The Data Breach: How to stay defensible before, during and after the incident.

Alex Ricardo, CIPP/US
Breach Response Services

beazley

What we are NOT doing today

Providing Legal Advice

- Informational Purposes Only
- You should consult with Privacy Counsel for any decisions surrounding your Incident Response Plan or Data Breach Response Methodology

A data breach isn’t always a disaster

Mishandling it is.

Agenda

- A Brief Review of Data Breaches and Breach Trends
- Regulatory Landscape
- The Breach Response Methodology
- Cases
- The Beazley Approach
- Best Practices at Crafting a Data Breach Response Plan

A Brief Review of Data Breaches and Breach Trends

What is a Data Breach?

- Actual release or disclosure of information to an unauthorized individual/entity that relates to a person and that:
  - o May cause the person inconvenience or harm (financial/reputational)
    - Personally Identifiable Information (PII)
    - Protected Healthcare Information (PHI)
  - o May cause your company inconvenience or harm (financial/reputational)
    - Customer Data, Applicant Data
    - Current/Former Employee Data, Applicant Data
    - Corporate Information/Intellectual Property
- Paper or Electronic

Types of Data Security Breaches

- Improper Disposal of Data
  - o Paper
    - Un-shredded Documents
    - File cabinets without checking for contents
    - X-Ray Images
  - o Electronic assets
    - computers, smart phones, backup tapes, hard drives, servers, copiers, fax machines, scanners, printers
- Phishing/Spear Phishing Attacks
- Network Intrusions/Hacks/Malware Viruses
- Lost/Missing/Stolen Electronic Assets
- Mishaps due to Broken Business Practices
- Rogue Employees

Commonalities of Cyber Breaches

- Will be an external attack involving hacking and malware
- Vulnerability created by third party vendor
- Will not be detected for months
- Breached entity will learn from third party
- Initial exploit relatively simple and avoidable

Why we should be careful with the word “Breach”

Perception is Half the Battle

- People use “breach” too frequently and you don’t want your customers or regulators to think you are subject to numerous breaches
- “Breach” suggests something bad happened or is going to happen
- “Breach” has legal significance
  - Train your Incident Response Team to not use “Breach” within internal communications as you vet out or investigate the “Security Incident”

