Assessing When a Vendor's Security Incident is a Breach

Session #85, February 12, 2019

Shari Lewison, CISO, University of Iowa Hospitals & Clinics

David Holtzman, VP Compliance Strategies, CynergisTek

Conflict of Interest

Shari Lewison, MBA, CISA, CRISC

Has no real or apparent conflicts of interest to report.

David Holtzman, JD, CIPP

Has no real or apparent conflicts of interest to report.

Agenda

- Breaches Caused by Security Incidents on the Rise
- Proactive Steps to Manage Business Associates
- What is a Reportable Breach: HIPAA & State Law Issues
- Questions to Ask When Vendor Reports an Incident
- Discuss Common Scenarios Involving Vendor Services

Learning Objectives

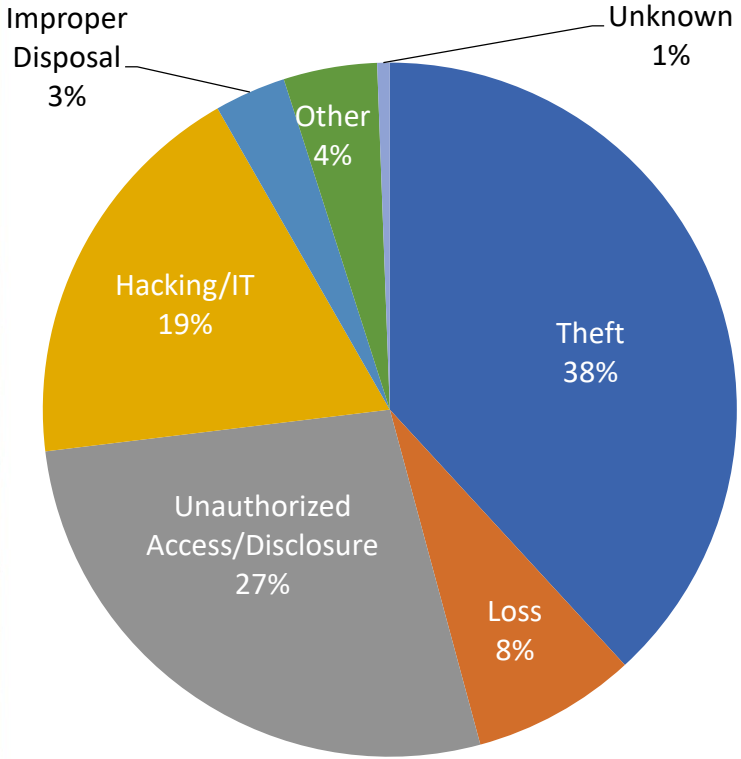
- Define how covered entities can determine if a reportable breach occurred with a business associate, and outline the roles privacy, compliance, security, in-house counsel, and outside consultants and advisers should play
- Identify the questions that covered entities need to ask their business associates to determine the root cause of a security incident, assess the extent of information needed to determine the risk of data compromise, and analyze how to view the vendor's self-assessment
- Interpret these questions through scenarios by applying HIPAA lens but also the patchwork of state health information privacy rules, for a complete picture on what is a reportable breach, who must be notified by whom, and when it must be reported

