Study of 1000 Vendor Security Practices
March 28, 2017

Peter N. Merrill, Dartmouth Hitchcock Health System
Danny Mimnaugh, CORL Technologies

Presentation Agenda

Regulatory Guidelines - Peter
  • Responsibilities
  • Regulatory Challenges
  • Breach data
  • Case Study - The Pennsylvania Institute

Introduction into the Third-party Security Risk Management World
  • HCO’s third-party profiles
  • Vendor Security Risk Management Program overview
  • Keys to an Effective VSRM program

Miscellaneous info on VSRM
  • Program Weaknesses
  • Why??
  • Collaboration amongst peers
  • Assurance
    • Types of Assurances
      • Will Business Associate Reimburse?

Third-party Breach Risks

Regulatory
  • CE remains responsible for Breach Notification
  • HIPAA also requires organisations to assess the risk for a breach of PHI whenever it is created, received, maintained or transmitted and to put measures in place to safeguard the information

Reputational
  • Headlines
    • Undermines Patient Trust
    • Undermines Employee Trust

Financial
  • Breach Notification is Expensive
    • Mailings
    • Call Centers
    • Credit Monitoring
  • Staff Time
  • OCR Penalties for non-compliance with HIPAA Rule (e.g., St. Elizabeth’s Medical Center)
  • Will Business Associate Reimburse?
What is required to comply with HIPAA?

- As a covered entity and business associate you are required to assess the risk to the confidentiality, integrity and availability of ePHI. This includes ensuring the safeguards that your vendors’ have in place to prevent any that they store, access, transmit or present for you.

**RISK ANALYSIS:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the third party.

This is what NIST says:

- “Establish Processes for Ensuring Compliance and Maintaining the Control of Security Requirements. Are Not Being Used”
- “Conduct periodic security reviews.”
- “See NIST SP 800-66, Section 7.3 "Considerations When Applying the HIPAA Security Rule." Available at

As a covered entity and business associate you are required to assess the risk to the confidentiality, integrity and availability of ePHI. This includes ensuring the safeguards that your vendors’ have in place to prevent any that they store, access, transmit or present for you.

**RISK ANALYSIS:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the third party.

This is what NIST says:

- “Establish Processes for Ensuring Compliance and Maintaining the Control of Security Requirements. Are Not Being Used”
- “Conduct periodic security reviews.”
- “See NIST SP 800-66, Section 7.3 "Considerations When Applying the HIPAA Security Rule." Available at

“Based on stats from whistleblowers, HHS’ Office for Civil Rights, and St. Elizabeth’s Medical Center, part of Boston-based Steward Health Care, 52% of data incidents were caused by third party vendors. The below diagram breaks down the different causes for data incidents during the 2016 study:

% Distribution - Cause of Data Incident

© 2013 CORL Technologies, Atlanta, GA. All Rights Reserved

The Ponemon Institute: Tone at the Top and Third Party Risk

- Third party risk has substantially increased due to disruptive technologies including the Internet of Things (IoT) and migration to the Cloud.
- The consequences of not managing third party risk can be extremely costly, as organizations represented in this research spent an average of approximately $20 million to respond to a security incident as a result of negligent or malicious third parties.
- Most third party risk management programs are generally informal and not effective, as most respondents admit that improving third party relationships is not a top risk management objective.
Implementing a Vendor Security Program

Why?
- More Vendors than ever have access to Covered Entities' data
- Vendors are supported by sub-contractors from around the globe
- Becoming more difficult to track where data is transmitted and maintained
- Need to control risk

How?
- Requires on-going process
- Requires a team effort with leadership support

Why?
- More Vendors than ever have access to Covered Entities' data
- Vendors are supported by sub-contractors from around the globe
- Becoming more difficult to track where data is transmitted and maintained
- Need to control risk

How?
- Requires on-going process
- Requires a team effort with leadership support

Health Care System Vendor Profiles

Initial Risk Profile
An effective Vendor Security Risk Management Program is engineered to deliver risk strategies as efficiently as possible.

Identify Risky Vendors

Review Vendor Questionnaire

Validate Questionnaire

Perform Audit

Risk Strategy: [improve security practices, insurance, limit access, accept, no additional business]

15-20% of vendors

Resource constraints with traditional approaches produce minimal results.
Efficient Vendor Risk Management Program

Vendor Profile: Distribution of Vendors by size (# of Employees)

Vendor Profile: Distribution of Vendors with and without a Security Certification

- Only 26% of vendors have a Security Certification
  - ISO 27001 - 10%
  - SOC 2 Type I - 6%
  - SOC 2 Type II - 5%
  - HITRUST - 10%
  - FEDRAMP - 15%
  - Others: PCI DSS, CSA Star, SOC1 Type 2, URAC
Vendor Profile: Distribution of Vendors with and without a Security Certification by vendor size (# of employees)

Vendor Profile: Distribution of Vendors with and without a Designated Security Team

- Only 39% of vendors have at least 1 designated security team member.
- Organizations without a security team are generally less likely to cooperate and provide adequate documentation during the risk assessment.
- Very difficult to conduct an efficient risk assessment of an organization that lacks designated security personnel.