Regulatory Landscape

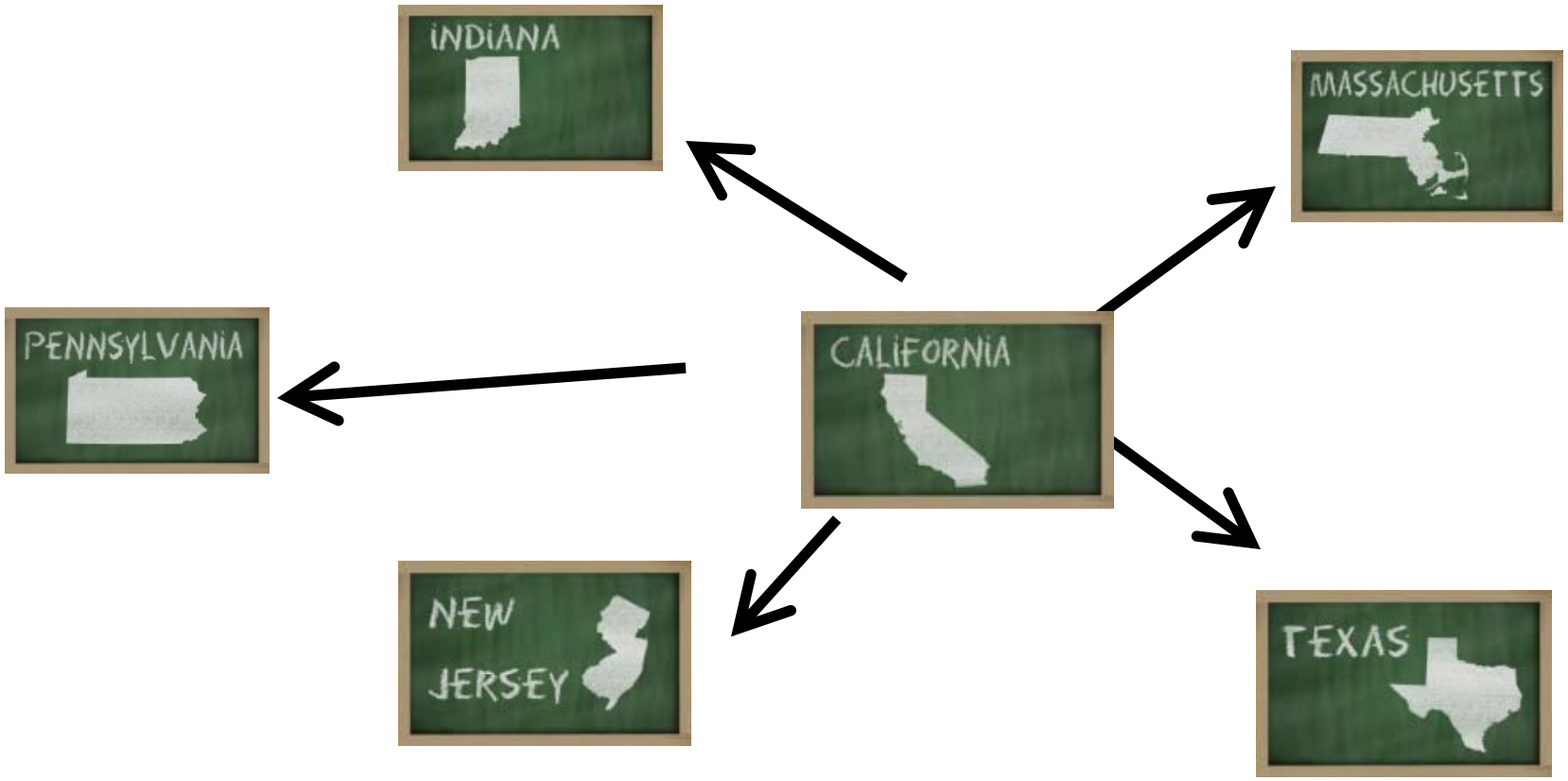
The Legal Landscape – US Federal Laws

- HIPAA-HITECH
  - o Do you handle PHI?
- PCI-DSS
  - o Do you accept transactional data? (Credit Card Data)
- FTC's Red Flags Rule
  - o Are you a creditor?
- FACTA (Fair & Accurate Credit Transactions Act)
  - o Do you use credit reports in the course of pre-employment background screening? (Not allowed – CA, CO, CT, IL, HI, OR, NV, MD, WA)
- FISMA (Federal Information Security Management Act of 2002)
  - o Are you a federal contractor?
- FTC – Section 5a
  - o Do you engage in unfair or deceptive acts or practices?
  - o Do you comply with your website's privacy policy?

The Legal Landscape – US State Laws

- State Laws
  - 47 States + DC, PR, VI
- Encryption is a safe harbor to most (not all) – (i.e. MA)
- Laws differ with respect to:
  - Notice Triggers
    - Data types (definition of PII)
    - Format of data (paper, electronic)
  - Timeliness
  - Required content for notification
  - Notification of attorneys general and various state agencies