Attacks in Healthcare on the Rise

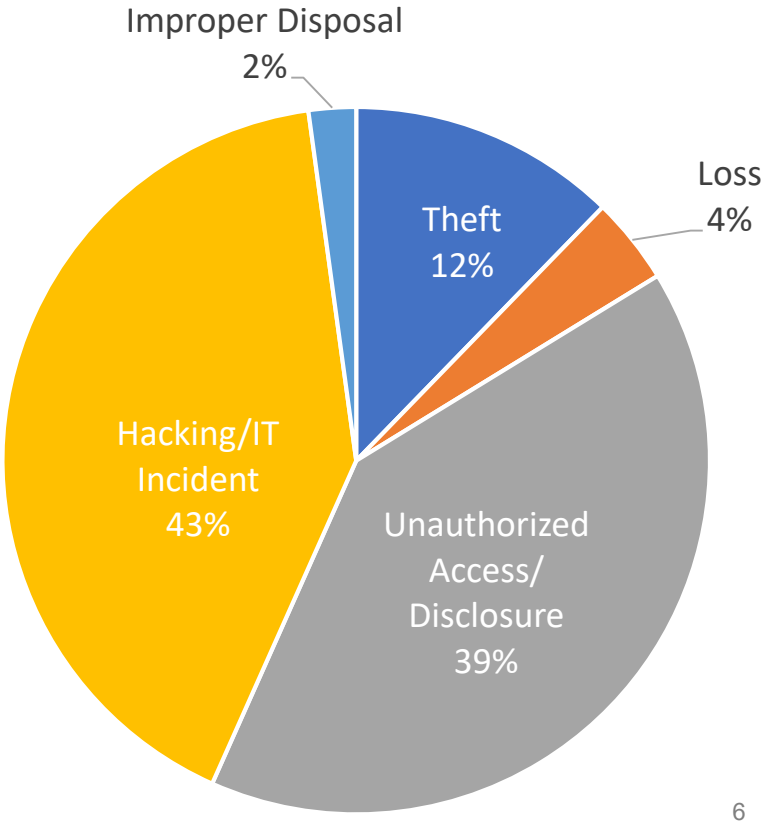
- Cybersecurity & hacking leading cause of healthcare breaches
- Increasing attacks since 2015
  - Highly valuable data (10x more than credit card number)
  - Lack of IT investment and thin margins
  - Highly connected systems with many participants
  - Push for interdependence and interconnectedness
  - Outdated software and devices
  - Vulnerability management issues

500+ Breaches Reported to OCR

September 23, 2009 through December 31, 2017



January 1, 2018 through December 31, 2018



Data source https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

#HIMSS19

Role of Business Associate

- 353 breaches affecting > 500 individuals reported to OCR in 2018 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- **71** of these large breaches reported to have involved a business associate https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- 2.65 million affected by cybersecurity incident striking 3rd party billing vendor largest of 2018 https://healthitsecurity.com/news/the-10-biggest-u.s.-healthcare-data-breaches-of-2018
- Largest OCR settlement to date $16 million, involving 79 million people was with a business associate (Anthem) https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html

Responsibilities Under HIPAA

- Privacy Rule – Reasonable safeguards to protect the privacy of PHI
- Security Rule – Risk Analysis and Risk Management Plan
- Under both – Must obtain satisfactory assurances that business associate "will appropriately safeguard" PHI in the form of a business associate agreement
- If covered entity knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligations, the covered entity must take steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the contract, if feasible
- And, as of HITECH, business associates have direct liability for CMPs for certain violations of the Privacy Rule and all of the Security Rule

Responsibility to Manage BA

- OCR Guidance on Cloud Computing
- "A covered entity (or business associate) that engages a CSP should understand the cloud computing environment and solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate BAAs."
  - And, while Guidance specifically states that CSPs are not required under HIPAA to provide documentation, or allow auditing, of their security practices, it notes:
    - Customers may require a CSP through the business associate agreement, service level agreement or other documentation to provide documentation of safeguards or audits, based on the customer's own risk analysis and risk management or other compliance activities

https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Is Your BA Prepared?

"Despite the requirements of HIPAA, not only do a large percentage of covered entities believe they will not be notified of security breaches or cyberattacks by their business associates, they also think it is difficult to manage security incidents involving business associates, and impossible to determine if data safeguards and security policies and procedures at their business associates are adequate to respond effectively to a data breach."

OCR Cyber-Awareness Monthly Update – May 3, 2016

What Can You Do Proactively?

- Identify who is and who is not a business associate
- Know your business associates!
  - Know:
    - Their names
    - Their mailing address and where they operate
    - Two points of contact for each
    - URL of their websites
    - Their services
    - The PHI involved and how it is used/disclosed

What Can You Do Proactively?

