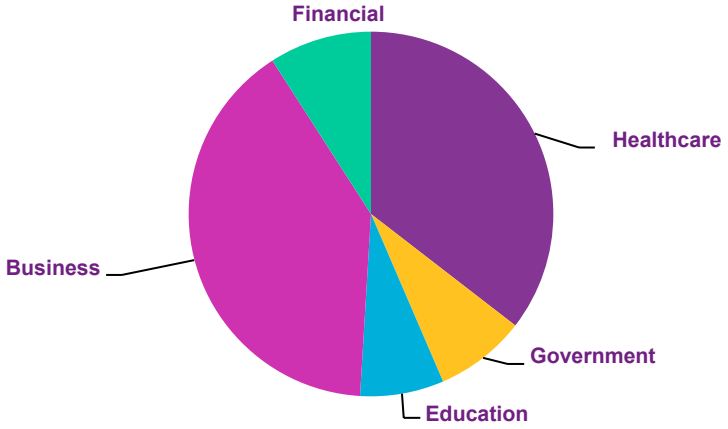
An Overview of Cyber Liability

Central Virginia Employee Benefits Council
Annual Meeting - June 1, 2016

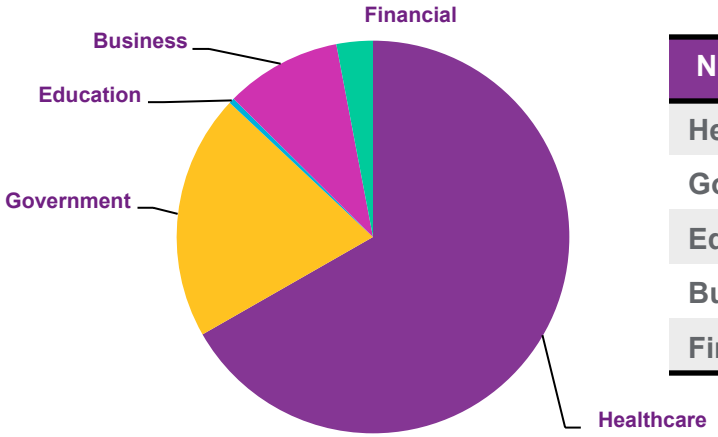
Jarrod Sudduth
Willis Towers Watson

Data Breach Statistics

2015 Statistics: Identity Theft Resource Center



Number of Breaches	
Healthcare	277
Government	63
Educational	58
Business	312
Financial	71



Number of Records Exposed	
Healthcare	112,832,082
Government	34,222,763
Educational	759,600
Business	16,191,017
Financial	5,063,044

The Identity Theft Resource Center has been tracking data breaches by sector since 2005. These graphs reflect their 2015 stats of reported data breaches as 1/4/2016.

