Security for Next Generation Healthcare

Carisa Brockman
Director of the Governance, Risk, and Compliance Practice
AT&T Security Consulting Services
Technology Trends Reshaping Healthcare

- Powerful Mobile Computing Devices
- Fast, Widespread Wireless/Wireline IP Networks
- Cloud Computing

Healthcare organizations are reengineering the way they do business.
2012 Healthcare Security Outlook

- Data breaches rose by 32% in 2011 Source: Ponemon/ID experts study
- Widespread use of mobile devices adds risk
- Negative productivity impact and financial consequences increase directly with an increase in number of incidents
- Number of cases of medical identity theft increased Source: Ponemon/ID experts study
- Breaches have consequences

Healthcare “business” is changing

Modern Healthcare System is growing!
Security and Privacy Challenges

• Evolving healthcare infrastructure
• Complex security and compliance challenges
• PHI information flow risks
• Increased data exposure
• Rising Medical Identity Theft

Healthcare providers are obligated to secure all data accepted from patients for treatment or other health care operations and to ensure that the privacy of that information is upheld.

Security Foundation: Agile, Trusted and Transparent Healthcare
Building Agile Healthcare
Sustainable Compliance

Healthcare Organizations need:

• A sustainable process and infrastructure for the safeguarding of PHI
• To maintain their risk and compliance posture on an ongoing basis and across extended business relationships
• To handle dynamic nature of modern healthcare organizations
• To continuously address IT risk, compliance, and loss incidents

How do you currently address sustainable compliance?
Building Trusted Healthcare

• Healthcare compliance and safeguarding PHI can be burdensome
• This requires a process and solution to manage documentation, tasks, reporting, and monitoring of requirements;
• Organizations need to ease the burden on the organization by leveraging common processes and assessments through technology integration and enablement
• Efficiency in healthcare compliance comes through automation of compliance and security processes

Questions
For Team
What unified frameworks are you currently adopting for compliance management?
Creating Transparent Healthcare

• Compliance in healthcare requires transparency in reporting across enterprise systems, IT networks and extended business relationships

• Healthcare organizations should be able to track and monitor the state of security, risks/vulnerabilities and action items impacting PHI across the organization

• Organizations seeking to achieve transparency in healthcare compliance and PHI security

Questions For Team

Does your organization view PHI risk holistically across multiple information systems, processes, and departments?

How closely does your business and IT work together so that IT knows where PHI is on the network and can adequately protect?
Top 3 Initiatives
Agile, Trusted and Transparent

1. Adoption of healthcare specific industry standard - HITRUST
   • Security is not equal to Compliance
   • Think beyond HIPAA-adopt industry framework such as ISO, HITRUST

2. Annual struggle with Risk Analysis - Information Risk Management
   • Basis for being able to address security proactively

3. Incident Response - Proactive Incident Response
   • It is not if, but when a breach occurs
What is HITRUST?

The Health Information Trust Alliance (HITRUST):

• Comprised of leading healthcare, business, technology, and information security leaders to standardize on a higher level of security to build greater trust

• Established a certifiable framework that any and all organizations in the healthcare industry can implement and be certified against

MISSION:

The Health Information Trust Alliance (HITRUST) exists to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges.
Case Study: Web Hosting Provider

HITRUST Certification Assessment

**Customer Challenge/Objectives**

- Provide customers within the healthcare industry assurance that the products are secure and meet the required regulatory requirements
- Implement the Common Security Framework (CSF) and obtain CSF Certification in the timeframe to meet market demands

**Solution**

- HITRUST CSF implementation and Trusted Advisor guidance
- HITRUST CSF Certification Assessment

**Value/Benefits**

- **Assurance to Customers**
  - Provide customers within the healthcare industry assurance that the products and services are compliant with applicable regulatory requirements
- **Market Differentiator**
  - Help provide security due diligence to differentiate products in the marketplace
- **Ongoing Management of Security Controls**
  - Help reach an end-to-end trusted and compliant state for services and related infrastructure

**Key Recommendations**

- Ongoing configuration, patch, and vulnerability management for infrastructure and systems.
- Implementation and maintenance of security controls for laptop and mobile media security.
Information Risk Management

Are You Managing the Right Risks?

