Business Associate Breaches – What You Don't Know May Cost You!

JANELLE BURNS, CORPORATE PRIVACY AND SECURITY OFFICER, BAPTIST MEMORIAL HEALTH CARE CORPORATION

CLIFF BAKER, CEO, CORL TECHNOLOGIES

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.

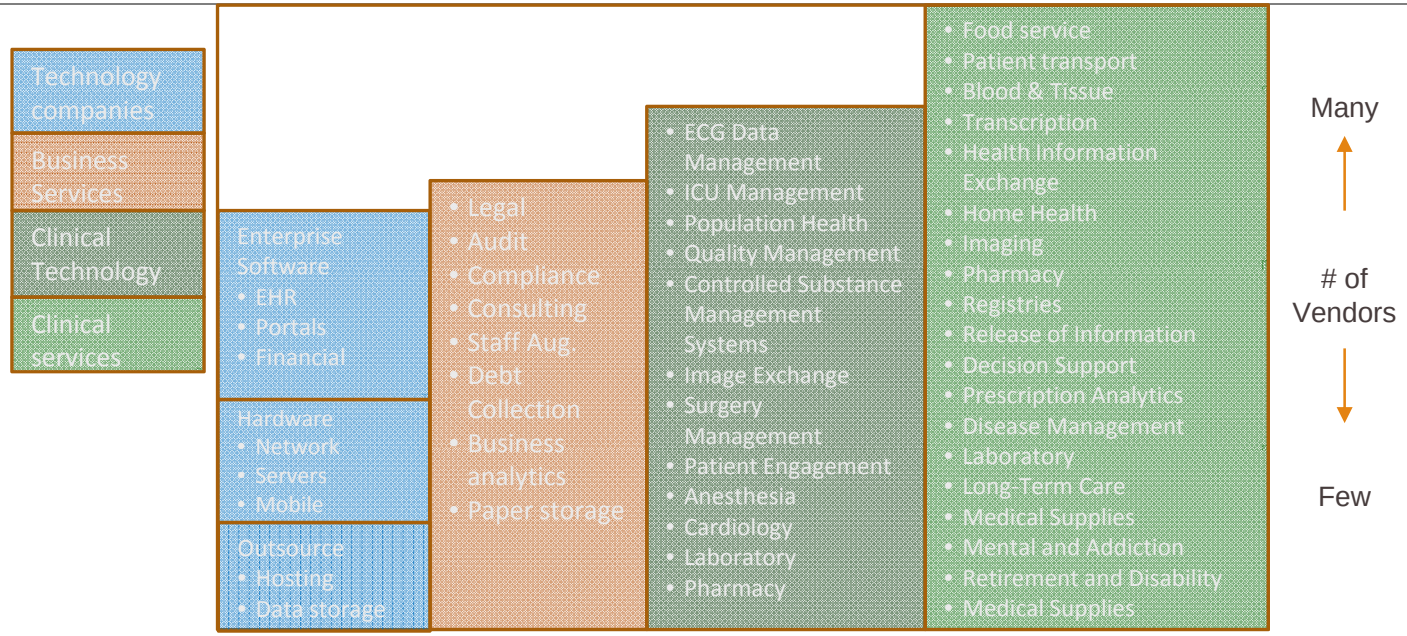
Reputational

- Headlines
- Undermines Patient Trust
- Undermines Employee Trust

Financial

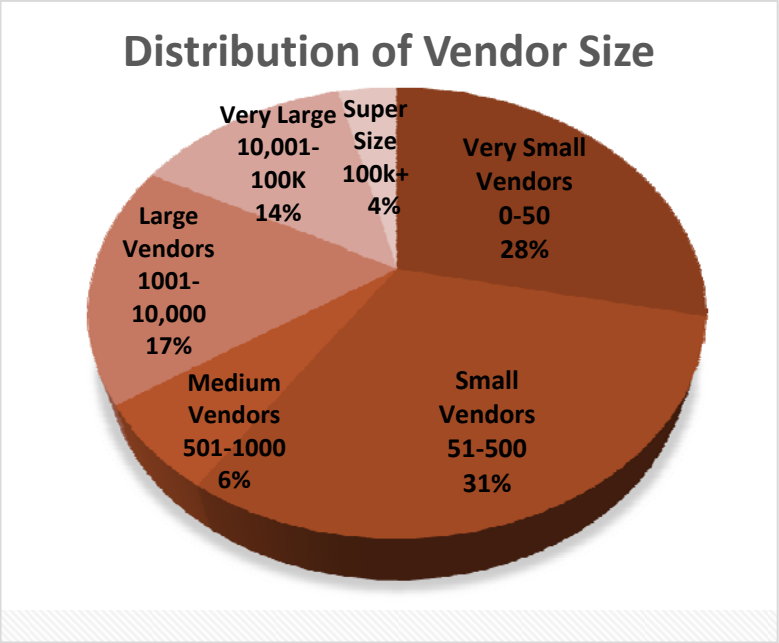
- Breach Notification is Expensive
  - Mailings
  - Call Centers
  - Credit Monitoring
  - Staff Time
- OCR Penalties for non compliance with HIPAA Rule (e.g., St. Elizabeth's Medical Center)
- Will Business Associate Reimburse?

