Data Breach Response: How to Respond to a Data Breach

December 9, 2015

Presented by

Paige M. Boshell

John E. Goodman

Amy S. Leopard

Elena A. Lovoy

Michael R. Pennington

Privacy and Information Security Team

- 16 attorneys
- 6 practice groups
  - SMEs in Banking, Government Contracts, Healthcare, Litigation, and IP
- 7 webinars in 2015
  - Let us hear from you

babc

Introduction

- Real time data breach tabletop
- Coordination of internal and external teams
- Execution of breach response and recovery plan
- Attorney-client privilege and compliance documentation
- Notice/law enforcement
- Litigation hold and voluntary relief
- Civil claims/ insurance issues
- Resiliency

babc

Data Breach Scenario – Large Health System

- Large, growing system
  - 12 Hospitals, 200+ locations, 25,000+ employees
  - History of small incidents with no financial harm, lost/stolen encrypted laptops
- Front desk employee at stand-alone breast cancer treatment center accused of stealing cash (from co-pays)
  - Matter referred to HR and Internal Audit for investigation
  - Internal Audit confirmed theft ($)
  - Employee terminated without exit interview

babc

Facts Known at Time of Referral to CPO (cont'd)

- Internal audit further noted employee had emailed credit card, SSN, and health insurance information on 200 individuals to a 3rd party and later reported concerns to Chief Privacy Officer
  - Time to date since determination of possible breach – over 1 month – no other investigation done during that time to determine extent of breach
  - Legal and CPO contacted outside counsel

- Forensics and IT later determine that employee also accessed insecure web sites and downloaded malware onto her PC
  - Early indication that network resources may have been compromised

babc

Assemble Internal and External Teams

- Collect policies and plans
  - Data breach response plan
  - Related IT, HR, Marketing, Legal and other policies and procedures
- Review policies and plans
  - Determine requirements
  - Implement planning
  - Decide when deviation is appropriate

babc

Assemble Internal and External Teams (cont'd)

- Internal team
  - GC, privacy officer, IT/IS, HR, Legal, PR, Customer service, senior management rep
    - Need centralized function and single communications channel and decision maker
    - Data breach response plan should assign specified roles and responsibilities
- External team
  - Legal, forensic and other investigators, PR, vendor representatives, and law enforcement
    - Need defined functions and centralized communications and accountability
    - All report to single, internal decision maker
- Coordination and centralization of message

babc

Implementation of Response Program – Coordination of Investigation and Response

Scoping - Determine scope of incident/compromise –

- **What was compromised? - Determine known/unknown data losses.**
  - *Scope of access* – Patient records at breast cancer treatment center or within company at large? Employee records? Payment card records?
  - *Type of information accessed or possibly accessed* – Insurance policy numbers, medical diagnosis, test results, and other records, SSNs, credit/debt card numbers, doctor/employee information, etc.
  - *Paper or digital trail* – What did employee do with data? Copies of records found in locker, e-mailed copies of records to her personal e-mail address or address of third party, etc.?
- **What do we have to work with and what do we need to do to know more?**
  - Internal audit review was performed, at direction of HR, to determine whether there were grounds to terminate employee. Does it tell us all we need to know about what may have happened?
  - Identify additional work need to develop inventory of affected data (and individuals). Who needs to conduct this forensic review?
  - Determine what other information relevant to incident may be available from security system data, logs, entry records, e-mail records, etc.
  - Scope and initiate additional investigation to ascertain nature and extent of breach.

babc

Implementation of Response Program (cont'd)

- **Who was involved from inside/outside the company?** - Determine involvement of employees, third party providers, vendors, consultants, and others. Interview relevant employees and others involved in or with knowledge of incident. Gather relevant vendor, etc. contracts.
- **Was data in "safe mode"?** - Assess whether compromised data was encrypted or password protected.
- **Are we insured?**
- **Are we receiving complaints about breach? Need to start tracking.**
- **Was problem due to a systemic or isolated issue?**

babc

Implementation of Response Program (cont'd)

