Cloud Security

Wesley H. Higaki
ACSAC - December 2009
Why is Cloud Computing So Hot?

- Reduced capital expenditures
  - Exchanging CapEx with OpEx
- Unlimited scalability
  - Flexible scale – up or down
- Instant provisioning
  - New features and capabilities available to everyone instantly
- “Pay as you go”
  - Don’t have to pay for excess capacity
- Improved security (for some)
- Shorter time-to-market
- Greater consistency across the enterprise
- Cost savings
What is Trustworthiness?

- Doing the “right things”
- Providing proof
- Why are cloud services hard to trust?

Levels of trust

1. Vendor assertion
2. Independent, third-party validation against claims
3. Independent, third-party validation against open, vetted standards
Trust Framework

Threats → Security → Compliance
Cloud Security and Trust Issues

• Multi-tenancy
  – Data leakage potential

• Ubiquitous access
  – Unauthorized access threat

• Flexible provisioning
  – Differences in configuration may cause different behaviors

• Lack of transparency
  – Reason for untrustworthiness
  – Regulatory compliance issues

• Doesn’t fit today’s compliance paradigms
Regulatory Requirements

- Payment Card Industry Data Security Standards (PCI-DSS)
- Health Information Portability and Accessibility Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Federal Information Security Management Act (FISMA)
- California Breach Notification

- Audits, evaluations and certifications
  - Depend on transparency and evidence
Perspectives

• Are CSP’s to be treated like third-party contractors or like products?

• Look at cloud computing as a new delivery mechanism for products and not just an extension of IT infrastructures and platforms.

• While IT seem to be talking about Cloud Security the most, business leaders will be the ones driving this.

• Traditional thinking about IT boundaries, assurance and compliance may not apply in the cloud era.
Cloud Service Provider Perspective

- Multiple, sometimes conflicting regulatory requirements from customers
- Compliance and audits on static systems
- Issues with transparency and visibility
- Transfer of risk and responsibility
Applicable References

- ISO 27001 and 27002
- Unified Compliance Framework
- Common Criteria?
- ENISA Assurance Checklist
- Cloud Security Alliance
Gaining Trust in Cloud Computing

• Develop standards on how to evaluate cloud services
  – Compliance/audit paradigm shift?
• Use of Private and Virtual Private Clouds