Cyber Liability: Beyond the Breach

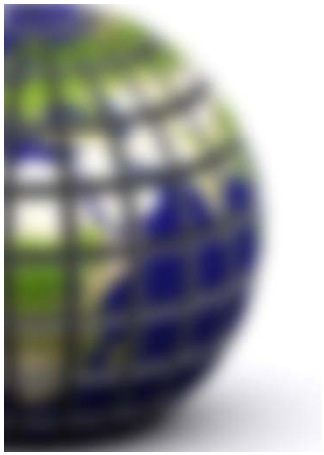
2014 Casualty Loss Reserve Seminar
San Diego, CA
September 2014

Catherine A. Mulligan
SVP, Specialty E&O
Zurich North America

Bob Parisi
Managing Director
Marsh

Topics of Discussion

- Overview of the Security & Privacy Landscape
  - Who / What is at Risk?
  - General Statistics
    - Causes of Loss
    - Cost of a Data Breach
  - Potential Loss Exposures
  - The Marketplace
  - Gaps in Traditional Insurance
- Coverage Basics
  - Review of Available Coverages
  - Vendor Services
- Beyond the Breach: Panel Q&A



Overview of Security & Privacy Exposures: Who is at Risk?

Finance	34%
Public	13%
Retail	11%
Accommodation	10%
Utilities	6%
Professional	5%

- United States Secret Service (USSS)
- Dutch National HiTech Crime Unit (NHTCU)
- Australian Federal Police (AFP)
- Irish Reporting & Information Security Service (IRISSCERT)
- Police Central e-Crime Unit (PCeU) of the London Metropolitan Police
- Any Organization or Individual holding:
  - Sensitive Customer/Patient Data
  - Sensitive Employee Information
  - Confidential Third Party Corporate Information protected by a non-disclosure or similar agreement

Source: 2014 Verizon Data Breach Investigations Report
Number of Security Incidents with Confirmed Data Loss by Victim Industry

Cyber Attacks and Main Street

- Cybercriminals unleash 3.5 new threats targeting small and medium businesses every second.*
- The number of online attacks specifically targeting small businesses surged 600 percent in 2010.*
- Small businesses are now the target of 31 percent of all attacks, a threefold increase from 2011.**
- 29 percent of small businesses experienced a computer-based attack.*** The consequences of those attacks included:
  - managing potential damage to their reputations (59 percent);
  - theft of business information (49 percent);
  - the loss of angry or worried customers (48 percent) and
  - network and data center downtime (48 percent).

Source:
*TrendMicro, **Symantec, ***Ponemon

Six Large and Notable Breaches

Company	Date	# of Records Compromised	Comment
Snapchat	Jan 2014	4.6 million	Breach included phone numbers and user names. Attackers used a website called SnapchatDB info to compile the information and made it available for download.
Neiman Marcus	Jan 2014	1.1 million	Hackers stole just over a million pieces of customer payment card information.
Target	Dec 2013	110 million	Hackers planted malware on a point of sale system to steal 40 million pieces of credit and debit card information. They also stole the contact information of roughly 70 million people.
Michaels Stores	Jan 2014	3 Million	The arts and crafts retail store was the victim of a malware attack that accumulated the payment card information of roughly 3 million people.
University of Maryland	Feb 2014	307,079	Hackers stole personal data of faculty, staff, and students from the University's database.
Sally Beauty	March 2014	282,000	Attackers broke into the network and stole roughly 282,000 credit cards. The information was sold on the same underground crime store as the data from the Target breach.

Notable Breaches – Other Causes

Company	Date	# of Records Compromised	Comment
LinkedIn	June 2012	6.5 million	User passwords stolen and dumped onto online forum resulting in clean up costs of $4M and a $5M lawsuit pending.
Emory Healthcare	April 2012	315,000	Lost back up tapes containing patient data dating back over 10 years. Class action lawsuit filed for over $200M.
Zappos	Jan 2012	24 million	Breach included names, email addresses, phone numbers, last 4 digits of SSN and encrypted passwords. Hacker gained access through Zappos servers. 10 class actions pending.
Department of Defense	Oct 2011	4.9 million	Stolen unencrypted back up tapes containing veteran health care records results in $4.9B class action suit.
Stanford University	Sept. 2011	20,000 records	Accidental disclosure of patient data by a 3rd party vendor results in $20M class action suit.