- Determine applicable legal requirements – HIPAA, GLBA, PCI, state laws?
- Determine applicable contractual requirements.
- Determine whether document hold is necessary or appropriate.

babc

Implementation of Response Program (cont'd)

- *You don't know what you don't know* - Privacy response team leader/team members must know the issues and the business to scope the parameters of this "deeper dive" into incident.
- *Anticipate the worst-case scenario.*
- *Do not have luxury of time. (Remember 1 month has elapsed from time internal audit discovered possible issues.)*
- *Building foundation that will determine who, what, when, where, and how company responds.*
- *Do not have luxury of static environment.*

babc

Implementation of Response Program (cont'd)

Pro-active Measures - Take *immediate* measures to prevent further compromise and unauthorized access, such as:

- Checking network security measures and closing off network intrusion.
- Activating enhanced system logging and monitoring.
- Evaluating whether any global or local password changes, modified access privileges, or other enhanced security measures are immediately necessary and implement any such needed changes.
- Ensuring that any current or former employees implicated in breach no longer have access privileges.
- Reviewing access privileges for contractors, vendors, and other third parties.
- Involving law enforcement.

Remember – What did you tell customers/patients in your privacy notices?

babc

Implementation of Response Program – Risk Assessment

Risk Assessment - Conduct initial risk assessment to assess whether:

- Misuse of data has occurred or is reasonably likely/unlikely; and
- What risks/harms could occur if data was misused.

State Laws - Evaluate "risk of harm" under applicable state data breach laws.

babc

Consider Regulatory Overlay in Response

HIPAA/HITECH Breach of Unsecured PHI Notification Risk Assessment 45 CFR §164.402

- Acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted by HIPAA Privacy Rule *presumed a breach* unless demonstrate low probability PHI compromised

- **LoProCo Risk Assessment requires** at least the following factors
  - Nature and extent of PHI involved (types of identifiers, likelihood of re-identification)
  - Who received/accessed PHI
  - Potential that PHI was actually acquired or viewed
  - Extent to which risk to PHI mitigated

HITECH removed risk of harm standard

babc

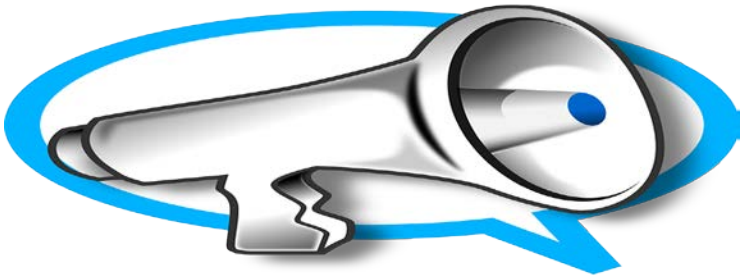
Implementation of Response Program (cont'd)

Report Up and Often

Keep senior management/Board of Directors/Audit Committee appraised of investigation and response plans.

Report Externally?

- File Suspicious Activity Report (SAR)?
- Notify regulators or others of possible breach – and when?
- Cooperation requirements under state law or by contract?



babc

What compliance documentation is needed?

- **What reporting and notifications are necessary and appropriate?**
  - Regulatory reporting
    - SEC Public Filing, US HHS Office for Civil Rights, State AG/Consumer Affairs division
  - Law Enforcement Reporting and Collaboration
    - FBI, Secret Service, Police, OIG
  - Consumer notification
    - State and federal specific elements

