GUY CARPENTER

Network Security & Privacy Liability:
An Overview of Loss Mitigation Concepts and Data Breach Response Services

March 20th, 2012

Brian Cole, Managing Director
Professional Liability Specialty Practice

MARSH & McLENNAN COMPANIES

Overview of Topics

- Cyber Security Risk
  - Recent Related News and Example Data Breaches
- Explanation of Cyber Liability Coverage
  - Cyber Coverage Segments
  - Examples of First Party Coverage “Traditional and Non-Traditional”
  - First Party Coverage Triggers and Types of Data Covered
  - 1st Party Expense Coverage - Data Breach Response and Services
- Current State of the *Cyber Liability Insurance* Marketplace
  - Premium Estimates, Market Size, Product Development
  - Rates and Retentions
  - Insurance Market Players and Potential Limits
- Current State of the Cyber Liability *Reinsurance* Marketplace

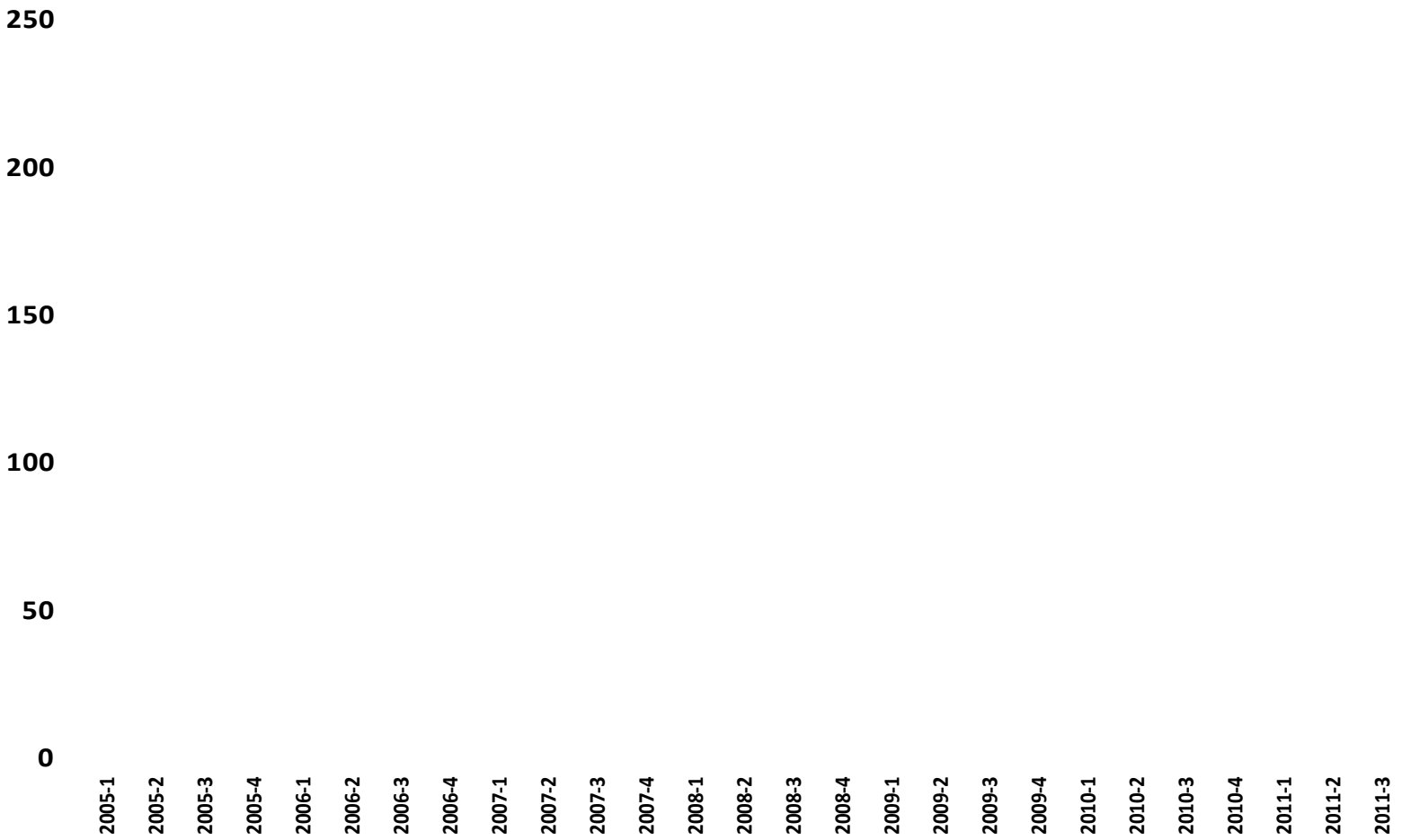
Cyber Security Risk

Recent Cyber Related News and Data Breach Examples:

- Identity Theft is the fastest growing crime in the United States
  - Incidents of cyber crime and “hactivism” are rampant today (The hacker group “Anonymous”)
- Privacy Rights Clearinghouse reported that since 2005 more than 534 million personal records have been compromised
- In 2011, over 270 breaches have been reported involving 22 million sensitive personal records
- Examples:
  - Two of the largest data breach in US history – Sony shut down Playstation network for a month with over $170M expense and over 100 million email address records stolen
  - Citigroup targeted by hackers that stole account information from over 300,000 customers
  - Other recent breaches: (Epsilon, Bank of America, RSA Security ID, Google, Heartland, TJ Maxx, Lockheed Martin, TD Bank, Netflix, etc.)
  - Largest Insured Loss to date $31M / Smallest $750K. This does not include Sony or Epsilon incidents