Source: DarkReading.com, June 2012

Security & Privacy Exposures

Network Security Breach

- Theft, Alteration, or Destruction of Electronic Data on a Company's Computer System;
- Unauthorized Access to or Unauthorized Use of the Company's Computer System;
- Denial of an Authorized User's access to a Company's Computer System,
- Participation by a Company's Computer System in a Denial of Service Attack directed against a third party's Computer System; or
- Transmission of Malicious Code from a Company's Computer System to a third party's Computer System.

Privacy Breach

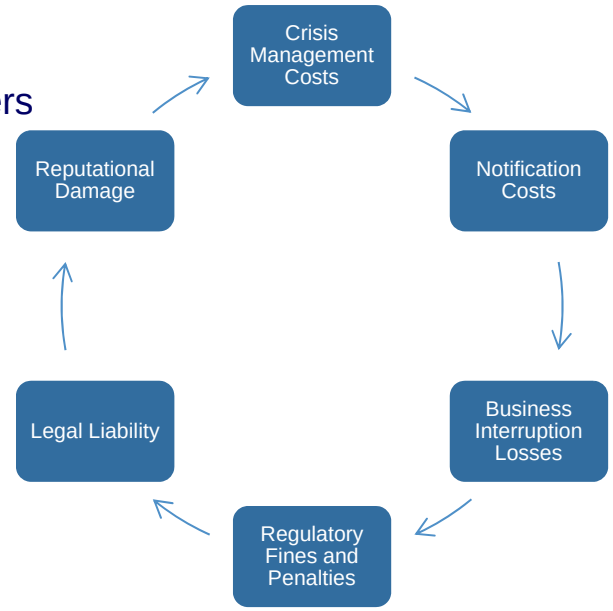
- an unauthorized disclosure or loss of:
  - Personal Information in the care, custody or control of any Insured or Service Provider; or
  - Corporate information in the care, custody or control of any Insured or Service Provider that is specifically identified as confidential and protected under a nondisclosure agreement or similar contract; or
- a violation of any Privacy Regulation

