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 Ponemon 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 rule requires organizations to assess the risk to a breach of PHI wherever 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?

Regulatory Challenges

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 assessing the safeguards that your vendors' have in place to protect ePHI that they store, access, transmit or process 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:

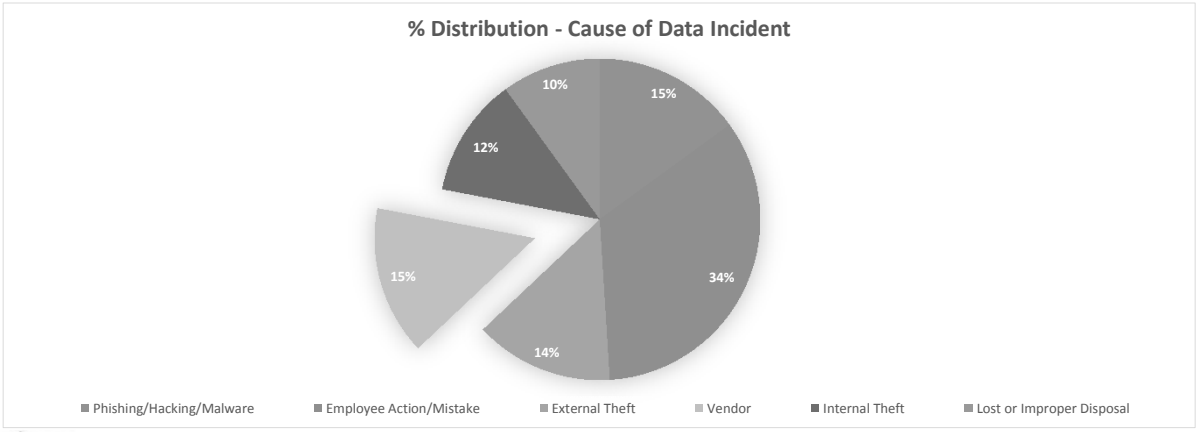
- "Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met"
- "Conduct periodic security reviews."
- [5] See NIST SP 800-66, Section #4 "Considerations When Applying the HIPAA Security Rule." Available at
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf – PDF

"Based on tips from whistleblowers, HHS' Office for Civil Rights fined St. Elizabeth's Medical Center, part of Boston-based Steward Health Care, $218,400 for using an Internet-based document sharing application to store documents containing PHI without first analyzing the risks associated with the platform. This lack of risk analysis put the PHI at risk."

Regulatory Challenges

Information surrounding Data Breaches?

- According to the BakerHostetler 2016 Data Security Incident Response Report, roughly 15% of Data Incidents were caused by Third Party Vendors the below diagram breaks down the different causes for Data Incidents during the 2016 study:



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 $10 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.

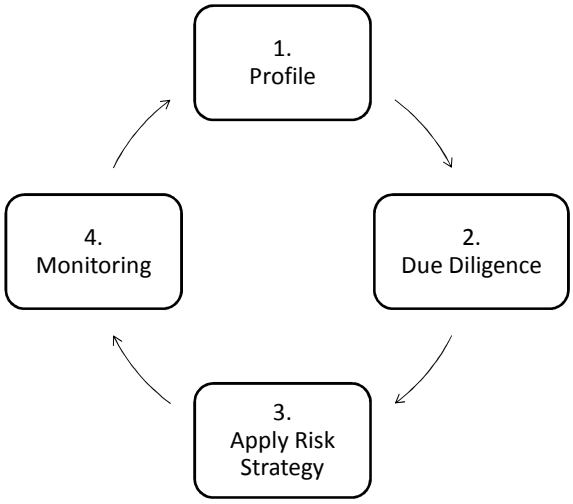
Implementing a Vendor Security Program

Why?