The Reach of State Laws



“The New Breed” - State Document Destruction Laws

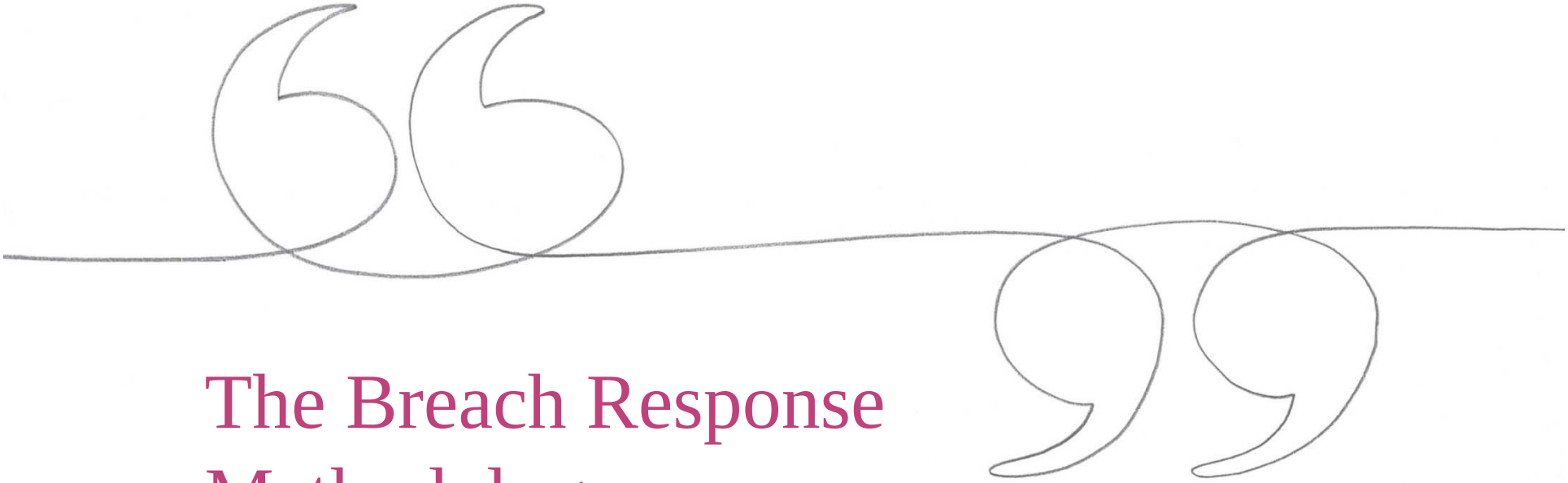
- DE Section 50C - “reasonable steps” needed
  - Destruction of PII (usual suspects, insurance policy #s, medical information)
  - Failure to comply may bring civil action by a DE resident
  - Exempts
    - Banks, Credit Unions, FIs, CRAs, Government
- DE Section 736 – “reasonable steps” needed
  - Employee who incurs damages due to his/her employer’s reckless or intentional lack of destruction may bring civil action against the employer for treble damages by a DE resident.
  - PII – similar to 50C, but also includes signature and full DOB.
  - No industry exemptions

The Legal Landscape – International Laws

- Canada
  - o PIPEDA, Ontario, Manitoba, Trans-Border Data Flow Laws
- EU Directive
  - o DPAs moving into mandatory notification. Some already do.
  - o Cookie Consent
- LatAm, APEC – various privacy frameworks
  - o Some DPAs have mandatory notification.
- Safe Harbor Provisions
  - o Some nations are “Adequate” with privacy requirements to the EU.
    - ▪ (Argentina, New Zealand, among others) - US is NOT.
  - o US Dept. of Commerce – Safe Harbor Provisions (EU, Switzerland)
- Binding Corporate Rules (BCRs)

