Today's Complicated

Breach Landscape:

Managing the Response and Consumer Expectations

September 18, 2014

Introductions – Michael Bruemmer

Michael Bruemmer, CIPP/US,
Vice President
Data Breach Resolution, Experian Consumer Services

Tony Hadley
Senior Vice President
Government Affairs & Public Policy, Experian

David Chamberlin
Executive Vice President and General Manager
Data Security & Privacy Group, Edelman

The Data Breach Plan

Tony Hadley

Meeting Policymakers' High Expectations

- Current Data Breach regulatory environment
- Congress continues to struggle with breach standard
- Ongoing experimentation by state lawmakers
- Designing a DBR plan to meet policymaker's expectations

Current Regulatory Environment

47 existing laws in States, DC & Puerto Rico

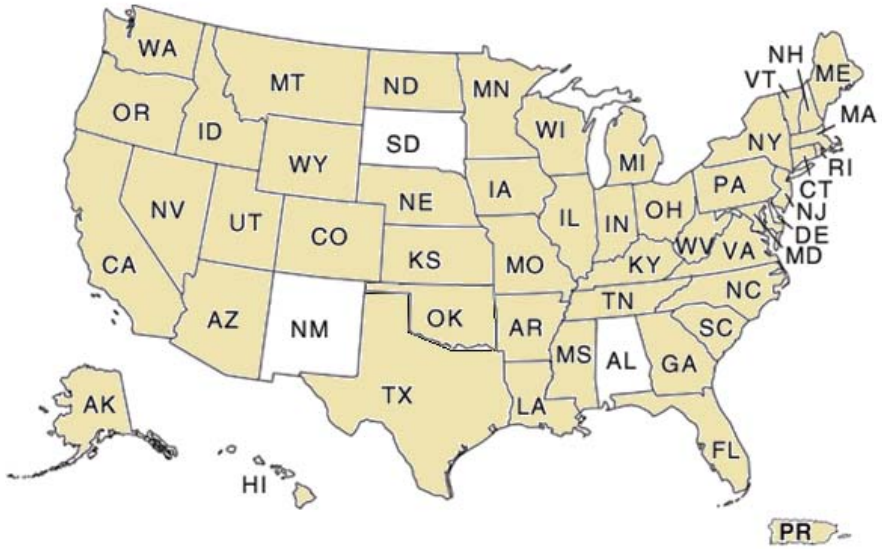
- Alabama, New Mexico and South Dakota are only ones without breach law

Two federal sectoral laws

- Health related data - Health Information Portability and Privacy Act (HIPPA)
- Financial data - Gramm Leach Bliley Act (GLBA)

FTC has well-established role in enforcement actions

- Over 50 cases taken since 2001



Will There Ever Be a National Standard?

High-profile breaches have increased scrutiny from lawmakers

- Several hearings in both House and Senate earlier this year
- Over seven breach notification bills have been introduced

Administration supports national breach standard

- U.S. Attorney Eric Holder video message
- White House Big Data report

But, pitfalls remain that prevent consensus

- Pre-emption of state laws
- Definition of personal information
- Congressional Committee turf battles

States Continue to Experiment

Until a Federal standard is set, states will continue to tinker

- Content of breach notice
- Decrease the timing of notice
- Expand the types of information that would trigger notification

Several states passed bills in the 2014 sessions

- Kentucky
- Iowa
- Florida

California AB-1710 addresses identity protection and mitigation services.

A Clear, Comprehensive DBR Plan is Expected

NY Attorney General
Eric Schneiderman

"Successful implementation of a thoughtfully designed plan can be one of the most effective ways to minimize the risk of a data breach."

CA Attorney General
Kamala Harris

"…businesses should put together a 'game plan' so that when a Cyber incident happens, your resources are used wisely and efficiently."

FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

"…financial institutions should develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information."

Who's on Your Data Breach Response Team?

Internal team members:

- Information Security / Information Technology
- Legal and Compliance
- Communications and Public Affairs
- Executive management

External participants

- Forensics investigator
- Vendor to assist with notification
- Outside legal counsel
- ID theft protection services

What Are Your Notification Requirements?

State laws are similar, but they do have nuances.

