*June 6, 2012*

# *Security Considerations for the Cloud*


***Presented by:***

*Mac McMillan*

*CEO CynergisTek, Inc.*

*Chair, HIMSS Privacy & Security Policy Task Force*

CYNERGISTEK

# Agenda

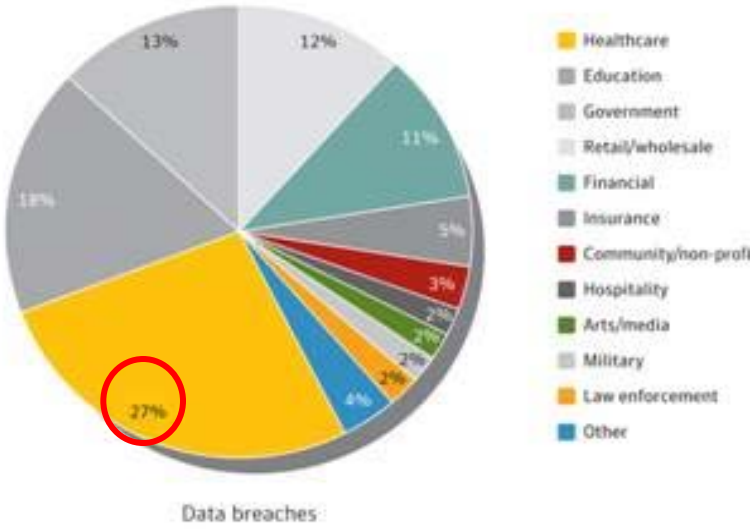
- Threat Implications
- Security Considerations
- Risk Assessment
- Last Thoughts

# Threat Implications

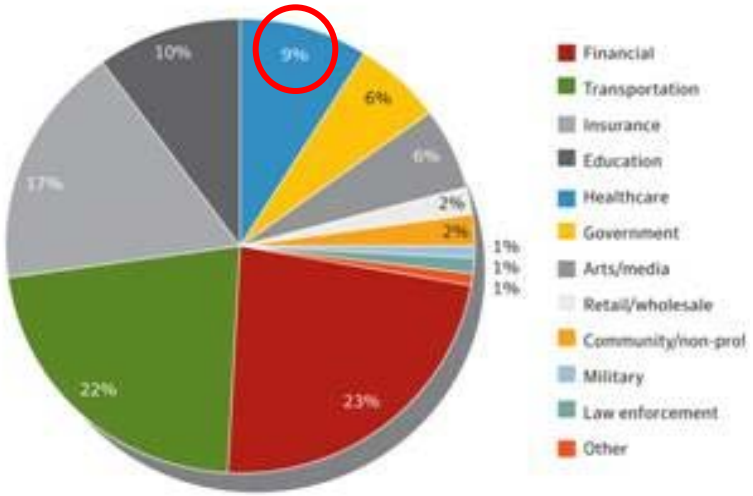
# Why Data Security Is Important


- People **choose** to disclose their most intimate information in order to get healthy
- Providers **earn** their trust by guaranteeing privacy
- Privacy is assured by properly **protecting** systems and information
- Breaches undermine patient **confidence**
- No Confidence and people avoid treatment, lie or omit information, opt-out, and potentially **get sicker**
- Therefore, privacy and security are integral to **care**

# 2011 Threat Picture




Data breaches




Identities exposed

2011 healthcare assumes number one position in total number of breaches, and fifth in overall identities exposed.

The total number of breaches reported in healthcare exceeds 55,000 including those less than 500 records.

*Symantec 2011 Internet Security Threat Report*

# What's Changing?


- Pervasiveness of information being made available electronically has made healthcare a target of cybercriminals. (1 in 6 attacks in 2009 were HC, greatest growth in attacks in 2010 and 2011.
- In general, healthcare may face bigger risks going forward than either the financial or retail sectors because the information they have is gaining value and there is expected to be greater distribution/access.
- The Cloud is only one example.  A recent ID Experts survey found that 33% of healthcare respondents are in the cloud, and 48% have plans to move there soon.

