PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Tips & Traps

Placing and Underwriting a Cyber Policy

Jesse Ammons

TRAVELERS

Michael Murphy

Endurance | ENDURANCE INSURANCE

Robert Rosenzweig

RS RISK STRATEGIES COMPANY

Marisa Combs - Moderator

LT LEWIS THOMASON

PLUS

Client/Broker Education

- Depending on industry and size of potential buyer, a great deal of education can be necessary
- New and developing exposure; less focus on this issue in the Middle Market
- Need to create understanding of threat matrix and regulatory environment
- Product education also required due to developing market and variation of products

PLUS

Application Process

- Applications & Supplemental Information
- Follow Up Questions
- Warranty Statements
- Meeting or Conference Call vs Written Submission
- Broker/Applicant Presentation Preparations
- Shortened Renewal Process

PLUS Negotiation of Terms/Conditions

- Identify Top Cyber Exposures
- Define Coverage Goals
- Approach Carriers with Coverage Goals Outlined in Advance
- Compare Coverage Wording
- Explain Limitations of Available Coverage to the Buyer

PLUS

Market Appetite

- 30 + insurers offering some modicum of Cyber Risk coverage
- Cyber Crime and traditional Cyber Liability
- Monoline & on other policies via endorsement
- Insurer appetite and coverage offering segmented by size of Insured & Industry Vertical

PLUS Coverage – Offering and Language

- 1st party coverages
- Contingent Business Income
- PCI Coverage
- Regulatory Coverage – Fines and Penalties
- Reputational Harm
- Social Engineering
- Computer System Property Damage
- Prior acts

PLUS Coverage – Industry Segments

- Certain industry verticals have become more volatile, creating stricter underwriting guidelines and limited capacity
  - Financial Services
  - Retail- Point of Sale
  - Healthcare
  - Higher Education
  - Technology
- As the exposure and the products continue to develop, specific coverage specifications and enhancements have materialized for certain industry verticals

PLUS

Changes in Underwriting

- Middle Market vs. Large National Accounts (depending on how you define these)
- Underwriting by Class of Business
- Breaches Dictating Underwriting
- Aggregation of Risk
- Small Business

Developments in Buying Influences

- Terrorism
- Coverage Litigation Decisions
- Dependent Business Interruption
- Internet of Things
- Property Damage/Bodily Injury
- Bitcoin & Other Cryptocurrencies

PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Data Breaches

How to prepare for and respond to the inevitable

David Cole

FMG LAW Freeman Mathis & Gary, LLP Attorneys at Law

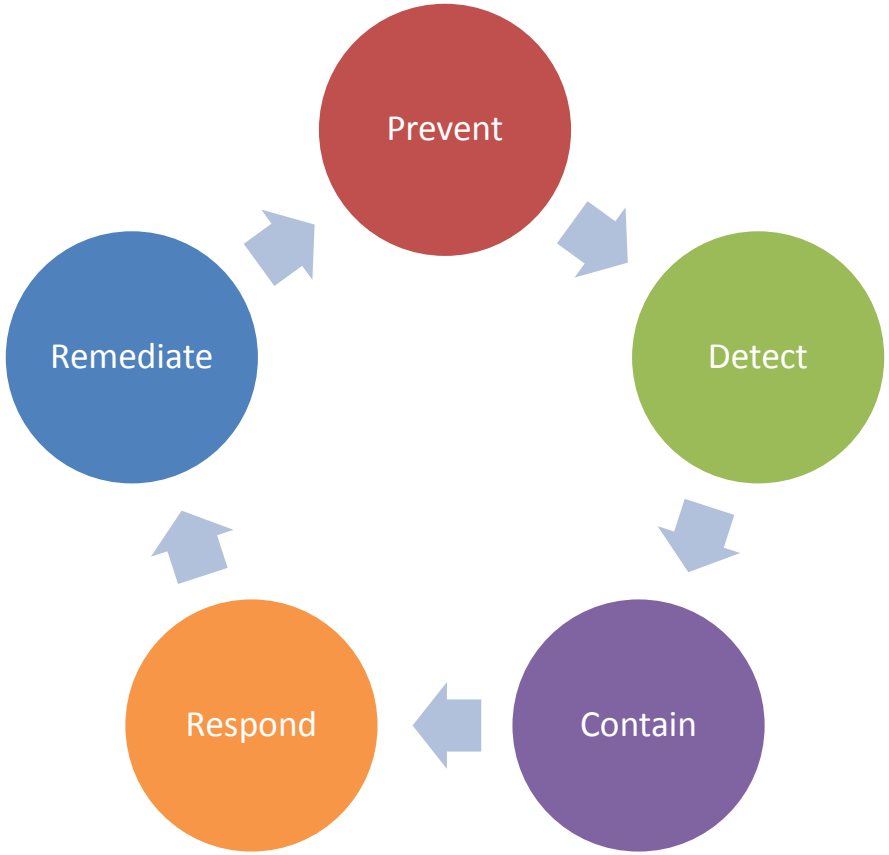
Tom Rizzuto

TRAVELERS

Brad Adler - Moderator

FMG LAW Freeman Mathis & Gary, LLP Attorneys at Law

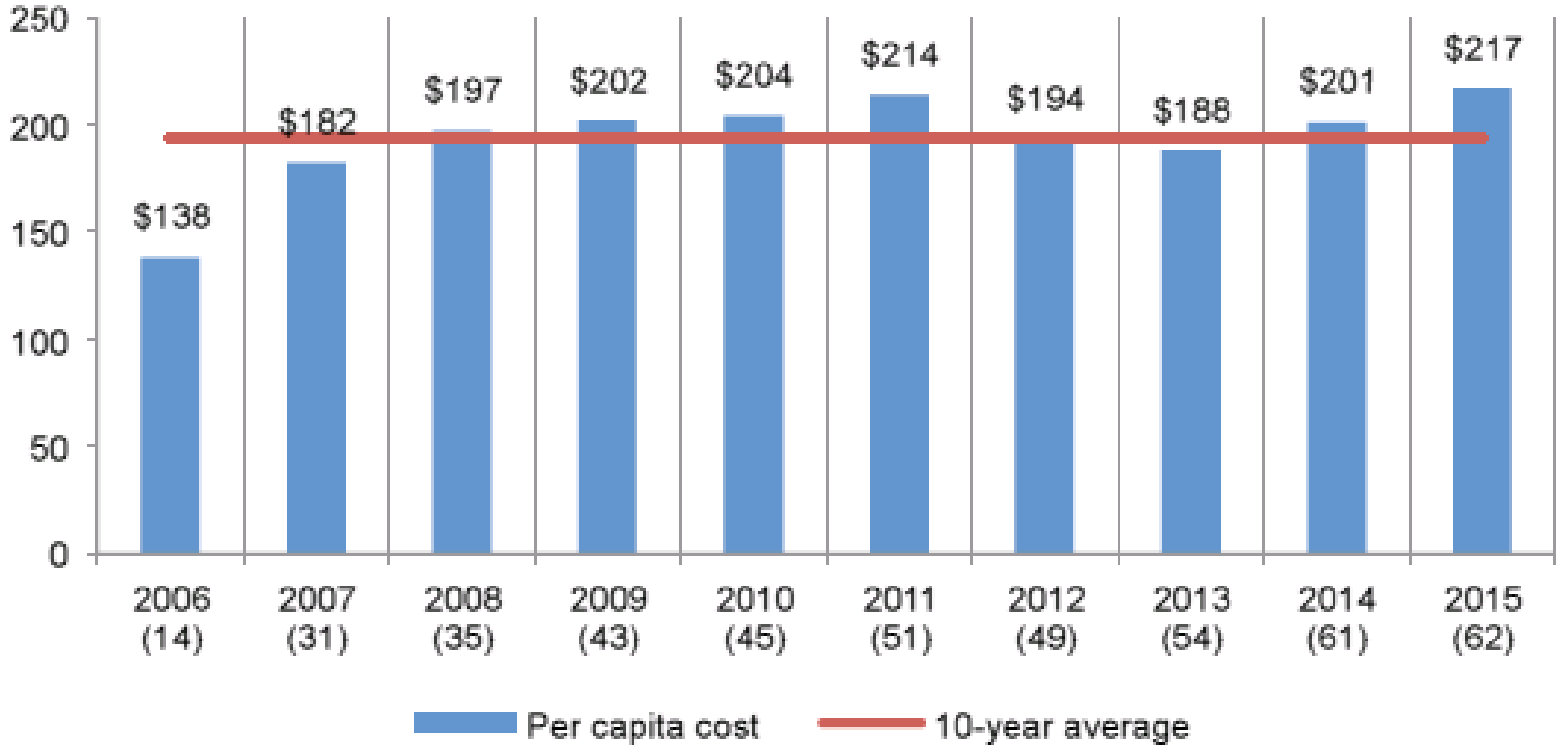
