Leveraging the Cloud & Managing Compliance
Introduction

• Greg Miller
  – Principal
  – Schellman & Company, Inc.

• Blake Sutherland
  – Vice President, Enterprise Business
  – Trend Micro
Agenda

- Cloud Increase
- Characteristics
- Deployment
- Type
- Challenges
- Compliance
- Q/A
The cloud services companies of all sizes…The cloud is for everyone. The cloud is a democracy.

Marc Benioff, CEO - Salesforce.com
The Increase

- Scalability
- Cost
- Efficiency
- Services

Healthcare Cloud Computing Market to Reach $9.48B by 2020
Characteristics

- Broad network access
- Resource pooling
- Measured service
- On-demand self-service
- Rapid elasticity (provisioning/de-provisioning)
Types

- Public
- Private
- Community
- Hybrid

1. Management includes: governance, operations, security, compliance, etc...
2. Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment
3. Infrastructure Location is both physical and relative to an Organization’s management umbrella and speaks to ownership versus control
4. Trusted consumers of service are those who are considered part of an organization’s legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.
Deployment

- **SaaS**
  - *On-Demand software typically in the cloud*
- **PaaS**
  - *Delivery of a computing platform and solution stack as a service*
- **IaaS**
  - *Delivery of computer infrastructure (virtualization) as a services along with storage and networking.*
Challenge: Infrastructure for improving patient health, engagement and wellness is always changing

- 6000 Apps in iTunes
- Telemedicine, e-Health
- Internet of Things
- Medical Devices
- Cloud Portals
- Mobile Clinician
Challenge: In an already complex environment

New & Legacy Systems
- Windows XP
- Windows 2003
- Office 365
- Cloud Environments with Azure, Amazon and others

Complexity is Growing
- Telemedicine
- mHealth
- Internet of Things

Call in the consultants!!!!
- Various consultants brought in due to lower IT spend

Patient Portal
- On-Premise Data Center
- Third Party / Cloud Hosted Data Center
- New & Legacy Systems
- Medical Devices & Video systems

© 2016 HITRUST Alliance.
Challenge: With Patient Data constantly in motion

- Home users accessing their Patient Portal
- In the doctor’s EHR system
- Medical Devices
- Enterprise data management systems, legacy and new environments, cloud email..

Managing patient data and keeping it secure along the way is of critical importance

- Healthcare staff on the go, mobile devices etc.
- POS Systems, payment, payers, insurance
- Government Health Exchanges
Challenge: Which is valuable to criminals

• And there are many ways to profit from this information (currently reported at selling for $50 per record):
  • Drug fraud
  • Create credit cards and/or use credit card information
  • Create new identity
  • Buy and sell prescriptions
  • File false Medical Claims
  • Tax fraud
  • Bribery and ransom with embarrassing health information

Figure 17. Patient data successfully targeted (healthcare organizations)

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015
Result: a predictable outcome

• Breaches escalating
  • Medical/Healthcare: 42% of all breaches (IDRC)
  • Multiple breaches in the last year at various healthcare organizations
• FBI: “Healthcare is not prepared”
• FDA to medical device manufacturers: “Improve security”
• Regulatory environment complex
  • HIPAA, HITECH, PCI DSS 3.0
• Healthcare organizations are behind in security
  • Spend less on IT security than any other industry
### Top 10 Healthcare Data Breaches 2015

<table>
<thead>
<tr>
<th>Organization</th>
<th>Records Breached</th>
<th>Type of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anthem</strong></td>
<td>78,800,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>PREMERA</strong></td>
<td>11,000,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>Excellus</strong></td>
<td>10,000,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>UCLA Health</strong></td>
<td>4,500,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>mHIN</strong></td>
<td>3,900,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>CareFirst</strong></td>
<td>1,100,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>DMAS</strong></td>
<td>697,586</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>Georgia Department of Community Health</strong></td>
<td>557,779</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>BEACON Health System</strong></td>
<td>306,789</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>DJO Global</strong></td>
<td>160,000</td>
<td>Laptop Theft</td>
</tr>
</tbody>
</table>