# What's Not Changing?


- Covered entities responsibility to ensure the confidentiality, integrity and availability of electronic Protected Health Information (ePHI).
- The requirement to assess all reasonable risks to ePHI.
- The requirement to insure that Business Associates are capable of protecting ePHI appropriately.
- The requirement to assure appropriate access and minimal necessary.
- The requirement to account for uses and disclosures.
- The requirement to respond effectively to incidents,
- And the list goes on…

# Security Considerations in the Cloud

# Cloud Appeal


- The cloud provides multiple value propositions for Covered Entities and Business Associates of all sizes by creating access to pools of economical information assets.
- Organizations can take advantage of Infrastructure, Platforms or Software as a Service deployment models.
- And, there are different service models to choose from – Public, Private, Hybrid and Community.
- Models count…

# Cloud Models


- Control of security varies greatly depending on model selected:
  - SaaS – The Provider has control
  - PaaS – Shared control
  - IaaS – The consumer has control

- Security assurance changes depending on model selected:

| | | |
|---|---|---|
| • Public | Untrusted | Assets provided for anyone |
| • Private | Trusted | Dedicated assets provided |
| • Community | Trusted | Assets shared by group |
| • Hybrid | Combination | Mix of delivery means |

# Top Three Concerns


- Performance and Reliability
- Compliance
  - Lack of visibility
  - Physical location of information
  - Jurisdiction issues
  - Ability to investigate
- Information Security
  - Unintended disclosures
  - Data privacy
  - System integrity
  - Multi-tenancy
  - Browser Support
  - Hardware integrity
  - Key Management

# Risk Assessment

# Key Questions for Management

*Cloud security Alliance*


- **What would the impact be if the asset were to become public or widely distributed?**
- **How would you be harmed  if an employee of the cloud provider accessed the asset?**
- **What if the process were altered or manipulated by an outsider?**
- **How would you be harmed if the process or function failed to provide the expected results?**
- **How would you be harmed if the information/data were to be unexpectedly changed?**
- **How would you be harmed if the asset were to be unexpectedly unavailable for a period of time?**

# Risk Assessment

CYNERGISTEK

- **Moving to/from the cloud:**
  - Identification of information suitable for the cloud
  - Procedures for interaction with information in the cloud
  - Plans for retrieval/destruction upon termination
  - Conduct data discovery and inventory information prior to moving to the cloud
- **Continuity of Operations:**
  - Assessing the venders plans for contingencies (back up/disaster recovery/continuity of operations)
  - Reviewing Service Level Agreements to insure timely actions
  - Legal/contractual protections for unexpected outages/loss of data

# Risk Assessment

CYNERGISTEK

- **Compliance requirements:**
  - Secure commitment to compliance (Security Agreement/BAA)
  - Review documentation of policies/controls
  - Request third party controls assessment
- **Physical/Personnel:**
  - Insure compartmentalization of provider/consumer administrative staff roles/responsibilities.
  - Request access to where information is stored.
  - Monitor all access to systems with ePHI.
  - Ensure the environment is regularly tested.

# Risk Assessment


- **Encryption:**
  - Encrypt prior to storing in the cloud, segregating key management.
  - Encrypt transmissions between provider and consumer.
  - Review encryption methods used by cloud service provider.

- **Policy/Legal:**
  - Review operating policies for completeness/currency.
  - Substantiate whether provider is available for audit.
  - Review incident response plans, procedures and readiness.
  - Insure capability to respond to legal requests such as litigation holds, data searches, etc.

# Transitional Thoughts

# Last Thoughts

CYNERGISTEK

- HIPAA, HITECH, PCI, etc. responsibilities follow the information and extend to the cloud, selection of the right cloud service provider is important.
- Third party certification can reduce risk such as cloud providers certified by FedRAMP.
- Risk assessment should be performed before moving to the cloud. In some cases moving to the cloud can improve the protection of data.
- There are many excellent resources on cloud computing to help inform approaches.
- There is a HIMSS, Cloud Security Working Group established specifically to focus on healthcare.