babc

HIPAA: Breach Risk Assessment = > Low Probability of Compromise factors

HITECH SECURITY BREACH ANALYSIS: PRIVILEGED AND CONFIDENTIAL WORK PRODUCT

➢ = No breach reporting required if answer is yes NOTES √

4 Factor Risk Assessment	➢Is there compliance documentation to support conclusion that there is a "Low Probability of Compromise of PHI" under at least the following factors?		
Factor 1:	**The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification** o Considerations: Probability higher if PHI is of sensitive nature (i.e., SSN, financial (credit card numbers), clinical information (treatment plans, BH/HIV/STD/CA dx, medications or medical histories).		
Factor 2:	**The unauthorized person who used the PHI or to whom the disclosure was made.** o Considerations: Probability could be lower if recipient bound by HIPAA obligations or other confidentiality requirements. Probability may be higher if recipient has ability to re-identify PHI.		
Factor 3:	**Whether the PHI was actually acquired or viewed.** o Considerations: Probability could be lower if PHI recovered without access		
Factor 4	**•The extent to which the risk to PHI has been mitigated.** o Considerations: Probability could be lower if credible recipient provides assurances that PHI will be destroyed or not further used or disclosed (i.e., confidentiality agreement).		

babc

HIPAA: Breach Risk Reporting = > # of Patients affected by state, timeframes for reporting and mitigation

HITECH SECURITY BREACH ANALYSIS: **PRIVILEGED AND CONFIDENTIAL WORK PRODUCT**

➢ = No breach reporting required if answer is yes

		NOTES	√
Other Factors to consider – risk of harm	• Does incident pose a potential risk of financial, reputational or other harm? Identify risks that need to be managed to mitigate patient harm, including steps individuals can take		
	Type and amount of PHI involved; circumstances of disclosure (e.g., inadvertent, intentional, targeted); method of disclosure; likelihood that harm (financial or reputational harm, embarrassment, inconvenience, or unfairness) will occur and ability to mitigate risk of harm; recipient response; disposition, particularly of data; whether any additional controls can be implemented to reduce risk of harm		
Document Remediation and other HIPAA duties	• Can any HIPAA violation be corrected within 30 days of discovery? • Mitigate to extent practicable, harmful effects of (a) use or disclosure violating HIPAA Privacy or organizational policies and procedures, and (b) known security incidents (unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations) • Identify and respond to security incident and document security incidents and their outcomes • Update Privacy and Security procedures to implement needed security and/or privacy safeguards • Review Sanction Policy if failure to comply with organizational policies and procedures		

babc

Attorney-Client Privilege – Recent Target Order

Data Breach Task Force —> Key: Confidential communication between attorney and client for legal advice

- Breach response team established *at counsel's request to obtain informed legal advice*
- Team coordinated activities on behalf of counsel *to provide counsel information* for class action defense
- Outside counsel retained external technical advice *"in anticipation of litigation"*
  - Separate external team (not engaged by Target counsel) for non-privileged investigation for credit card companies
- Response team focus: ***not in ordinary-course-of-business*** investigation or on remediation
  - Focus to inform counsel about breach to obtain legal advice and defend pending and expected litigation
- CEO updates to Board in aftermath of breach not privileged
  - Mere updates on business-related interests
- Certain communications work-product privileged
  - Separate Verizon report to credit card companies provided forensic images, how breach occurred, Target response so no undue hardship or substantial need for privileged materials to prepare lawsuit

– *In re: Target Corporation Customer Data Security Breach Litigation*, US DC Minnesota MDL No. 14-2522 (10.23.15)

babc

Having No Advance Data Breach Response Plan is Risky and Costly

- At the same time you are trying to comply with these reporting and notification laws, you will be in the midst of a public relations crisis
- Without a data breach response plan in place, mistakes are more likely, and likely to be costly
- On cost alone, studies show that responding to a data breach costs 10 times as much without an advance plan
- If you have an advance plan, implement it

babc

Preparing For Litigation in the Midst of a Data Breach Event

- Step 1: PRESERVATION OF DOCUMENTS AND DATA
- All emails, data, and information relating to the breach and the state of your affected data and recordkeeping systems at the time of the breach must be preserved.
- Err on the side of over-preservation at this stage.
- Failure to preserve can result in serious sanctions, especially if the failure is intentional.
- Preserve first, worry about privilege later.

