Data Breaches: Mitigating Enterprise Risk

Health Care Compliance Association

Alaska Regional Conference
February 23-24, 2017

Rebecca L. Williams, RN, JD
Chair, Health Information Practice
Davis Wright Tremaine LLP
beckywilliams@dwt.com
206.757.8171

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

1

Overview

Trends … evolving threats

Ransomware

Security Incident Cycle to manage the risk

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

2

Breaking News

January 13, 2017

Number of U.S. healthcare data breaches almost doubles in 2016

2016 averaged 1 healthcare data breach per day

National

Health insurance data breach affects thousands in Delaware

Criminal hackers now target hospitals, police stations and schools

Presence Health agrees to $475,000 settlement over data breach report

Data breach exposes info for 400,000 Community Health Plan members

Banner Health Breach Affects 3.7 Million

Officials: Foreign Government May Have Breached Health Data

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

3

Trends in data security

Trends

- Data breaches
- Denial of service
- Ransomware
- Malware, malware, malware …
- Attacks on all sectors and all systems

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

4

Ransomware

- OCR issued guidance concerning ransomware
- Malware that encrypts an organization's data with cyber criminals then demanding the organization pay a ransom to regain access; also can result in loss of data
- Whether ransomware constitutes a breach is a facts and circumstances analysis
  - Guidance suggests that encryption of ePHI, could be an impermissible disclosure, subject to HIPAA risk assessment
- Often results from social engineering (clicking on the wrong link)

Ransomware

- Risk analysis to include ransomware
- Implement security safeguards
- Information security awareness
- Routinely back up ePHI
- Test your monitoring and response processes
- Test your disaster recovery processes
- Consider table-top exercises, with ransomware as a potential scenario
- Cyber insurance with cyber extortion coverage

6

Why should you be concerned?

- State Requirements
- Federal Requirements
  - FTC and OCR
- Industry Regulations
  - PCI DSS
- Reputation

Class Actions/Derivative Suits

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

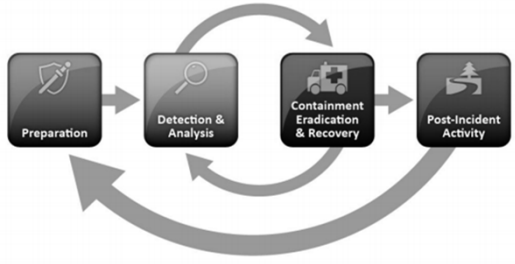
Increase security, decrease cost

Factors that decrease the cost of a data breach	Factors that increase the cost of a data breach
▪ Strong security posture	▪ Lost or stolen devices
▪ Incident response planning	▪ Third party involvement
▪ Business continuity management	▪ Notification before investigation completed
▪ CISO appointment	

Source: 2014 Cost of Data Breach Study: Global Analysis
Sponsored by IBM, Conducted by Ponemon Institute LLC

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Information security incident cycle



Computer Security Incident Handling Guide, NIST SP 800-61 Rev. 2

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The most important step … preparation … prepare and you will increase security

Conduct inventory of data

- What type of information is processed, transmitted or stored?
  - Personally identifiable information (PII)
  - Protected health information (PHI)
  - Payment Card Industry (PCI) information
  - Corporate confidential information
  - Employee information
- Where is the information stored?
  - Servers/devices onsite?
  - Services in the cloud?
  - Laptops, mobile phones, portable media?
  - Record storage vendors?
  - Paper records?
- How is the information protected?
  - Is data encrypted?
  - Who has access?
- How long is the information retained?
  - Is there a data retention policy?
  - How is the information destroyed?

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

10

Risk analysis and risk management

- Conduct and update risk analysis
  - Accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI
  - Revisit regularly and as changes occur
  - Make sure it is a HIPAA risk analysis
- Risk management
  - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- Heart and soul of HIPAA security

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

11

Implement best practices

- Conduct inventory of all hardware and software
- Use current version of operating systems
- Automate security patching
- Enable intrusion detection and prevention systems
- Segment network
- Control access based on need to know
- Use multi-factor authentication
- Eliminate unnecessary data and processes
- Protect data
- Monitor endpoints
- Conduct due diligence on all third party service providers
- Conduct vulnerability testing
- Encrypt, encrypt, encrypt

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

12

Develop incident response plan

Preparation

Purpose
- Improve information security
- Prepare efficient, effective response to security incident
  - Systematic
  - Minimal loss or theft
  - Minimal disruption
  - Legally compliant
  - Preserve reputation
- Collect evidence of attack
- Coordinate remediation
- Recover and restore information system