Technology Failures

- Business Income and Extra Expense
- Dependent Business Income

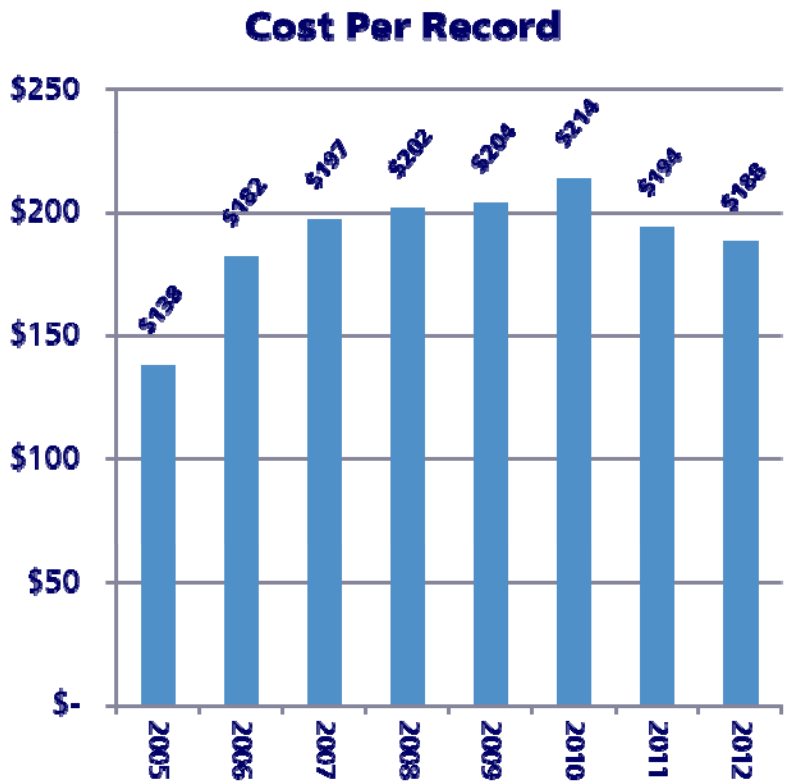
Security & Privacy Loss Cost Types

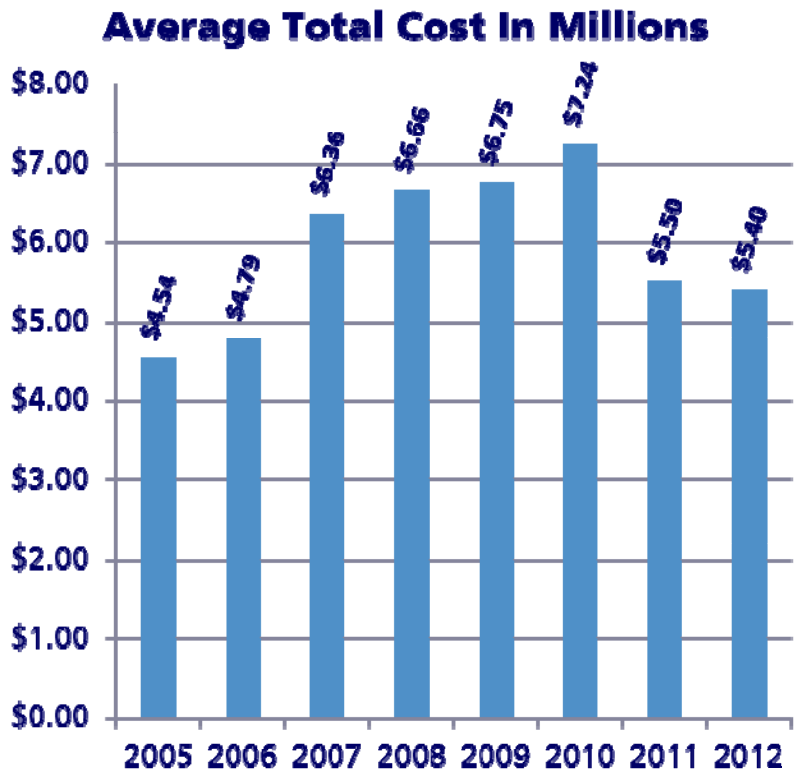
- **Crisis Management Costs**
  - Legal, public relations or other service fees
  - Advertising or related communications
- **Costs of Notification**
  - Forensic investigation
  - Printing, postage or other communications to customers
  - Credit monitoring services
- **Business Interruption Losses**
  - Loss of Income
  - Costs to Recreate Lost or Stolen Data
  - Extra Expenses
- **Regulatory Fines and Penalties**
- **Legal Liability**
  - Class action litigation
  - Suits from Customers and Vendors
- **Reputational Damage**



U.S. Breach Cost Trends (Direct and Indirect Cost)

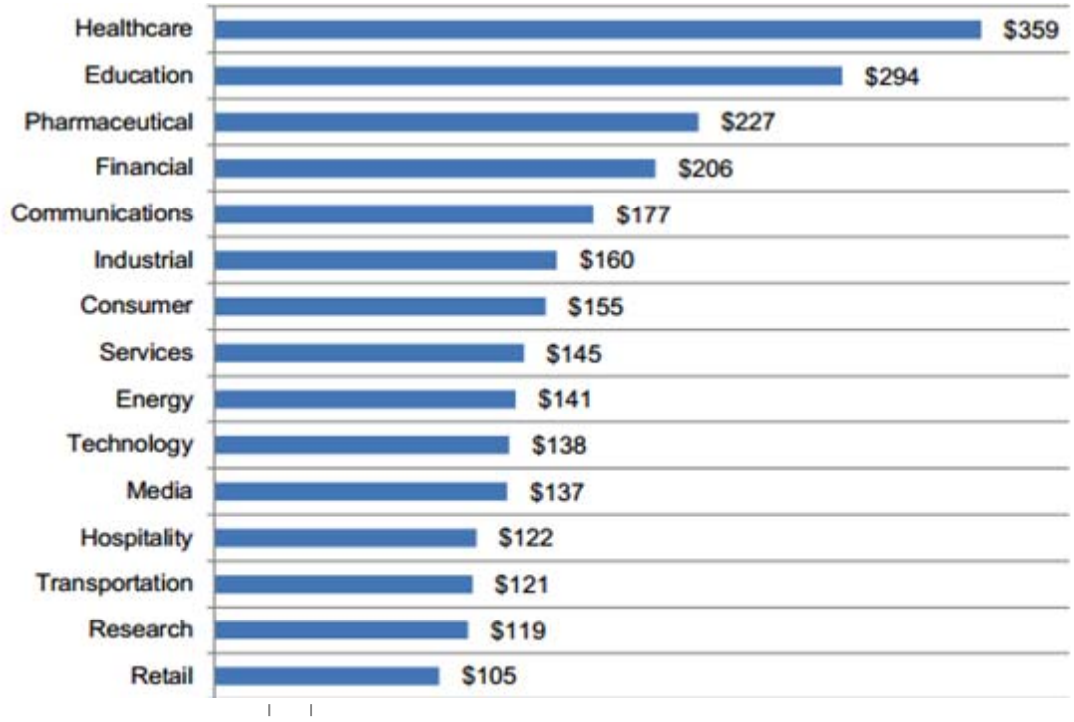
*Ponemon Institute; 2013 Cost of Data Breach Study: United States