Cyber Security Risk

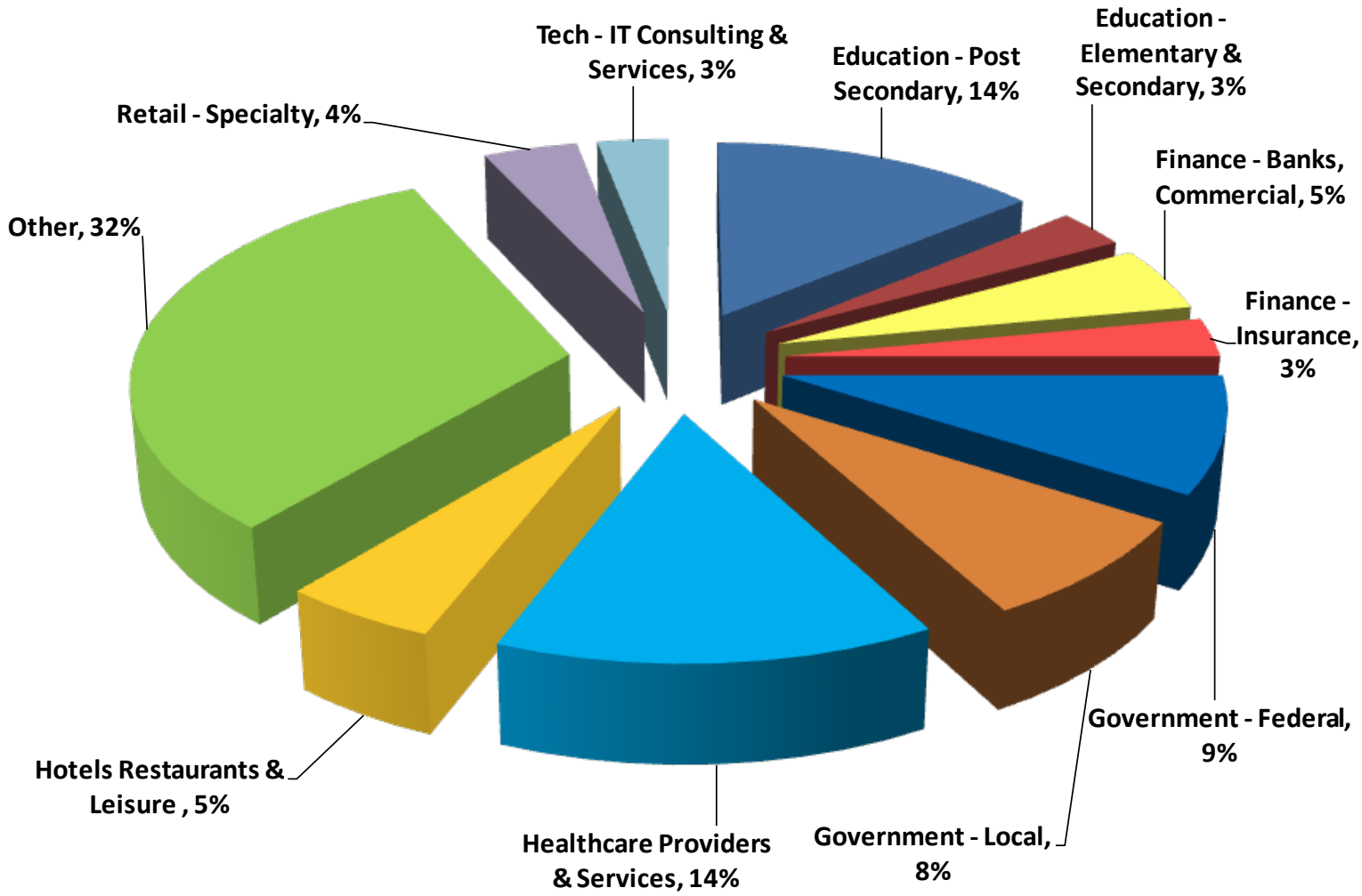
Number of Data Breach Events by Year



Source: Advisen MSCAd.
Includes System security breaches, other lost and stolen data, phishing, etc.

Cyber Security Risk

Percentage of Data Breach Events by Industry Segment



Source: Advisen MSCAd.
Includes System security breaches, other lost and stolen data, phishing, etc.

Explanation of Cyber Liability Coverage

Cyber Coverage Segments:

- Third Party Cyber Coverage: "Liability"
  - Liability (3rd Party): Defense and settlement costs for the liability of the insured arising out of its failure to properly care for private data.

- First Party Cyber Coverage: "Property and Theft"
- Fines and Penalties (1st Party): The cost to investigate, defend and settle fines and penalties that may be assessed by a regulator.
  - *Note: Coverage for Fines and Penalties was not offered under traditional cyber policy. Several Carriers recently added this coverage due to increased market competition and regulatory requirements for insureds.*

- Property, Theft and Repair: (1st Party): Response costs following a data breach, including investigation, public relations, customer notification and credit monitoring. This also includes coverage for the loss of income and expense caused by a system shutdown due to a breach.

Note: The nature of the coverage and primary terms/conditions vary greatly between carriers

Explanation of Cyber Liability Coverage

Examples of "*Traditional*" First Party Coverage:

- ***Business Interruptions or Denial of Service Attack:***
  Covers loss of income and extra expense arising out of the interruption of network service due to an attack on the insureds network.
- ***Contingent Business Interruption:***
  Covers loss of income and extra expense arising out of the interruption of network caused by a key service provider.

Explanation of Cyber Liability Coverage

Examples of *"Non-Traditional"* First Party Coverage:

- ***Asset Loss Protection:***
  Covers cost incurred to replace, restore or recollect data which has been corrupted or destroyed as a result of network security failure.
- ***Cyber Extortion:***
  Coverage addresses threats made against insured by a third party that has illegally breached the covered network and is threatening to release sensitive data or release malicious code or virus unless paid extortion monies.
- ***Security Failure Notification Loss (Privacy Breach):***
  Coverage offers reimbursement for compliance/regulatory expenses incurred under personal privacy and identity theft regulation (Regulation requirements vary by State)
- ***Crisis Management (Privacy Breach):***
  Coverage offers reimbursement of expenses for insured to hire breach experts (Attorney, Public Relations, Forensic Specialist) to assist with resolving data breach, notifying insureds and identifying cause of breach.