Data Breach Life Cycle



PLUS

Costs of a Data Breach

Figure 1. The average per capita cost of data breach over 10 years
Bracketed number defines the benchmark sample size

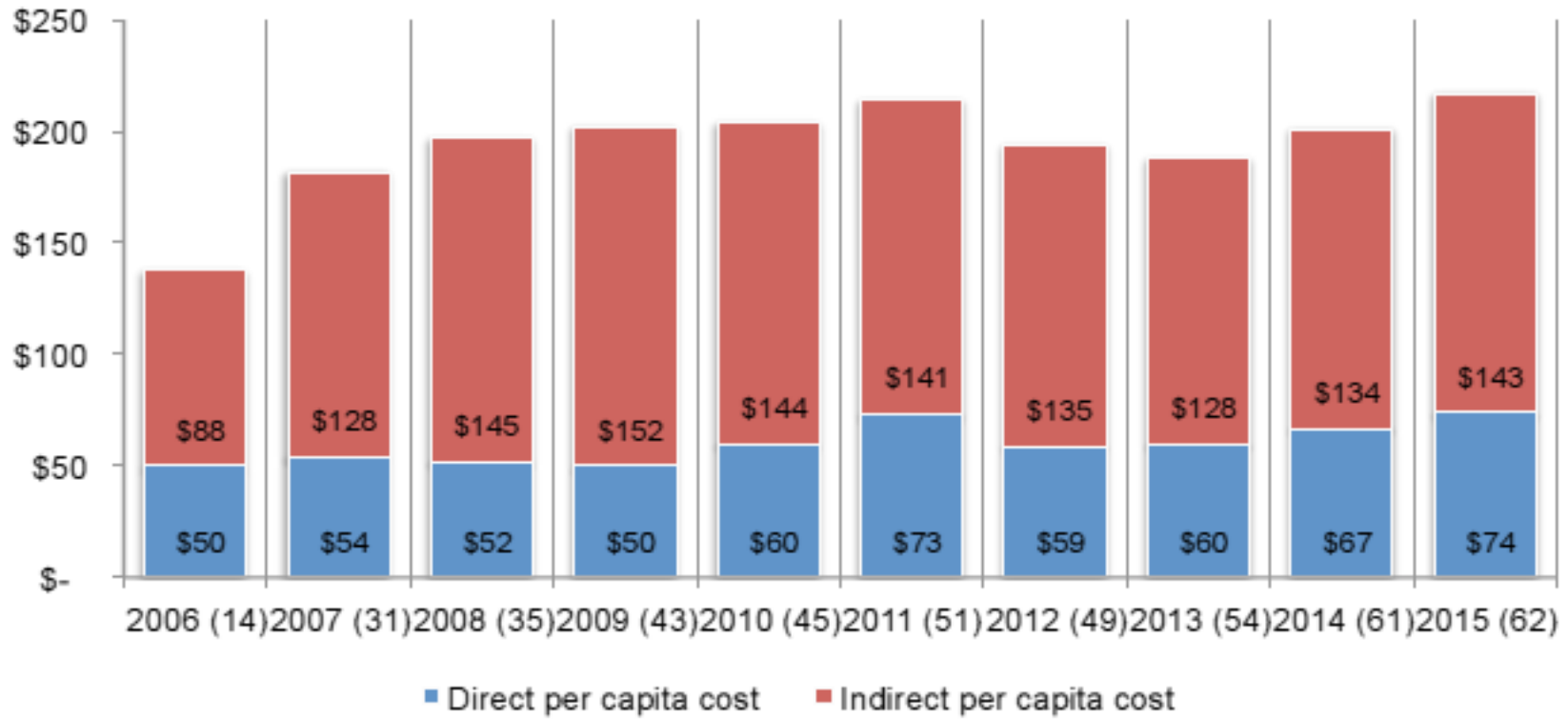


Ponemon Institute 2015 Cost of Data Breach Study
http://www.ponemon.org/library/2015-cost-of-data-breach-global