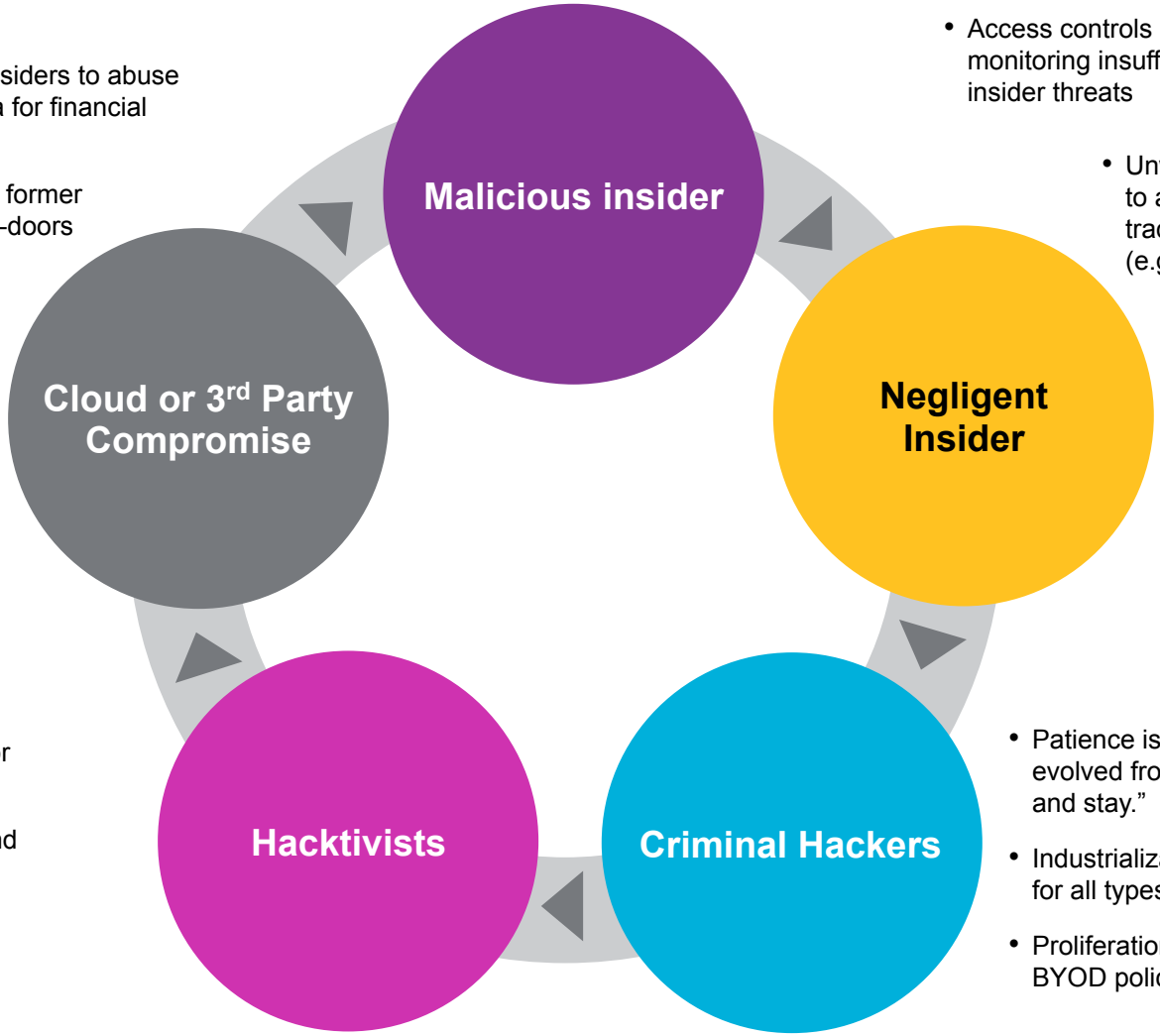
In 2015, the Healthcare Sector had the highest severity with 12,832,082 records exposed resulting from 277 reported data breaches.

The Business Sector had the highest frequency with 312 reported data breaches exposing 16,191,017 records.

Source: www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

The Threat Environment

- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors
- Theft of Intellectual Property
- Security compromise – loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim



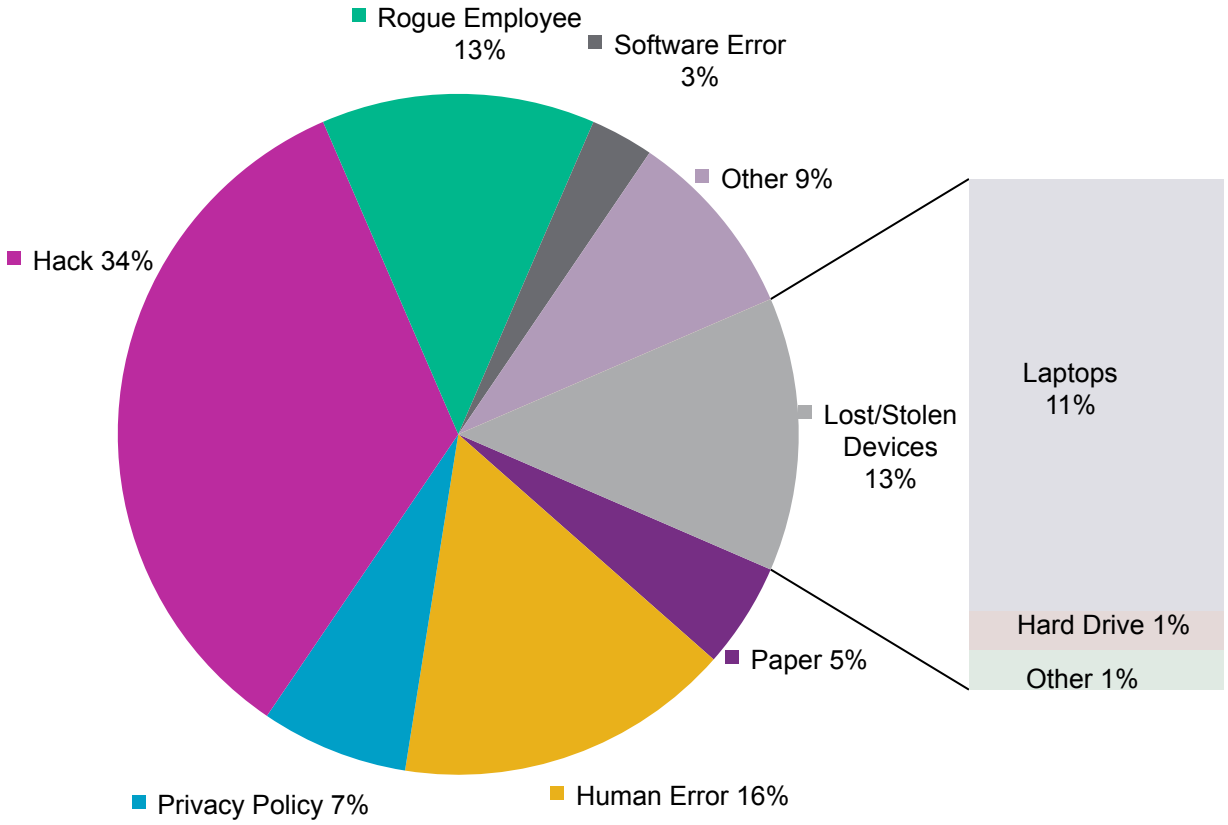
- Access controls and behavior monitoring insufficient to detect insider threats
- Unwary insiders susceptible to attacks that exploit traditional security controls (e.g. spear phishing)
- Users who fail to embrace “culture of security” will find ways to circumvent ‘inconvenient’ security controls

