LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

**Lewis Brisbois Presents**

# Practical Strategies to Address Cyber Risk in Your Business

*What Boards, Business Owners and General Counsel Need to Know Now*

**November 18, 2014**

**Presented by**


*Bob Hartwig*

*Charles White*

*John Mullen & Lori Anne Czepiel*


INSURANCE INFORMATION INSTITUTE

pwc

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

# Overview

- Insurance Strategies and Solutions
  - ✓ Assessing coverage for your company's cyber risk exposure
  - ✓ Available products for specific cyber risks and industries
  - ✓ Leveraging your insurer's expertise to develop cyber risk strategy and response
- Corporate Governance and Compliance Considerations
  - ✓ Best practices
  - ✓ Overview of relevant legal and regulatory frameworks
- Developing your Crisis Management and Response Plan
  - ✓ What should you do to be ready?
  - ✓ Responding to a data security event

# Presenters

**Bob Hartwig,**
*Insurance Information Institute*

**Charles White,**
*PricewaterhouseCoopers*

**John Mullen,**
*Lewis Brisbois*

**Lori Anne Czepiel,**
*Lewis Brisbois*

INSURANCE INFORMATION INSTITUTE

# Cyber Insurance:
## *Product History, Evolution & Structure*

**Cyber Risk Webcast**
**November 18, 2014**

Robert P. Hartwig, Ph.D., CPCU, President & Economist
Insurance Information Institute ♦ 110 William Street ♦ New York, NY 10038
Tel: 212.346.5520 ♦ Cell: 917.453.1885 ♦ bobh@iii.org ♦ www.iii.org