- Information as an asset
- Value of the asset
- Risk Exposure

- Risk Appetite
- Choose control
- Manage Risk
Risk Assessment Action Plan

• Conduct thorough risk assessment/use third party for objectivity/due diligence
• Assess against all reasonable threats/regulatory requirements
• Implement regular risk analysis of the IT environment
• Use third party support to ensure objectivity and due diligence
• Follow a doctrinal approach to risk analysis
• Develop detailed remediation roadmap/project plan to guide decisions
## Case Study: A 200+ Bed Hospital

### Information Security Risk Assessment

<table>
<thead>
<tr>
<th>Customer Challenge/Objectives</th>
<th>Solution</th>
<th>Value/Benefits</th>
<th>Key Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Properly document security and privacy requirements for the Medicare/Medicaid Electronic Health Record (EHR) Incentive Program</td>
<td>• Information Security Risk Assessment</td>
<td>• Meet Security &amp; Privacy Requirements for Meaningful Use</td>
<td>– Recommended security strategy beyond compliance initiatives</td>
</tr>
<tr>
<td></td>
<td>– Conducted an analysis of its EHR security, specifically geared to the requirements of the Meaningful Use Attestation.</td>
<td>– Provided a comprehensive risk assessment of the customer’s implemented EHR, supporting infrastructure, and select connecting applications</td>
<td>– Recommended updates for security management processes relating to the implemented EHR and supporting infrastructure</td>
</tr>
<tr>
<td></td>
<td>– Provided specific recommendations for upgrading certain security practices in light of HIPAA regulations.</td>
<td>– Help Meet Security Requirements for HIPAA, as well as Accepted Industry Standards</td>
<td>– Recommended Improvement in application security lifecycle (SDLC) processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Beyond the required scope of the risk assessment, provided a holistic view of the posture of the security program</td>
<td></td>
</tr>
</tbody>
</table>
Incident Response Readiness: Key Questions

- Was personal data compromised from your systems?
- Did a data breach really occur?
- Is the intrusion or data breach still occurring?
- Have you created a defensible and diligent plan to remediate the intrusion?
- Was the data breach accidental or malicious?
- Have you alerted outside counsel?
- Do you understand your legal obligation for breach notification?
- How effective is your crisis communications plan?
- Was your data breach response plan effective in responding to this incident?
- How can we avoid a data breach in the future?
Case Study: A Leading Non Profit Health Plan
Incident Management Program

Customer Challenge/Objectives
• Improve the ability to respond quickly to external and internal threats to the network, systems, applications and data that may compromise the ability to deliver required services and meet existing SLAs.
• An effective incident management program in a highly complex and distributed environment
• Determination of whether a SOC should be implemented internally or outsourced

Solution
• Incident Response Program (Framework) Assessment and Development
• Technology Evaluation, Assessment, Reconfiguration, and Integration
• Incident Management Program and SOC Recommendations and Implementation Roadmap

Value/Benefits
• Customized Incident Management Program
  – Provided an incident management program customized to the organization that ensured coverage within the distributed environment
• Streamlined existing processes
  – Leveraged existing healthcare industry experience to address applicable threats and risks, as well as effective incident management models used with industry peers
• Optimization of security controls
  – Evaluated existing client technology for optimization rather than investing in new technology

Key Recommendations
• Incident management program, policies and procedures
• Existing technology solutions optimization
• Evaluation and recommendation to implement an in-house SOC based upon various criteria
Key Takeaways

• **Adopt** a security program that is based on industry standards

• **Build** scalable security programs that evolve with technology

• **Analyze** security risks based on information as an asset

• **Quantify** security risks

• **Streamline** security operations

• **Propagate** best practices across the organization

• **Address** information security in contracts
Security
A Risk that Needs to Be Managed

Strike the Balance

Convenience
Security