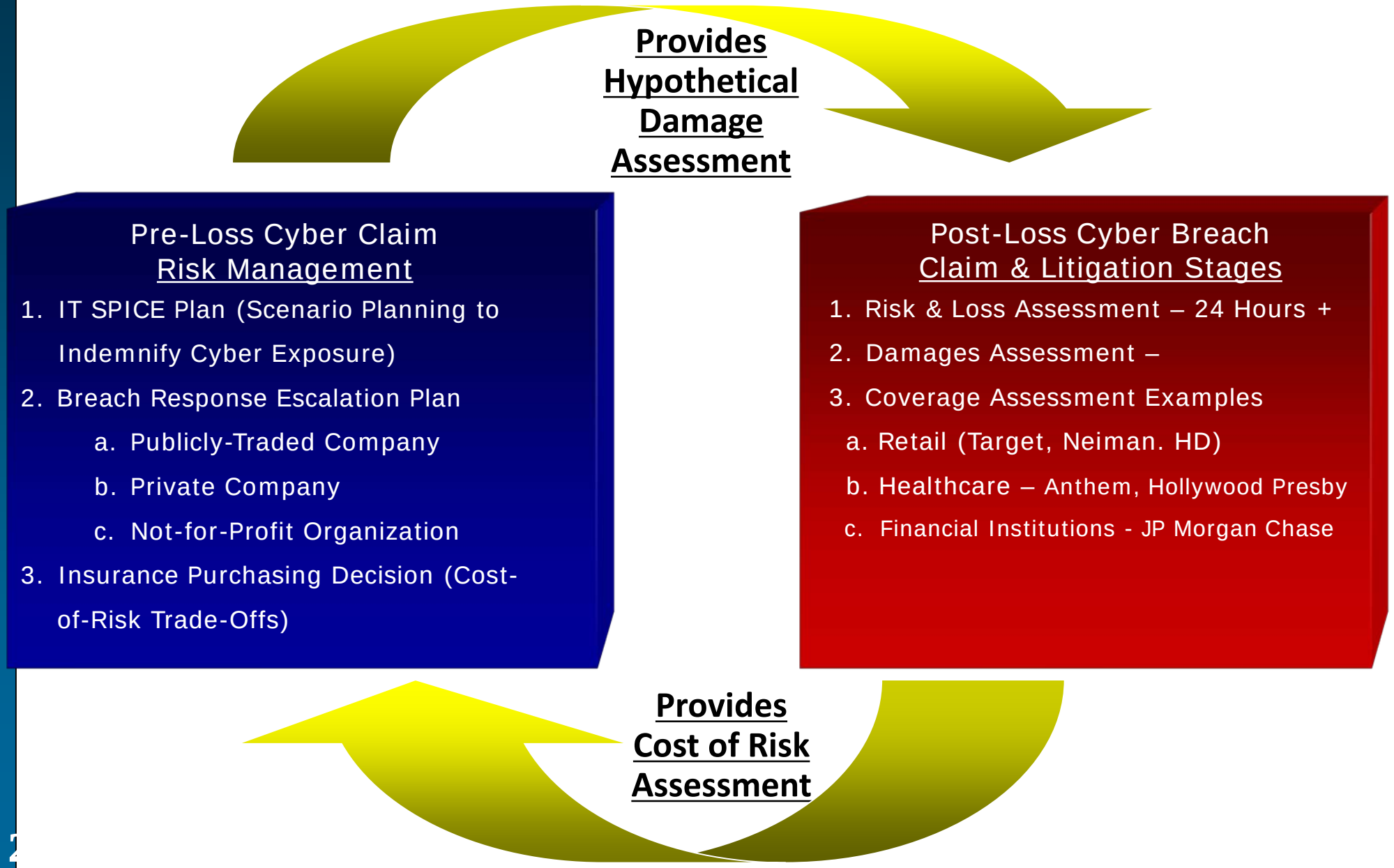
Information Security, Privacy Liability & Breach Response: A Risk Management Approach to Preparedness

September 29, 2016

Steve McElhiney
EWI Re, Inc.
Three Lincoln Centre
5430 LBJ Freeway, Suite 1595
Dallas, Texas 75240
972.560.0675
smcelhiney@ewirisk.com

Cyber Liability Claims Analysis:
The Benefit Of A Post-Loss Review For Pre-Breach Planning