- Intent is to disrupt and/or embarrass a target
- Motivations are fickle and unpredictable
- Massive DDoS attack

- Patience is a virtue. Tactics have evolved from “hit and run” to “infiltrate and stay.”
- Industrialization - Black markets exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors

Chubb/ACE Cyber Claims and Industry Trends

3 Year Trend - as of 10/2015



Industry Breakout 2013-2015:

- Healthcare – 31%
- Technology – 9%
- Professional Services – 15%
- Retail – 9%
- Financial Institutions – 6%

Targeted Attacks for PII:

- Lost/Stolen Devices
  - 2013 – 17%
  - 2014 – 12%
  - 2015 – 11%
- **Hack**
  - 2013 – 29%
  - 2014 – 27%
  - 2015 – 43%
- **Rogue Employee**
  - 2013 – 14%
  - 2014 – 16%
  - 2015 – 11%

2015 Average Cost of a Data Breach in the U.S. = $6.5M

Costs Increased 11% in 2015

Factors Impacting Data Breach Costs

Factors Decreasing Costs

- Incident Response Team (IRT) = $12.60
- Extensive Use of Encryption = $12
- Employee Training = $8
- Business Continuity Management (BCM) = $7.10
- CISO Appointed = $5.60
- Board-Level Involvement = $5.50
- Insurance Protection = $4.40

$55.20 ⬇

Factors Increasing Costs

- Consultants Engaged = $4.5
- Rushing Notification = $8.90
- Lost or Stolen Devices = $9.00
- Third-Party Error = $16.00

$38.40 ⬆

Average Per Capita Cost	Implementing Decreasing Factors	Implementing Increasing Factors
U.S. = $217	$161.80	$255.40
Globally = $154	$98.80	$188.40

Source: 2015 Ponemon Cost of a Data Breach Global Study, sponsored by IBM; * Per Compromised Record

U.S. Cost Per Record $217= $143 Indirect (Abnormal Turnover/Customer Churn);$74 Direct (Notification/Legal Fees Forensics)

These factors are significant. Considering a breach scenario in the U.S. involving 50,000 PII records. At the average cost per record of $217, total breach costs would be **$10,850,000**; with implementation of cost decreasing factors, total breach costs would be **$8,090,000** and with application of the increasing factors, the total breach cost would be **$12,770,000**.

The History of Cyber Liability Insurance

The Early Challenges of Cyber Coverage

- First policy written in 1997 by AIG
  - Third-party liability only for breaches outside of the insured company
- Limited availability in the marketplace
- No loss data to assist in underwriting coverage or pricing
- Variability in coverage made comparisons difficult
- Slow-paced evolution of coverage
- Early predictions for the growth of coverage fell considerably short

The Evolution of Cyber Coverage

- Coverage later broadened to include first-party coverage for the entity, but malicious employee activity was excluded
- Next round of expansion provides cover beyond the virtual world of electronic information, resulting in both network security and privacy insurance policies
- Policy enhancements in recent years include:
  - Business Interruption
  - Data Restoration
  - Network Extortion
  - Computer Forensics
  - Legal and PR Expenses
  - State Breach Notification Laws
    - Lead to surge in cyber policy demand
  - Fines and Penalties
    - Defense and Penalties

Cyber Liability Insurance Structure

Cyber Liability Insurance – Main Coverage Parts

First-Party Coverage

- Network Extortion - Covers extortion monies and associated expenses arising out of a criminal threat to release sensitive information or bring down a network unless such consideration is paid.
- Business Interruption - Indemnification for loss of income and incurred extra expenses that arise directly out of a network security breach that occurs on the policyholders' systems.
- Digital Asset Loss - Indemnification for costs to recreate, rebuild or recollect digital information assets that were directly damaged as a result of a network security breach that occurs on the policyholders' systems.