- Timing
- Content of Notice
- Whether the breached data triggers a notice

Work with internal legal and compliance teams, as well as outside counsel to stay updated on changing requirements.

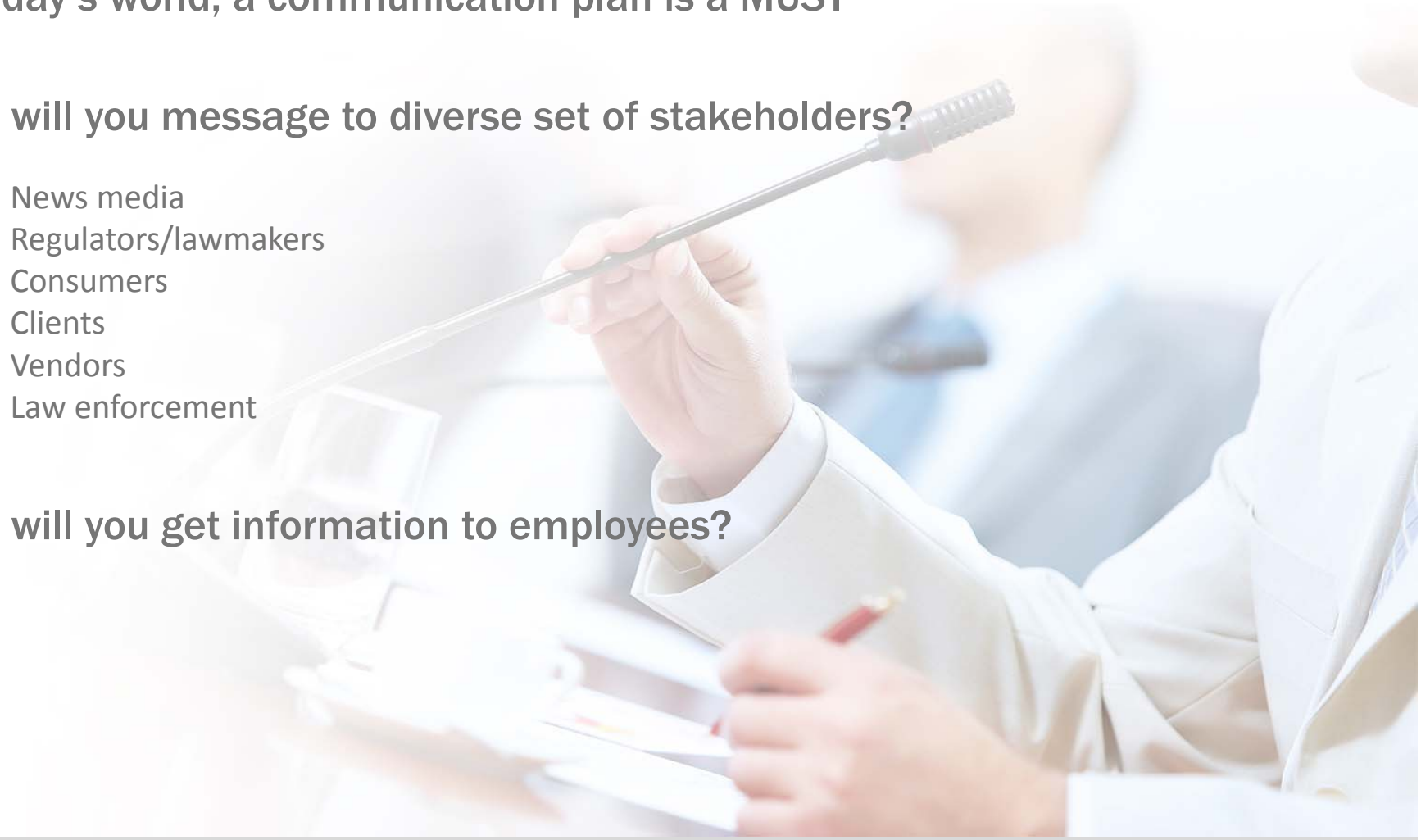
Do You Have a Communication Plan?

In today's world, a communication plan is a MUST

How will you message to diverse set of stakeholders?

- News media
- Regulators/lawmakers
- Consumers
- Clients
- Vendors
- Law enforcement

How will you get information to employees?