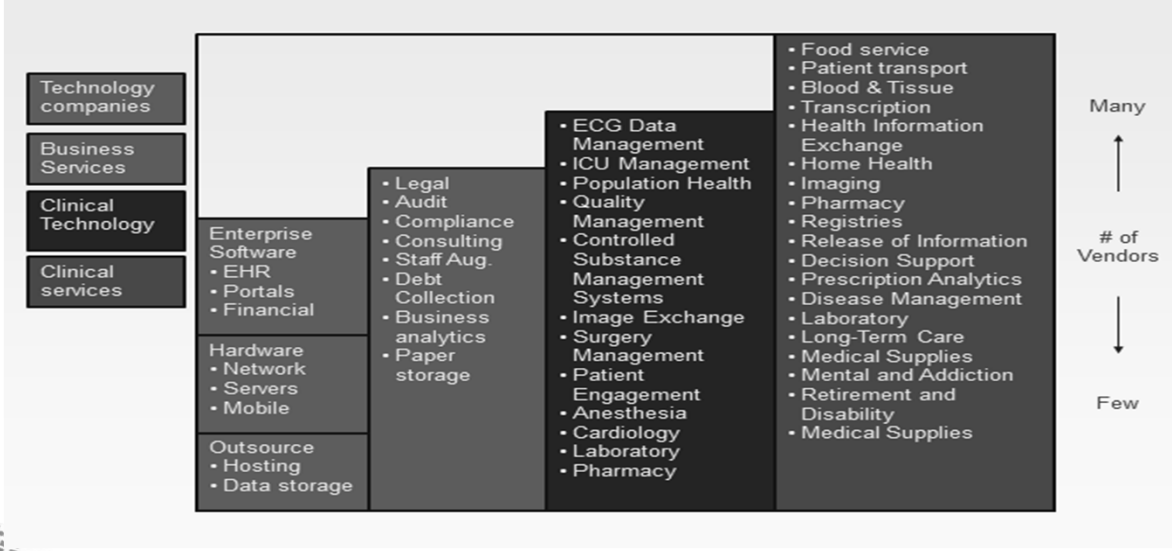
- More Vendors than ever have access to Covered Entities' data
- Vendors are supported by sub-contractors from around the globe
- Becoming more difficult to track where data is transmitted and maintained
- Need to control risk

How?