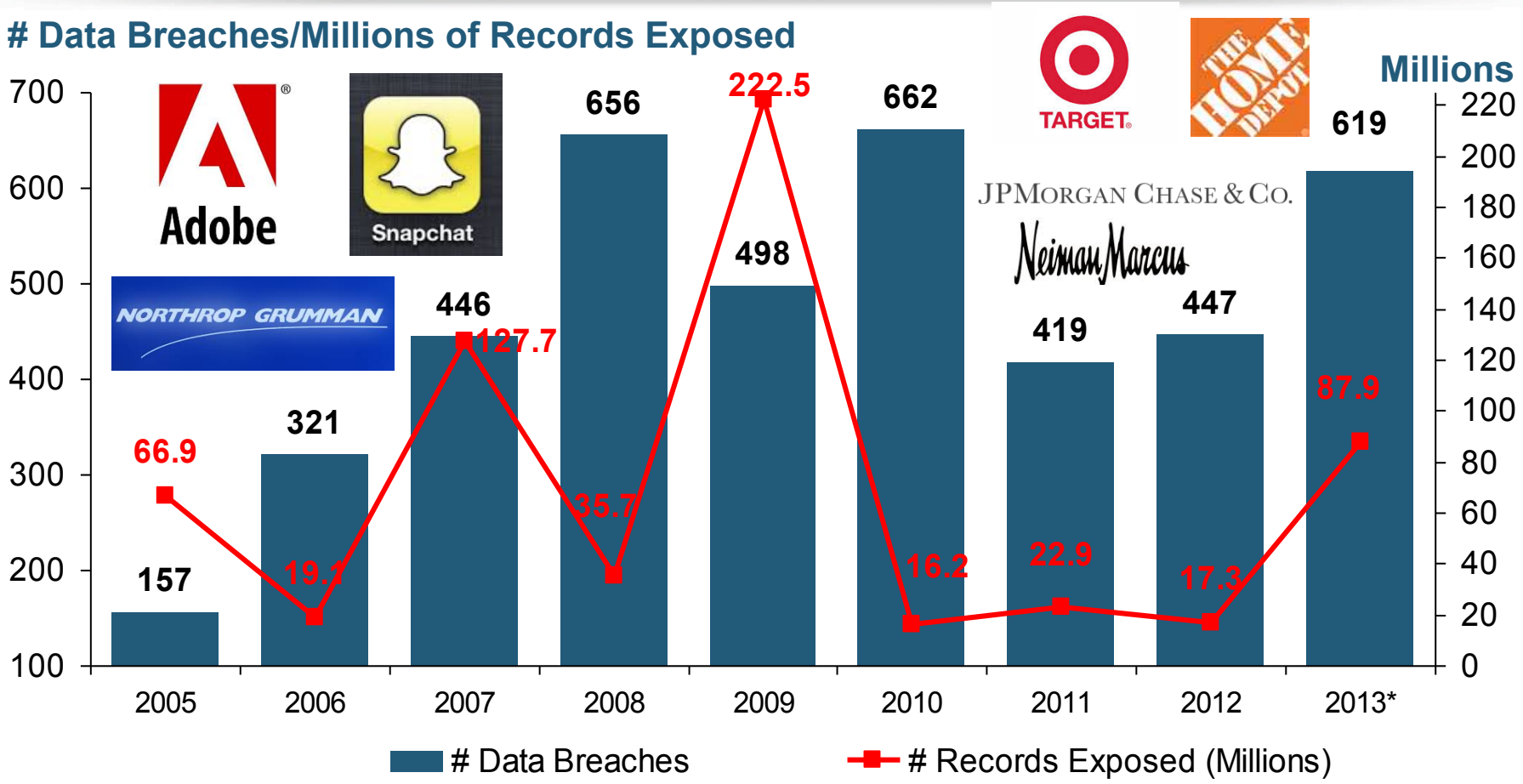
INSURANCE INFORMATION INSTITUTE

# CYBER RISK

## Cyber Risk is a Rapidly Emerging Exposure for Businesses Large and Small in Every Industry

# Data Breaches 2005-2013, by Number of Breaches and Records Exposed

INSURANCE INFORMATION INSTITUTE

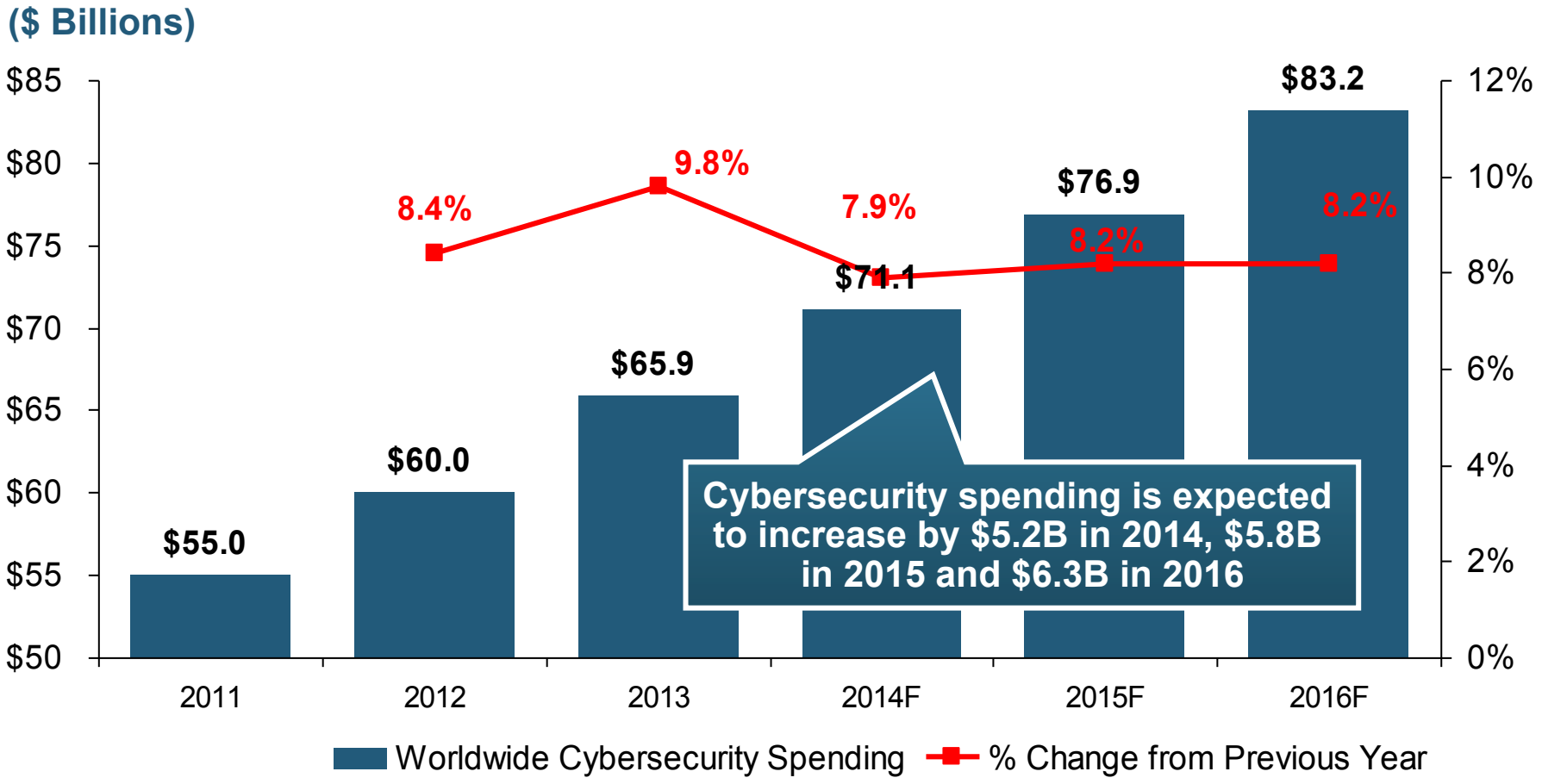



**The Total Number of Data Breaches (+38%) and Number of Records Exposed (+408%) in 2013 Soared**



* 2013 figures as of Jan. 1, 2014 from the ITRC updated to an additional 30 million records breached (Target) as disclosed in Jan. 2014.
Source: Identity Theft Resource Center.

# Worldwide Cybersecurity Spending, 2011- 2016F




**Cybersecurity Spending Is Rising Sharply, Up by About 8%+ Annually through 2016—a Projected Increase of $12.1 Billion from 2014 to 2016**