Information Security & Privacy Liability Insuring Agreements

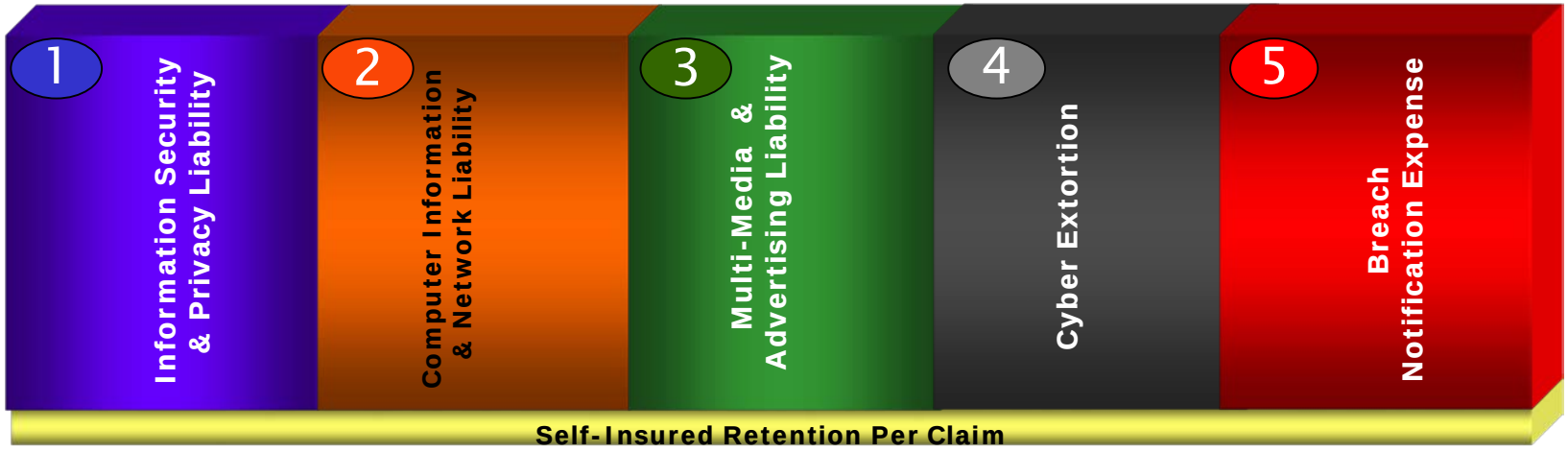
1 **Information Security & Privacy Liability Insuring Agreement:** Defense expense and compensatory damages for any actual or alleged breach, violation or infringement of any right to privacy, consumer data protection law, or other legal protection for personally identifiable information (including HIPPA & HiTech Acts), including but not limited to breach of a person's right of publicity, false light, intrusion on a person's seclusion, public disclosure of a person's private information, or misappropriation of a person's picture or name for commercial gain;

2 **Computer Information/Network Liability:** Negligence claim(s) as a result of a failure to prevent unauthorized access, use or tampering with data or systems, accidental introduction of malicious code in data systems and failure to prevent denial of service attacks or negligent misrepresentation & related IT security failures, & cyber extortion. Breach response expense and Crisis Management expense sub-limits included.

3 **Electronic Multimedia, Advertising Liability & Website Media Content Liability:** Libel, slander, defamation, disparagement, invasion of privacy, breach of confidentiality, or public disclosure of private facts including copyright, trademark infringement, cyber squatting violation & others.

4 **Cyber Extortion Coverage (1st Party):** A direct or indirect illegal threat from a third-party to damage, destroy or corrupts company website, intranet, network, computer systems, or any programs or data held electronically and/or the dissemination, divulgence, or use of any commercial information for which company is responsible which is not in the public domain and will cause commercial harm if made public – from a third-party who then demands a ransom for their own benefit as a condition of not carrying out this threat.

5 **Information Breach Notification Expense:** all reasonable and necessary expenses incurred necessary to comply with the data security breach notification requirements of federal, state or local statute, rule or regulation, or of a judgment, settlement, or other legal obligation. Credit Monitoring Services, Crisis Management & public relations expense, and computer forensic expense included.



Claims & Litigation Stages: Three Area's to Manage

Phase I
Post-Breach
Risk/Loss Assessment

1. Implement Incident Response Plan
   a. Key internal personal meeting
2. Engage Outside Vendors
   a. Outside counsel/Breach Coach Specialist
   b. Other Outside Vendors
3. Notification (Harm or acquisition trigger by state)
4. Regulatory