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



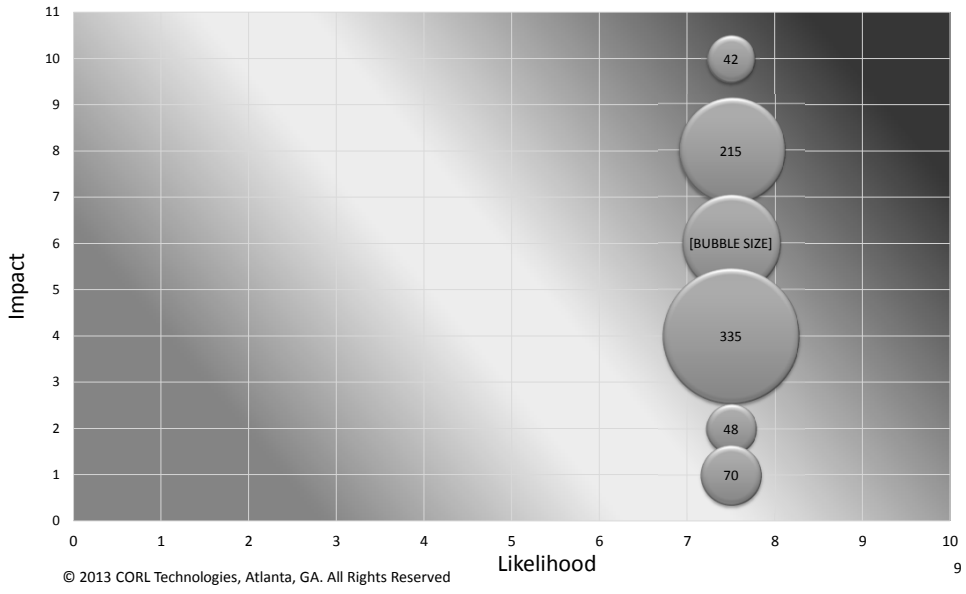
Health Care System Vendor Profiles



8

Initial Risk Profile

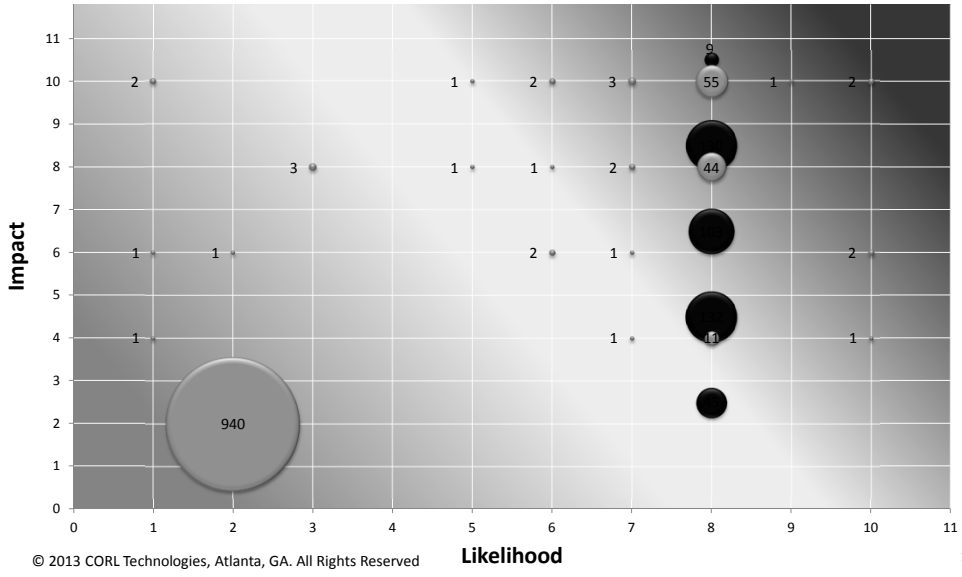
- Size of circles = # of vendors
- See references to vendors on next page
- **Impact** = the volume of PHI at risk to a breach
- **Likelihood** = the security capabilities of a vendor to protect data and avoid a breach
- **Green area** = high confidence that vendor can protect data
- **Yellow area** = uncertain of vendor's security capabilities
- **Red area** = low confidence that vendor can protect data



9

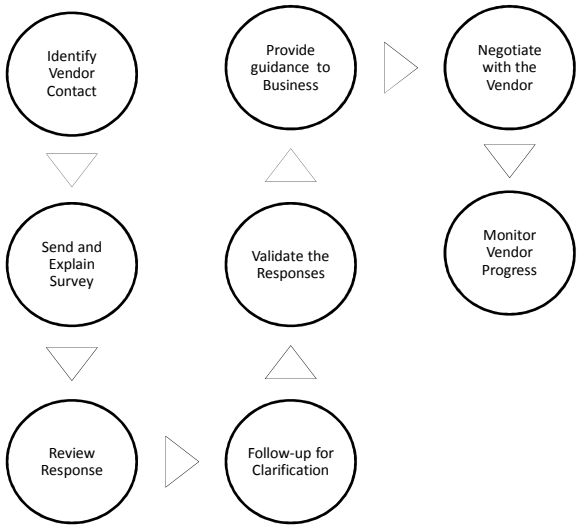
Residual Risk Profile

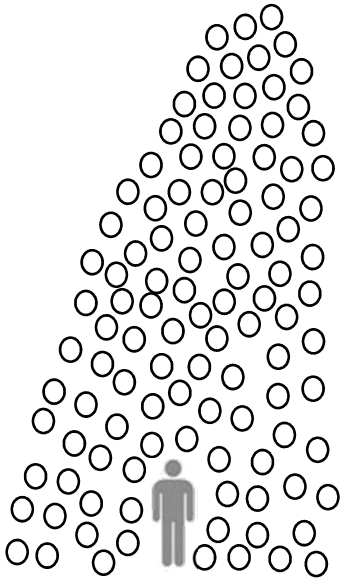
- Size of circles = # of vendors
- See references to vendors on next page
- **Impact** = the volume of PHI at risk to a breach
- **Likelihood** = the security capabilities of a vendor to protect data and avoid a breach
- **Green area** = high confidence that vendor can protect data
- **Yellow area** = uncertain of vendor's security capabilities
- **Red area** = low confidence that vendor can protect data