PLUS

Direct and Indirect Costs

Figure 15. Direct and indirect per capita data breach costs over 10 years

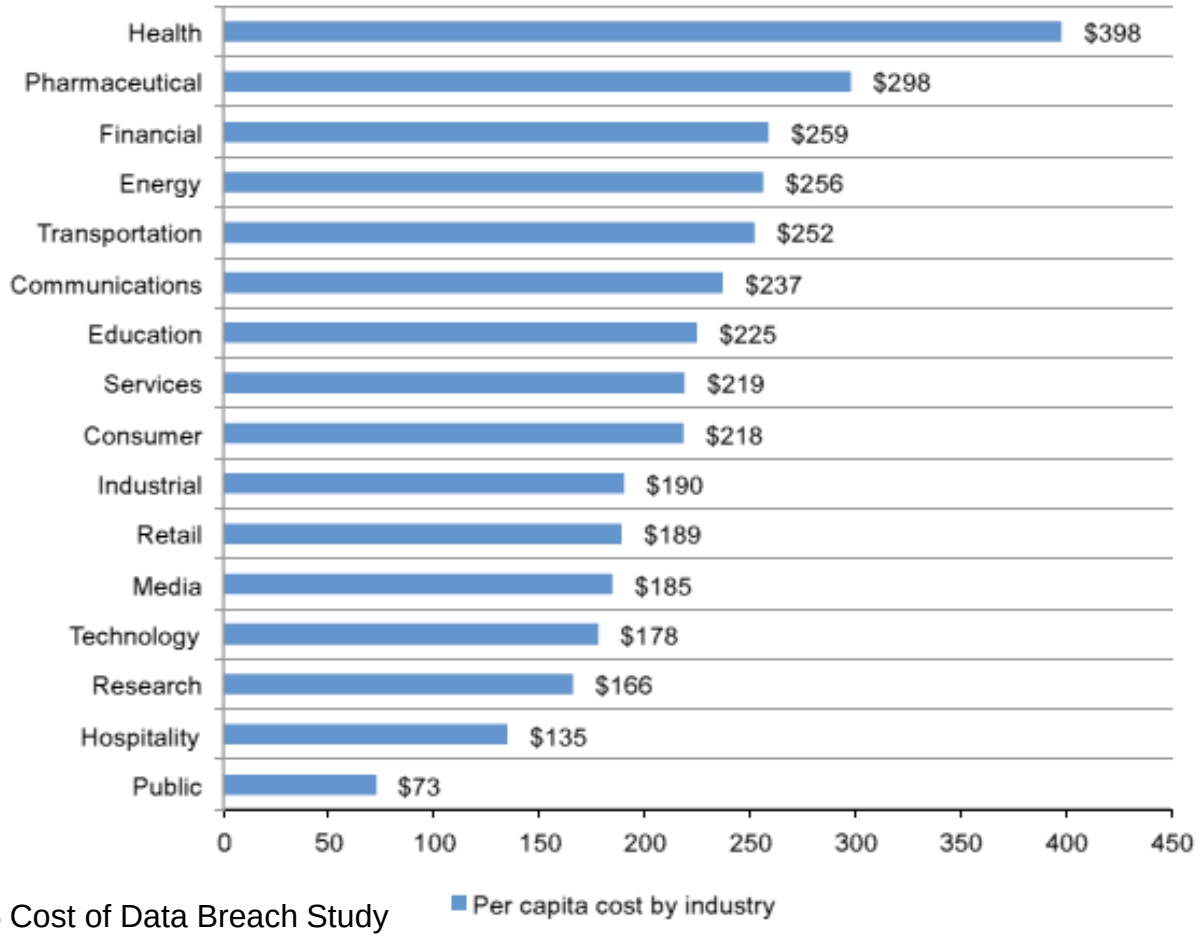


Ponemon Institute 2015 Cost of Data Breach Study
http://www.ponemon.org/library/2015-cost-of-data-breach-global