Data Breach Total Cost Per Record By Industry 2013-2014

Figure 4. Per capita cost by industry classification
Consolidated view (n=314)

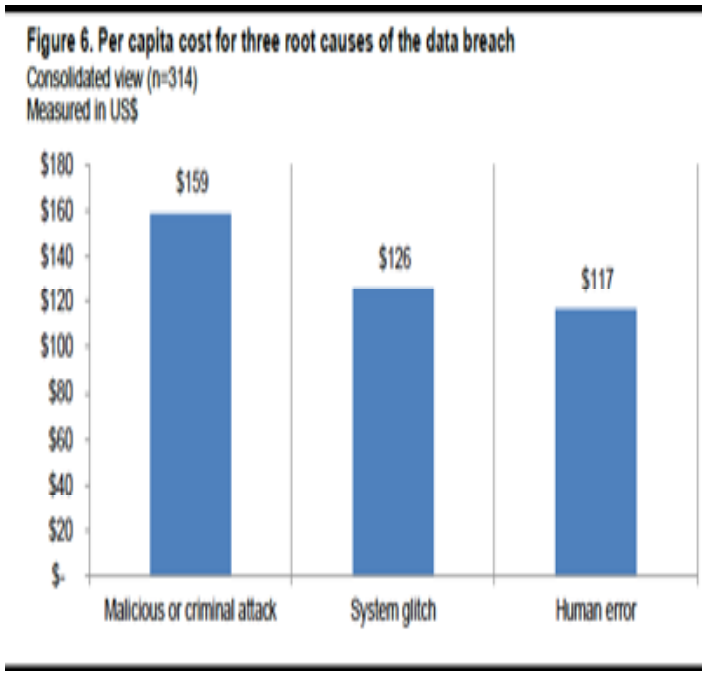


"Heavily regulated industries such as healthcare, education, pharmaceuticals and financial services had a per capita data breach cost above the industry mean of $145. Public sector organizations and retail companies had aper capita cost well below the overall mean value."

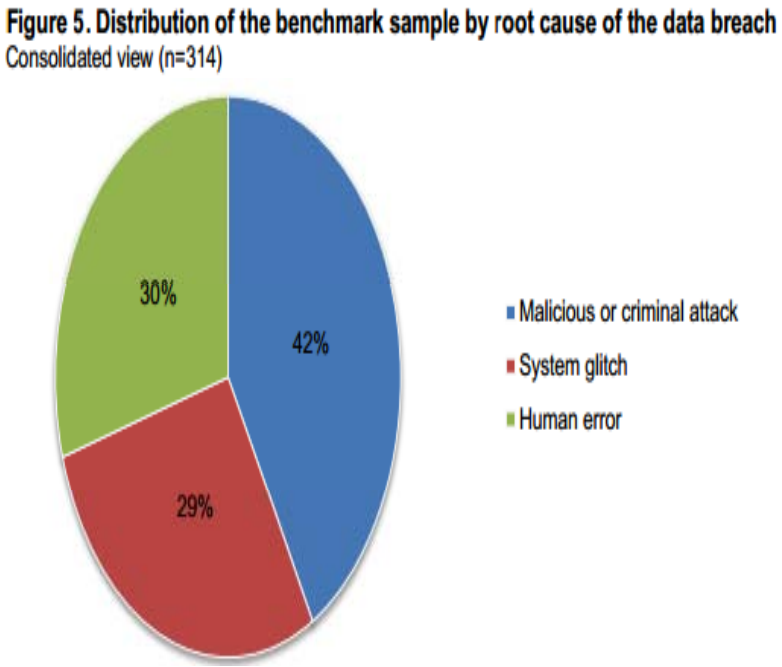
*Ponemon Institute; 2014 Cost of Data Breach Study: United States