Breach Response/Crisis Management Fund

- Legal Data Breach Coach
- Forensics Investigation Expenses
- Notification and Call Center Services
- Public Relations/Crisis Communications Costs
- Credit Monitoring/Credit-Fraud Remediation Services

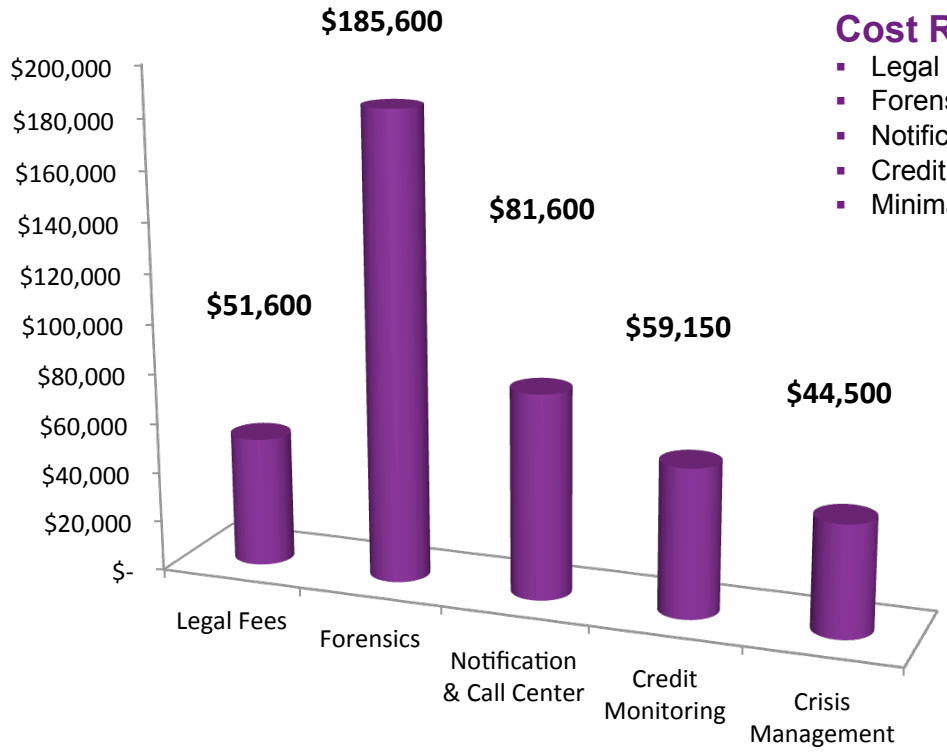
Third-Party Coverage

- Network Security Liability - Affords legal defense costs and indemnity for third-party claims alleging failure to protect against transmission of malicious code, denial of service attacks and unauthorized access and/or use of computer systems.
- Privacy Liability - Affords legal defense costs and indemnity for third-party claims alleging negligent use or disclosure of non-public personally identifiable information (PII) and corporate confidential information.
- Internet Media Liability - Affords legal defense costs and indemnity for third-party claims alleging wrongful acts (i.e. defamation, disparagement, copyright/trademark infringement) in the dissemination of internet content and media.
- Regulatory Actions - Affords legal defense costs for regulatory actions brought by federal regulators such HHS/OCR (HIPAA/HITECH); FTC (COPPA,GLBA), FCC (TCPA) or State Attorneys General (State Breach Notification Laws).
- Regulatory Fines/Penalties - Covers monetary fines or penalties resulting from failure to comply with state or federal laws.
- PCI DSS Violation Coverage - Covers monetary penalties resulting from the failure to comply with PCI DSS requirements.

Every Breach is Unique

Average Cost - 1st Party Expenses
Chubb/ACE Claims 10 Year Trend as of 10/2015

The circumstances or cause of the breach has a major impact on the First Party Response Costs. A lost lap top or mobile device is different than hack attack, extortion attempt or a phishing campaign; however, the costs of forensics is typically the highest.

