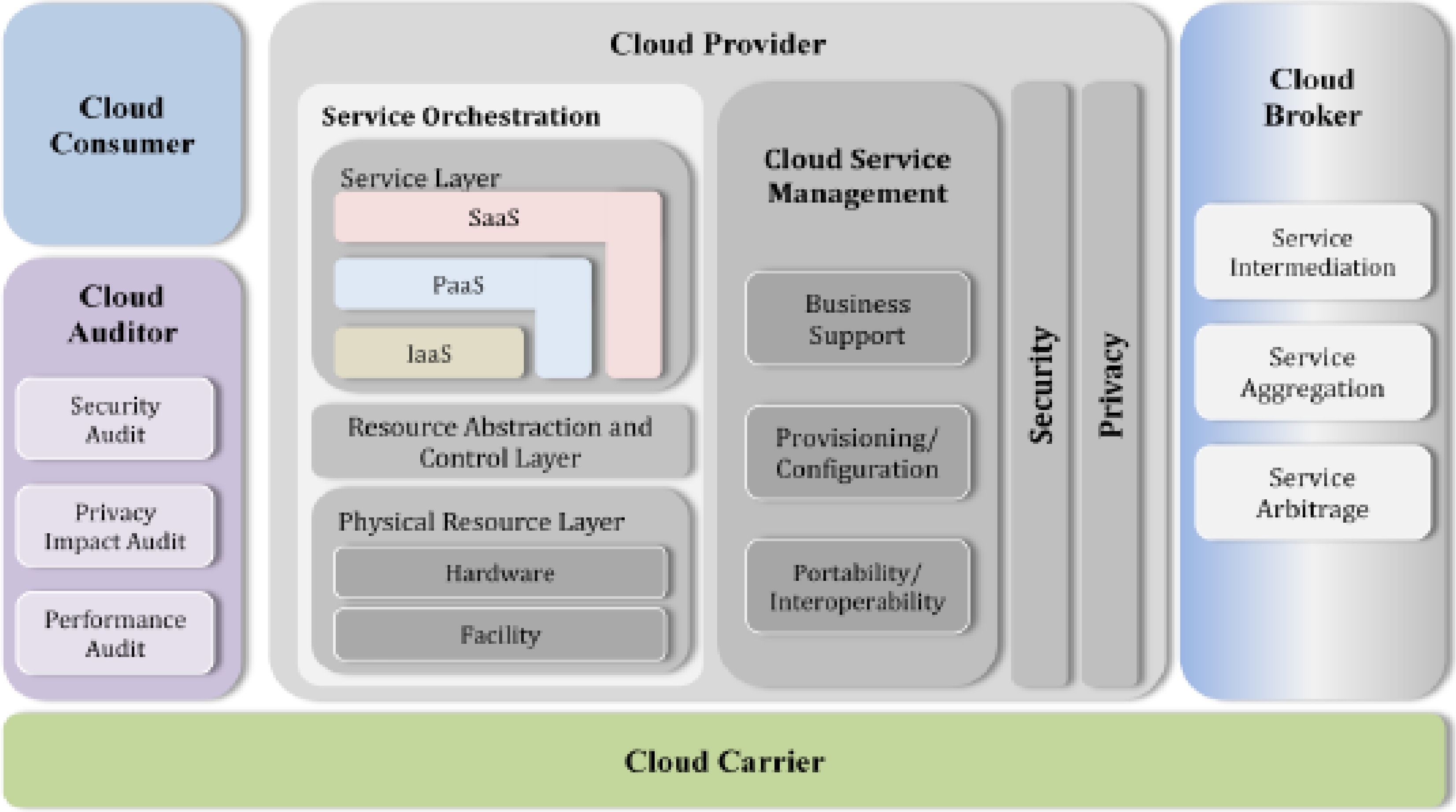
Security

- Dr. Vogels, CTO @ AWS
- Attacks
- Malware
- Shared Infrastructure

Legal

- Federal
- State
- International
- Jurisdiction: Residency of Data

Technical: Cloud Reference Architecture



NB: NIST Special Publication 500-292

Figure 1: The Conceptual Reference Model

Security: Scope of Control

NB: NIST Special Publication 500-292

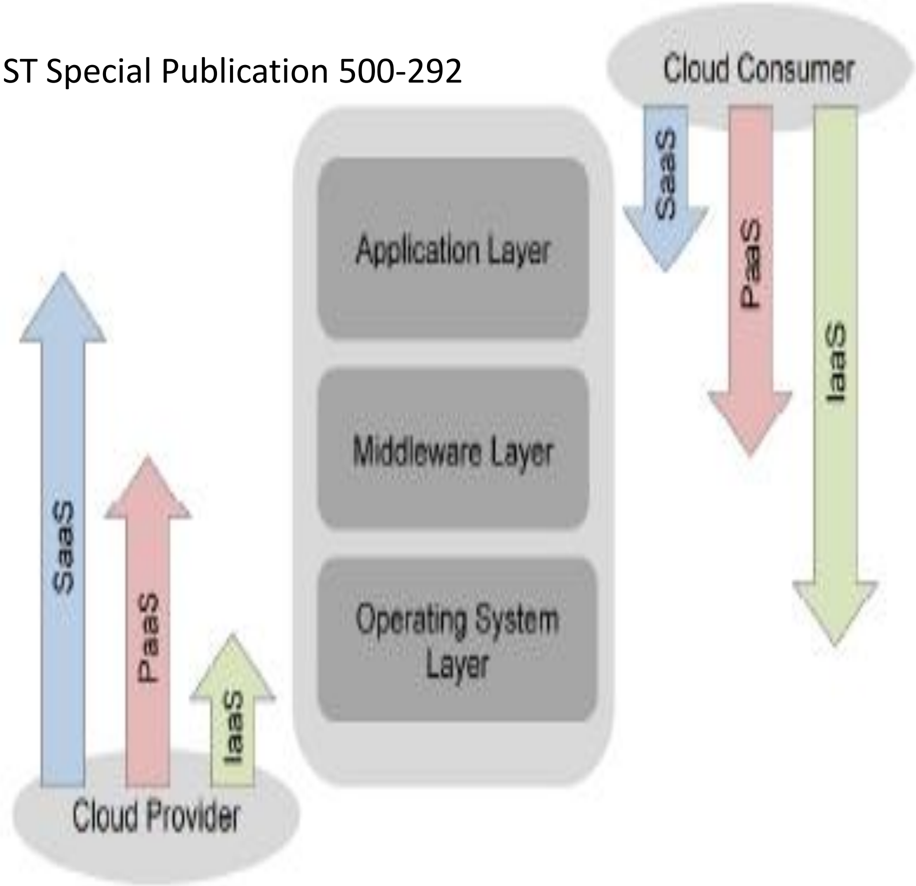


Figure 8: Scope of Controls between Provider and Consumer

<u>Security Spans:</u>

1) Cloud Provider
2) SaaS
3) PaaS
4) IaaS
5) I&A Management
6) Security Monitoring
7) Audit
8) Incident Response
9) Security Policy

Cloud and Networks: The Face of Risk
The Attacker and the Attacked

Anonymous **vs.** **DOJ, FBI, CIA and others**

KeepShooting.com

FreakingNews.com

Legal Risks: Cloud & Cybersecurity

Migration / Port to Cloud Requires Review re (US only):

- FISMA
- SOX
- HIPAA
- CFAA
- UETA
- ECPA
- Economic Espionage Act
- UCITA
- COPPA
- CIPA
- US Patriot Act

Best Practices In Cloud

- NIST Publications
- Government Reports (from US, Germany, Australia, and others)
- Cloud Leaders – define your Layer:
  - IaaS
  - PaaS
  - SaaS
- Due Diligence & Research

Mitigating Risks in Cloud Environments

Presented by Jim Lippard, Senior Product Manager, EarthLink Business

Real-World Cloud Failures

- June 2009: VAserv.com compromise.
- April 21, 2011: Amazon Web Services EC2 outage.
- August 17 & September 8, 2011: Microsoft Office 365 outages.
- September 2011: Google Docs outage.

Areas of Gain

- Efficiency
- Flexibility
- Specialized Support and Expertise
- Platform Strength

Areas of Risk

- Governance
- Compliance
- Trust
- Architecture
- Identity and Access Management
- Software Isolation
- Data Protection
- Availability
- Incident Response

(From NIST SP 800-144, Section 4)

Indicators of Trustworthiness

- Formal
  - Third party audit (SSAE 16, PCI, Shared Assessments)
  - Certifications (vendor, CCSK, security, ITIL)
  - Use of emerging standards on controls (CSA CCM, ISACA)
- Informal
  - Transparency
  - Accountability
  - Other customers with known strict requirements (esp. financial, healthcare, government)

Questions to Ask

- Is the data or functionality business critical?
- Does the provider have a BCP/DR plan?
- Will you keep your own backups?
- Will you replicate to another provider? Can you easily move to another provider?
- Does the provider have adequate SLAs? With compensation if not met?
- If you accidentally delete data, can provider quickly restore?
