Why is building a foundation of trust with your patients and with those in your organization so critical to cybersecurity?

Sri Bharadwaj  MS, FCGMA, CPHIMS, CISSP, CLSSBB, PMP  
Director, Information Services  
University of California, Irvine Health, Orange County, CA

November 9, 2015
Abstract

Organizations nowadays have a high degree of technical literacy. And information access and information management have both achieved new heights. It’s essential that every organization needs to have a deep understanding of healthcare privacy and security to meet regulatory requirements, such as HIPAA, and prevent unauthorized access, use, and disclosure of the information. In other words, every organization needs to understand privacy as well as security as they go hand in hand.

You cannot keep a patient’s information private if it is not secure. Similarly, if a patient’s information is not secure, you are not keeping it private.

In today’s world, you need to have a strong privacy and security program within your organization, with every workforce member playing a key role in its success, in order to satisfy not only regulatory requirements, but also for effective risk management. In addition, you need to create a privacy and security program which is tailored to your size and nature of organization.
Healthcare in Time of Transformation

- Healthcare Reform Driving Innovation and New Technologies
- Exponential Increase of Online Information
- Cloud & Mobile, IoT & Social Media, Medical Devices, HIEs & Multi-system Integration

Are we Ok?
On 17 April 2014 the Federal Bureau of Investigation (FBI) issued a Private Industry Notification to healthcare organizations, stating:

The threat landscape is changing very rapidly.

- Electronic Health Records (EHRs) create rich targets of opportunity:
  - According to the FBI, stolen medical records are fetching $50 each on black markets, much higher in value than stolen credit card records and most other financial records (around $1 each).

- Medical information is being used primarily for identity theft and prescription drug fraud.

- There are new and sophisticated threat actors:
  - Medical data is now being targeted by cyber-criminal gangs, foreign governments, and even hacktivists.
  - Medical devices have gaping security holes, creating serious patient safety issues.

According to the Identity Theft Resource Center, there were 333 medical data breaches in 2014, compared to 271 breaches in 2013 – a 23 percent increase year-over-year.

Why health care now?
- High intrinsic value of data.
- Credit cards tend to be quickly canceled while stolen medical identities are not easily detected.

In 2015, the trend is not improving...

Anthem – March 13, 2015

Data breach affected approximately 80 million individuals and may cost up to $100M.

Lawsuits frequently follow the announcement of a major breach.

Premera – March 17, 2015

Breach impacted nearly 11 million members and applicants.
Many programs focus on the symptoms not the issue

Something will always need fixing

Prioritize and focus on the causes

*Sisyphus Worked Hard, We Need To Work Smart*
20% of all breaches involve some form of theft or loss of a device not properly protected.

26% of breaches in healthcare are carried out by knowledgeable insiders for identity theft or some form of fraud.

33% of breaches are caused by mistakes or unintentional actions such as improper mailings, errant emails, or facsimiles.

There was nearly a doubling of breaches due to cyber attacks in 2015. 2nd year in a row of 100% increase.

Verizon 2015 Data Breach Investigations Report
How is Risk Created?

Understanding the formula in order to identify risk

A risk exists when a vulnerability can be exploited by a threat source.

Vulnerability + Threat Source = Risk

Vulnerability
An exposure

Threat Source
Intentional or unintentional exploitation

Risk
An event that could occur

Example
Systems containing ePHI are not encrypted

Vulnerabilities exist in varying magnitudes across an Healthcare Organization’s various business lines.

Computer criminal

Threat sources may be more prominent in one business line versus another.

Breach of ePHI due to malicious outsiders’ actions

Risks are ranked based on the impact and likelihood of the event, if it were to happen, in that business line.
Cyber Security
*Sounds pretty technical…*

**Sources of Risk**

**Insiders:**

Well-intentioned staff sometimes expose sensitive information when corresponding with outside parties.

**Outsiders:**

Malicious outsiders are looking to steal sensitive information to use for themselves or to sell in the ever-growing medical information black market. Typically 3 categories: (1) Nation State Sponsored, (2) Organized Crime, and (3) Hacktivists.

---

**What is “Cyber Security?”**

Cyber Security refers to “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.”¹

The term is believed to have been coined in 1994 – to keep pace with related terms “cyber space” and “cyber crime.”

---

¹According to Merriam-Webster Dictionary
### Insider Risk Scenario
Transmitting Sensitive Information Outside the Corporate Network

As part of daily operations, sensitive information must often be sent to business partners, members, and patients. Sending that information accurately and securely is critical to preventing that information from falling into the wrong hands.