**2015 Total**: 111,022,154 (almost 35% U.S. population)
The Statistics

• 253 breaches
• 112 million records
• 35% of the population
• 21% of the total number of incidents
• Compared to 2014, increase by 10%
Cloud Model

Security Control Model

- Applications
  - SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
- Information
  - DLP, CM, Database Activity Monitoring, Encryption
- Management
  - GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- Network
  - NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- Trusted Computing
  - Hardware & Software RoT & API's
- Compute & Storage
  - Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
- Physical
  - Physical Plant Security, CCTV, Guards

Compliance Model

- PCI
  - Firewalls
  - Code Review
  - WAF
  - Encryption
  - Unique User IDs
  - Anti-Virus
  - Monitoring/IDS/IPS
  - Patch/Vulnerability Management
  - Physical Access Control
  - Two-Factor Authentication...
- HIPAA
- GLBA
- SOX
Cloud Security is a Shared Responsibility

Cloud providers deliver a secure infrastructure.

But YOU need to protect what you put IN the cloud—your workloads.

Cloud User

Cloud Provider

Foundation Services
Compute | Storage | Database | Networking

Global Infrastructure
Domains, Availability Zones
Regions

Content and Applications
Platform, Applications
Operating System, Network & Firewall Configuration
Data Encryption | Network Traffic Protection
Who’s responsibility… depends on the cloud service

Source: Gartner April 2015
# Mapping products to compliance

<table>
<thead>
<tr>
<th>Deep Security</th>
<th>HITRUST CSF 2011</th>
<th>HiPAA Security Rule</th>
<th>HITECH Breach Notification Specification</th>
<th>PCI DSS v2</th>
<th>§ 495.6 (Stage 1) Meaningful Use Stage 1 Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Feature(s)</strong></td>
<td><strong>Control Reference</strong></td>
<td><strong>Specification</strong></td>
<td><strong>Regulation not covered</strong></td>
<td><strong>2.2.3 Configure system security parameters to prevent misuse.</strong></td>
<td><strong>(i)(15)(v) / (i)(14)(v) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP’s, eligible hospital’s or CAH’s risk management process.</strong></td>
</tr>
<tr>
<td><strong>Agent/v. Anti-malware for VMware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05.x Information Access Restriction - Level 2</td>
<td>(a)(3)(iii)(B) Protection from malicious software (Addressable)</td>
<td>2.2.3 Configure system security parameters to prevent misuse.</td>
<td>5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.</td>
<td>5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.</td>
<td></td>
</tr>
<tr>
<td>06.x Controls Against Malicious Code - Level 1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06.x.k Controls Against Mobile Code - Level 1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Intrusion Detection and Prevention</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.x Controls Against Mobile Code - Level 1/2</td>
<td>Regulation not covered</td>
<td>Regulation not covered</td>
<td>1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.</td>
<td>1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.</td>
<td>1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.</td>
</tr>
<tr>
<td>09.m Network Controls - Level 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.x Electronic Commerce Services - Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.ab Monitoring System Use - Level 2/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09.ad Administrator and Operator Logs - Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.m Control of Technical Vulnerabilities - Level 1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.a Reporting Information Security Events - Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Connected Threat Defense**

Enable rapid response through shared threat intelligence and delivery of real-time security updates.

Gain centralized visibility across the system, and analyze and assess impact of threats.

Detect advanced malware, behavior and communications invisible to standard defenses.

Assess potential vulnerabilities and proactively protect endpoints, servers and applications.
Constantly improve our products


- 2015 NSS Labs Breach Detection Tests

- Trend Micro Blog, January 2015
- [http://www.av-test.org](http://www.av-test.org) (Jan 2014–Aug 2015 test results, Corporate Solutions on Win XP, 7, 8 Systems)
Options

ISO

HITRUST Health Information Trust Alliance

AICPA Service Organization Control Reports

PCI

NIST

CSA cloud security alliance

FedRAMP
Questions?
Thank You!