Phase II
Post- Breach
Damages Assessment

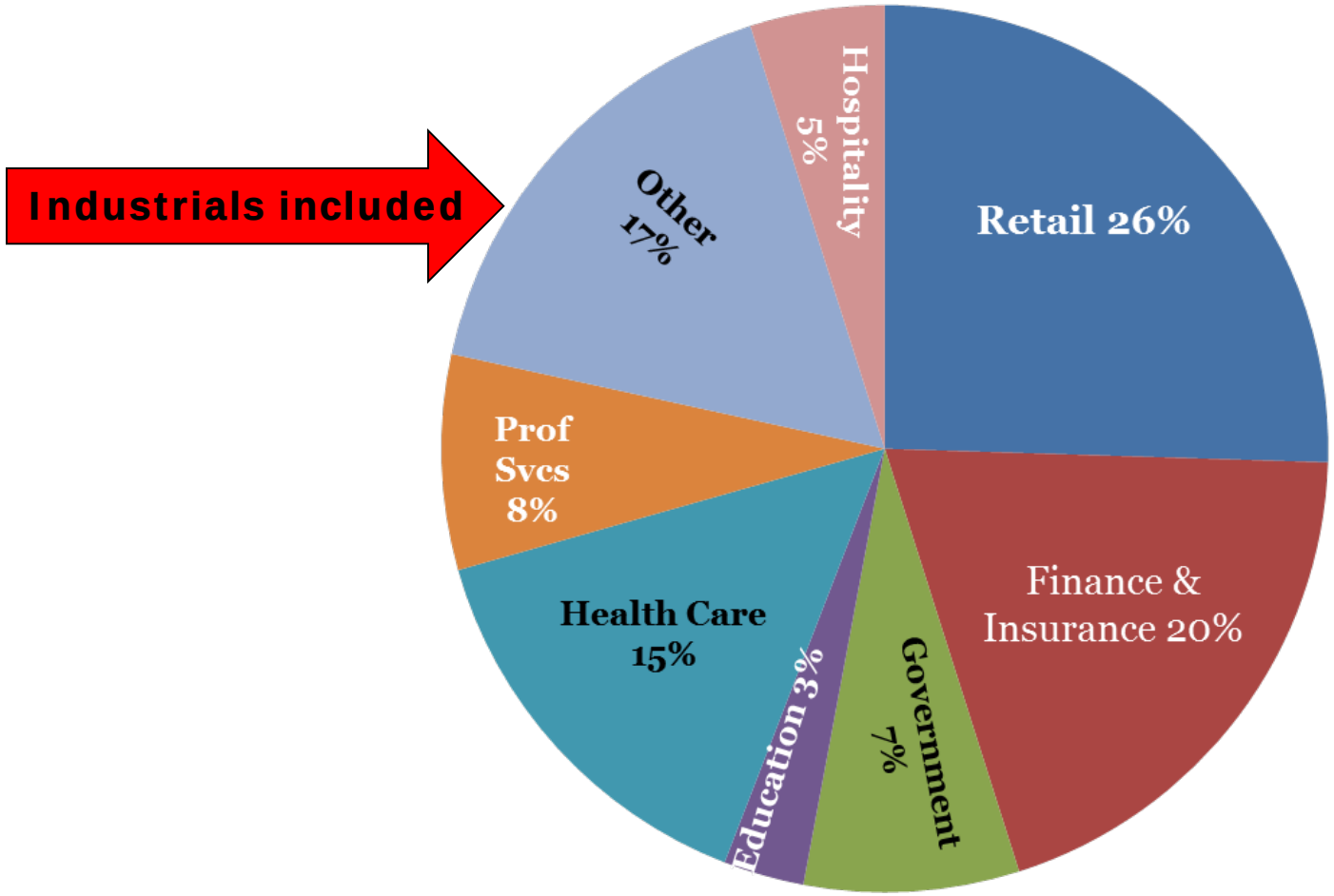
1. Analysis of harm to individuals or Corporation (PII, PHI, PCI, IP)
2. Fines & Penalties (AG, Agency, VISA/M-C Breach)
3. Tort & Statutory Liabilities

