Data Breach: Hot Topics Roundtable Discussion

Wednesday, December 7, 2016

Presented by:
Paige M. Boshell, John E. Goodman, Amy S. Leopard, J. Thomas Richie, and Jordan A. Stivers

Introduction

Paige Boshell

Bradley

Cybersecurity and Privacy Team

- 17 attorneys
- 5 practice groups
  - SMEs in Banking & Financial Services, Government Contracts, Litigation, Healthcare and IP
- 7 webinars in 2016
  - Let us hear from you

Bradley

Today's Panel

John E. Goodman

Amy S. Leopard

Paige M. Boshell

J. Thomas Richie

Jordan A. Stivers

Bradley

Agenda for our Roundtable Discussion

- Real time data breach tabletop
- Coordinate internal and external teams
- Execution of breach response and recovery plan
- Compliance documentation
- Notice/law enforcement
- Attorney-client Privilege, litigation hold, voluntary relief
- Civil claims/ insurance issues
- Resiliency

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

Recovery "Playbook" In Place Before Breach

- Have an actionable recovery plan "playbook" before cyber incident
- Continuously improve recovery capability through practice, training, and learning from previous incident response
  - Develop set of formal recovery processes
  - Determine criticality of organizational resources required for organization's mission
  - Create functional and security dependency maps to help recovery team understand order of restoration priority
  - Identify/select technology and key personnel responsible for defining and implementing recovery plan
  - Prepare comprehensive recovery communications plan with fully integrated internal and external communications considerations
  - Practice recovery processes for timely recovery team coordinate

Guide for Cybersecurity Event Recovery – Draft NIST Special Publication 800-184 (June 2016)

2 Data Breach Scenarios

The network has been breached. While entry method and specific attack type are not immediately relevant to the recovery team, the breach jeopardizes the trustworthiness of the business unit and IT management systems.

- 1. Anomalous activity detected during recent log reviews indicate a malicious actor used stolen credentials to gain access to critical business and IT infrastructure systems.
  - Network monitoring equipment confirms a significant amount of personally identifiable information exfiltrated, including customer financial data
- 2. “Locky has encrypted your computer. You have 96 hours to pay in BitCoin or all your files will be permanently encrypted.”

Sources: *Guide for Cybersecurity Event Recovery* – Draft NIST Special Publication 800-184 (June 2016)
How to Protect Your Networks from Ransomware, US Government Interagency Technical Guidance Document

Implementing the Recovery Plan

Jordan Stivers

Bradley

Assemble Internal and External Teams

- Internal team
  - GC, privacy officer, IT/IS, HR, Legal, PR, Customer service, senior management rep
    - Centralized function and single communications channel and decision maker
    - Response plan assigns specified roles and responsibilities
- External team
  - Legal, forensic and other investigators, PR, vendor representatives, and law enforcement
    - Defined functions and centralized communications and accountability
    - All report to single, internal decision maker
- Coordinate and centralize message

Assemble Internal and External Teams (cont'd)

- 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

Bradley

Implement Recovery Plan: Scoping

Determine scope of incident/compromise

- **What was compromised?** Determine known data losses and identify additional work needed to develop inventory of affected data (and individuals).
- **Was problem due to a systemic or isolated issue?**
- **What do we have to work with?** Determine what information relevant to incident may be available from security system data, logs, entry records, etc.
- **Are we "safe"?** Assess whether compromised data was encrypted or password protected.
- **Who was involved from inside/outside the company?** Determine involvement of employees, 3rd party providers, vendors, consultants, and others. Interview relevant employees and others involved in or with knowledge of incident. Gather relevant vendor, etc. contracts.

Implement Recovery Plan: Scoping (cont'd)

What do we have to work with?

Check physical security measures and their logs, including:

- Reception or entry checkpoints
- ID scanner or other access records
- Video or still footage
- Physical logs
- Elevator or garage records

IT forensics

- Algorithmic steps taken by malware
- Extent of intrusion, whether malware propagated to other systems

Implement Recovery Plan: Summary

- Incident response team informs the recovery team of event
- Recovery team determines criticality and impact of cyber event to formulate approach and set of specific actions
- Since recovery plan may alert the intruder, increase monitoring before action taken to determine compromised systems
- Incident response and recovery teams work seek to uncover intruder's motivation and footprint on infrastructure, command and control channels, tools
- Based on recovery playbook criteria, designated personnel determine when recovery process begins and inform relevant parties
- Network-based communications (e.g., email) may be insecure and cannot be trusted, so use in-person meetings and phone as alternate means of communication
- After determining which accounts and systems were compromised, contain and regain control of underlying infrastructure without alerting intruder
- Prioritize mission critical systems for recovery
  - dependency map to build the restoration plan
- Inventory backup hardware, software, and data and account for responsible personnel

Guide for Cybersecurity Event Recovery – Draft NIST Special Publication 800-184 (June 2016)

Execute Recovery Plan

Pro-active Measures - *immediate* measures to prevent further compromise and unauthorized access:

- Check network security measures and close off network intrusion
- Activate enhanced system logging and monitoring
- Consider whether any global or local password changes, modified access privileges, or other enhanced security measures are immediately necessary and implement any needed changes
- Ensure that any current or former employees implicated in breach no longer have access privileges
- Review access privileges for contractors, vendors, and 3rd parties

Bradley

Execute Recovery Plan (cont'd)

- Coordinate remediation countermeasures (recovery, incident response team, IT) to mitigate re-introduction of underlying weaknesses, minimize likelihood intruder re-enters
  - Handle high-value assets first

- Restore additional business services and communicate per pre-existing communications criteria and coordinate with legal and public affairs offices, regarding the restoration status.