babc

Litigation Hold

- Document your preservation efforts with formal litigation hold notices to all relevant employees and IT personnel
- Hold should include the helpful as well as the harmful—e.g., prior policies, bulletins, hardware and software additions showing efforts to maintain data security
- Involve outside counsel in affected states, external ESI preservation expertise and consult with any external breach auditors in designing litigation hold if possible

babc

Constantly Assess and Update the Litigation Hold

- The litigation hold should not be static
- It should evolve as new information is obtained about the scope of the breach, the persons and data potentially impacted
- It should encompass past *and future* communications with regulators, customers and third parties about the breach
- It should be adjusted in light of legal claims as they are made, with the input of the defense team for each case

babc

Identify Claims and Prosecutions You May Want to Undertake

- Report the employee to appropriate state and federal criminal authorities
- Is there evidence a competitor or other third party was behind the breach?
- If so, consult with counsel about appropriate civil actions

babc

Legal Action Against Cyber Criminals

- Depending on nature of attack/breach, legal action against criminals may be impractical
- Potential "Jane Doe" action against hacker to subpoena ISP for hacker's identity
- For copyrighted materials, consider DMCA subpoena action against ISP for hacker's identity
- Claims available under federal CFAA, WA, ECPA, SCA, RICO, and various state laws

babc

Consider Voluntary Relief in Advance of Litigation

- **Most companies responding to a data breach offer some form of voluntary relief to their customers**
  - e.g., free identity theft protection for a certain period of time, free credit monitoring services, etc.
- **In *Remijas v. Neiman Marcus Group*, 7th Circuit found such voluntary relief to be an admission that affected consumers had an increased likelihood of harm from the breach, which it deemed enough to confer standing**

babc

Voluntary Relief Post- *Neiman Marcus*?

- Courts inclined to find standing from increased likelihood of harm are likely to find it with or without voluntary relief
- If you don't provide it, they will claim it as a form of relief
- Providing it voluntarily can be a good PR move, with in the long run is more important that litigation
- Consult with legal counsel in affected states before deciding

babc

Insurance Issues

- Analyze your insurance portfolio in the event of a breach
  - While the law is mixed, some courts have found coverage for data breach losses under traditional CGL policies
  - Besides "property damage" and "advertising injury" coverage, also look at D&O and EPLI coverages, depending on nature of incident and resulting claims
  - Even if coverage is ultimately denied, most policies require the insurer to defend if the claim is "potentially" covered

babc

Insurance Issues

- Consider cyber coverage
  - In US, primarily covers 3rd party claims, on claims-made basis
  - Insurance risk market is growing quickly
    - From $850M in premium globally in 2012 to $2.5B in 2015
  - Potential coverage for losses clearly not covered under traditional policies
    - e.g., response and notification costs
  - Application process for such coverages important

babc

Lessons Learned

- Determine needed improvements to prevent or minimize recurrence
- Eliminate residual or persistent threats
- Determine whether to revise or augment company information security policies, practices and training
- Determine whether response plan can be improved

babc

Resiliency

- Identify deficiencies in pre-breach policies
  - Procedural - operational, legal, IS
  - Technological – IT
  - Training and culture - HR, management

babc

Resiliency

- Fill in the gaps
  - Identify ways to mitigate defects
  - Revise procedures and policies
  - Educate management and personnel

babc

Resiliency

- Empasize: reaffirmation of company's commitment to privacy and security
- External messaging, as appropriate: PR, marketing, advertising, customer service

babc

Questions?

Paige M. Boshell
205.521.8639
pboshell@babc.com

Elena A. Lovoy
205.521.8746
elovoy@babc.com

John E. Goodman
205.521.8476
jgoodman@babc.com

Michael R. Pennington
205.521.8391
mpennington@babc.com

Amy S. Leopard
615.252.2309
aleopard@babc.com

babc

BRADLEY ARANT BOULT CUMMINGS LLP