<table>
<thead>
<tr>
<th>Workforce</th>
<th>Transmitting Sensitive Data</th>
<th>Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Analytics/Reporting</td>
<td>Texting</td>
<td>Members</td>
</tr>
<tr>
<td>Pharmacy</td>
<td>Non-approved websites</td>
<td>Group Customers</td>
</tr>
<tr>
<td>Practitioners</td>
<td></td>
<td>Law Enforcement</td>
</tr>
<tr>
<td>Member Services/Administration</td>
<td>Texting</td>
<td>Patients</td>
</tr>
<tr>
<td>Claims</td>
<td>Personal email (e.g., Gmail)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-approved cloud storage</td>
<td></td>
</tr>
</tbody>
</table>

**Secure Solutions**
- Lotus Notes “Send Secure”
- Secure File Transfer (e.g., SFTP)
- Secure messaging
- Secure texting

Given the variety of methods and scenarios for transmitting sensitive information, multiple teams are working collaboratively to bring risk mitigation solutions to the areas where we have the highest risk.
Outsider Risk Scenario

Anatomy of a Potential Attack Aimed at the Corporate Network

Reconnaissance & Delivery

1. A malicious outsider decides to target the organization.

2. The outsider finds a clinician’s email address and sends a link to click on.

Installation & Control

3. The clinician clicks on the link while checking his email.

4. The counterfeit link installs a keystroke logger on his device, which subsequently captures his log-in credentials.

5. The stolen credentials are sent back to the malicious outsider.

6. The malicious outsider uses the credentials to log in to clinical systems.

7. Sensitive data is extracted and sent to a hidden location.

Action & Extraction

8. Once out of the corporate network, the data can be sold on the Internet or used by others to perpetrate identity theft or theft of medical services.

9. Healthcare organization will have to notify state and federal regulators of the breach and respond to member, patient, and group customer inquiries about privacy and security practices.
We Need A Paradigm Shift

Healthcare must think and act differently when it comes to data security and privacy.
Closing The Security Gap

Security is the ceiling.

Leadership are the walls that bring security and compliance together.

Compliance is the floor.
What We Need The Board To Do

• Ensure roles & responsibilities are defined & empowered
• Require regular reports regarding risk mitigation
• Identifying and auditing potential areas of risk
• Encourage accountability and respect

Organizations whose Board of Directors are highly engaged with information security risks and include cyber-security in their annual audit plan manage risk more acceptably.

Protivity Survey, 2015
Five Things Leaders Should Do

1. Empowering the chief security and compliance officers with the authority to do their jobs.

2. Elevating the CISO role so that it gets the appropriate recognition at the organization’s highest levels.

3. Forming a security governance framework that includes senior business and clinical leaders.

4. Building a strong, resilient security program that prioritizes risk and plans proactively for breaches.

5. Boards/CXOs need to lead and enforce accountability.
The Cost of Security

- Discovery, Notification & Response
- Business Disruption
- ID Theft Monitoring
- Investigation/Review
- Civil Penalties
- Federal CAP/RA
- State Actions
- Law Suit Defense
- Criminal Penalties
- Insurance
- Degradation of Brand/Image
- Distraction of Staff
- VBP Payments Impacts
- HCAPPS Score Impacts
- Patient Confidence/Loyalty
- Physician Alignment/Nurses and Staff Agreement
Staffing Cost Calculation for Incident Response

Median staff needed to respond to an incident (per 1000 employees):
- Initial stage: 4.3
- After incident: 4.4

Example: Hospital with 6000 employees

**Number of staff members needed**
- Initial: $6 \times 4.3 = 25.8$
- After: $6 \times 4.4 = 26.4$

**Total time spent addressing issue**
- Initial: 12 hours/person $\times 25.8 = 309.6$
- After: 36 hours/person $\times 26.4 = 950.4$

**Total amount paid for time spent (based on average salary of $110,000)**
- Initial: $309.6 \times 52.88 = 16,392.80$
- After: $950.4 \times 52.88 = 50,236.00$
- Total: $66,628.80
How Effective Is Cyber Security Insurance?

• Most cyber security insurance only covers a fraction of large breach costs

• Insurance providers are looking to increase premiums, enhance underwriting provisions and increase exceptions to avoid losses associated with large incidents

• Columbia Casualty vs. Cottage Health System

• Cyber Insurance will continue to be useful in responding to smaller incidents, but will be harder to get, cost more and not address large breaches adequately
Five steps to building a foundation of trust with your patients and with those in your organization
1. Gain Executive Management Support

Executive management support is critical! P&S is first a senior leadership concern.

P&S should be seen as a strategic value that is discussed at the board level.

P&S crosses all service/business lines – it’s not just the IT or Security Dept.

Commitment to invest in IT and P&S, and drive change. (Other regulated budgets are 6-12% of IT budget, not 1% as in healthcare)

Senior IT leaders (CIO) needs to operate at SVP/executive level, report to CEO, and be seen as strategic leader. Talk in business, not technical, terms.