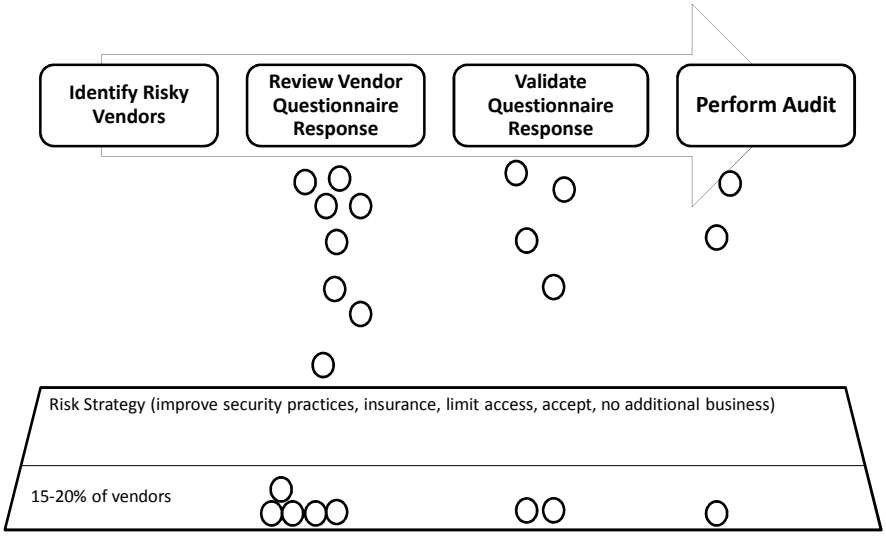
10

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

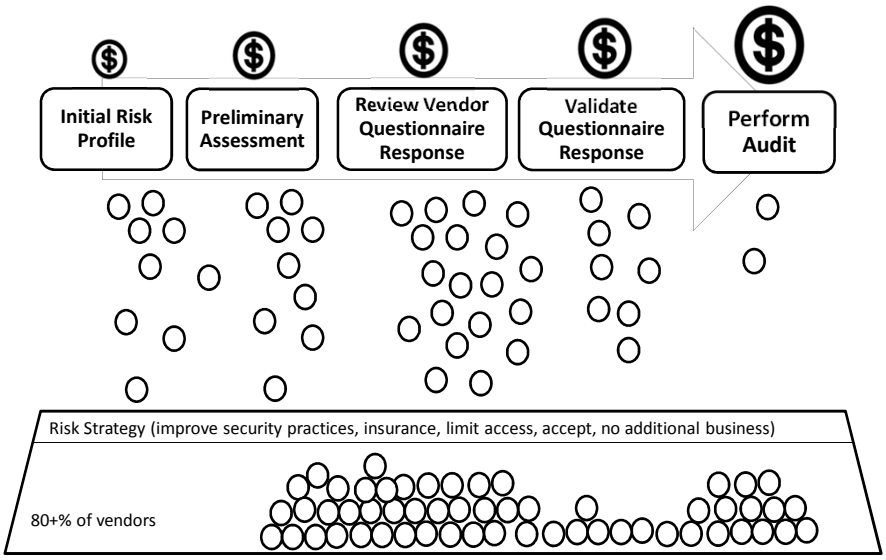




Resource constraints with traditional approaches produce minimal results

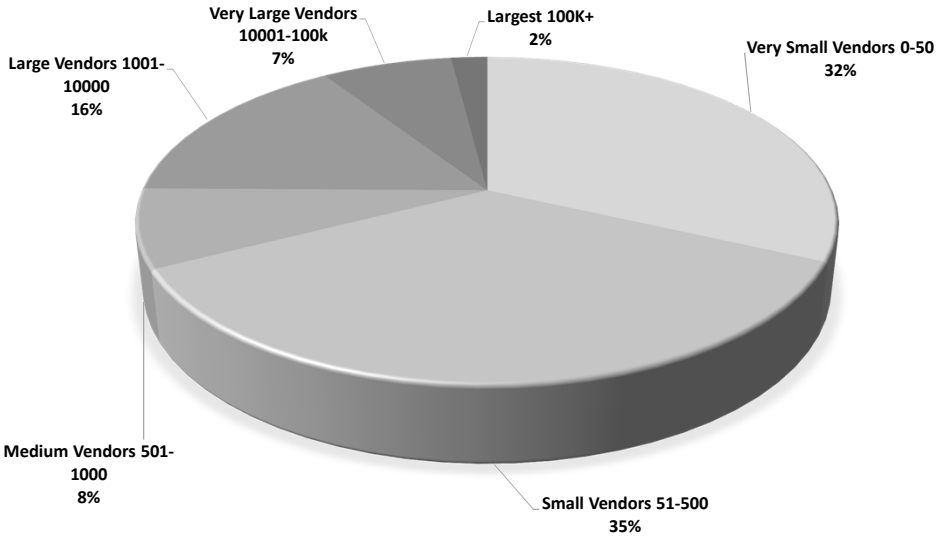


Efficient Vendor Risk Management Program



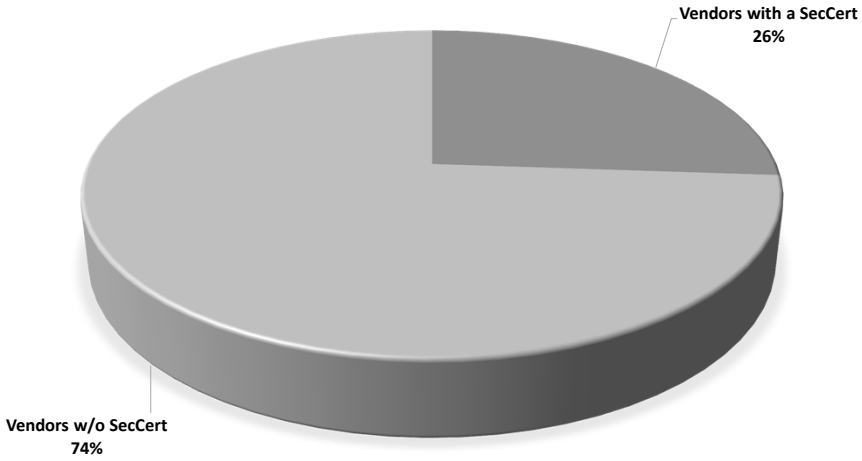
Vendor Profile: Distribution of Vendors by size (# of Employees)

- Hundreds of vendors with access to PHI
- Types of organizations vary greatly in terms of size, geographic scope, types of products and services