Health Care System Vendor Profiles with Access to PHI



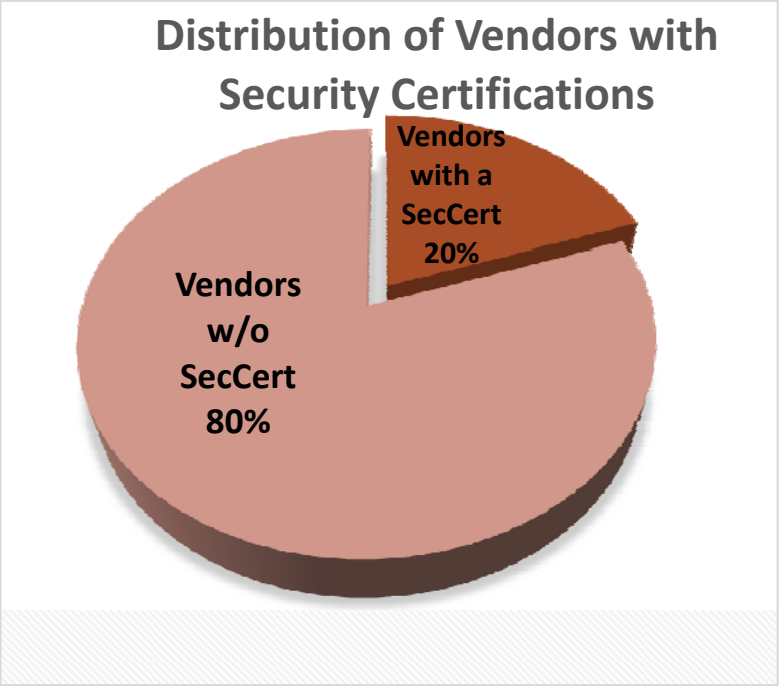
Vendor Portfolio – Typical Profile

- 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 small companies with limited resources
- Very difficult to track down where data is stored and accessed as vendors sharing data with sub-contractors

