Healthcare and IT Working Together

2013 KY HFMA Spring Institute
Introduction

• Michael R Gilliam
  o Over 7 Years Experience in Cyber Security
  o BA Telecommunications – Network Security
  o CISSP, GHIC, CCFE, SnortCP, Security+, Network+
  o Previously provided security solutions while working in the Federal Government, Military, State Governments, and Private Consulting

• Jimmy Noll
  o 26 Years in Information Technology
  o 18 Years in IT Security and Risk Management
  o Consultant to Healthcare for Risk and Impact Analysis and Security Management Programs
  o CTO at SDGblue – started Security Practice, Ohio Business Unit, Managed Security Services
Contents

• Changes in Healthcare Information Technology
• Where IT and Health-care Meet
• What is a Risk Analysis
• Cyber Security Challenges Presented
• How Cyber Security Can Impact Healthcare
• How To Protect Critical Information
• Additional Information
Changes in IT and Healthcare

HITECH - Health Information Technology for Economic and Clinical Health

Attempts to spur the rapid adoption of Electronic Health Records (EHR)

- Financial Incentives to encourage the adoption of EHR
- Financial Incentives will soon give way to penalties

- Non-Adoption by 2015 – penalized 1% of Medicare Payments
  - Depending on the volume of
HITECH – Breach Notification Law

Requires

- Providers who experience a breach to promptly notify affected individuals
- Notification of HHS secretary and media in the case where

During a recent study of Healthcare breaches

- 94% of respondents had at least one data breach in the previous two years
- 45% report that

<table>
<thead>
<tr>
<th>Breaches by Type</th>
<th>2010</th>
<th>2011</th>
<th>2012 (Q1 and Q2)</th>
<th>2012 (Projected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>107</td>
<td>82</td>
<td>41</td>
<td>88</td>
</tr>
<tr>
<td>Loss</td>
<td>34</td>
<td>15</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>Unauthorized Access/Disclosure</td>
<td>22</td>
<td>20</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>Incorrect Mailing</td>
<td>10</td>
<td>10</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>11</td>
<td>9</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Hack</td>
<td>11</td>
<td>8</td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>
## Healthcare Cyber Security Statistics

<table>
<thead>
<tr>
<th>Breaches by Organization Type</th>
<th>2010</th>
<th>2011</th>
<th>2012 (Q1 and Q2)</th>
<th>2012 (Projected)³³</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital/Health System</td>
<td>82</td>
<td>48</td>
<td>14</td>
<td>41</td>
</tr>
<tr>
<td>Physician Practice</td>
<td>48</td>
<td>48</td>
<td>24</td>
<td>54</td>
</tr>
<tr>
<td>Health Plan</td>
<td>25</td>
<td>22</td>
<td>6</td>
<td>19</td>
</tr>
<tr>
<td>Academic Medical Center</td>
<td>16</td>
<td>6</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Government Agency</td>
<td>12</td>
<td>4</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Academic Institution</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>11</td>
</tr>
</tbody>
</table>
“Most CFO's would agree that it is their primary responsibility to ensure the fiscal resources of the organization are used wisely and in such a way to support the business needs and future growth of the organization.”

From the Financial Side – we need to plan for

- IT Hardware
- Software
- People and Training
Challenges

Moving Personal Health Information (PHI) to an electronic format (ePHI) introduces a new set of threats. Healthcare organizations needs to ensure these critical digital assets are adequately protected by using the following types of controls.

• Physical
• Technical
• Administrative
Cyber Security in Healthcare

Need to implement new controls
• How should these items be budgeted for and prioritized?

Ensure that the solution proposed meets the long term needs of the organization and does so in a financially responsible way – this can be accomplished by a standard proper Cost-Benefit Analysis (CBA)

• Cost of doing Nothing
• Cost of Solution
• Weigh the Benefits vs the Cost
What is a Risk Analysis

A risk analysis is a periodic assessment of the electronic personal health information and other critical data or assets owned by the organization.

- Discovery / Inventory
- Identify Threat Sources
- Vulnerabilities
- Control Analysis
- Likelihood Analysis
- Impact Analysis
- Mitigation
Financial Impact to Healthcare

- Cyber Attacks on Medical Devices
- Modification of Records
- Loss of Patient Data
  - Legal Liability
  - Reputation Damage
  - Cost of Downtime
  - Fines

<table>
<thead>
<tr>
<th></th>
<th>Each Violation</th>
<th>All such violations of same incident within calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>B) Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>C) Willful Neglect - Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>D) Willful Neglect - Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
“A business will have good security if its corporate culture is correct. That depends on one thing; tone at the top. There will be no grassroots effort to overwhelm corporate neglect.”

--William Malik – Vice President and Research Area Director for Information Security At Gartner

•Make Cyber Security a priority – build security into all procedures and processes from the beginning
What Healthcare should be Doing

• Build an Information Security Program
• Fundamentals
  o Network Architecture Design
  o Physical Security
  o Awareness Training
    ▶ Well Developed Policies and Procedures
  o Limited User Access
  o Vulnerability Remediation and Testing
  o Disaster Recovery / Business Continuity
What Healthcare Should be Doing

• Knowing Where You Stand
  o Testing, Testing, and more Testing
  o Annually Performing a Risk Analysis
  o Annually Conducting a Technical Assessment measuring the effectiveness of
    • Policies
    • Procedures
    • Practices
    • Security Controls

• Retest every year to measure progress and be able to benchmark yourself
What Healthcare Should be Doing

• Incident Response Program
  o Preparation
  o Identification
  o Containment
  o Remediation
  o Restoration
  o Reporting

• Crucial to limit the impact of a breach when they do occur
What Healthcare Should be Doing

Regulatory Compliance
HIPAA 12 Administrative Controls


HIPAA Security Rule

Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

Identify and protect against reasonably anticipated threats to the security or integrity of the information;

Protect against reasonably anticipated, impermissible uses or disclosures; and

Ensure compliance by their workforce.

Reduce the financial impact of a breach
Conclusion

• Changes introduce additional complexity / threats
• Threats are Real
• Need to Make Security a priority
• Do the Fundamentals Right
• Use Risk Analysis to determine balanced approach
Additional Resources

• US Department of Health and Human Services
  • http://www.hhs.gov
• National Institute for Standards and Technology
  • http://www.nist.gov
SDGblue Service Lines

What services do we offer?

- Security Services Group (SSG)
  - Security Assessments & Testing (Hacker type things)
    - Internal - External - Firewalls – Applications
    - Social Engineering - Malicious Activities – Regulatory (HIPAA)
  - Audit, Compliance & Risk
    - Financial Systems - Policy Reviews - Disaster Recovery
    - Regulatory (HIPAA) – Technical, Administrative, Physical
    - Risk Identification
- Hosted Security Services
  - Log Management – Firewall Management

www.sdgblue.com
Thank You!

Michael R Gilliam
Senior Security Engineer
859-685-3498
Michael.Gilliam@sdgblue.com

Jimmy Noll
Chief Technology Officer
513-618-8960
Jimmy.Noll@sdgblue.com