- Conduct initial and ongoing due diligence
  - Audits and questionnaires
    - Risk introduced by the vendor
    - Type and volume of PHI
    - Criticality of vendor's functions
  - Require
    - Written privacy and security policies
    - Risk analysis and risk mitigation plan
    - An incident response plan
    - Business continuity and disaster recovery plan
    - Training and sanction policy
  - Know
    - How they address risks of subcontractors
    - Whether they use offshore subcontractors

What Can You Do Proactively?

- Enter into business associate agreements that:
  - Incorporate the right to perform ongoing due diligence
  - Require notification of all impermissible uses and disclosure of PHI, including security incidents and breaches of unsecured PHI
    - Consider timing – if breach, without undue delay but not more than 60 days from discovery
    - Does that timing still seem appropriate?
  - Address
    - Responsibility for determining breach (see next slide)
    - Information to be reported – and how and when and to whom
    - Duty to report to affected individuals and OCR (and state officials)
    - Right to review and approve notifications
    - Mitigation
    - Costs and indemnification
  - Require cyber insurance
  - Permit termination if terms violated

Is it a Breach?

- HIPAA – Acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of PHI
  - There are few exceptions
  - Otherwise, presumed breach unless demonstrate a low probability that the PHI has been compromised based on a risk assessment
    - Nature & extent of PHI involved
    - PHI actually acquired or viewed
    - Unauthorized person who used PHI or to whom it was disclosed
    - Extent of mitigation

Assessing for Breach Notification

- Understand what HIPAA Requires
  - The clock starts when the event is discovered or notified received from business associate
  - Notification must occur without undue delay
    - Must be completed within 60 days
- Your business associate must notify the you of a breach without undue delay but not more than 60 days from discovery
  - Your BAA agreement may have a shorter timeframe
- If you are a business associate you must notify the covered entity of a breach without undue delay but not more than 60 days from discovery
  - Your BAA agreement may have a shorter timeframe

Breach Notification

- HIPAA is not the only potentially applicable data protection and notification requirement
- There is a patchwork of state breach notification laws that may apply
  - Reporting deadlines may differ
  - Content of notice may differ
  - Notice to state regulatory bodies may be necessary

Patchwork of State Laws

- Inventory who is contributing to your data and where they reside
- Get advice on where your organization is “doing business”
- Understand what state law requires
  - Your state law may differ in:
    - Defining what data is protected
    - Process for assessing if breach notification is required
    - Timelines from federal law
  - You may have obligations in other states
    - Because you are a multi-state entity
    - Because you have data of residents from other states

Your Vendor Reports an Incident

- Activate your incident response plan
- Key action step: review the vendor agreement
- Identify documentation needed from 3rd party to assess extent of data compromise
  - Obtain and review forensic reports & inventory of data
- Who to involve at early stage of investigation
  - Legal counsel
  - Compliance team
  - Impacted business owner
  - Impacted business partners such as affiliated health care providers

Your Vendor Reports an Incident

- Require preservation of evidence for forensic analysis, if necessary
- Identify needed documentation, if any, to conduct a root cause analysis
  - Description of what happened, including the date of the incident and the date of discovery, types of unsecured PHI involved, and investigative steps
  - Inventory of data
  - Forensic reports
- Determine whether law enforcement should be notified
- Report cyber threats to federal and information-sharing and analysis organizations (NCCIC, NH-ISAC)

Your Vendor Reports an Incident

- Determine HIPAA and state reporting obligations, if any
  - If reporting, determine if PR firm necessary and potentially establish call center
  - Document assessment, even if no reporting
- Log improper disclosures, if necessary for accounting purposes
- Re-evaluation relationship with vendor
- Take stock of lessons learned from incident

Thank You!

e complete your online session evaluation!

Questions?

Shari Lewison
CISO
University of Iowa Hospitals & Clinics
Shari-lewison@uiowa.edu

David Holtzman
Executive Advisor
CynergisTek
David.holtzman@cynergistek.com
Follow me @HITprivacy