Cost Per Record Based on Type of Breach

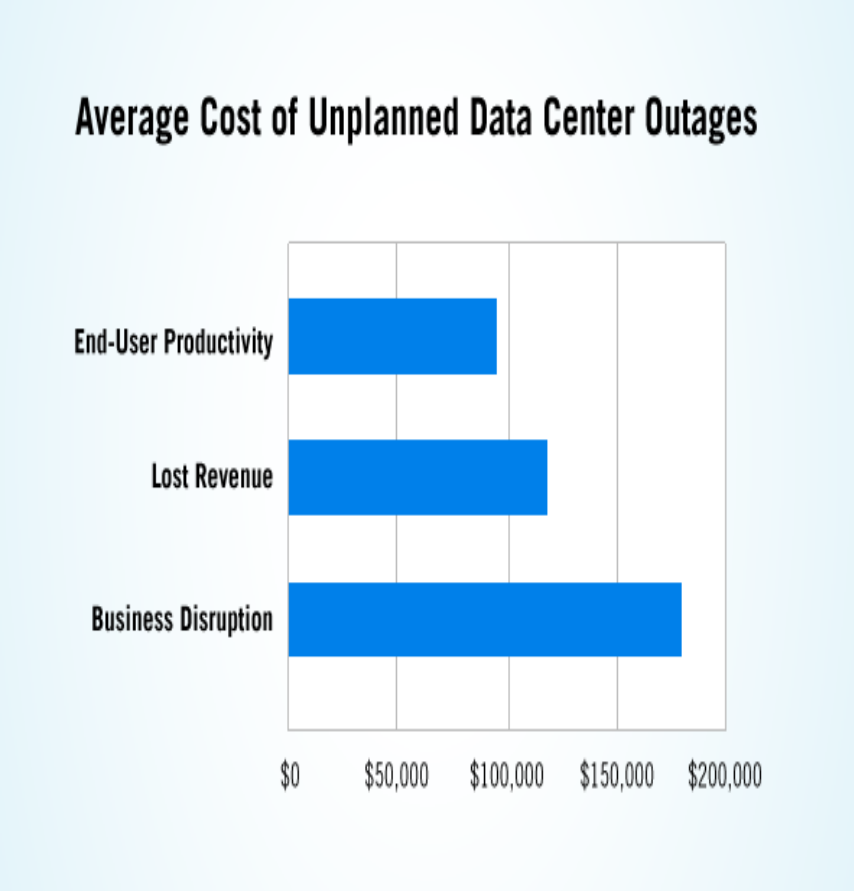
Per Record Cost of a Breach Based on Root Cause