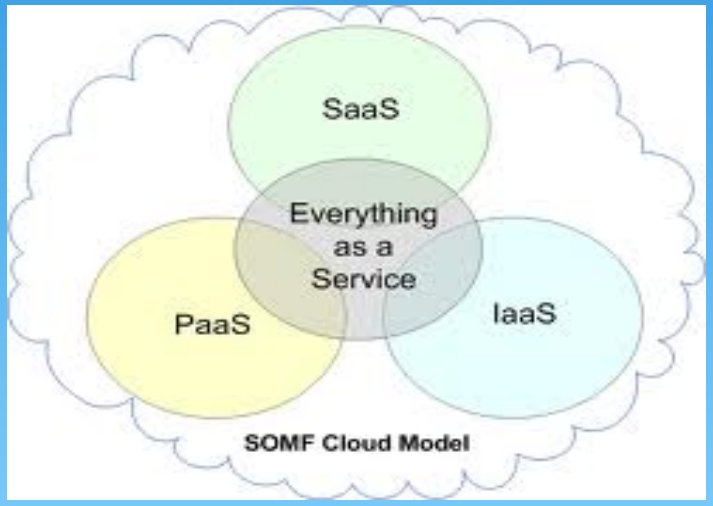
# Thank You

For more Information please visit our blog site.

www.cynergistek.com

**Mac McMillan**
Mac.McMillan@cynergistek.com
(512) 402-8555

# View from the cloud




## Security Assurance considerations for a purchaser

*5th Annual Safeguarding Health Information: Building Assurance through HIPAA Security - Conference*
Hosted by NIST and HHS Office for Civil Rights
June 6-7, 2012
Washington, DC

# Is there a Cloud in the Future of Healthcare ?

- ✓Market Prognosis
- ✓Unique opportunities
- ✓Unique Challenges

# MARKET PROGNOSIS

- ✓ Revenue Growth – $16b (2009)/$55.5b(2115)
- ✓ Proxy for IT Outsourcing
- ✓ Federal Programs
- ✓ Major market participants

# UNIQUE OPPORTUNITIES

- ✓ Monetary rewards for IT modernization
- ✓ Connectivity / Big Data
- ✓ Leverage cost efficiencies / IT competencies
- ✓ Access to IT agility

# UNIQUE CHALLENGES

- ✓ Compliance overhang
- ✓ Security requirements
- ✓ Governance / Management
- ✓ Contracting
- ✓ Governmental oversight

# Security Guidance Playbook


- √ Risk Assessment
- √ Governance
- √ Operations
- √ Reporting
- √ Monitoring

# Assessment Resources


- ✓NIST / FISMA
- ✓HiTech
- ✓Cloud Security Alliance
- ✓ ISO 27001

# Cloud Security Alliance

## Tools / Research


www.cloudsecurityalliance.org

- ✓Security guidance
- ✓Cloud controls matrix
- ✓Cloud Audit
- ✓GRC stack
- ✓Cloud data governance