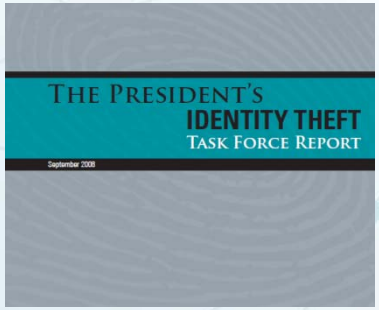


What Will You Do To Protect Consumers?

Policymakers expect to see a post-breach mitigation service

NY Attorney General
Eric Schneiderman

"...policies should address whether, how, and when to inform affected individuals of the loss of their data, and whether to offer services such as free credit monitoring to those individuals."



"While not required by law, New Yorkers affected by a data breach should be provided with mitigation services for free."

Your Data Breach Response

Michael Bruemmer

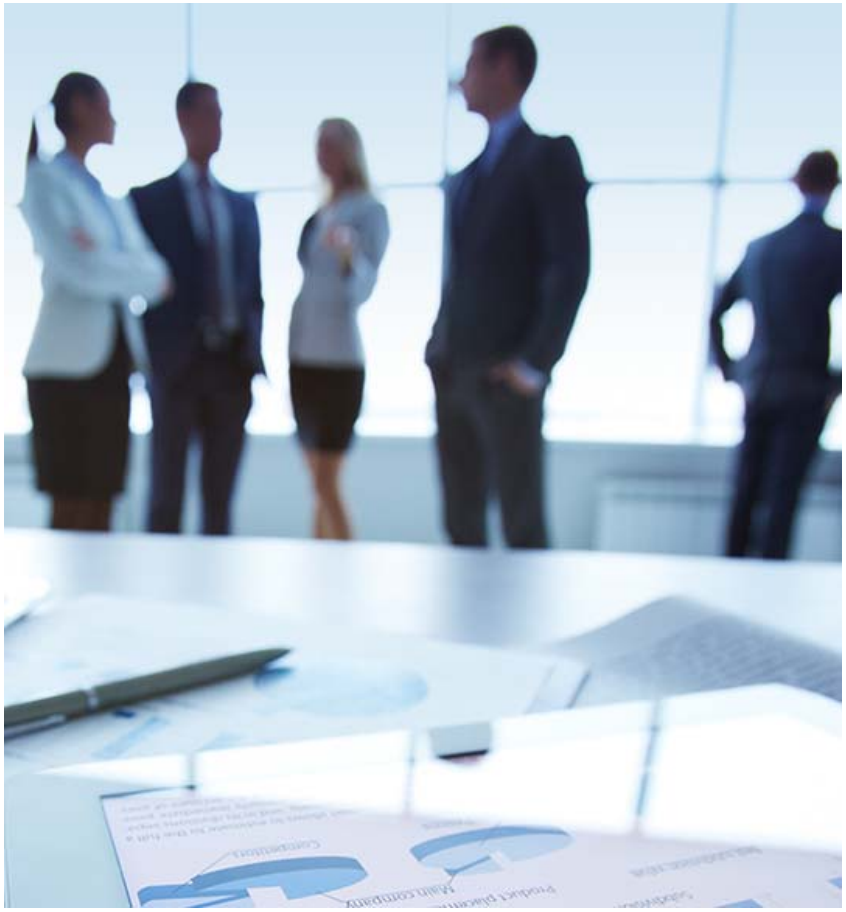
Tackling Your Data Breach Response

- Select the right partners
- Provide identity theft protection for your consumers
- Go above and beyond

Selecting the Right Partners

Don’t settle for less than a COMPREHENSIVE APPROACH

- Outside legal counsel
- Forensics
- Public Relations
- Incident management
- Notifications
- Identity theft protection
- Call center support
- Incident reporting



Identity Theft Protection - Minimum Standard

- Credit Report
- Fraud detection alerts
- Internet scanning
- National change of address
- Insurance coverage
- Full service fraud resolution

Going Above and Beyond

Regaining the trust of the consumer is your TOP PRIORITY

The cost of lost business increased from $3.03 million to $3.2 million last year.

- Abnormal customer turnover
- Increased customer acquisition activities
- Reputation losses & Diminished goodwill

*2014 Cost of Data Breach Study Ponemon Institute

Managing Reputation

David Chamberlin

What are some *best practices* for a data security incident event?