- Can you meet compliance requirements with the provider’s services? Does the provider have necessary certifications?
- Does the provider adequately destroy data when a customer leaves?
- Can you use existing management and monitoring tools?
- Do you retain legal ownership of your data?
- Does the provider have a security posture supported by policies, processes, and direct controls? Are they attested to by third-party auditors?
- Does the provider support integration with your identity and access management systems?
- Is your data segregated from that of other customers?
- When was your last known compromise? How long did it take you to detect? What do you now do differently?

(From Australian DOD, “Cloud Computing Security Considerations”)

Helpful Guidance

RISKS AND BEST PRACTICES

NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

European Network and Information Security Agency (ENISA), Cloud Computing Risk Assessment
http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

Australian Department of Defense, Cloud Computing Security Considerations
http://www.dsd.gov.au/publications/Cloud_Computing_Security_Considerations.pdf

Cloud Security Alliance, Security Guidance for Critical Areas of Cloud Computing, v3.0:
https://cloudsecurityalliance.org/research/security-guidance/guidance-v3/

Helpful Guidance 2

ASSESSMENT, AUDIT AND CONTROLS

Cloud Security Alliance, Cloud Audit: Automated Audit, Assertion, Assessment, and Assurance:
http://cloudaudit.org/CloudAudit/Home.html

Cloud Security Alliance, Consensus Assessments Initiative:
https://cloudsecurityalliance.org/research/cai/

Cloud Security Alliance, Cloud Controls Matrix:
https://cloudsecurityalliance.org/research/ccm/

Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide
http://sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf

ISACA, IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud:
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx

ISACA, Cloud Computing Management Audit/Assurance Program:
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Management-Audit-Assurance-Program.aspx

CLOUD SECURITY KNOWLEDGE CERTIFICATION

Cloud Security Alliance, Certificate of Cloud Security Knowledge:
https://cloudsecurityalliance.org/education/certificate-of-cloud-security-knowledge/

Contact

Don Douglas

President and CEO

Liquid Networx

Don.Douglas@liquidnetworx.com

Jebb Dykstra

CEO

Meetrix Communications Inc.

jebb@meetrix.us

Jim Lippard

Senior Product Manager for Security Products

EarthLink IT Services

jlippard@corp.earthlink.com