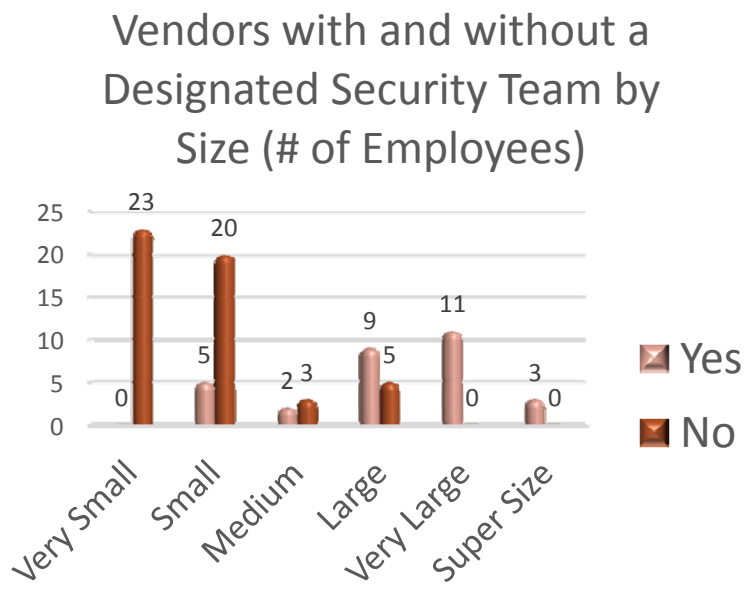


Request a Security Certification? – Think Again

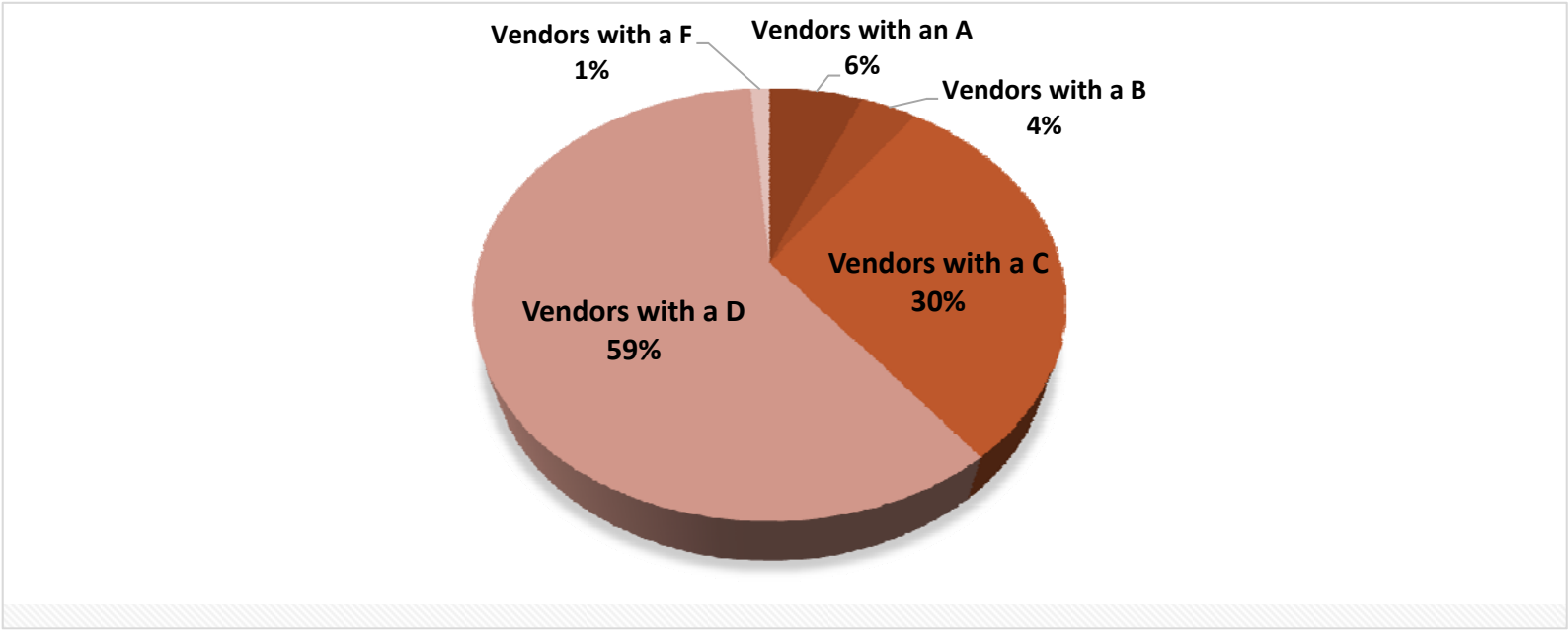
- Only 20% of vendors have a Security Certification
  - ISO 27001 – 45%
  - SOC 2 Type 2 – 50%
  - SOC 3 – 20%
  - HITRUST – 10%
  - FEDRAMP – 30%
  - Others: PCI DSS, CSA Star, SOC1 Type 2, URAC



Many Vendors Lack Resources



Exposure is significant



Implementing Vendor Security Program

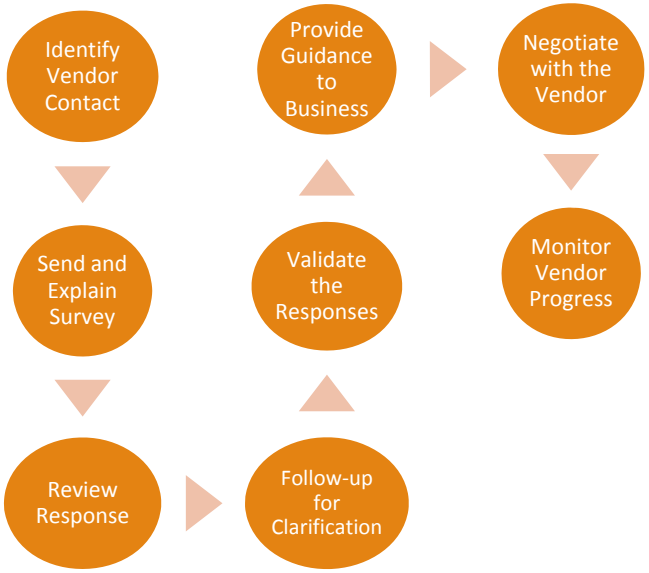
Why?