- Majority of vendors are very small/small companies with limited resources
- Very difficult to track down where data is stored and accessed as vendors sharing data with sub-contractors

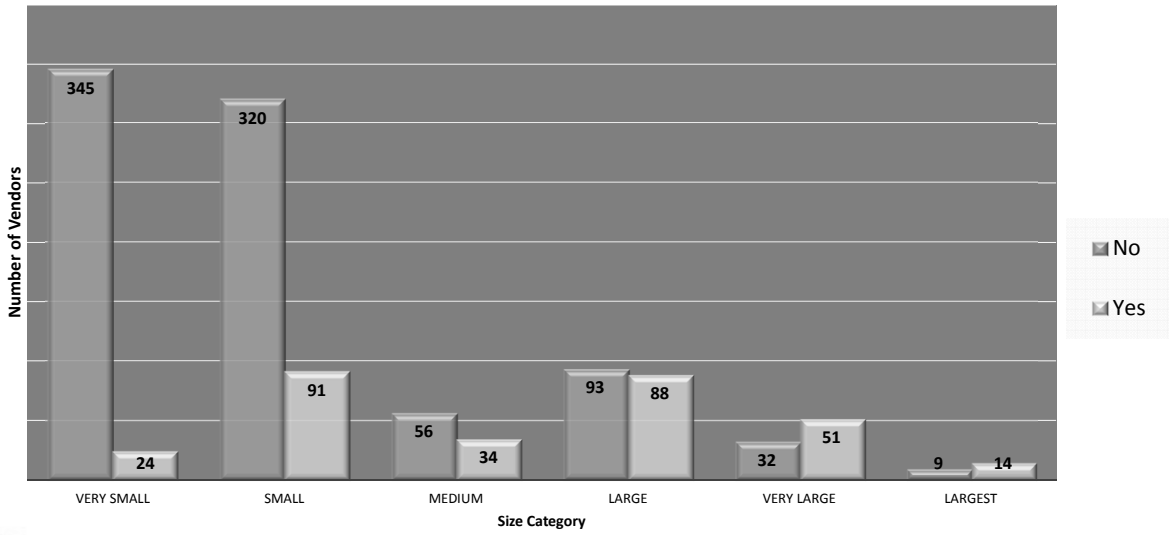


Vendor Profile: Distribution of Vendors with and without a Security Certification

- Only 26% of vendors have a Security Certification
  - ISO 27001 – 45%
  - SOC 2 Type 2 – 50%
  - SOC 3 – 20%
  - HITRUST – 10%
  - FEDRAMP – 30%
  - Others: PCI DSS, CSA Star, SOC1 Type 2, URAC