Key Team Members
- Compliance Lead
- Privacy Officer
- CISO/IT Lead
- Legal/Outside counsel
- Financial management
- Risk management
- Human resources
- Breach response vendors
  - Outside counsel
  - Forensics
  - Notification/Call center
  - Credit monitoring
  - Identity restoration
  - Public relations/crisis communications

Test incident response plan with "tabletop" exercises

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

13

Establish incident response team

Preparation

Outside Counsel
- Project management skill
- Crisis management skill
- Breach response experience
  - Knowledge of breach notification requirements
  - Knowledge of privacy and security law
- Existing relationship
  - Engagement in place
  - Trusted partner
  - Knowledge of business
- **Attorney/client privilege**

Breach Response Vendors
- MSAs in place
  - Fewer decisions during digital crisis
  - Reduced costs
  - Instant response
- Existing relationship
  - Knowledge of network
  - Knowledge of vulnerability test data

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

14

Cyber insurance

Preparation

- Risk cannot be completely mitigated by technology …
- Do you have cyber insurance?
- What does your policy cover?
  - First party losses and costs?
  - Third party costs?
  - Remediation costs?
  - Fines and penalties?
  - Risk management services?
- Does your policy allow you to choose
  - Outside counsel?
  - Breach responders?
- Do the limits of liability match your realistic exposure?


BANKINFOSECURITY

Buying Cyber-Insurance: 5 Tips

How to Make Sure Policy Meets Organization's Needs

2. Selecting Vendors, Legal Counsel

5. A Knowledgeable Broker

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

15

Anatomy of a breach: the initial response

- Conduct initial assessment
  - CISO/IT Lead/Privacy Officer/Compliance Officer
  - If possible breach – implement incident response plan
- Notify insurer
  - Confirm approval of all breach response vendors
- Engage outside counsel
- Engage digital forensics team through outside counsel (if applicable)
- Implement "litigation hold"
- Document as you go
- Begin to assess whether additional breach response vendors may be necessary
  - Public relations/crisis communications
  - Notification
  - Call center
  - Remediation services

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

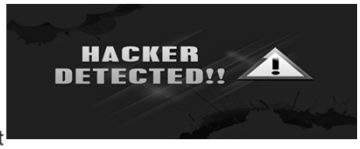
Containment/eradication/recovery

- Assess, contain, eradicate, & remediate
  - Identify target of breach, e.g., PII, PHI, IP, PCI data, financial account information, etc.
  - Determine whether data loss occurred; if so, whether it has stopped
  - Eliminate threat
  - Determine extent of loss
  - May involve forensic firm
- Preserve and secure evidence: remember log files
- Determine whether to notify law enforcement
- Recovery – return affected systems to normal operations

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

HIPAA breach notification

- Upon the **discovery**
- Of a **breach** of
- **Unsecured**
- **Protected Health Information**
- C**overed Entities** and **business associates** have **notification** obligations



Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

HIPAA breach analysis

Step 1 – Is it an impermissible use or disclosure of PHI under Privacy Rule?

Step 2 – Is the PHI secured through appropriate destruction or encryption?

Step 3 – Does a statutory exception apply?

- Unintentional use, good faith, no further impermissible use/disclosure
- Inadvertent disclosure within organization (or OHCA), recipient had authorized access, no further impermissible use/disclosure
- Good faith belief that unauthorized recipient could not retain information

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

19

Presumption of breach

Step 4 - Presumption of breach

Step 5 – Can overcome presumption by demonstrating a *low probability of compromise* based on documented breach risk assessment of at least:

- Nature of PHI (e.g., identifiability, sensitivity)
- Unauthorized recipient (e.g., subject to confidentiality requirements?)
- Whether PHI was actually acquired or viewed
- The extent that risk has been mitigated

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

20

HIPAA notification and timing

- Individuals: without unreasonable delay & no later than 60 calendar days after discovery
- OCR (through OCR website):
  - 500 or more – contemporaneous with (actually immediately after) notice to individuals and media
  - Fewer than 500 – within 60 days of end of calendar year.
  - **For small breaches in 2016: March 1,2017**
- Media: without unreasonable delay & no later than 60 calendar days after discovery (if required)
- Subject to law enforcement delay

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

21

Discovery

- First day known, or, by exercising reasonable diligence would have been known
- Deemed to know when any workforce member or agent (except the bad actor) knew or should have known
- Business associate = agent (e.g., covered entity can control manner in which business associate performs contract) → covered entity timing starts when business associate discovers breach
- Business associate ≠ agent → covered entity timing starts when receives notification or otherwise becomes aware of breach