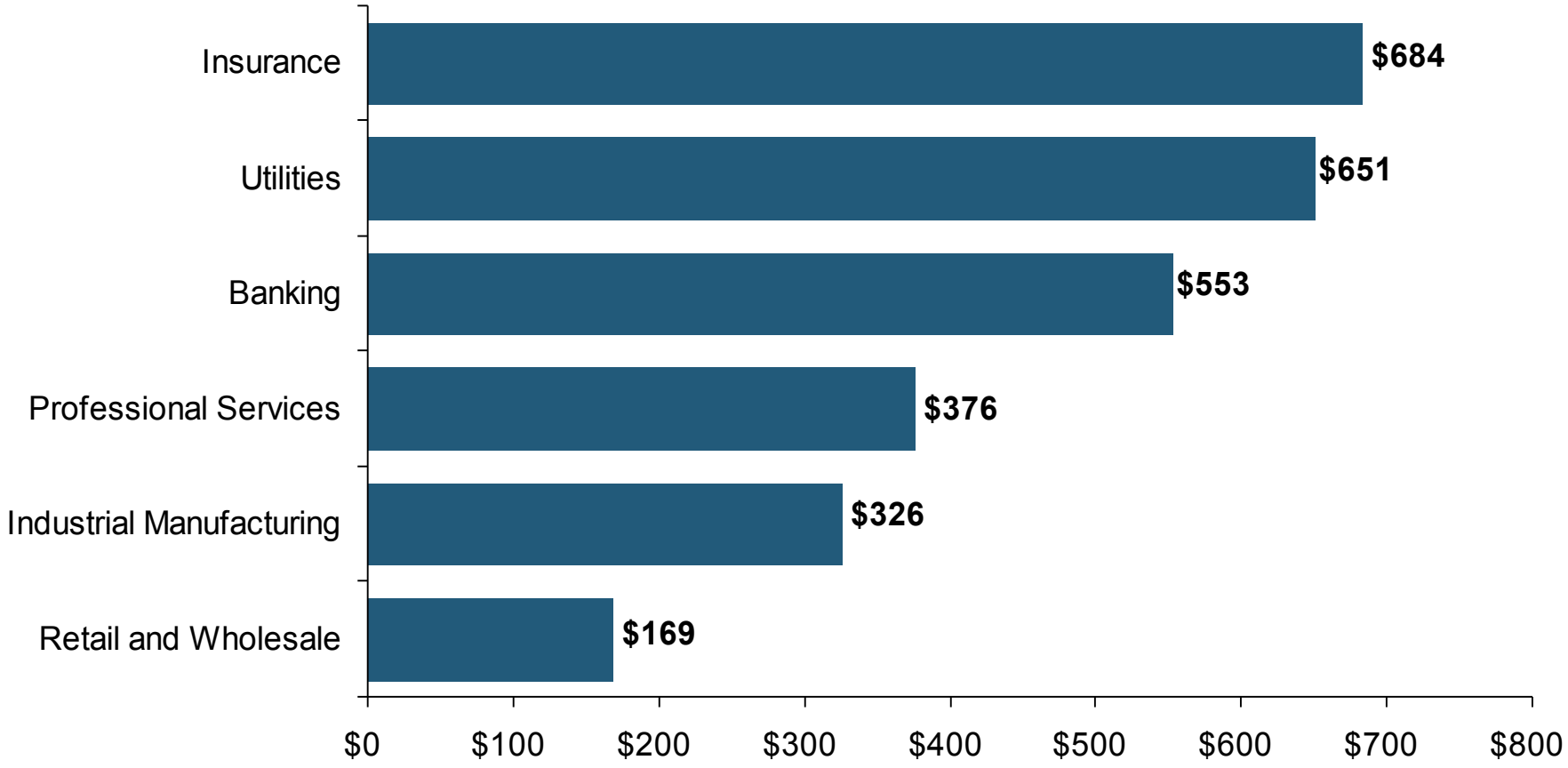


Source: Gartner Group; Insurance Information Institute; Adapted from *Wall Street Journal*: "Financial Firms Boost Cybersecurity Funds," Nov. 17, 2014.