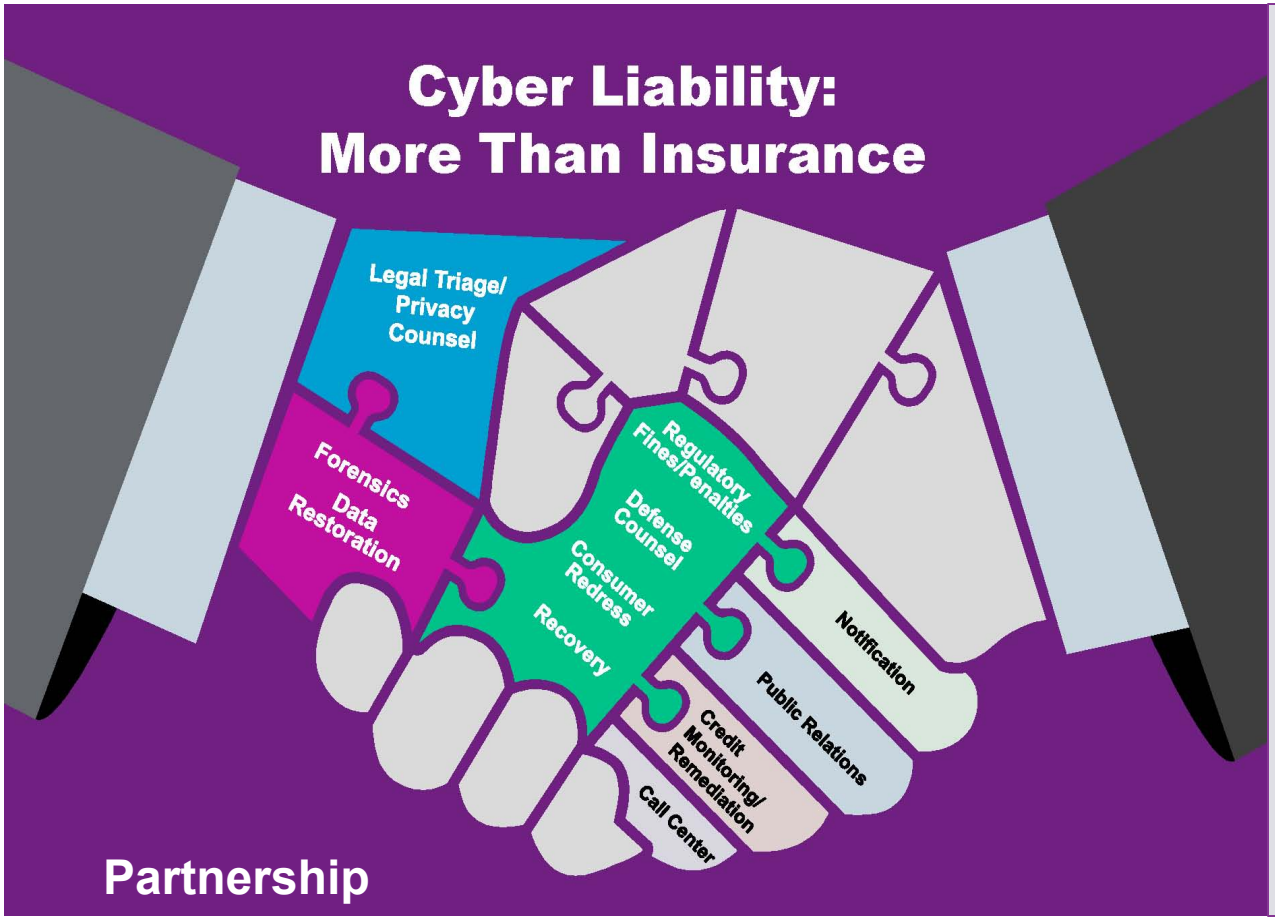


Cost Range of Each Service

- Legal Fees: Under $5,000 up to about $50,000
- Forensics: $10,000 to Seven Figures
- Notification & Call Center: Up to $80,000
- Credit Monitoring: Payment per Enrollee or Restoration Service
- Minimal Crisis Management Costs

Cyber Liability Insurance Pays

Unlike other third-party professional liability policy coverage forms; Cyber Liability policy forms can include first-party coverage parts that pays for the immediate first-party breach response expenses, in addition to, loss of income resulting from network failures; extortion expenses as well as fines or penalties associated with regulatory actions.