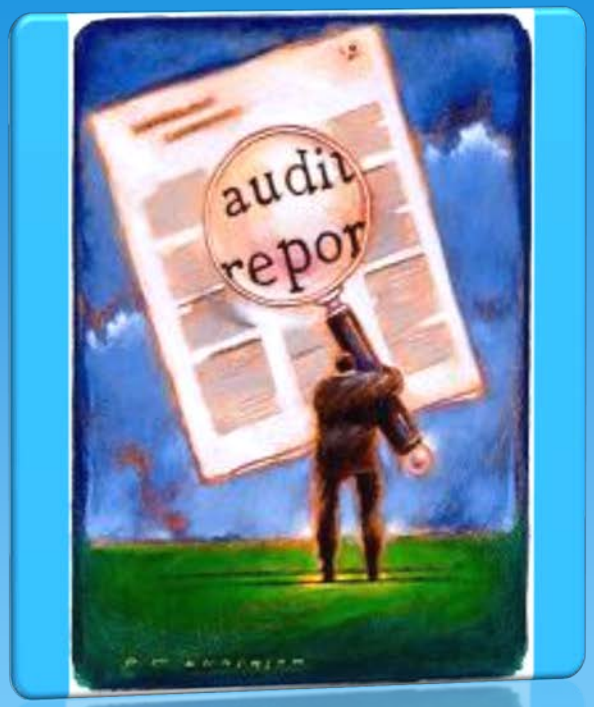
# Provider Accountability

# Questions to ask Cloud Providers


## Does the contract adequately protect the buyer?

- Service levels
- Service availability
- Data Security
- Insurance
- Indemnification
- Exclusivity
- BAA
- Intellectual Property
- Limitation of Liability
- Implementation
- Assignment
- Warranties
- Exit strategy

# Questions to ask Cloud Providers

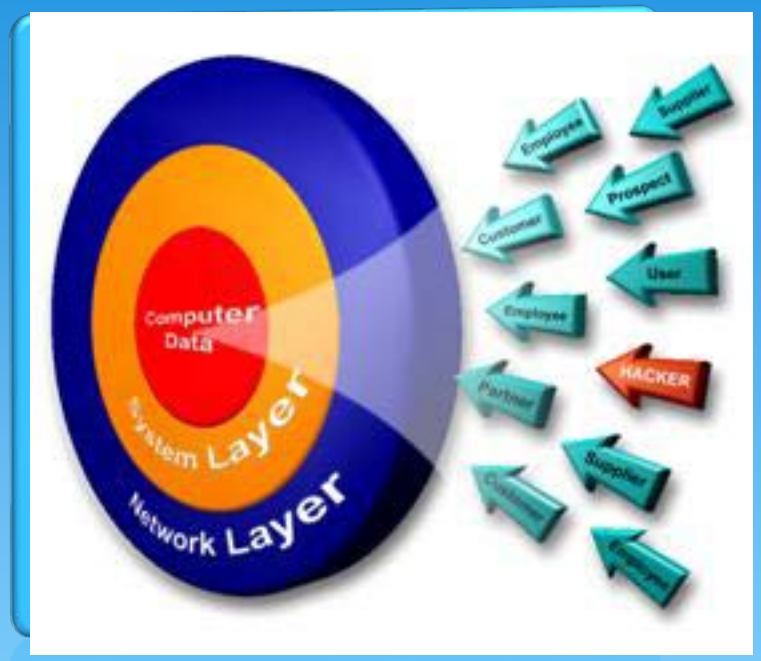



Are the results of internal and external audits available to customers at their request?

# Questions to ask Cloud Providers

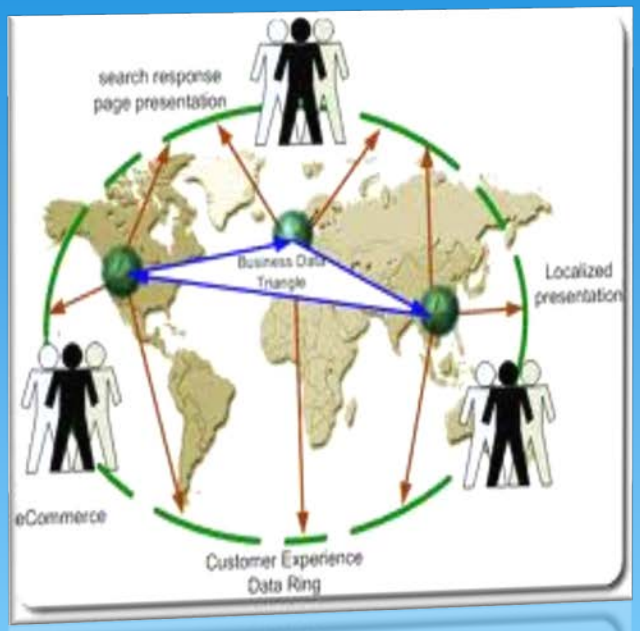

Are customers allowed to view the provider's third party audit reports?