# Worldwide Information Security Spending per Employee, by Industry, 2013

INSURANCE INFORMATION INSTITUTE

**(Dollars per Employee)**



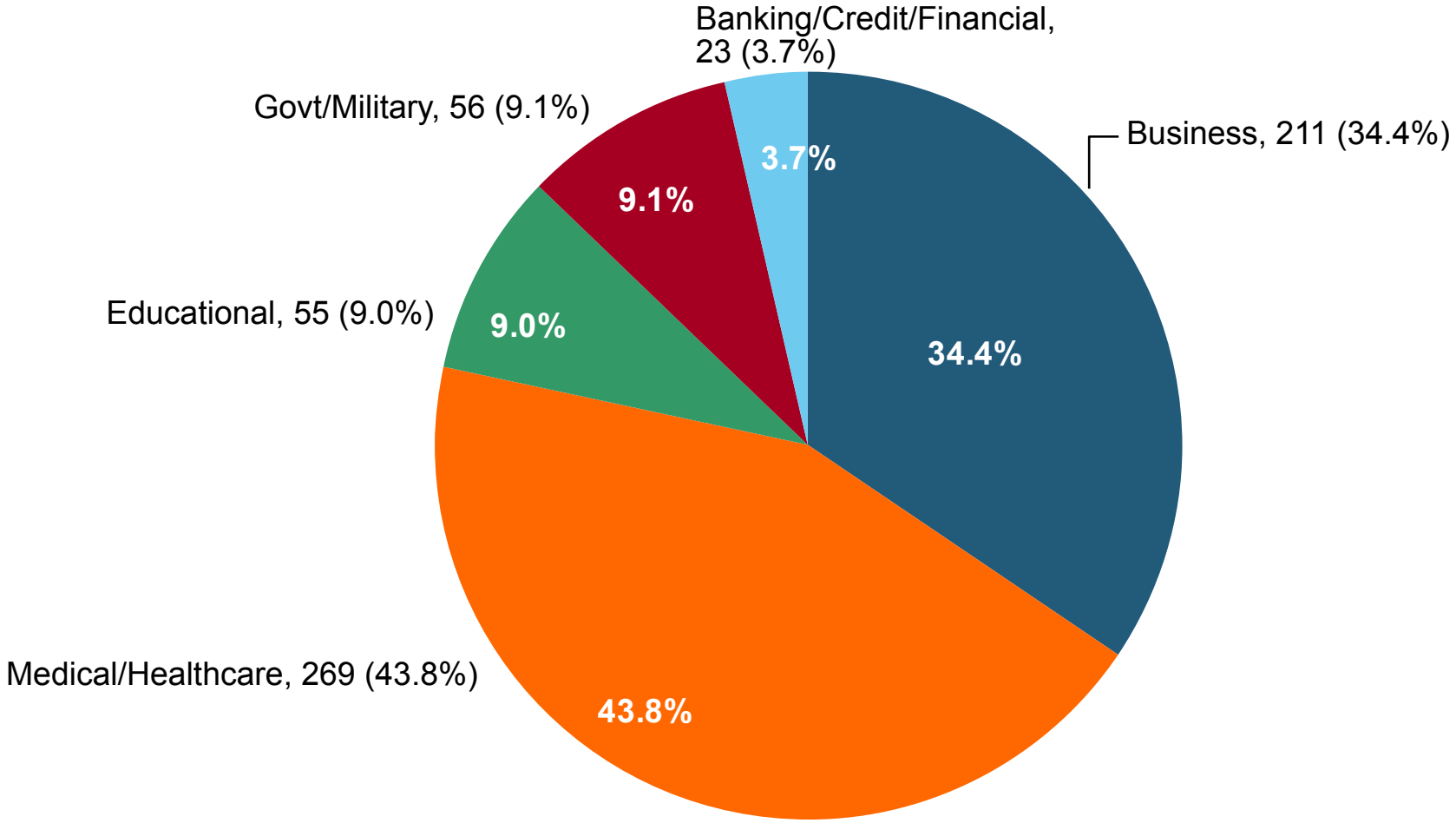

**Information Security Spending by Financial Services and Critical Infrastructure Industries (e.g., Utilities) Outpaces that of Other Industries**



Source: Gartner Group; Insurance Information Institute; Adapted from *Wall Street Journal*: "Financial Firms Boost Cybersecurity Funds," Nov. 17, 2014.