Partnership

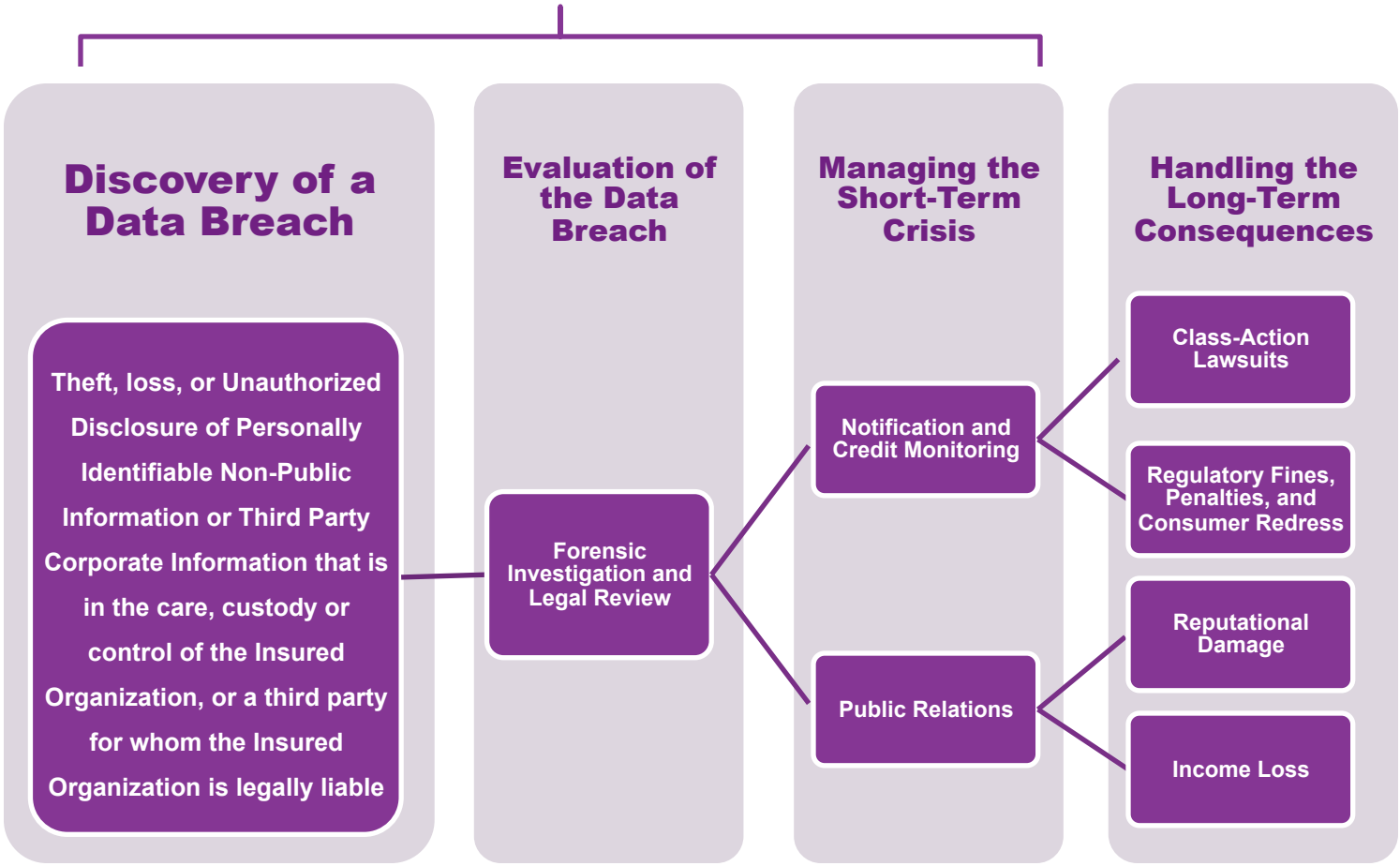
Most Cyber Liability insurers offer their policyholders a choice of breach response services, typically from a list of pre-approved vendors. Many allow the policyholders own choice of vendor.

Most insurers also grant policyholders access to a complimentary cyber risk management portal that includes the most updated information on emerging cyber threats and the latest reports on risk mitigation measures and practices.

Carrier Partnership

Cyber Liability insurers partner with policyholders to help mitigate risks

Unlike other professional liability policies, Cyber Liability policies include a dynamic response fund for these immediate expenses in the wake of a data breach, which aides organizations in their incident response efforts.