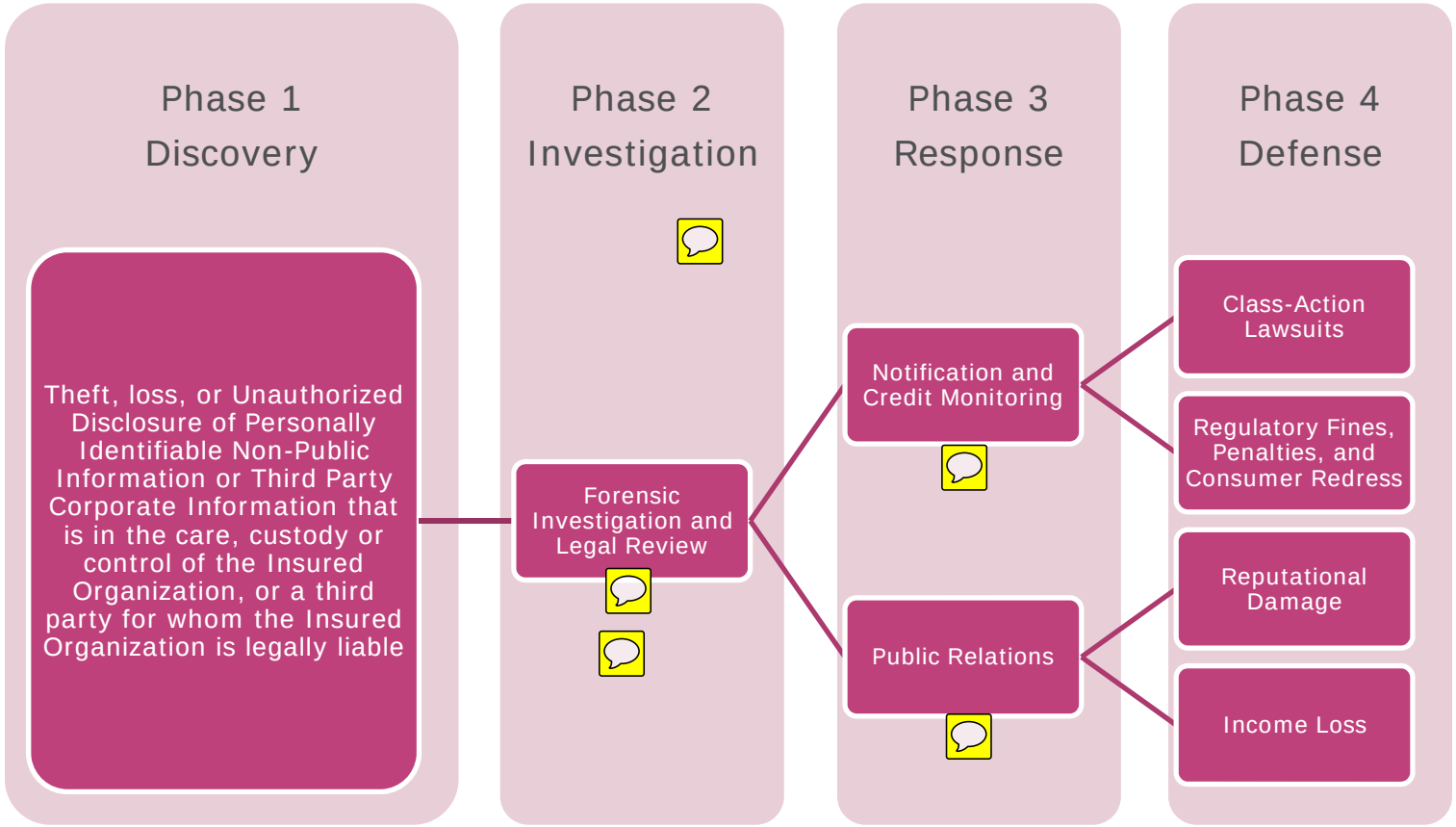
What Do All Regulators Dislike?

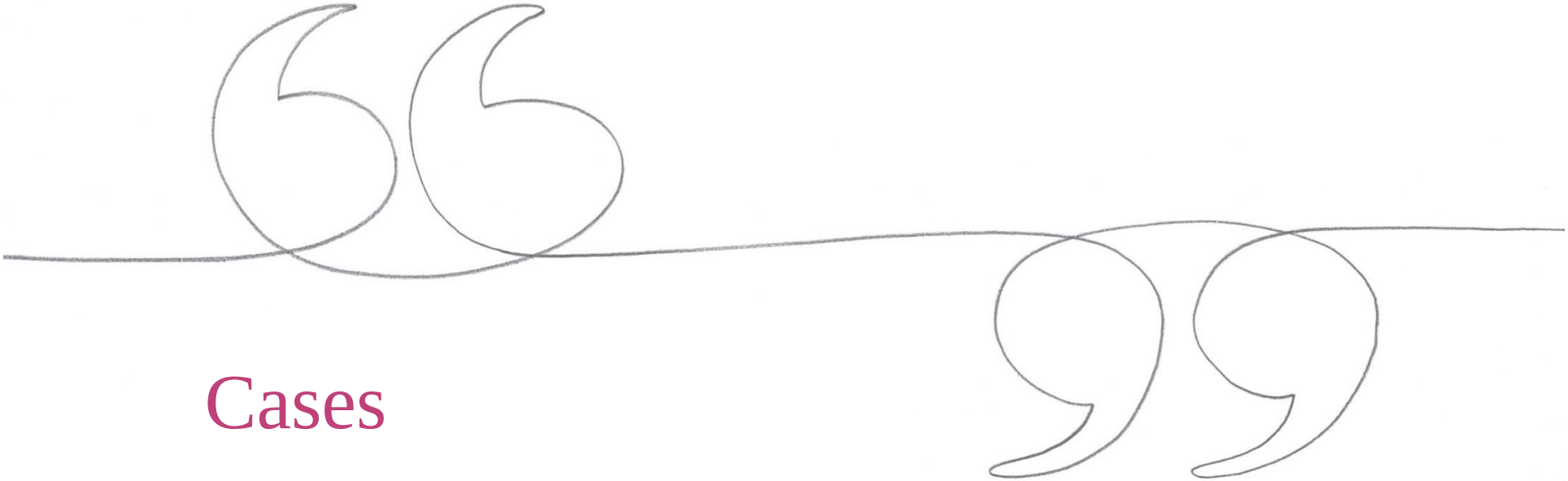
- Unencrypted backup tapes
- Unencrypted portable devices
- SQL injection
- Slow incident detection and notification
- Default configurations/passwords
- Absence of appropriate policies
- Insufficient employee training/awareness
- Insufficient dedicated security roles
- Failure to address issues identified by risk assessments
- Refusal to provide incident reports and forensic investigation report



