Trust Modeling for Cloud Services

North Texas ISSA

April 24, 2015
“Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers.”

Wikipedia
...And that does not mean that your services are necessarily where you think they are.
Concept of Trust

- Trust is based on a business relationship
- Necessary precursor to interaction
- Assurance is required to establish and maintain positive trust
- Different levels of assurance required based on level of risk to the business
Who is the Relying (Trusting) entity and who is the Claimant (Trusted) entity?
What type of due diligence (i.e. assurance) would you do for each transaction?

Why is the level of assurance different?
How sensitive is the information I am sharing?

How critical is the relationship to my organization?

How am I assuring the relationship?

Where should I focus my energy?

How sensitive is the information I am sharing?
Components of Risk

- **Assets**—value? (qualitative or quantitative)
- **Threats**—Who are the threat agents and what is the likelihood of the threat?
- **Business Impact**—What is the impact to the asset if threat is realized?
- **Vulnerabilities**—Are we exposed and where?
- **Control Effectiveness**—How mature and effective are our controls?
Business Context

Threat Analysis

Risk Modeling

Vulnerability Analysis

Control Framework Selection

Control Framework #1

Control Framework #2

Control Framework #n
Risk Heat Map

1. Global Health

2. Regional Health

- For profit business
- Patient Care
- Clinical research
- Facilities Management
- Community Outreach
- etc.

3. eBusiness Services (VP, Client Services)
   - D3a. Bank Products (Director)
   - D7. Claims Processing (Director)
   - D7a. Client Domain

4. Corporate Solutions (CIO)
   - D4a. Functions e.g. HR, Finance (VP/Director)

5. Shared Services (CTO)
   - D6a. Component e.g. network platform (Manager)

D8. Alliance Partners (VP, Alliances)
   - Partner 1 (CEO)
   - Partner 2 (CEO)
   - Partner 1 (CEO)
   - Partner 2 (CEO)
D1. Global Heath

D2. Regional Health

D3. eBusiness Services (VP, Client Services)
   - D3a. Bank Products (Director)
   - D7. Claims Processing (Director)
   - D7a. Client Domain

D4. Corporate Solutions (CIO)
   - D4a. Functions e.g. HR, Finance (VP/Director)

D5. Shared Services (CTO)
   - D6a. Component e.g. network platform (Manager)

D8. Alliance Partners (VP, Alliances)
   - Partner 1 (CEO)
   - Partner 2 (CEO)
   - Partner 1 (CEO)
   - Partner 2 (CEO)

- HIPPA
- HITECH
- FISMA
- Etc
• For profit business
• Application hosting
• Applications as a service
• Payment Processing
• Data Management
• Etc.
- PCI-DSS
- ISO 2700x
- NIST
- HIPPA
- FFIEC
- GLBA
- Etc.
• Lower cost?
• Higher processing capacity?
• Expertise?
• SLA’s?
• Liability?
- Risk?
- Accountability?
- Control Enforcement?
- Disclosure?
- Liability?
Risk Heat Map

- **High Assurance** (A)
- **Medium Assurance** (B)
- **Low Assurance** (C)

Contracts and Service Level Agreements

1. Specify any regulatory or industry security standards you expect the vendor to follow.
2. Specify who is responsible to make sure the service is protected with the right security controls.
3. Specify how the controls will be validated and any remedies if they are not.

http://blog.norscorpr.com/2015/03/04/four-security-issues-all-business-contracts-should-address
Concept of Trust

- Trust is based on a business relationship
- Necessary precursor to interaction
- Assurance is required to establish and maintain positive trust
- Different levels of assurance required based on level of risk to the business
Patrick M. Hayes
Managing Director
Seccuris Inc.
phayes@seccuris.com
linkedin.com/in/phbalance