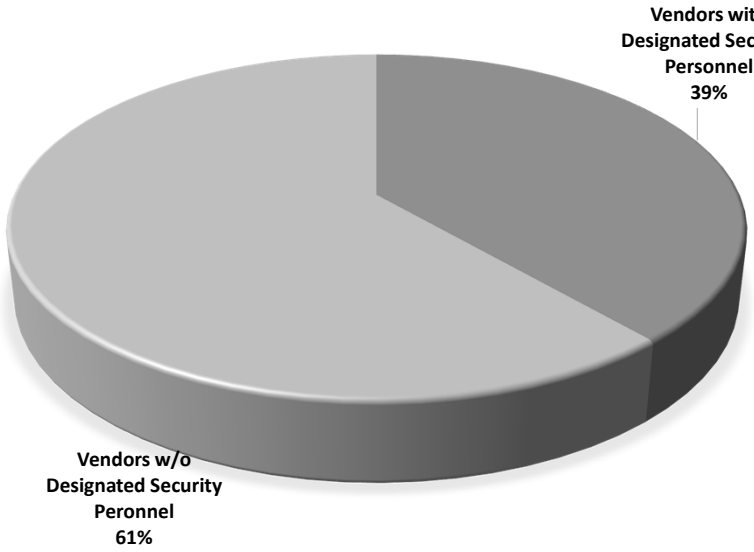


Vendor Profile: Distribution of Vendors with and without a Security Certification by vendor size (# of employees)

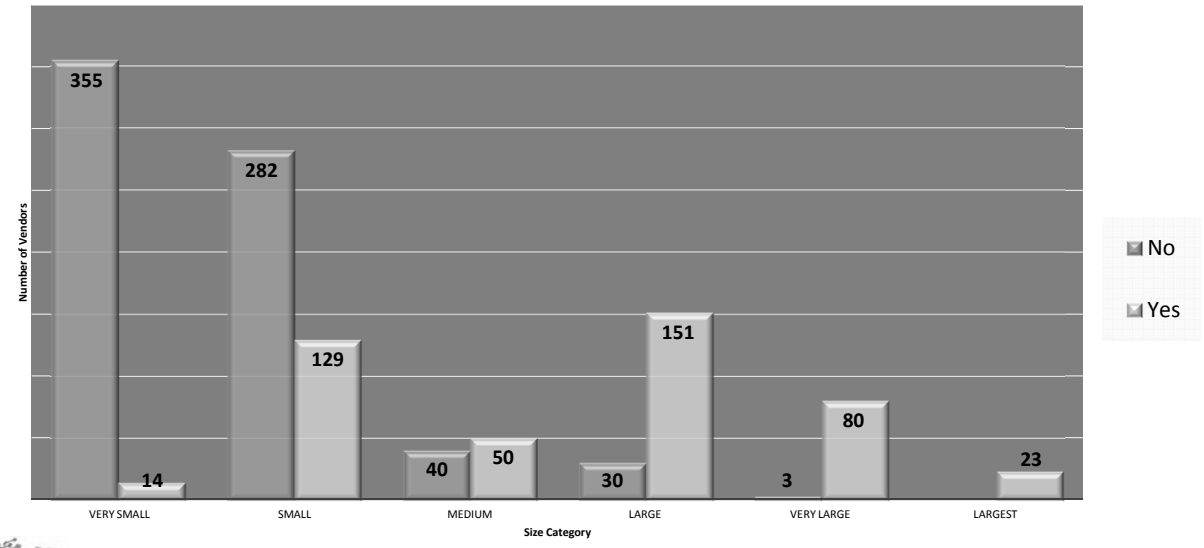


Vendor Profile: Distribution of Vendors with and without a Designated Security Team

- Only 39% of vendors have at least 1 designated security staff member
- Organizations without a security team will generally struggle to cooperate and provide adequate documentation during the risk assessment
- Very difficult to conduct an efficient risk assessment of an organization without appropriate vendor personnel