# Questions to ask Cloud Providers



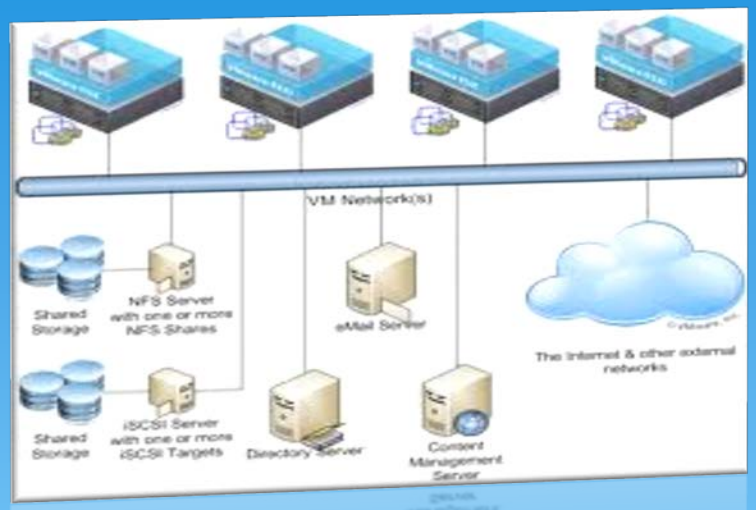

Does the cloud provider conduct network penetration tests of its cloud service infrastructure on a periodic basis?

# Questions to ask Cloud Providers




Does the provider document scenarios where data may moved from one physical location to another?

# Questions to ask Cloud Providers




Does the provider use encryption to protect data and virtual machine images during transport across and between networks?

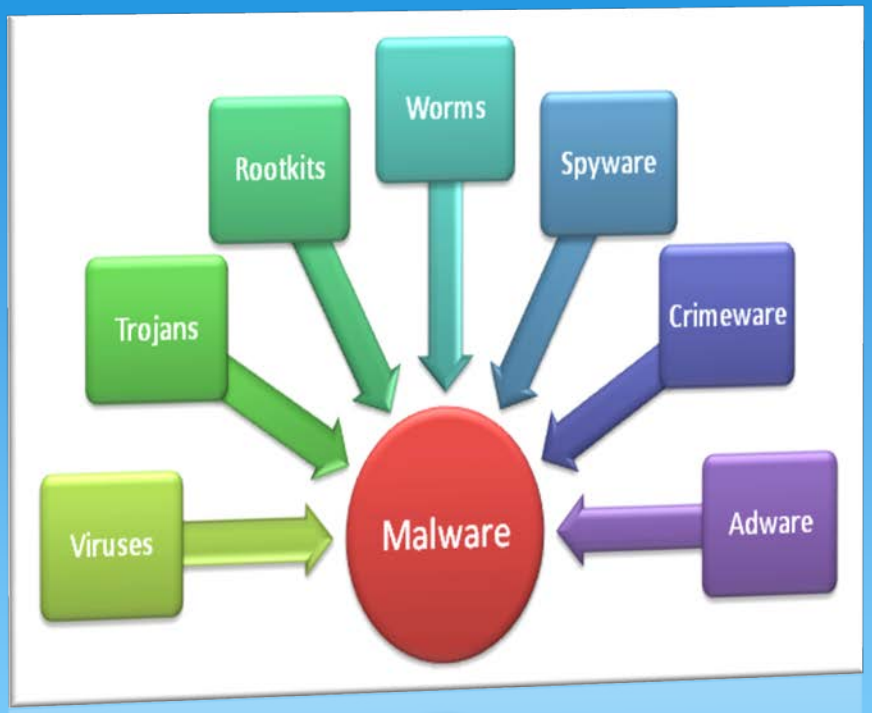
# Questions to ask Cloud Providers

Can the cloud provider logically segment and recover data for a specific customer in the case of a failure or data loss?

# Questions to ask Cloud Providers


Does the provider encrypt user data at rest(on disk/storage) as well as in transit?

# Questions to ask Cloud Providers




Does the provider have anti-malware programs installed on all systems that support the cloud service offerings?