Preparation is Key

Proactive steps to take:

- Identify internal and external crisis team
- Develop communications chain of command for multiple scenarios
- Meet your state's legislators, regulators and policy makers
- Determine your lobbying, forensics and legal firm before a crisis
- Conduct a mock crisis situation
- Keep the team lean and empower a decision-maker

Why is managing reputation such an

important part

of the data security response process?

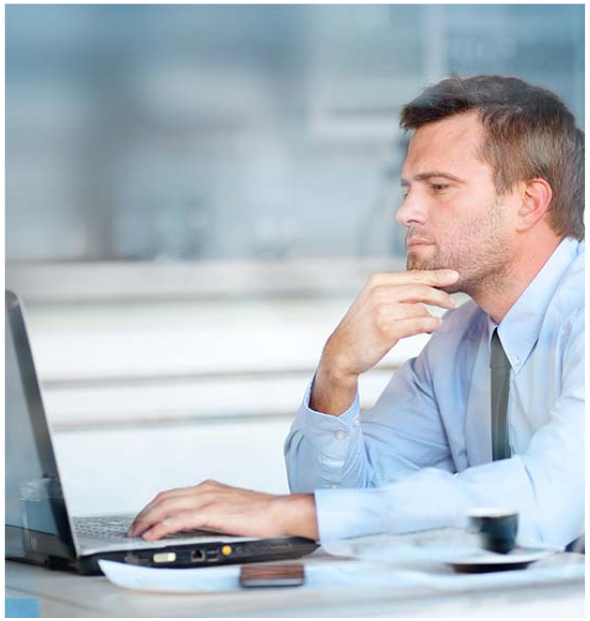
Reputation Matters

Company Struggles

The early bird doesn't always catch the worm.

- **Move quickly – but not too early**
  - Resist communicating numbers early in the investigation
  - Be careful of claiming the issue is fully resolved
  - Focus initial messages on the steps being taken to investigate the issue

- **"Facts" are fluid**
  - Avoid dissemination of inaccurate information
  - Compromising more data
  - Damaging company reputation further by breaking trust again



Dealing with a Live Security Incident

Manage the Message

- Think of your customers are your North Star
- Don’t neglect the wide variety of stakeholders interested in breaches
- Be lean, but integrate groups into communications planning
- Think through what you push out via social media
- Conduct media training for executives
- Monitor traditional and social media
- Develop a long-term reputation recovery strategy

Communicating to Internal Audiences

Keep Your Employees Informed and Engaged

"Me to We": Addressing concerns and engaging employees in the solution

Types of Threats

- **Payments** – Steal payment data to sell on the black market; typically done via malware or direct attacks on web infrastructure

- **DDOS/DOX** – Denial of Service attack disrupts the availability of a website or internet service. DOX exposes personal information to cause difficulty or embarrassment of an orgs leadership.

- **Personal Health Info (PHI) Loss** – Loss of patient health information that brings federal regulatory demands for notification. Considered by consumers to be some of the most sensitive info that can be lost.

- **Product Vulnerability** – Security vulnerability or misconfiguration is found in a network enable device or online service (bug). The severity is dependent upon the application of the device.

- **IP Lost** -- Competitive advantage typically conducted by rouge nation-states.

- **Personally Identifiable Information (PII)** -- Loss of customer/employee information (e.g. DOB, SS#, etc.) that brings different state regulatory demands for notification. Can cause significant difficulty for those affected due to time intensive remediation.

Brand Recovery

The Goals are CLEAR

- Protect client relationships
- Respond swiftly to client concerns
- Chart a course for preparation

Brand Recovery: Strategies

Strategies

- Creating a consistent, credible story about company's strengths, areas for improvement and commitment to excellence in data security.
- Setting a sustained course to build awareness, comprehension and thought leadership for the company and its executives.
- Maximizing our efforts through an engagement model that crosses multiple channels, drives message penetration across audiences and leverages third parties for credibility, where applicable.

Brand Recovery: Tactics

Tactics

- Develop a message framework
- Establish relationships
- Reach out to partners
- Leverage existing industry events
- Create content
- Develop an expert positioning document

Thank You

#PrivacyAcademy

#CSA Congress