Senior security officer (CISO) also needs a seat at the table. Peer w/CIO, possess credentials to develop a budget, report to CEO. Partner with business leaders.
Gartner Security Maturity Levels

Level 1
- CIO
  - Infrastructure & Operations
  - Application Development
  - Etc.
- Network
- Servers
- Applications
- Operations

Level 2
- CIO
  - Infrastructure & Operations
  - Operations
  - Security
- Application Development
- Etc.

Level 3
- CIO
  - Infrastructure & Operations
  - Application Development
  - Etc.
  - CISO
    - Security Operations
    - Security Analysts
- Network
- Servers
- Applications
- Operations

Level 4
- CIO
  - Infrastructure & Operations
  - Application Development
  - Etc.
- CISO
  - Risk Assessment
  - Security Analysis
- Infrastructure
- Operations
- Security Operations
2a. Perform a HIPAA Risk Analysis

- Meaningful Use a driver
- Should be done annually
- Use NIST SP 800-30 to assess risks & vulnerabilities of C-I-A of ePHI systems
- Methodology addresses management, operational, and technical controls
- Scope includes People, Processes, and Technology
- Determine location of all ePHI
- Threats - insider attack, physical intrusion or theft, external attack
- Threat rating: Likelihood X Impact = Risk (High, Medium, Low)
- Develop remediation roadmap
2b. Complete a HIPAA Gap Analysis

Based on the Office for Civil Rights (OCR) Audit Protocol.

Methodology addresses 7 control domains, representing separate elements of the HIPAA Privacy, Security and Breach Notification rules.

Scope is limited systems that create, receive, maintain, or transmit ePHI

Typical gaps:
- Policies & Procedures
- Critical Systems mapping
- User account management
- System access
- Encryption
- CISO and security staff
- System patching
- Security awareness
- System/log monitoring

Partial credit or full credit (based on documentation and actual controls being in place).

Results can be used to create a Remediation Plan
3. Establish a Cybersecurity Program

- Encompasses People, Process, and Technology
- Update Policies and Procedures
- Select a Privacy and Security Framework
  - ISO 27001/27002*
  - CSF/HITRUST*
  - Gartner, IBM
  - COBIT, ITIL, COSO, FISMA, OCTAVE
- Implement Cybersecurity Monitoring and Technical Controls
- Consider using Managed Security Services
  - Addresses constraints with technical solutions, staffing, and budget

* Certification
4. Remediate the High Risk Areas

- Laptops & Mobile Devices
- USB Drives
- Texting
- Email
- Document Sharing
- Web
- Patching
- Clinical IT & Imaging
- Photo Copiers & IoT
- PCI DSS Systems
4. Remediate the High Risk Areas

Redspin Survey
50% of breaches due to lack of encryption!
4. Remediate the High Risk Areas

**Ponemon Survey**
- 800,000 devices lost/stolen each year
- 74% missing USB drives due to employee negligence
- 65% missing USB drives not reported
4. Remediate the High Risk Areas

- **Texting/Email**
  - Physician-to-Physician texting using SMS and pagers
  - Some organizations still are not using email encryption

- Laptops & Mobile Devices
- USB Drives
- PCI DSS Systems
- Photo Copiers & IoT
- Clinical IT & Imaging
- Patching
- Web
- Document Sharing
- Texting
- Email
4. Remediating the High Risk Areas

**uSamp Survey**
- 41% workers used unsanctioned cloud file sharing in last 6 months
- 87% knew organization had policies restricting this
4. Remediate the High Risk Areas

- Malicious websites grew 600%
- 85% of malicious hosts were found on legitimate sites
4. Remediate the High Risk Areas

Symantec Internet Threat Report
- 51,644 vulnerabilities have been identified over the past two decades
4. Remediate the High Risk Areas

- Laptops & Mobile Devices
- USB Drives
- Texting
- Email
- Document Sharing
- Web
- Patching
- Clinical IT & Imaging
- Photo Copiers & IoT
- PCI DSS Systems

Outliers and Unmanaged IT
Privacy/Security is Everyone’s Concern

It’s everyone’s role, not just the security staff or CISO

From Board of Directors & CEO to Volunteers

25% of internal data theft done w/hard copies
Symantec Report

Most security problems discovered by non-IT staff
Techtarget.com

“Culture is often more powerful than law”
Glenn Harlan Reynolds

Most security problems discovered by non-IT staff
Techtarget.com

“Culture is often more powerful than law”
Glenn Harlan Reynolds
5. Implement Privacy & Security Awareness Training

- Top-down approach improves user awareness
- Have a training model in place
- Train the security pros early on
- Offer continuous security awareness training
- Engage the user to help avoid human error

Patrick Ouellette, 2013
HealthITSecurity.com
Any Questions?