The Breach Response Methodology

A Simplified View of a Data Breach Response Methodology





Cases

Why background screening / vendor vetting is important.

- Entity Affected: College/University
- Incident Details: Lack of proper vetting of employer-attendees allowed criminals impersonating an employer to attend a job fair for college seniors. Criminals successfully secured identities via job application forms.
- Data Format: Paper records
- Information Compromised: Name, DOB, SSN#, Email Address, Address, Phone #
- Breach Universe: 500+

Why forensics is important. Don't assume you know the facts.

- Entity Affected: Financial Services Firm
- Incident Details: Company suffered a malware intrusion and initially believed all 280,000 customers' PII was compromised. Forensics reversed engineered the malware to determine it was only collecting credit card numbers beginning with "3". (American Express Cards) Without Forensics, the company would have notified the entire population.
- Data Format: Electronic
- Information Compromised: Name, Credit Card #
- Breach Universe: 30,000+

Paper Breaches Do Happen

- Entity Affected: College/University
- Incident Details: Alumni Newsletter mailing label accidently included the SSN# field. As such all alumni SSN#s were exposed publicly on the mailing label.
- Data Format: Paper records
- Information Compromised: Name, SSN#, Address
- Breach Universe: 125,000+

Don’t assume you know the facts.

- Entity Affected: Hospital
- Incident Details: Hospital did a “disaster drill”. Set up 20 laptops, one in each ER suite. To replicate lost power, each laptop was to be set up with all 500,000 EHRs of the hospital. During course of drill, 1 laptop went missing.
- Initial Response: Hospital called a press conference to acknowledge a loss of 500,000 EHRs. They held the press conference BEFORE the investigation.
- Investigation: Investigation identified time of loss via surveillance cameras in the ER. IT reviewed network logs for downloading the 500,000 EHRs to each laptop and noticed 1 laptop did not receive the 500,000 EHRs. Investigation took 48 hours.
- Conclusion: It was forensically concluded that the missing laptop was stolen BEFORE the download of 500,000 records occurred.
- Data Format: Electronic
- Information Compromised: PHI
- Breach Universe: ZERO – “Non-Event”
- Aftermath: The hospital had to hold a second press conference about the “false alarm”.

Incident Response Plan Crafting

Objectives for a Data Breach Incident Response Plan

- "Living Document"
    - Routinely updated to keep current
- Clear and Easy-to-Use in the midst of a crisis incident
    - Succinct
    - Organized by sections
- Not a "phone book" but not a "leaflet"
    - Background information on regulations and laws
    - Detailed procedures and steps on incident management
    - Contact details of the Incident Response Team
- Document all discoveries for evidentiary needs

Regulatory Satisfaction for a Data Breach Incident Response Plan

- HIPAA Security Rule (Section 164.308)
- PCI DSS (Section 12.9)
- ISO 17799/27002 (Section 6.3)
- Red Flags Rule – FACT Act (Section .90(d)(1))
- Certain State Information Security Laws
    - MA 201 CMR 17

The Anatomy of the Data Breach Incident Response Plan

- Background
- Incident Response Team
- Incident Management
    - o Risk Transfer Requirements
    - o Threat Level Definitions
    - o Incident Triaging
    - o Breach Universe Definitions
    - o Breach Response Methodology
    - o Mitigation/Remediation

The Anatomy of the Data Breach Incident Response Plan

- Background
  - o Purpose of the Plan
  - o High-Level Legal Landscape / History
  - o Internal Policies
  - o Versioning
  - o Custodian/Contact for revisions

The Anatomy of the Data Breach Incident Response Plan

- Incident Response Team
  - o Roles & Responsibilities
  - o Internal Members of the IRT
  - o External Members of the IRT
  - o Contact Information of Members of the IRT
  - o Define “Threat Levels” to members of the IRT

The Anatomy of the Data Breach Incident Response Plan

- Incident Management
  - Risk Transfer Requirements
    - The IRT should be in sync with risk management and insurance requirements
  - Threat Level Definitions
    - Establish threat levels for incidents
    - A breach of 1 individual is not like a breach of 1,000,000.
    - A breach of 12 individuals due to fax error is not like a malware virus intrusion leaking 100,000 records of PHI.

The Anatomy of the Data Breach Incident Response Plan

- Incident Triaging
  - o Threat level defined to trigger appropriate members of the IRT
  - o Insurance Carrier need to be advised?
  - o Privacy Counsel needed?
  - o Investigation needed?
    - ▪ Forensics
    - ▪ Traditional
    - ▪ Both
  - o Electronic data? Paper-based data? Both?
  - o Is a 3rd party involved? Or the cause?
  - o Law Enforcement Needed?
    - ▪ FBI? Secret Service? State/Local?
    - ▪ Police Report needed? (Theft involved?)
  - o PR/Crisis Management Needed? Media Involved (yet)?

The Anatomy of the Data Breach Incident Response Plan

- Breach Universe Definitions
  - o Size of affected population
  - o Types of Data Compromised
    - PII
    - PHI
    - Other
  - o Individuals
    - Name
    - DOB (or age, adult/minor status)
    - Deceased?
    - Foreign National?
    - Most recent mailing address
    - Localization of individual (Preferred Language)

The Anatomy of the Data Breach Incident Response Plan

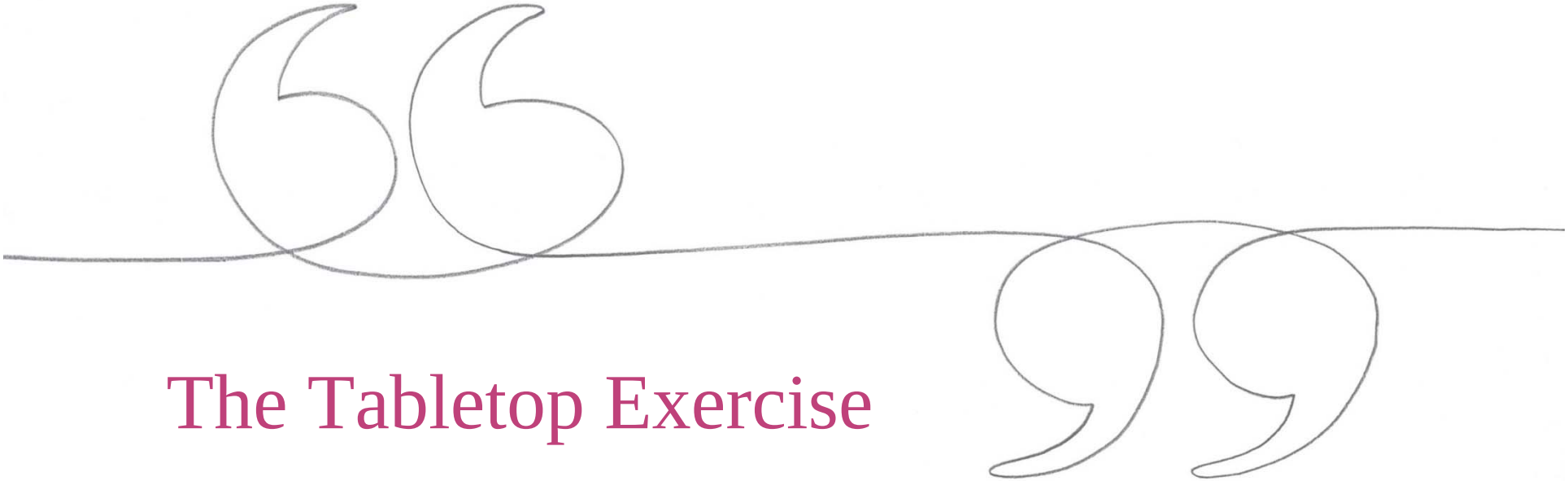
- Breach Response Methodology
  - Notification Procedures
    - Define timing strategy of all communications
    - Police Report needed? (if theft involved)
    - Affected Individuals' notification fulfillment needed?
      - Draft notification letters
        - Description of what happened
        - Description of data types involved
        - Steps to protect oneself
        - What entity is doing to investigate and mitigate harm. Remedy? (credit monitoring)
        - Contact details for questions
        - Apology
      - Obtain corporate logo and signature image
    - Affected Individuals' call center needed?
      - Establish escalation contacts
      - Draft FAQs
      - Draft Scripts