# 2013 Data Breaches By Business Category, By Number of Breaches

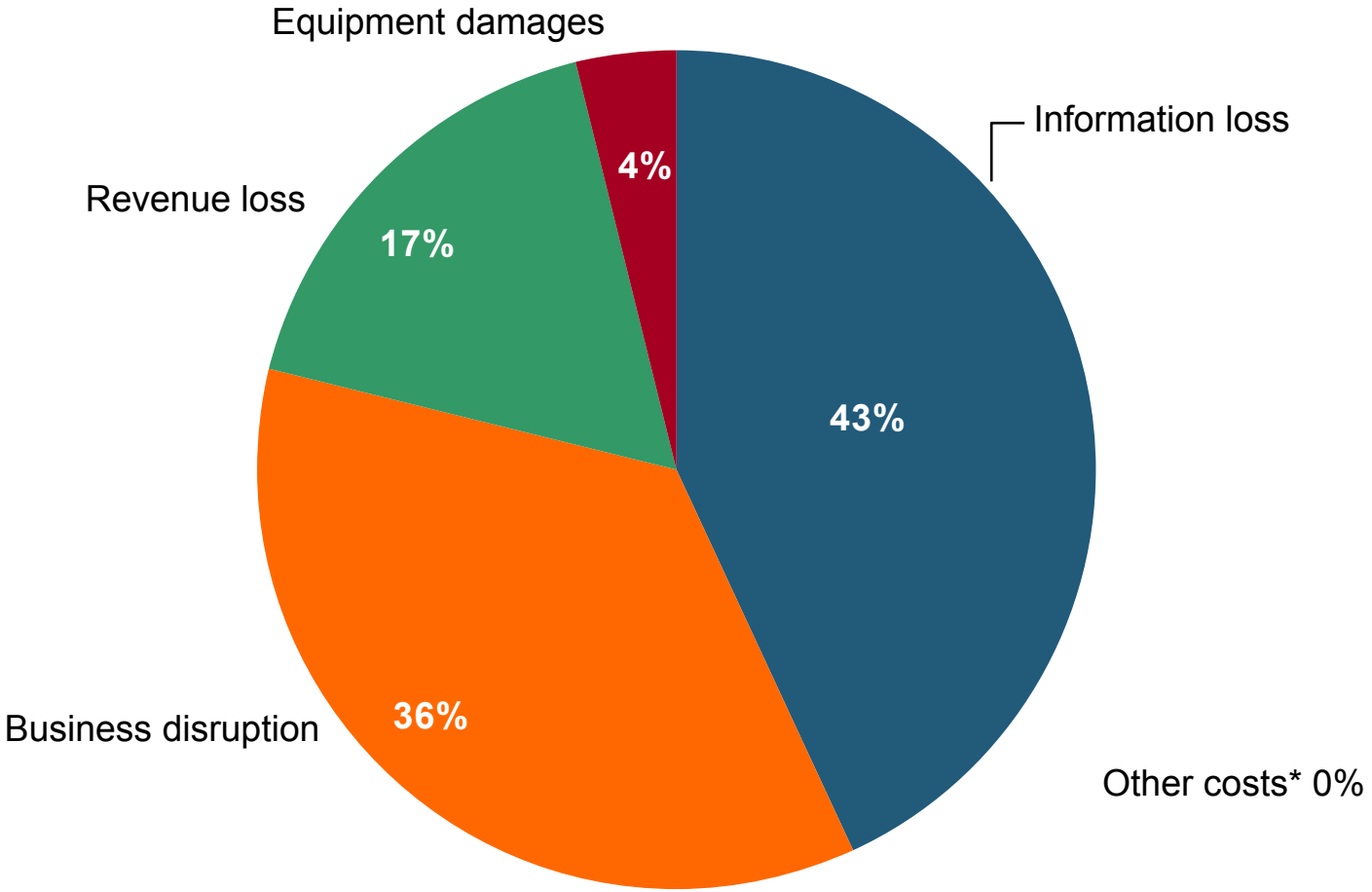
**The majority of the 614 data breaches in 2013 affected business and medical/ healthcare organizations, according to the Identity Theft Resource Center.**