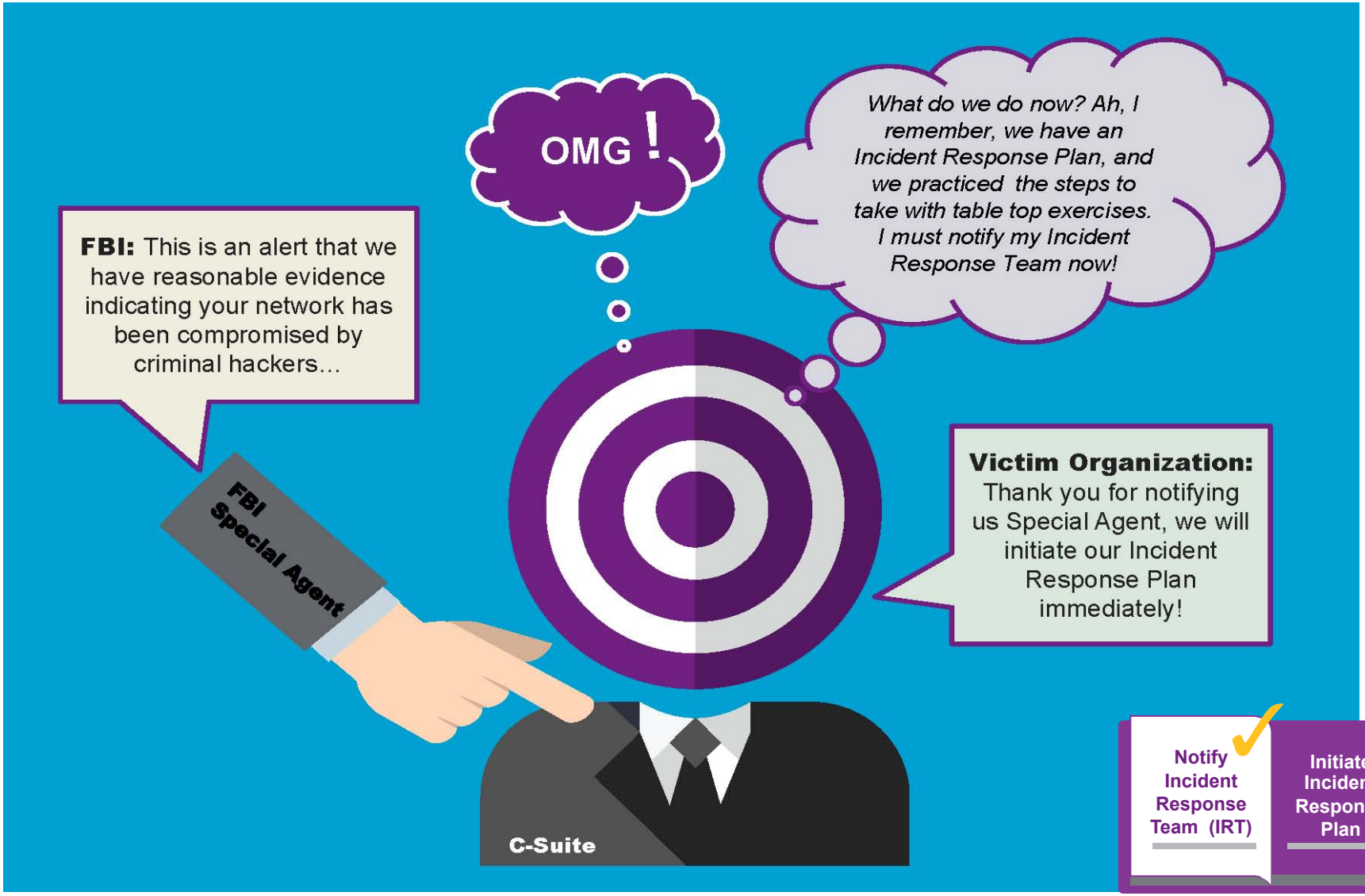


Cyber Insurance Marketplace

- Total annual Cyber premiums have reached $2B. Some industry observers expect premiums to reach $20B by 2025.
- The market is in a state of flux, especially for healthcare organizations. Traditional, low-profile risks can expect with renewal rates from 0% to +10% while Point of Sale retailers and healthcare organizations may experience higher increases (50 - 100%) due to the facts established out of the large headline breaches. Smaller to mid size healthcare providers can expect renewal rates from 0% to +15%.
- There is the potential for hardening market conditions for healthcare related organizations based on claims activity, although not to the level of POS exposed businesses.
- Excess markets are revaluating their portfolios and pricing and we are seeing turnover in excess towers. Some markets have decided to exit the product all together, while others are increasing their pricing or lowering their capacity.
- Underwriting guidelines are tightening and requirements are increasing. Carriers are requesting more information than what was previously required. Primary and some excess markets are requiring conference calls utilizing third party cyber security specialists. We see that building a more comprehensive submission yields more favorable coverage terms and conditions.
- Organizations are continuing to purchase as first-time buyers.
- Current policyholders are increasing their limits. Available limits in the marketplace are approximately $350M to $400M.