  Note: Most carriers offer the above First Party coverage on a sub-limited basis. They are typically sub-limited to 20% - 40% of the Third Party Liability limits, however there are carriers that offer full policy limits for First Party business.

Explanation of Cyber Liability Coverage

First Party Coverage Triggers:

- Coverage under a cyber policy can be triggered by the following:
  - Failure to secure data
  - Loss caused by an employee
    - Employee checking e-mail at work and unknowingly downloads a virus or worm
    - Employee conducting research online is redirected to website that automatically downloads virus or worm
  - Acts by person other than insureds
  - Loss resulting from the theft or disapperance of private property (such as data that resides on a stolen laptop or missing data storage media)
- Types of Data Covered by Cyber Liability Policy:
  - An individual's personally identifiable information (PII)
  - Non-public data (i.e. corporate information)
  - Non-electronic data (i.e. paper records and printouts)

First Party Expense Coverage “Property, Theft and Repair”

Data Breach Response Strategy: *Prior to Data Breach*

- *A company should have a prepared plan on how to respond to a breach once detected and the resources that will be required.*
- *There are several risk management firms that offer various cyber tools and resources to firms such as:*
  - *Assessment Surveys*
  - *Breach notification guides*
  - *Evaluation of insureds system and level of defense against hackers*
  - *“What-if” modeling tools to estimate the cost of a breach*
  - *Research tools to monitor the type, frequency and severity of incidents occurring in the companies business sector.*
  - *Referral source to help find qualified third party experts in pre- and post-breach disciplines*

Note: The above risk management services are offered free by majority of Cyber Insurance Carriers.

First Party Expense Coverage “Property, Theft and Repair”

Data Breach Response Strategy: *Post Data Breach*

- ***Identify The Problem****:*

  “What happened”. A small to med-size firm will need to hire a third party forensic and technical expert to help determine the root cause of the breach and the extent of the damage.

- ***Identify and Comply with Regulatory Requirements****:*

  Majority of US states have statutes outlining the requirements of a company in the event of a data breach and that all parties impacted by the event must be notified.

  With increased Privacy laws in 47 states (Breach Notice Laws) the notification cost can become enormous when you consider the thousands of clients that have to be notified (Example Sony with over 100 million registered users). A company should obtain outside legal counsel to ensure compliance with all applicable laws and regulations.

- ***Protecting the Customer****:*

  After customers have been notified that their data has been stolen, the firm will offer credit monitoring and recovery assistance. Offering these services will assist the firm with repairing its reputation and retaining clients. The cost of credit monitoring can range from $10 to $200 per customer, per year.

First Party Expense Coverage “Property, Theft and Repair”

Data Breach Services Provided and Benefits:

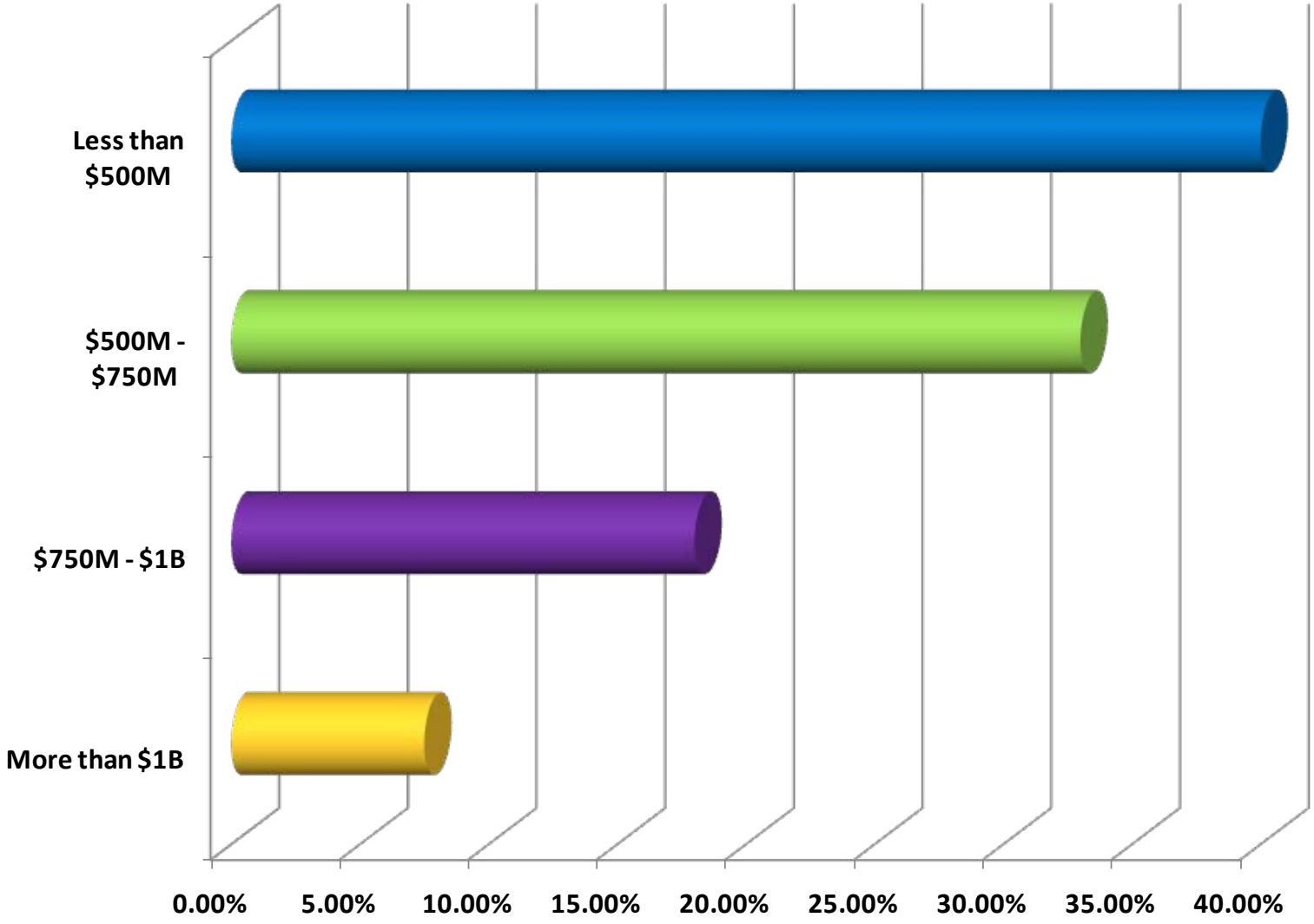
- Several Insurance Carriers offer policyholders access to various risk management tools and data breach resources (i.e. Data Breach Team) to assist with mitigating and managing the rising expense of data breaches.
  - Access to a panel of third party specialist to assist with data breach in all areas:
    - Privacy Lawyers to assist in addressing the legal requirements of a breach
    - Computer Forensic specialist to uncover exactly what happened
    - Notification Service Providers to print, mail and e-mail notices to affected clients
    - Credit monitoring, identity restoration and fraud response service providers
    - Public Relations Specialist

- Benefits from Risk Management and Data Breach Services:
  - More educated insureds with reduced loss potential for carrier
  - Reduced expenses for insureds (Pre-nogotiated rates from service providers)
  - The company’s reputation and business is protected

State of the Cyber Liability *Insurance* Market

- **Premium:** *Estimated Annual GWP $670 to $800 million (Total U.S CyberRisk Market)*
- Coverage for organizations that offer products and services via the internet
  - 1st party or 3rd party coverage products
- Coverage for technology companies – Technology E&O
- Coverage for others – Cyber Risk
  - Vast majority of premium emanating from 3rd party product
  - Competition increasing as new markets continue to enter space
  - Several Carriers looking to carve out niche position by offering coverage for high risk exposure classes (i.e Schools/Universities, Hospitals, Large Retailers)
  - Continues to be a discretionary purchase
  - Estimates believed to include Technology E&O business

State of the Cyber Liability *Insurance* Market
US Market Size - Written Premium by Size of Insured (Revenue)



Source: Advisen MSCAd.