PLUS

Costs by Industry

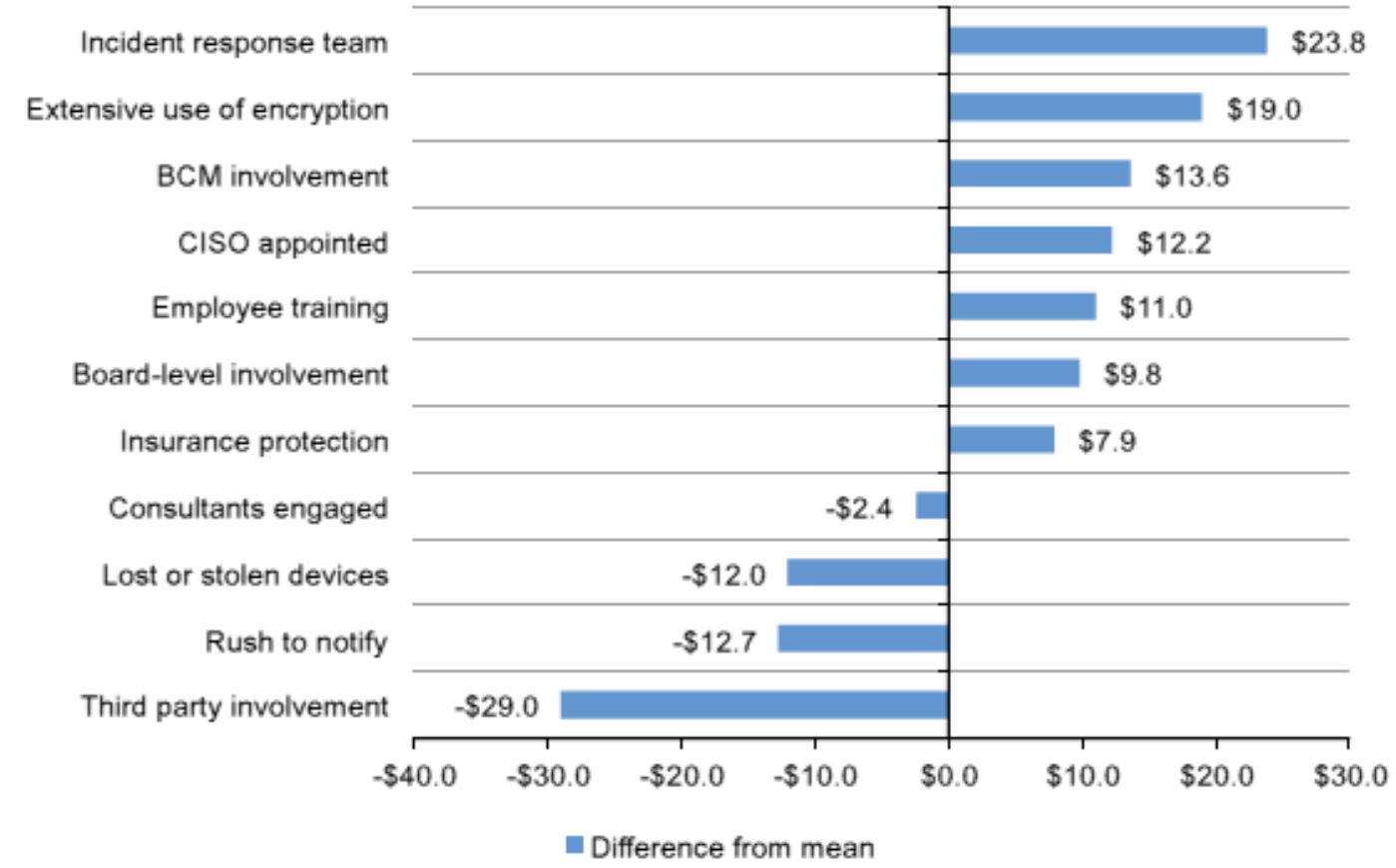
Figure 4. Per capita cost by industry classification of benchmarked companies



Ponemon Institute 2015 Cost of Data Breach Study
http://www.ponemon.org/library/2015-cost-of-data-breach-global

Factors Affecting Cost

Figure 7. Impact of 11 factors on the per capita cost of data breach



Ponemon Institute 2015 Cost of Data Breach Study
http://www.ponemon.org/library/2015-cost-of-data-breach-global