Phase III
Post-Breach
Coverage Assessment

1. Traditional Insurance vs Cyber Liability Insurance
2. Claim-Made policy
3. Defense Cost Erosive Policies

State of California – 2014 Breach Statistics

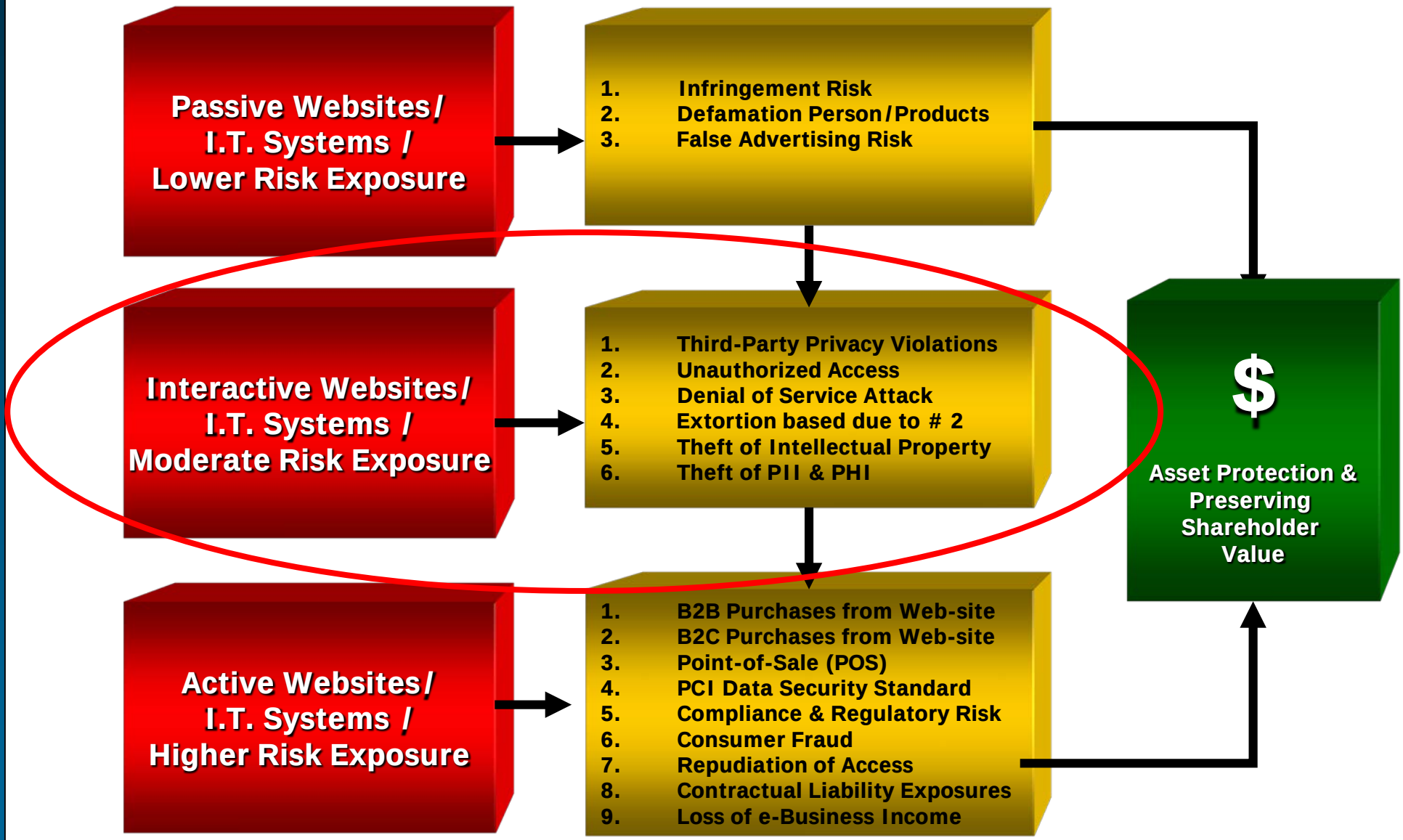
Breaches by Industry Sector*



* Data Breach Report 2014, Kamala D. Harris, Attorney General
California Department of Justice, Privacy Enforcement & Protection Division
www.oag.ca.gov/privacy

Cyber Liability Risk Categories' & Exposure Matrix

I.T. & e-Business Risk Identification & Assessment



Breach Response Escalation Plan – 5 Steps

Pre-Breach Response Planning

- Identify Internal Response Team & Incident Lead Person
- Establish Analysis & Communication Protocol (The Team)
- Complete Data Breach Response Plan
- Evaluate Vendor & Customer Notification Requirements
- Remediation & Recovery Vendors
- Stress Test Response Plan
- Fraud Prevention

Incident Analysis

- Contact the Team
- Identify Information (PII, PHI, Payment Card compromised)
- Breach Containment
- Harm Determination Forensic Analysis
- Legal Analysis
- Security Breach Incident Analysis:
  - California
  - United States
  - Globally

Incident Disclosure

- Analyze Requirements
- Consider Alternative Notice Methods
- Notify in compliance with laws
- Consider third-party vendors for notification
- Stagger Notification
- Public Reporting
- Cyber Insurance Carrier Notification

Loss Mitigation

- Credit Monitoring
- Fraud Monitoring
- Documentation and discoveries manifest
- Customer Service
- Human Resources

Communication And Remediation

- External Solutions
- Consumer Protection Notification Letter
- Customer Hotline Number Established
- Breach Website ?
- Senior Management Updates
- Human Resource Updates
- Cyber Carrier Communications
- D&O Carrier Noticed (if material)
- Limit Communication