Vendor Profile: Distribution of Vendors with and without a Designated Security Team by Vendor Size (# of employees)

Vendor Profile: Distribution of Vendors with and without a Designated Security Team by Vendor Size (# of employees)
A strong majority of vendors lack adequate Security Practices. Organizations without strong security practices ultimately lead to investments at both the CA and BA levels as well as the BA level.

Vendor Profile: Distribution of Vendors based on the quality of their Security Practices

Vendors with a D: 0%
Vendors with a C: 42%
Vendors with a B: 8%
Vendors with an A: 2%
Vendors with an F: 2%

Vendor Profile: Distribution of Vendors based on the quality of their Security Practices by Vendor Size (# of employees)

Number of Vendors

Vendor Profile: Vendors who have and have not had a reportable breach

Of the 1157 vendors sampled, 75 have had a reportable breach within the last 3 years.

Vendor Profile: Vendors who have and have not had a reportable breach
Vendor Profile: Vendors who have and have not had a reportable breach by vendor size (# of employees)

<table>
<thead>
<tr>
<th>Size Category</th>
<th>No Breach</th>
<th>Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Small</td>
<td>617</td>
<td>4</td>
</tr>
<tr>
<td>Small</td>
<td>394</td>
<td>18</td>
</tr>
<tr>
<td>Medium</td>
<td>162</td>
<td>36</td>
</tr>
<tr>
<td>Large</td>
<td>63</td>
<td>10</td>
</tr>
<tr>
<td>Very Large</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>Largest</td>
<td>9</td>
<td>0</td>
</tr>
</tbody>
</table>

Leadership communication
- Difficulty to accurately communicate risk exposure to leadership
- Communication is inconsistent

Vendor communication and accountability
- Communication is sporadic, inconsistent and unclear
- Absence of linkage between vendor information management failures and contract management

Why are there Weaknesses

Seeing the forest for the trees...
- Too busy gathering data...
- Leaves limited time for risk management.
- Unclear objectives for vendor information risk management...
- "Check the box" compliance or true reduction of risk?
- Lack of executive level reporting.
- Disconnect from contract management.
Collaborative Approach to Vendor Security Risk Management

- Legal/Compliance
- Procurement/Contracting
- IT
- Frequent Users (Finance, Revenue & Reimbursement, Quality)

- Review existing contracts to search for frequent users

Focus on Assurance

- Third party audit – Assurance
- Review of evidence of control described in a response to a questionnaire – Assurance
- Response to a questionnaire – Information not Assurance
- Interview with vendor – Information not Assurance
- Status update from vendor – Information not Assurance
- Vendors responsibility to provide Customer assurance that information is safeguarded

Security Audits/Certification

- SOC 2, Type II: covering security, availability, processing integrity, confidentiality and privacy, and applying your (sometimes CIA) standards, is the more comprehensive audit.
- Type I means tested, Type II only noted as policy.
- The term SSAE 16 alone can be interpreted as a SOC 1, focusing on controls only to the extent “material” to financial reporting.
- ISO 27001: Int’l standard – certification for management frameworks for security. (ISO 27017 is new cloud-specific standard)
- CSA Cloud Controls Matrix (CCM): cloud security playbook
- FedRAMP: federal standard
Red Flags for Initial Security Assessment

- Assessment partially completed and vague responses
- "We already performed a security assessment & everything was fine."
- "We've been in the industry a long time and nobody has asked us these questions before."
- "HIPAA doesn't require that we answer these questions."
- "We don't need to do a security assessment because it's a big company and they have good security."
- "You don't need to worry; we only capture employee data, not patient data."
- Refusal to let you contact the subcontractor who is actually handling the data

Who/What to Assess?

- Who houses the data?
- How does the data get from the source to the end recipient?
- Follow the trail and assess all points along the way
- Remember: The trail may not be a straight line!

Example: Risk Reduction Terms

- Obtaining Independent Security Assessment - provide evidence
- Developing a plan to address issues – provide evidence
- Requiring adherence to a timeline
- Allowing for termination of contract for failure to meet timelines
- Indemnification
Care New England Health System (CNE): Third-party Breach

- Care New England Health System (CNE) has agreed to pay $400,000 and employ a corrective action plan to settle HIPAA violations.
- The breach, which was reported to the OCR in 2012 by Women and Infants Hospital in Rhode Island, a business associate of CNE, included missing unencrypted backup tapes that held PHI of some 14,000 individuals.
- The business associate agreement between the two entities, originating in 2005, had not been updated until the 2015 OCR Investigation, and did not incorporate revisions required under the HIPAA Omnibus Final Rule.


As we see in this particular case, vendor/B.A. security can be the unlocked backdoor to healthcare data. As the healthcare provider, it is ultimately your responsibility to safeguard Protected Health Information, and perform due diligence on vendors with PHI access.

Questions?

© 2013 CORL Technologies, Atlanta, GA. All Rights Reserved