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

HIPAA notification content

- Covered entity required content:
  - Brief description of what happened (dates of breach and discovery, if known)
  - Description of types of unsecured PHI involved
  - Any steps individuals should take to protect themselves from potential harm
  - Brief description of what is being done to investigate the breach, mitigate harm to individuals, and protect against any further breaches
  - Contact procedures (e.g., toll-free phone number or e-mail address)
- Business associate required content to the extent possible:
  - Identification of each individual
  - Same content as covered entities
- May include state requirements (except Massachusetts)

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Other obligations to notify

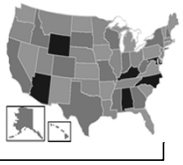
- Business associate reporting requirements
  - Reporting of impermissible uses and disclosures – required by contract
  - Reporting of security incidents – required by contract
  - Reporting of breaches of unsecured PHI – direct and contract requirement
- Other contractual requirements

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

State law notification

Post-Incident Activity

- 47 state data breach notification statutes (plus Guam, Puerto Rico, Washington D.C., and the Virgin Islands)
- Notification obligation determined by residence of consumer, not location of business
- Notification may include:
  - Residents of the State
  - State regulatory officials, such as Attorney General
  - Credit reporting agencies



Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

State law notification

- Does state law require breach notification?
  - Limited to computerized data?
  - Definition of "personal information"?
  - Definition of breach
  - Timing requirements?
    - Sooner than HIPAA?
    - Advance notification?
  - Risk of a harm threshold?
  - Content of notification?
  - Number of individuals/residents involved?
  - For information on state breach laws, visit: http://www.dwt.com/statedatabreachstatutes/

Alaska Personal Information Protection Act

- Applicability: Breach notification requirements apply to persons doing business, governmental agencies, or persons with more than 10 employees, that own, license, or maintain covered information (Some exceptions) A1
- Notification: for unauthorized acquisition -- or reasonable belief -- that compromises security, confidentiality, or integrity of covered information (Some exceptions)
- Covered information: first name/ initial and last name + at least:
  - Social Security number
  - Driver's license or State identification card number
  - Financial account, credit or debit card number in combination with any required security of access code, PIN, or password permitting access
  - Passwords, PINS, or other access for financial accounts

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Slide 27

A1 Under the terms of the statute, the covered person does not have to be doing business in Alaska to fall within the requirements of the statues. All that is required is that the covered entity have personal information about an Alaska resident.
Author, 2/14/2017

Alaska Personal Information Protection Act

- Harm Threshold: Notification not required IF
  - After appropriate investigation, covered entity determines that there is not a reasonable likelihood that harm to consumer has resulted or will result
  - Any determination that the harm threshold is not reached, written notification must be provided to the Alaska AG
- Notifications:
  - Residents
  - Owner of the data
  - Attorney General (depending on harm threshold determination)
  - Consumer Reporting Agencies (if more than 1,000 residents are notified)
  - Substitute notice

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Alaska Personal Information Protection Act

- Timing:
  - Most expeditious time possible and without unreasonable delay
  - Law enforcement delay
- Method: By written notice to most recent postal address, or electronic notice if it is the primary method of communication with resident or is consistent with E-SIGN

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Notification and wrap-up

- If breach notification is required
  - Determine whether remediation services will be provided e.g., identity theft protection
  - Draft notifications, talking points, and frequently asked questions
  - Send/submit notifications (e.g., individuals, OCR, media, state regulators, consumer reporting agencies, etc)
  - Identify any advanced notifications
- Documentation
  - Security incident
  - Privacy event
  - Breach, including
    - LoProCo risk assessment
    - Timing (consider a chronology to demonstrate "without unreasonable delay")
    - Appropriate notification
  - Log disclosure for accounting of disclosure
  - Other, including corrective action

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Notification and wrap-up

- Prepare for post-incident regulatory response
  - Verify documentation is complete and accurate
  - Revisit risk analysis and risk management
  - Corrective action plan – carry through
- Conduct post-incident debrief
  - What can be learned from the breach?
  - Circle back to preparation

Questions?

24/7 BREACH RESPONSE TEAM
844-GoToDWT
(844-468-6398)

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Questions?

Becky Williams, RN, JD, is a nationally recognized authority on HIPAA, health information, privacy, and data breach notification. She is a partner of the law firm Davis Wright Tremaine, LLP where she is Co-Chair of the Health Information Practice. Ms. Williams has been named one of the "Best Lawyers in America" in health law by Woodward/White. She also is a registered nurse with hands-on experience in hospital and other health care environments.

Rebecca L. Williams, RN, JD
Davis Wright Tremaine LLP
beckywilliams@dwt.com
206.757.8171

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER