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

Alex Ricardo, CIPP/US
Breach Response Services
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 it is.
Agenda

- A Brief Review of Data Breaches and Breach Trends
- Regulatory Landscape
- The Breach Response Methodology
- Cases
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:
  - May cause the person inconvenience or harm (financial/reputational)
    - Personally Identifiable Information (PII)
    - Protected Healthcare Information (PHI)
  - 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
  - Do you handle PHI?
- PCI-DSS
  - Do you accept transactional data? (Credit Card Data)
- FTC’s Red Flags Rule
  - Are you a creditor?
- FACTA (Fair & Accurate Credit Transactions Act)
  - 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)
  - Are you a federal contractor?
- FTC – Section 5a
  - Do you engage in unfair or deceptive acts or practices?
  - 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
  - PIPEDA, Ontario, Manitoba, Trans-Border Data Flow Laws
- EU Directive
  - DPAs moving into mandatory notification. Some already do.
  - Cookie Consent
- LatAm, APEC – various privacy frameworks
  - Some DPAs have mandatory notification.
- Safe Harbor Provisions
  - Some nations are “Adequate” with privacy requirements to the EU.
    - (Argentina, New Zealand, among others) - US is NOT.
  - 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
A Simplified View of a Data Breach Response Methodology

Phase 1
Discovery

Theft, loss, or Unauthorized Disclosure of Personally
Identifiable Non-Public Information or Third Party
Corporate Information that is in the care, custody or
control of the Insured Organization, or a third
party for whom the Insured Organization is legally liable

Phase 2
Investigation

Forensic Investigation and Legal Review

Notification and Credit Monitoring

Phase 3
Response

Public Relations

Phase 4
Defense

Class-Action Lawsuits

Regulatory Fines, Penalties, and Consumer Redress

Reputational Damage

Income Loss
Beazley’s Breach Response Methodology
Beazley’s Breach Response Methodology

**Phase 1: Discovery**
- Insured’s incident management protocols initiated
- Notice to broker/Beazley
- Triage call

**Phase 2: Investigation**
- Privacy counsel
- Forensics
- PCI-related investigations (PFI)

**Phase 3: Response**
- Notification drafting
- Address verification
- Remedy selection
- Mail merging
- Notification production
- Postage/Mailing
- Return mail processing
- FAQ Drafting
- Escalation preparation
- Crisis call center
- Remedy enrollment
- Identity restoration

**Phase 4: Defense**
- Claims
- Defense counsel
- Fine/Penalties
- PCI re-certification (QSA)

**Crisis communications**
- Regulatory/Agency notices
- Substitute notice
- Media
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+
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+
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+
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”.
"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."

The descriptions contained in this broker communication are for preliminary informational purposes only. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd’s. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497).