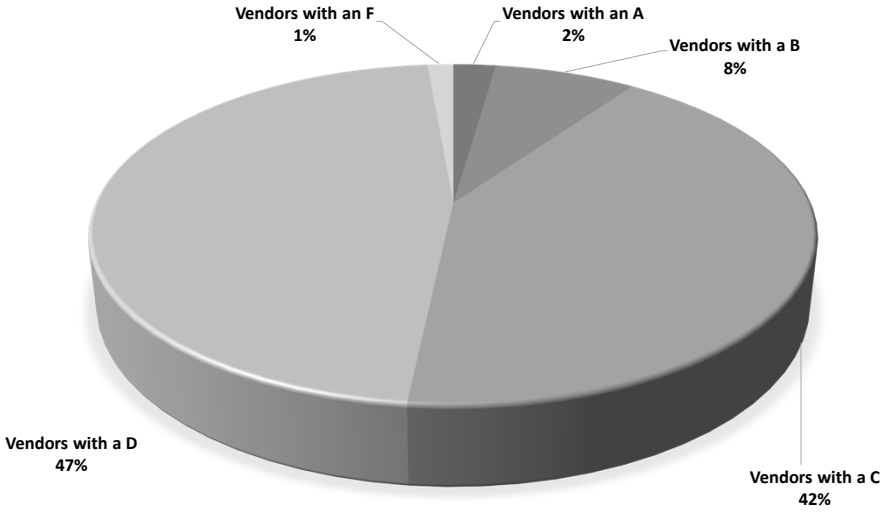


Vendor Profile: Distribution of Vendors with and without a Designated Security Team by Vendor Size (# of employees)

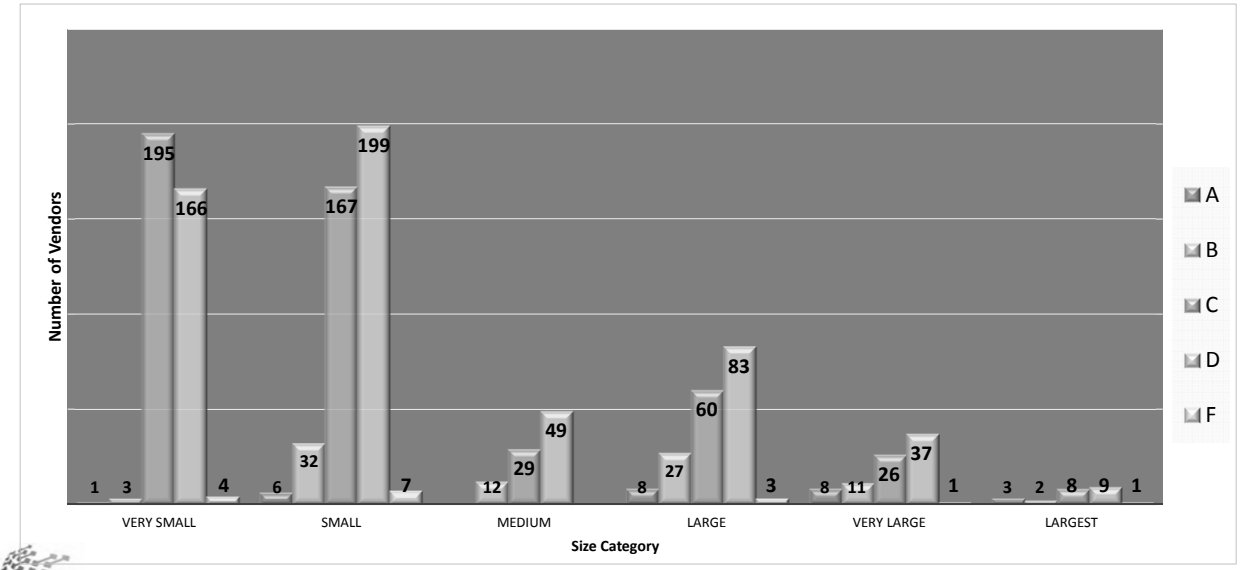


Vendor Profile: Distribution of Vendors based on the quality of their Security Practices

- A strong majority of vendors lack adequate Security Practices
- Organizations without strong security practices ultimately lead to investments at both the CE level as well as the BA level