State of the Cyber Liability *Insurance* Market

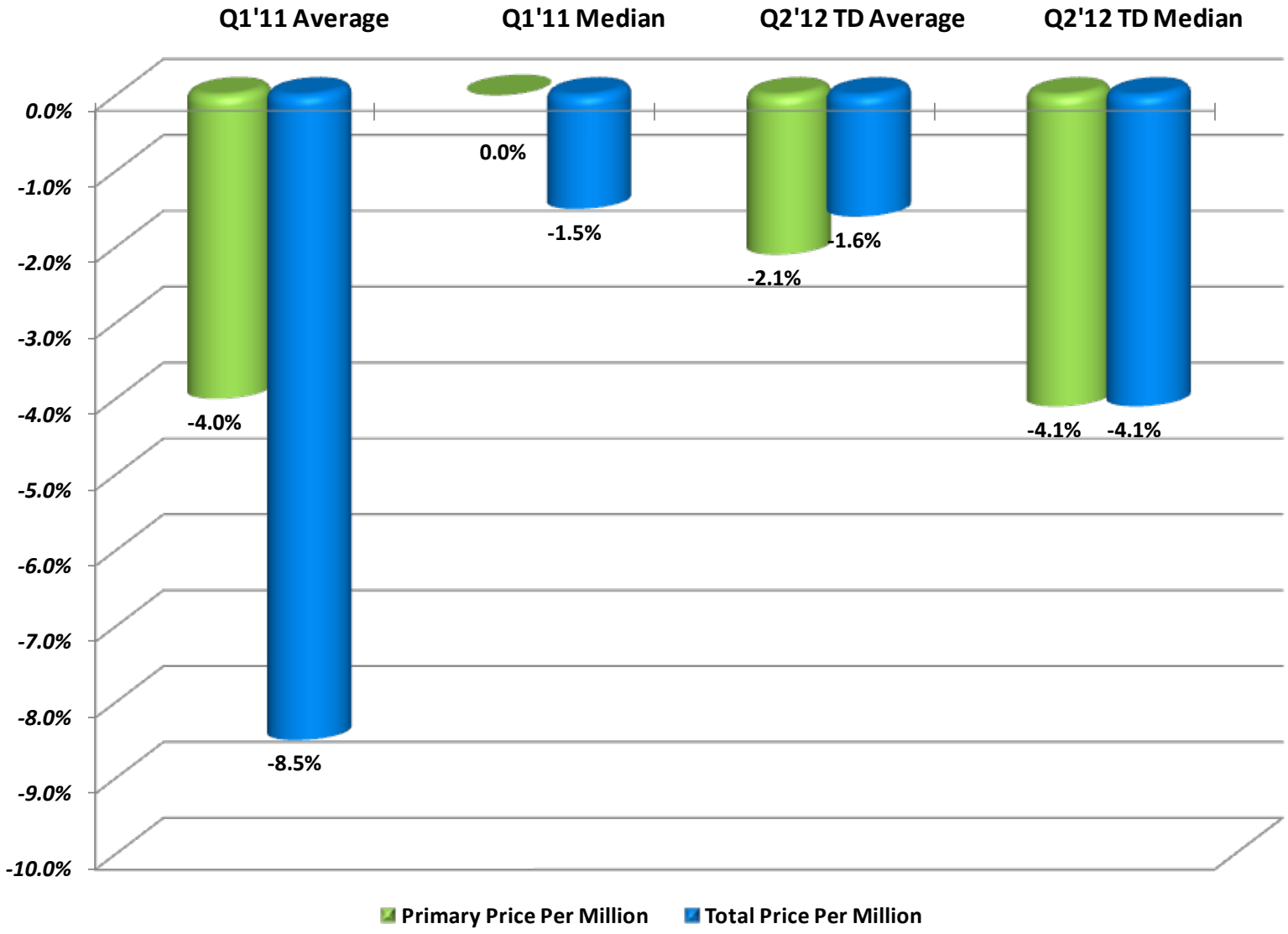
➢Product Development / Hot Topics

- Potential for a Catastrophic Loss involving multiple insureds remains unquantified
- Privacy coverage is driving the growth of the product in 2012 and 2013
- Several Carriers currently in the market offering the following:
  - Expanding 1st Party Coverage to include system failure due to System Error, Power Outage and Administrative Errors
  - Offering cyber coverage in package policy (i.e Management Liability)
    - ✓Due to new SEC reporting requirements for Public Companies
  - Offer larger limits excess of $50,000,000 (largest cyber tower $175M in limits)
  - Offer turnkey cyber endorsement that attaches to BOP or GL policy
    - ✓Exposure for smaller business growing due to greater reliance on internet to conduct business

State of the Cyber Liability *Insurance* Market

- **Rates and Retentions:**
  - CyberRisk market showing signs of softness. This has been driven by:
  - Good results since 2002 with small amount of loss activity
    (large data breaches reported in the news are either partially or not insured)
  - Increased appetite from existing players
  - Increased level of competition from new players;
    - Rates flat to -5% for large limit ($15M to $25M) Cyber coverage and -5% to -10% for smaller limit ($5M to $10M) Cyber coverage
    - No signs of decrease in retentions or deductibles
    - Deductibles generally 5% to 10% of limits purchased or equivalent to the E&O deductible (if purchased). Minimum deductibles are US $5,000 to $25,000 based on coverage purchased
    - Minimum waiting period deductibles used for Business Interruption Coverage

State of the Cyber Liability *Insurance* Market
Historical Rate (Price Per Million) Changes – Cyber Liability