Data Breach Response Team

- Typically coordinated by CIO/CISO
- Other members from divisions that also could be source of or affected by breach: sales, human resources, operations, finance/accounting
- Legal counsel (cyber/data breach experience)
- Computer forensics vendor
- Public relations company
- Insurance claims professional

PLUS

Data Breach Response Plan

- Identify team members (contact list)
- Identify sources of data and risk
- Define what constitutes a breach
- Process for investigation (who, what, when?)
- Process for containing threat and preserving evidence (e.g. offline)
- Process for notification
- Post-incident remediation

PLUS

Other Useful Forms

- Incident report form
- Emergency response communication plan
- Data breach response checklist
- Chronology of events
- Chain of custody forms

PLUS

Training Your Workforce

- Create a culture of security that starts from the top – make it a “boardroom issue,” not an “IT department issue”
- Traditional in-house training
- Internal phishing campaign/testing
- Services offer online videos, weekly emails, etc.

PLUS

Containing the Breach

- Disconnect, but do not unplug, reboot, or run anti-virus or scanning software
  - Do not attempt to repair damages/broken system
  - No action that could overwrite data on affected system
- Change passwords
- Disable remote/external connections
- Notify insurance carrier and outside counsel
- Notify law enforcement
- Do not rush to notify affected people

PLUS

Investigation

- Legal counsel should direct the process and all communications and retention of vendors
- Maintain chronology of events and records of the chain of custody of physical items
- Use forensic analysis to determine:
  - How breach occurred
  - When it occurred
  - Who has been affected
  - What data was disclosed

PLUS

State Notification Laws

- 47 states have adopted some form of data breach notification law
- Require prompt notification, and some establish penalties and rights of action
- Typically define data breach, types of protected information, and thresholds for the notice requirement
- States without laws: Alabama, New Mexico, and South Dakota

PLUS

Federal Laws

- Healthcare: HIPAA
- Financial: Gramm-Leach-Bliley Act
- Public companies: Sarbanes-Oxley Act
- Federal regulatory agencies:
  - Federal Trade Commission
  - Consumer Financial Protection Bureau
  - Federal Communications Commission
  - Department of Health and Human Services

Non-Government Regulatory Action

- Financial Industry Regulatory Authority (FINRA)
- Payment Card Industry Council
  - Designed to establish common security guidelines
  - PCI DSS

PLUS

Georgia Personal Identify Protection Act

- Passed in 2005
- Amended in 2007 to apply to state and local governments
- Requires covered entities to provide notice to affected Georgia residents and others in the event of a breach of covered information

PLUS

Covered Entities

- “Information broker” – anyone who, for monetary fees or dues, collects personal information for primary purpose of furnishing it to third parties
- “Data collector” – any state or local government, except agencies whose records are kept primarily for traffic safety, law enforcement, licensing, or access to court or property records

PLUS

Covered Information

- First name or initial and last name plus:
  - Social security number
  - Driver's license number or state ID number
  - Credit, debit, or account number
  - Account passwords or PINs
  - Any combination of above when not in connection with name if sufficient to attempt identity theft
- Does not include encrypted, redacted, or publicly available information

PLUS

Notification Required

- Timing: “in the most expedient time possible and without unreasonable delay.”
- Scope: “to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”
- If more than 10,000 residents affected, must also notify consumer reporting agencies that compile info on nation-wide basis.

PLUS

Form of Notification

- Three primary methods: written notice, telephone notice, and electronic notice consistent with 15 U.S.C. § 7001.
- Substitute methods include email, website, or major state-wide media if:
  - Cost of primary methods exceeds $50,000
  - More than 100,000 individuals affected
  - Not enough contact information for primary notice

PLUS Communicating About a Breach

- Timing
- Explain in straight-forward and honest manner:
  - What occurred
  - What data was disclosed
  - What you are doing to fix it
  - What people should do to protect themselves
- Consult law enforcement first
- Standard to offer credit monitoring services

PLUS

Remediation

- Meet with your Incident Response Team to debrief after a data breach
  - What worked and what did not
  - How can security be improved?
  - How can our response be improved
  - Do changes need to be made to your policies?
- Communicate with your employees and reinforce the importance of awareness and security