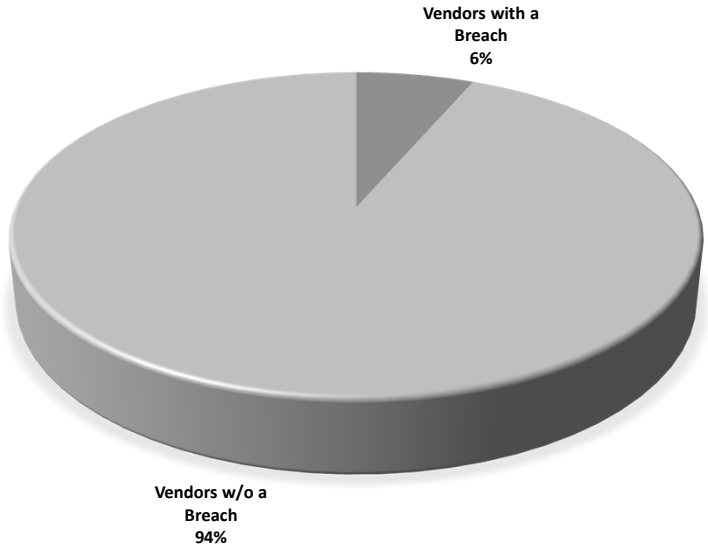


Vendor Profile: Distribution of Vendors based on the quality of their Security Practices by Vendor Size (# of employees)

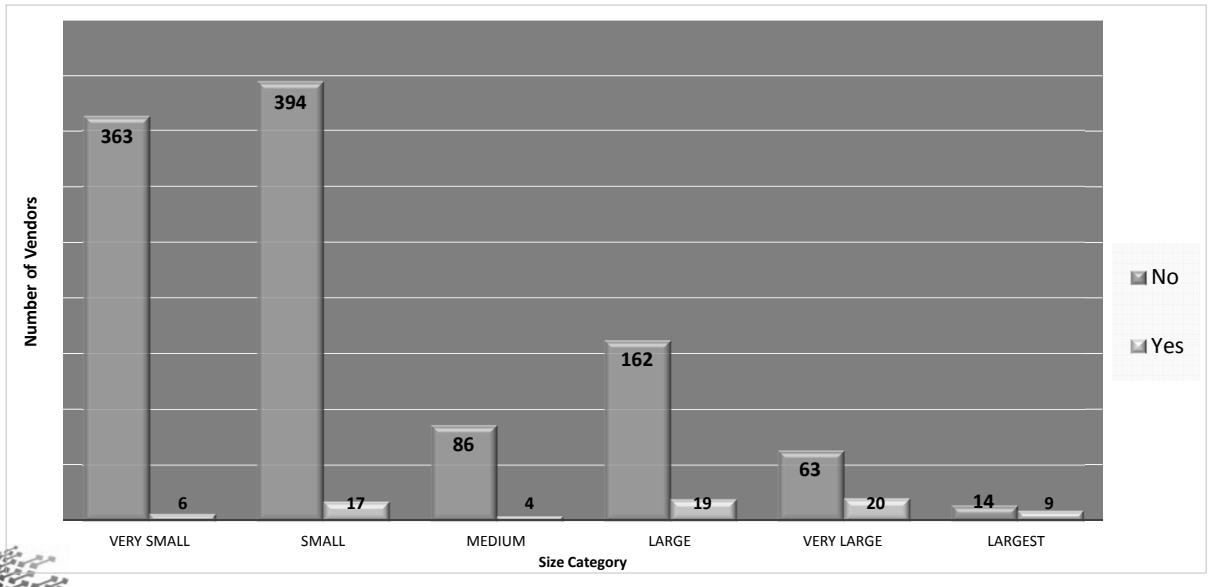


Vendor Profile: Vendors who have and have not had a reportable breach

- 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 by vendor size (# of employees)



Common Vendor Information Risk Management Program Weaknesses

Leadership communication

- Difficultly 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 CSA) standards, is the more comprehensive audit.
- **Type II** means tested, **Type I** 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)
- **PCI-DSS 3.0 standard:** Security of payment networks.
- **CSA Cloud Controls Matrix (CCM):** cloud security playbook
- **FedRAMP:** federal standard

 27

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**

 28

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

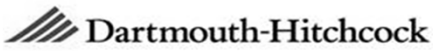
Care New England Health System (CNE): Third-party Breach

- 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.

http://www.healthcareitnews.com/news/care-new-england-pays-400000-hipaa-fine-lost-phi-business-associate-breach

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?



Peter N. Merrill

Peter N. Merrill
Director Information Systems
Peter.N.Merrill@Hitchcock.org
phone 603.650.6666

Danny Mimnaugh
CORL technologies
Client Engagement Associate
danny.mimnaugh@corltech.com