- Track actual time critical services unavailable or diminished, comparing actual outage with agreed-upon service levels and recovery times.
  - Advise organization managers on objectives that may not be accomplished and consider impact for proactive actions may be taken (e.g., routing traffic to a pre-arranged alternate service provider with pre-approved notification pages)

Guide for Cybersecurity Event Recovery – Draft NIST Special Publication 800-184 (June 2016)

Execute Recovery Plan (cont'd)

- Document issues arising and newly identified dependencies for later in recovery process or immediately after recovery achieved.
  - Continuously capture, update and document indicators of compromises
- Work with senior leadership, HR Legal to discuss appropriate notification activities.
  - Notices for employees, affected customers, and public
  - Keep customers informed of recovery status, sharing status accurately while abiding by pre-agreed decisions on may be shared with whom, and when
- Initialize additional recovery steps (e.g., external interactions, services such as pre-arranged credit monitoring services, additional customer support staff) to help restore confidence and protect customers
- Confirm with IT personnel and external subject matter experts that system is ready to be restored to service and that restoration has fully occurred

Guide for Cybersecurity Event Recovery – Draft NIST Special Publication 800-184 (June 2016)

Legal, Regulatory and Risk Management

Amy S. Leopard

Bradley

Legal, Regulatory and Risk Management

- **Risk Assessment**
  - Misuse of data reasonably likely/unlikely?
  - What risks/harms occur if data misused?
  - Re-creation of affected data?

- **Reporting and Notifications, Law Enforcement contact**
  - Law Enforcement Reporting and request for assistance
    - FBI, Secret Service, Police, OIG
  - Regulatory reporting
    - SEC Public Filing, US HHS Office for Civil Rights, State AGs, etc.
  - Consumer notification
    - State and federal specific elements
- **Applicable contractual requirements**
  - Contractual obligation to notify impacted individuals
  - Indemnifications, reimbursement of expenses

Bradley

Regulatory Overlay Impacts Incident Response

- Security Incident Response - HIPAA Covered Entities/Business Associates
  - *Security Incident*: the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system
- Covered Entities and their Business Associates must initiate Security Incident response plan to identify and respond to suspected or known security incidents
  - Mitigate, to extent practicable, harmful effects of known security incidents
  - Business Associates of Covered Entities must report Security Incidents according to the terms of the Business Associate Agreement
  - Document incidents and their outcomes

➢ = 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		

HIPAA: Breach Risk Reporting = > identify and mitigate harm, address remedial measures

Bradley

Regulatory Overlay Impacts Breach Response

- Breach Response for HIPAA Covered Entities:
  - *Breach:* 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 was compromised

- **HIPAA Breach Low Probability of Compromise Risk Assessment** factors
  1. Nature and extent of PHI involved (identifiers, data elements, re-identification)
  2. Who received/accessed PHI
  3. Potential that PHI was actually acquired or viewed
  4. Extent to which risk to PHI mitigated

➢ = 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).		

Ransomware Risk Assessment

- HHS Ransomware Guidance (July 2016)
  - If ePHI encrypted during ransomware attack = HIPAA breach if unencrypted PHI was "acquired" (unauthorized individuals took possession or control of the information) and thus is an unpermitted "disclosure" unless Low Probability of Compromise Risk Assessment factors proven
  - HIPAA 4 factors Plus:
    - Whether there is a high risk of unavailability of PHI?
    - Whether there is a high risk to the integrity of the PHI ?

- *HHS Guidance on Ransomware* - breach risk assessment also should consider:
  - Exact type and variant of malware discovered
  - Algorithmic steps undertaken by malware
  - Communications (including destruction or exfiltration attempts) between malware and attackers' command and control servers
  - Whether or not malware propagated to other systems, potentially affecting additional sources of ePHI
  - Impact of ransomware on integrity of ePHI (are there backups, can data be restored)

- Likewise, is there a state law interpretation of "Disclosure" of "Personal Data"?
  - Review state law elements on acquisition, risk of harm

Litigation Issues

John E. Goodman
Thomas Richie

Bradley

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)**

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.

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

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 3rd 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

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 3rd party was behind the breach?
- If so, consult with counsel about appropriate civil actions

Bradley

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

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

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, which in the long run is more important that litigation
- Consult with legal counsel in affected states before deciding

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

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

Debriefing

Bradley

Post Recovery

- Recovery team debriefs to consider metrics gathered during event
  - efficacy of training, additional plans required, assumptions made, recovery objective performance, and stakeholder communications
- Compare team performance during recovery vs. estimated performance for adjustments to plans
- Identify deficiencies in pre-breach policies
  - Procedural - operational, legal, IS
  - Technological – IT
  - Training and culture - HR, management
- Develop root cause analysis and plan for longer-term correction
  - Eliminate legacy technology that cannot be protected adequately
  - Adopt enhanced and modern protection and detection mechanisms

Guide for Cybersecurity Event Recovery – Draft NIST Special Publication 800-184 (June 2016)

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

Resiliency

- External messaging, as appropriate: PR, marketing, advertising, customer service
- Determine whether response plan can be improved
  - Continually improve cyber event recovery plans, policies, and procedures by addressing lessons learned during recovery efforts and periodically validating recovery capabilities
- Emphasize: reaffirmation of company's commitment to privacy and security

Questions?

John E. Goodman
jgoodman@bradley.com
205-521-8476

Amy S. Leopard
aleopard@bradley.com
615-252-2309

Paige M. Boshell
pboshell@bradley.com
205-521-8639

J. Thomas Richie
trichie@bradley.com
205-521-8348

Jordan A. Stivers
jstivers@bradley.com
615-252-3542

Thank You!

Bradley