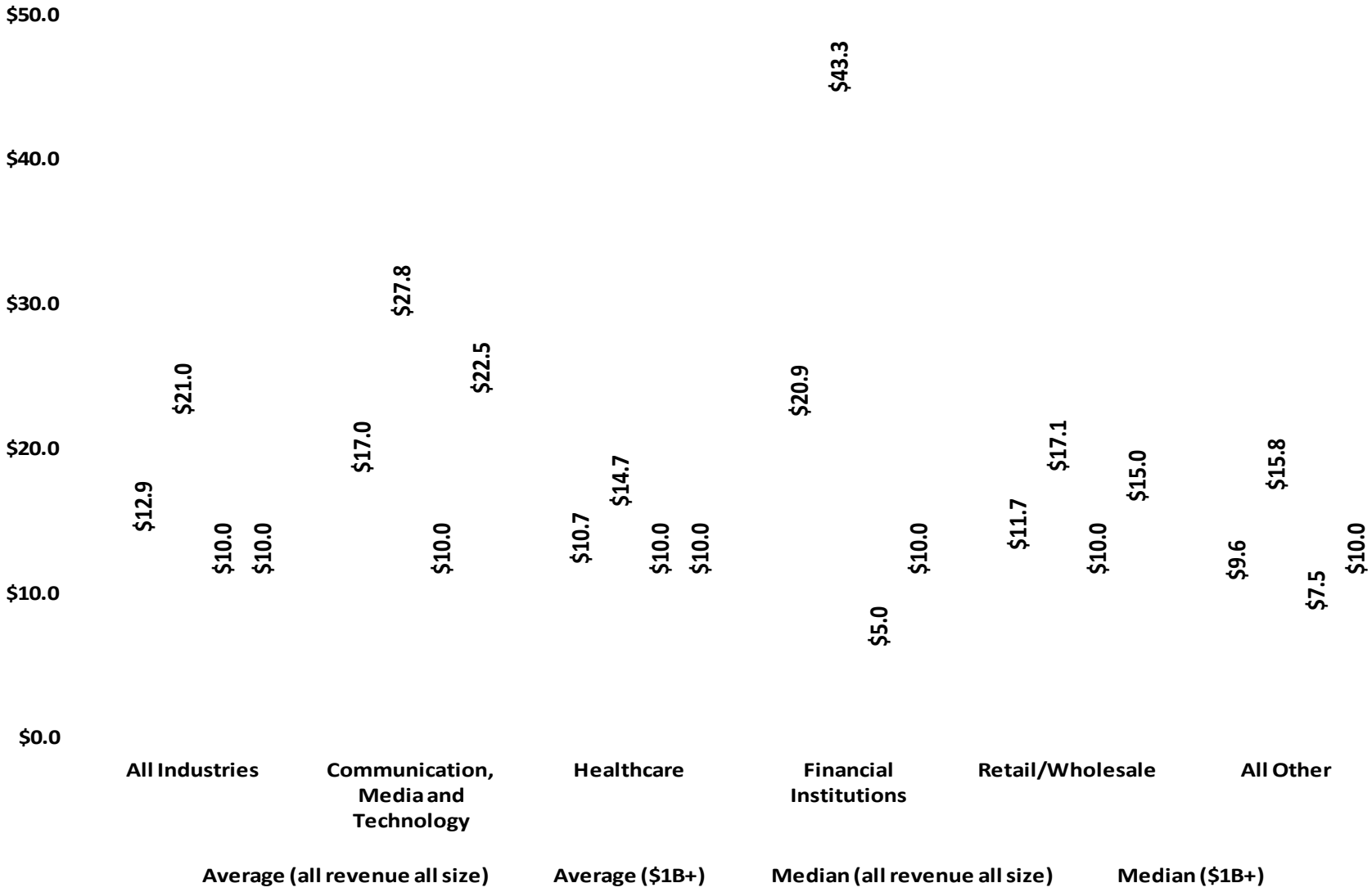
Source: Marsh Insight Report

Cyber Liability
Market Players and Potential Limits

$15M to $25M Capacity	$10,000,000 Capacity	$5,000,000 or Less Capacity
▪ *ACE*	▪ *Arch*	▪ *Admiral*
▪ *Allied World*	▪ *Aspen*	▪ *Barbican Syndicate*
▪ *Axis*	▪ *Brit*	▪ *Evanston*
▪ *Beazley*	▪ *CFC Underwriting*	▪ *Hartford Steam Boiler*
▪ *Chartis*	▪ *CNA*	▪ *NAS*
▪ *Chubb*	▪ *Crum & Forster*	▪ *Philadelphia*
▪ *Digital Risk Managers*	▪ *Euclid Managers*	▪ *Public Entity*
▪ *Ironshore*	▪ *The Hartford*	▪ *RLI*
▪ *Safeonline*	▪ *Hiscox*	
▪ *Travelers*	▪ *Liberty*	
▪ *Zurich*	▪ *Markel*	
	▪ *Navigators*	
	▪ *One Beacon*	
	▪ *XL*	

▪ ***Significant liability limits capacity exists; Limits offered from $1M to $25M on a primary or excess basis***

State of the Cyber Liability *Insurance* Market
Distribution of Total Cyber Risk Limits Purchased



Source: Marsh Insight Report

State of the Cyber Liability *Reinsurance* Market

- Reinsurers remain interested in CyberRisk product
  - Viewed by some as the way to grow Professional Liability portfolios
  - Concerned with rate activity/pricing in highly competitive marketplace
- Reinsurers concerned over accumulation of 1st Party Exposures across programs
  - Potential for a Catastrophic loss involving multiple insureds remains unquantified
  - Primary Carriers viewed as purchasing reinsurance coverage for increased protection from Catastrophic loss event
  - Several large claims ranging from $5M to over $50M in the past few years; (***Heartland, TJ Maxx, Citizens Financial, Nextran Group, First Bank, OmniAmerican Bank, Sony, Epsilon, Citibank, TD Bank, Netflix, etc.)***
  - Reinsurance market concerned over accumulation of 1st Party Exposures
- Several reinsurers reducing capacity for new cyber treaties due to rate/pricing environment and large data breaches reported by the media.
- Reinsurance program have been renewing flat with little or no change in terms
- All Stand alone Reinsurance Cyber Programs include several types of limitations: (i.e. Limit, premium, loss event caps, etc).


GUY CARPENTER