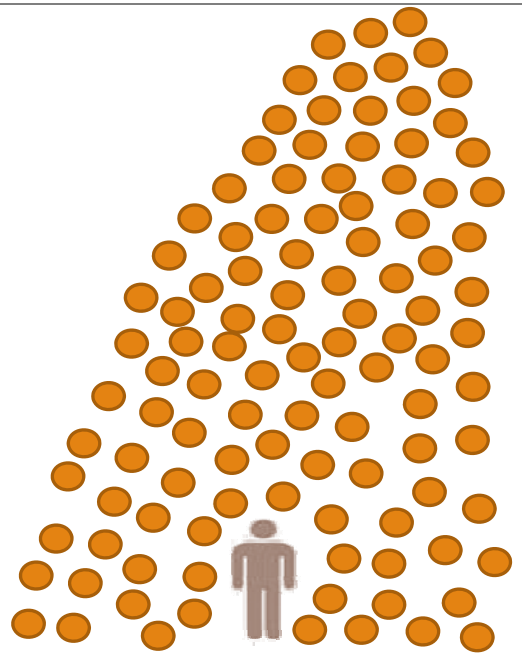
- More Vendors than ever have access to Covered Entities' data
- Vendors are supported by sub-contractors from around the globe
- Becoming more difficult to track where data is transmitted and maintained
- Need to control risk

How?

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

Be Smart About Process





Common Vendor Information Risk Management Program Weaknesses

Leadership communication

- Difficult to accurately communicate risk exposure to leadership
- Communication is inconsistent

Vendor communication and accountability

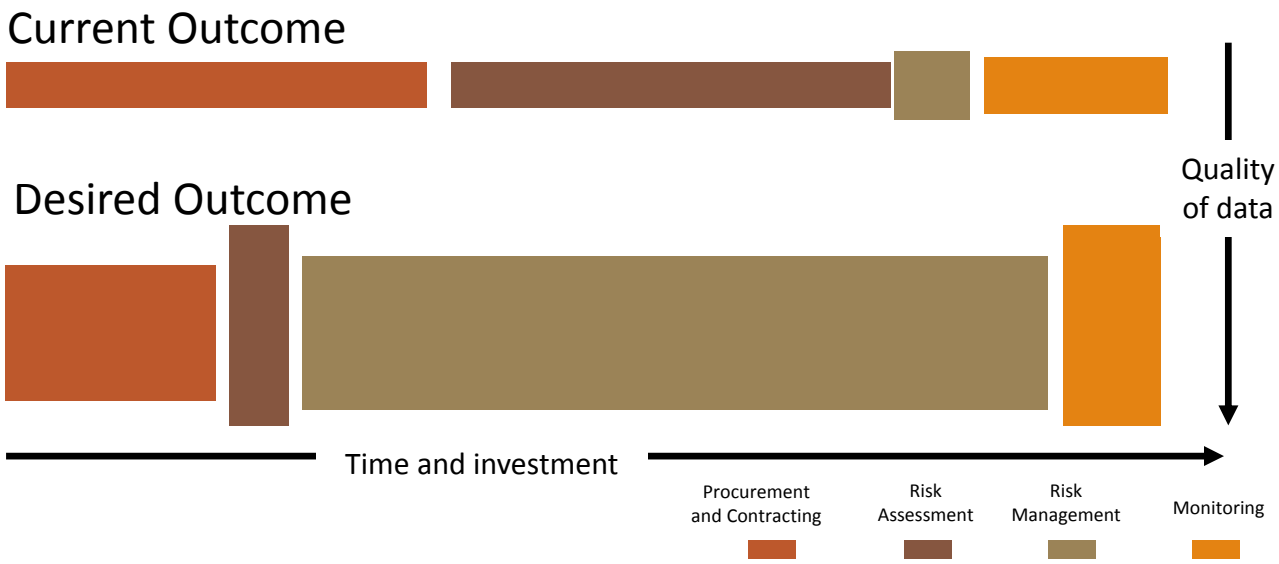
- Communication is sporadic, inconsistent and unclear
- Absence of linkage between vendor information management failures and contract management

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.