The Anatomy of the Data Breach Incident Response Plan

- Breach Response Methodology
  - Notification Procedures
    - Government Agencies / Attorneys General
      - Draft notification letters - Federal, State, Local (where applicable)
    - Press Releases
      - Draft Press Releases and Scripts for Media
    - Internal Communications
      - Draft internal memos
      - General Workforce, Management, Board of Directors
    - Website
      - HITECH Substitute Notice (if applicable)
      - Public Posting
      - Require separate phone # from notification #
    - Assess need for localization (multiple languages)
    - Accompanying remedy with notice
      - Credit Monitoring / Credit Reports
      - Identity Theft Resolution
        - Credit-related fraud restoration
        - Healthcare record fraud restoration

The Anatomy of the Data Breach Incident Response Plan

- Mitigation and Remediation
  - o Recovery
    - ▪ Eradicate vulnerabilities
    - ▪ Reinstate repaired/hardened systems
  - o Review – Lessons Learned
    - ▪ Log/Record incident in an incident database for trending/historical analytics
    - ▪ Review with incident response team
      - • Review information security systems, policies and procedures, workflows
      - • Review physical security systems, policies and procedures, workflows
      - • Update training program accordingly
    - ▪ Update incident response plan



The Tabletop Exercise

"Practice Makes Perfect"

Decisions, Decisions, Decisions …

What is a Tabletop Exercise?

- Structured data breach response drill
- Triggers your Incident Response Plan (IRP) for testing purposes
- Involves members of your Incident Response Team (IRT) (both internal and external)
- Tests the effectiveness and accuracy of the workflow of your current IRP
- Not the time “for the Marriott conference room”

Why Conduct a Tabletop Exercise?

- "Practice Makes Perfect"
- Practice/learn on an exercise vs. "the real deal"
- Identifies any holes in your current IRP that need to be resolved and updated
- Assures that members of your IRT and their contact details are current and accurate
- Assures that members of your IRT (both internally and externally) know of one another before any real incident
- Demonstrates to inquiring regulators your team's readiness and "seriousness" in conducting a sound data breach response methodology.

Leaking the Hypothetical Facts

- Break up the facts into realistic pieces
- Start with a minimal amount of information, similar to the information you might receive when the information revolving around the event is discovered
- Take a reasonable amount of time to come up with the plan and identify their response activities; depending on the complexity of the breach scenario, 20 minutes should be enough time
- Continue dishing out the factual information, giving the IR team time with each additional piece of information to develop a plan and prepare a list of their response activities

Alex Ricardo, CIPP/US
Breach Response Services

Beazley Group

Rockefeller Center
1270 Avenue of the Americas
New York, NY 10020

t: +1 (917) 344 3311
c: +1 (646) 477 1321
e: alex.ricardo@beazley.com

For More Information: www.beazley.com

"It's bad enough a company may possibly face liability from the data breach itself. The last thing you want is to create further liability exposure from how you respond to the incident.

Making sure you are kept in the best defensible position possible during the course of your breach response methodology should be a priority."