Incident Response

Discovery/Notice of Compromise



Condensed Data Breach Timeline

Discovery

The victim organization may not be the first to discover that they have been compromised, so it is very important to act quickly to determine the nature and scope of the breach. Methods of discovery include: Self Discovery/ Vendor Discovery, Law Enforcement or Regulatory Discovery, Consumer Report or Other (Brian Krebs)

Initial Analysis

- Determine Nature of Compromise
- Notify Cyber/Privacy Liability Insurer
- Initiate Incident Response Plan (IRP)

Assessment & Deployment

Initiate Incident Response Plan, Deploy Incident Response Team (IRT), Deploy Third Party Forensic Firm to Determine Scope of Breach; and Mitigate Damage to Systems/Data Loss:

- Determine Type of Data Compromised and Affected Systems/Services
- Notify Third Party Service Providers
- Determine State/Federal Compliance Requirements/Timing of Notice

External Response

- Notification to Affected Individuals/Regulators
- Credit Monitoring /ID Theft Remediation/ Restoration Services
- Public Relations/ Crisis Management/Media Message

Continuing Concerns

- Loss of Income
- Brand Damage
- Digital Asset Loss
- Regulatory Actions/ Fines/Penalties
- Consumer Redress
- Third Party Law Suits
- Civil Litigation

Forensic Analysis & Legal Review

Determining Who, What, When, Where, and How…

The purpose of the forensic investigation is to determine the attacker(s) identity and what data was taken or compromised, and the when and where aspects of how the attacker(s) got in to the compromised system(s); and more importantly, if the attacker(s) are still present. Similar to Crime Scene investigators, Forensic investigators are first responders. Taking action before the Forensic investigators arrive such as shutting down systems or trying to remediate the problem can destroy critical evidence and may also alert attackers that their presence is known.

The forensic process can be time consuming depending on the size of the victim organization, the type and kind of breach, and the scale of outsourced services and connected systems. Breach response efforts to remediate a security breach involving a lost lap top or vendor compromise differs from response efforts for hacker attacks or malware infection. Once forensics investigators complete their assessment and determine exactly what data was compromised, Data Privacy counsel or a Legal Breach Advisor can develop an effective breach response for notification to affected individuals, state attorney generals and government agencies.

Crisis Management

Determining Who to Notify, When and How…

The wrong corporate public message can negatively impact the bottom line. Public relations experts can assist with developing the appropriate message.

After forensic investigators have identified the nature of the crisis or security compromise and determined exactly what data has been breached, the Data Breach Legal Advisor or Breach Coach will then determine the applicable laws and develop a notification plan to meet legal compliance.

This can be a complicated process depending on the breach population so the Data Breach Legal Advisor or Coach's role is paramount. For example, notifying the affected individuals must be in accordance with the laws of their resident state and each state has different time requirements for notice and certain states require notice to the AG's office prior to any notice been sent to affected individuals.

Other considerations include offering credit monitoring or credit remediation services and establishing a call center to assist affected individuals.

Assessing Cyber Liability Risks

What Should Companies Be Thinking About?

- Identify the cyber exposures the company faces and what the plan to address these risks is?
  - Do we have any digital or physical documents that are considered corporate confidential information?
  - Could you receive negative media due to a network breach exposing information you have on your networks?
- How informed is Executive Leadership about the current level and potential business impact of cyber risk to the company?
  - Is your CEO and Board of Directors aware of Cyber exposures for your company?
- What coverage gaps exist in traditional insurance policies that would not respond to a cyber event?
  - For example: Cyber Business Interruption vs. Property Business Interruption)
- What is the potential loss of net income/profit if a network breach is mishandled?

What Should Companies Be Thinking About?

- Is there a well thought-out Incident Response Plan for cyber events and has it been tested? Does the Plan respond enterprise wide and does it include how to handle public relations?

- How much information PII (Personally Identifiable Information), PHI (Personal Health Information) & CCI (Corporate Confidential Information) is in your possession?
  - Is there sensitive information of high net worth individuals stored on the network or in paper files?

- Do you have any obligations if data is outsourced to a 3rd party? What do vendor agreements dictate? (i.e. cloud support for data storage)

- How many and what types of incidents does the IT department detect in a normal week? Is there a company mandated threshold in place for notifying Executive Leadership?