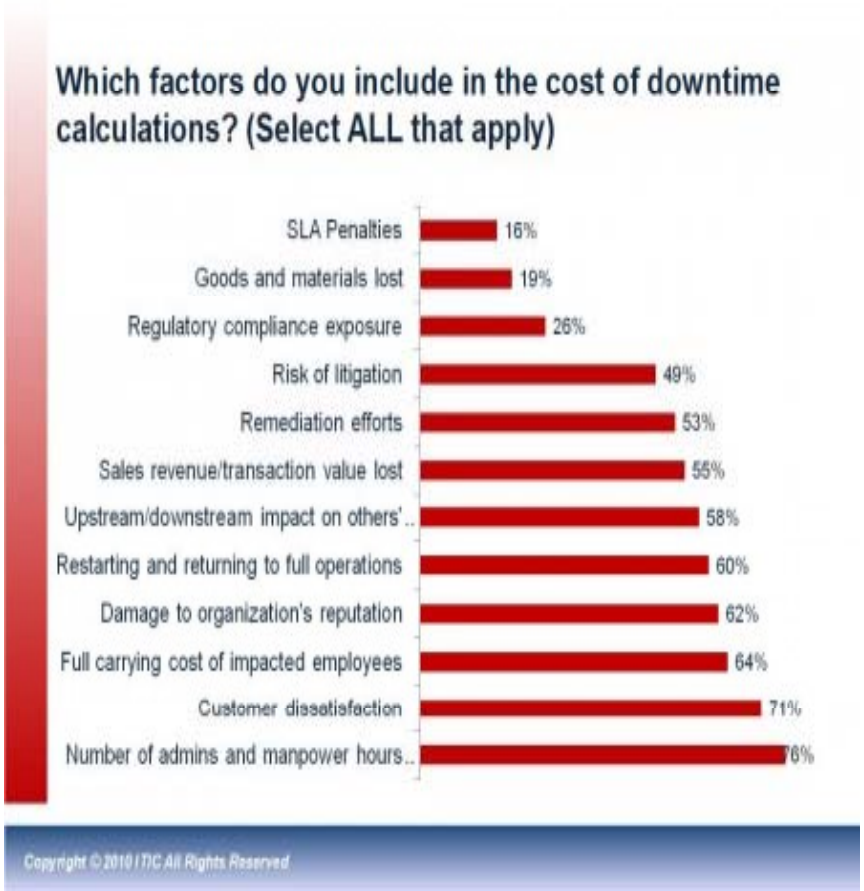


Distribution By Cause



Direct Loss Costs



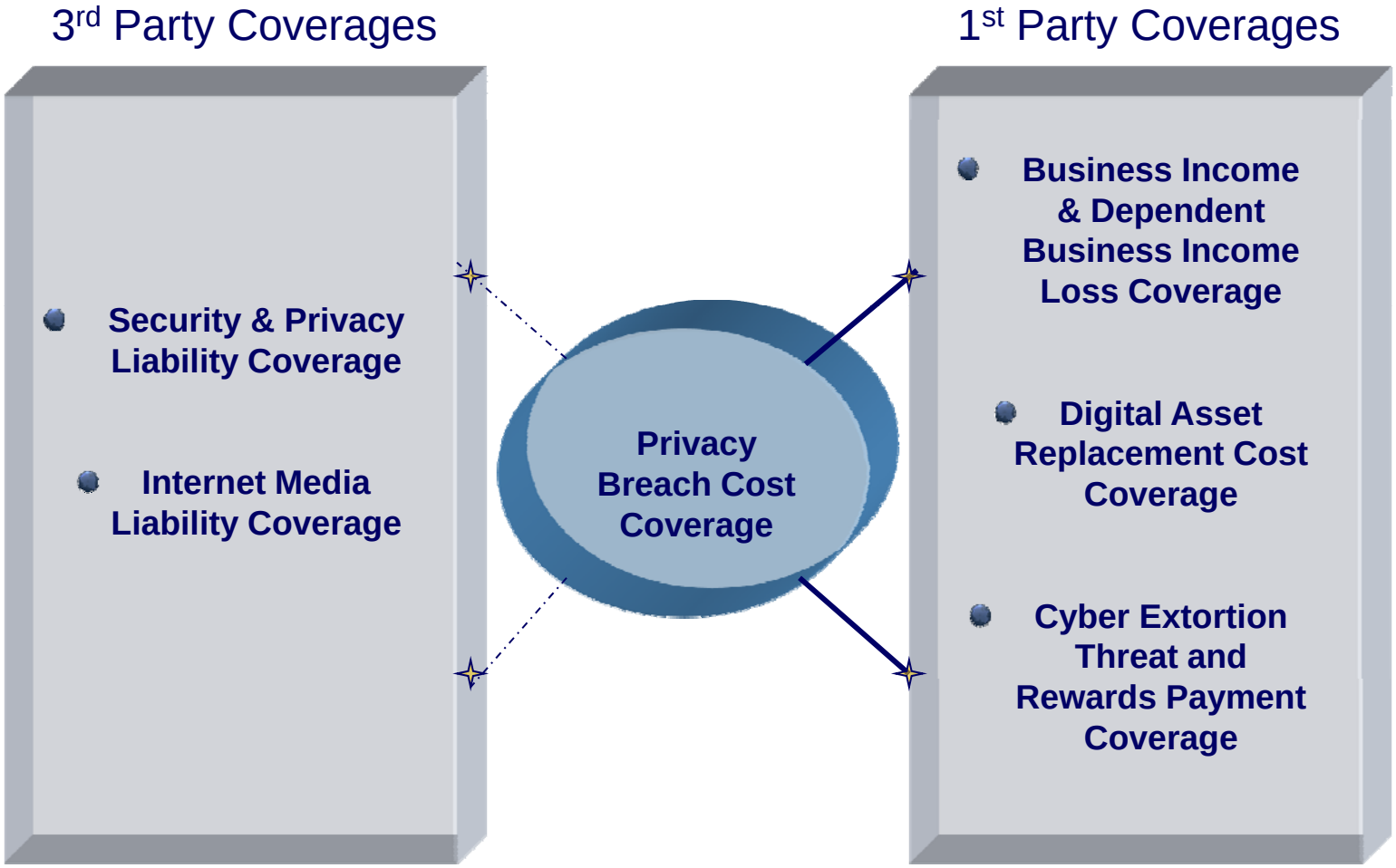


Security & Privacy Marketplace

- Estimated $1.0-$1.3B GWP market YE 2013[1]
- Buyers of S&P have increased 35% in 2011 to 52% in 2012[2]
- Global brokers:
  - 30% increase in new buyers
  - 20% increase in new limits
- New and varied capacity
- Dozens of markets offering over $500M in capacity
- $200M available in capacity for a single organization or policyholder
- Shortening sales cycle
  - New industries
  - Increased BoD awareness
- Emerging exposures
- Loss data is a moving target

1. Guy Carpenter's State of the Tech/Cyber market report (2012) and Management Liability – Market Overview report (Oct. 2013)
2. Advisen 2013 Information Security & Cyber Liability Risk Management Survey of Risk Managers

Coverage Overview



Cyber Coverage Overview

- **Network Security Liability:** liability to a third party as a result of a failure of your network security to protect against destruction, deletion, or corruption of a third party's electronic data, denial of service attacks against internet sites or computers; or transmission of viruses to third party computers and systems
- **Privacy Liability:** liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.
- **Regulatory Investigation Defense:** coverage for legal expenses associated with representation in connection with a regulatory investigation, including indemnification of fines & penalties where insurable.