Focus on Risk Management



Collaborative Approach to Vendor Security

- Legal
- Procurement/Contracting
- IT
- Frequent Users (Finance, Revenue & Reimbursement, Quality)
  - ✓ Review existing contracts to search for frequent users

Focus on Assurance

- Vendor's responsibility is to provide Customer assurance that information is safeguarded
- 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

Layered Approach

- Initial Assessment of Vendor using security assessment questionnaire
- Review & Follow-up Questions
- Obtain assurance
- Choose to proceed with Vendor or terminate negotiations
- If proceeding, include risk reduction requirements in contract language
- Follow-up with Vendor to determine compliance with terms

Examples of Risk Reduction Terms

- Obtaining Independent Security Assessment - provide copy
- Developing a plan to address issues – provide copy
- Requiring adherence to a timeline
- Allowing for termination of contract for failure to meet timelines
- Indemnification

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!

Security Audits/Certification

- **SOC 2, Type II (SSAE 16),** 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

Contracting for Accountability

Provide a mechanism to ensure that the Vendor is held accountable for safeguarding information:

- **Warranty** to the **Specifications in the RFP and Documentation**
- **Termination Rights** (e.g., **Transition Termination, Service Level Termination Event**)
- Definition of **Direct Damages**
- Require a Right to **Audit** the Vendor (including fees charged, obligations performed and compliance with agreement)

Cloud Data: Ownership & Use

Definition of "Customer Data"

- *"means any content, materials, data and information that Customer or its Authorized Users enter into the Service"*
- *"means all data and/or information provided or submitted by or on behalf of Customer, all data and/or information stored, recorded, processed, created, derived or generated by the Vendor as a result of and/or as part of the Service, regardless of whether considered Confidential Information"*

Privacy

Agreement should cover:

- Requirement to maintain all legal technical, physical and procedural requirements of privacy and security laws (optimally) applicable to the **customer** as well as the vendor;
- Identity theft/national & state breach notice laws;
- Address user privacy and vendor's rights to retain and use data; and
- Notice of requests for data (e.g., subpoenas, government inquiries) and, where appropriate, opportunity to object.

Include a data breach provision that requires early cooperation, and try to make sure it's realistic (through testing, credits?)

- Immediate (no more than 5 business days) notification of a suspected or attempted security breach (work on this definition together until it satisfies your breach response team)
- Cooperation with the investigation, including providing access to auditors / forensic investigators (including if it's a credit card breach or your regulator needs access)
- Full, uncapped (if possible) liability for all costs arising from a security breach including the costs of providing notice, credit monitoring services, identity theft prevention or restoration services, fraud insurance, a call center for customer inquiries, forensic investigations and attorneys' fees. For credit card breaches, should also include costs relating to reissuance of credit cards, charges for operating expenses of the card brands, fraud recovery costs assessed by the card brands, and fines and penalties imposed by the card brands
- Customer control over content and timing of notifications

Data Access, Storage and Return

- Who can access my data?
- How and where is it stored?
- How do I get my data back and for how long?
- What happens if the cloud vendor goes out of business or files for bankruptcy?
- How do I ensure compliance with our data retention policy?

Exit Strategy in the Cloud

Termination

- Customer ability to terminate
- Vendor ability to suspend or interrupt services
- Escrow of cloud application
- Termination charges

Termination Assistance

- Scope of termination assistance
- Post-termination rights
- Price protection

Cyber Insurance - Top Ten Questions

1. Do you have concurrency/gaps between your cyber policy, your crime policies, and/or other policies?
2. Are your first-party loss sub-limits reasonable in light of your size/risk?
3. Does your policy cover third party vendor systems/negligence?
4. Does your policy cover all potential first-party losses, or is it "opt-in"?
5. Is there an "acts of foreign governments" exclusion?
6. Is there an exclusion for claims alleging violations of consumer protection laws?

Jonathan Neiditz, Kilpatrick Townsend & Stockton LLP

Cyber Insurance - Top Ten Questions

7. Is there an exclusion for “any malfunction or error in programming or error or omission in processing” or for losses arising from “mechanical failure,” “error in design,” or “gradual deterioration of a computer system”?

8. Is there an exclusion for an insured’s failure to follow minimum required practices, such as the failure of the insured to continuously implement the procedures and risk controls identified in the application for insurance and related materials?

9. To what extent does the policy cover regulatory risks?

10. Does the carrier mandate its choice of counsel, forensic experts, and crisis management firms?

Thank You

Janelle Burns
Corporate Privacy and Security Officer
Baptist Memorial Health Care Corporation
janelle.burns@bmhcc.org

Cliff Baker
CEO
CORL Technologies
cliff.baker@corltech.com