- **Crisis Management and Event Response Expenses**: expenses incurred in responding to a data breach event, including retaining forensic investigator, crisis management firm and law firm. Includes expenses to comply with privacy regulations, such as communication to impacted individuals and appropriate remedial offerings like credit monitoring or identity theft insurance.
- **Cyber Extortion:** ransom or investigative expenses associated with a threat directed at you to release, divulge, disseminate, destroy, steal, or use the confidential information taken from the insured, introduce malicious code into your computer system; corrupt, damage, or destroy your computer system, or restrict or hinder access to your computer system.
- **Network Business Interruption:** reimbursement of your loss of income and / or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption.
- **Data asset protection:** recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., software applications) that are corrupted or destroyed by a computer attack.

NOTE: Some Carriers offer elements of Risk Mitigation and Loss Prevention services, like the Crisis Management & Event Response Expenses as a service bundled with the insurance coverage but not eroding the policy's limits

Pre / Post Breach Consulting Services

- Information Security Consulting
  - Risk Assessments & Recommendations
  - Tabletop breach readiness exercises
- Risk Manager Tools
  - Incident Roadmap
  - eRisk Hub News Center
  - Learning Center - Access to webinars / blogs / white papers
- Carrier / vendor relationships
    - Legal breach coaches
    - Forensic Analysis
    - Notification Services
    - Call Center Services
    - Credit/Identity Monitoring
    - Identity Restoration Services
    - Fraud Consultation

Beyond the Breach
Questions & Answers