Source: Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf

# External Cyber Crime Costs: Fiscal Year 2013

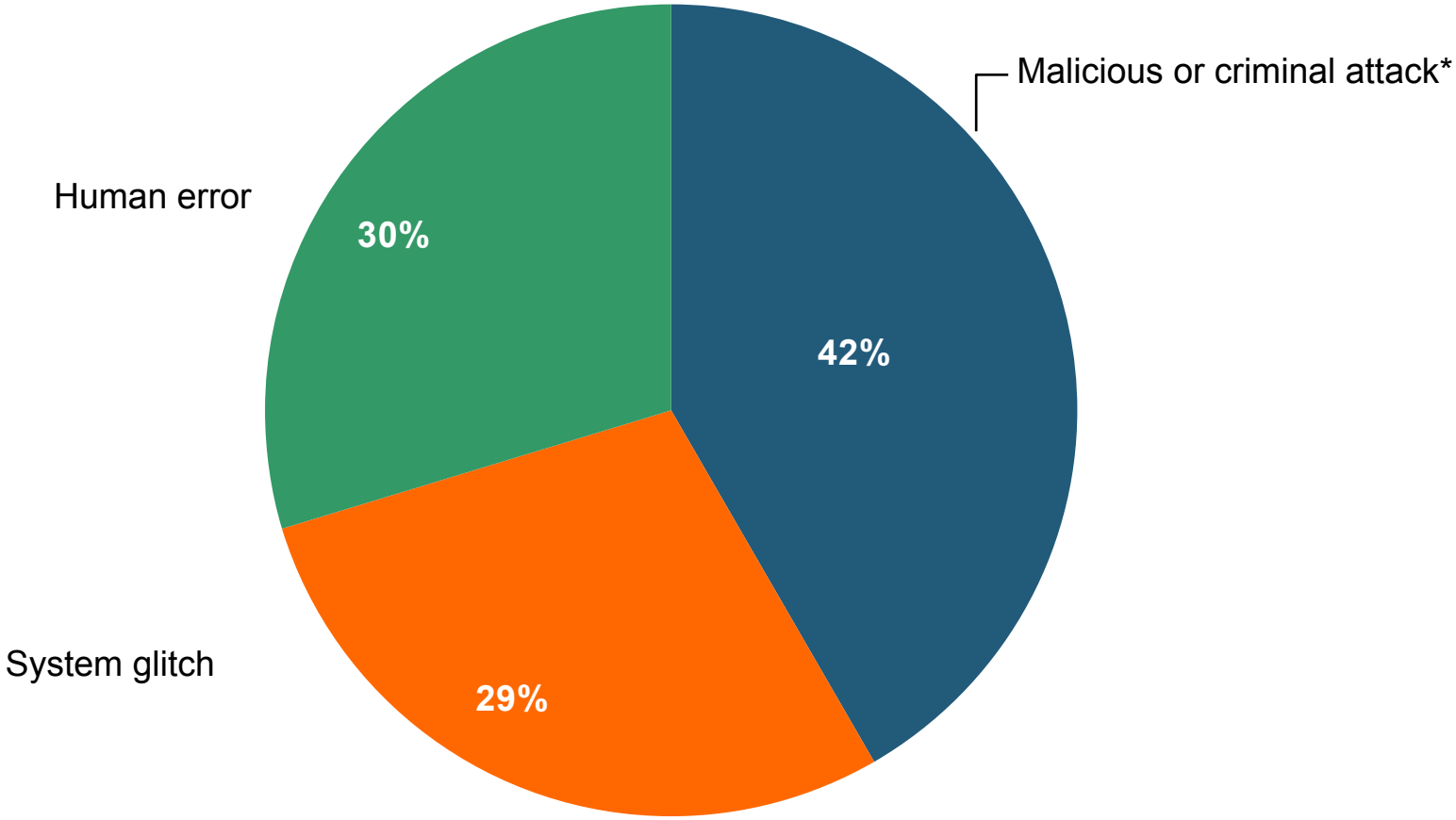
**Information loss (43%) and business disruption or lost productivity (36%) account for the majority of external costs due to cyber crime.**




* Other costs include direct and indirect costs that could not be allocated to a main external cost category
Source: *2013 Cost of Cyber Crime: United States*, Ponemon Institute.

# Main Causes of Data Breach Globally

**Malicious or criminal attacks are most often the cause of data breach globally. Some 42 percent of incidents concern a malicious or criminal attack, while 30 percent concern a negligent employee or contractor (human factor).**

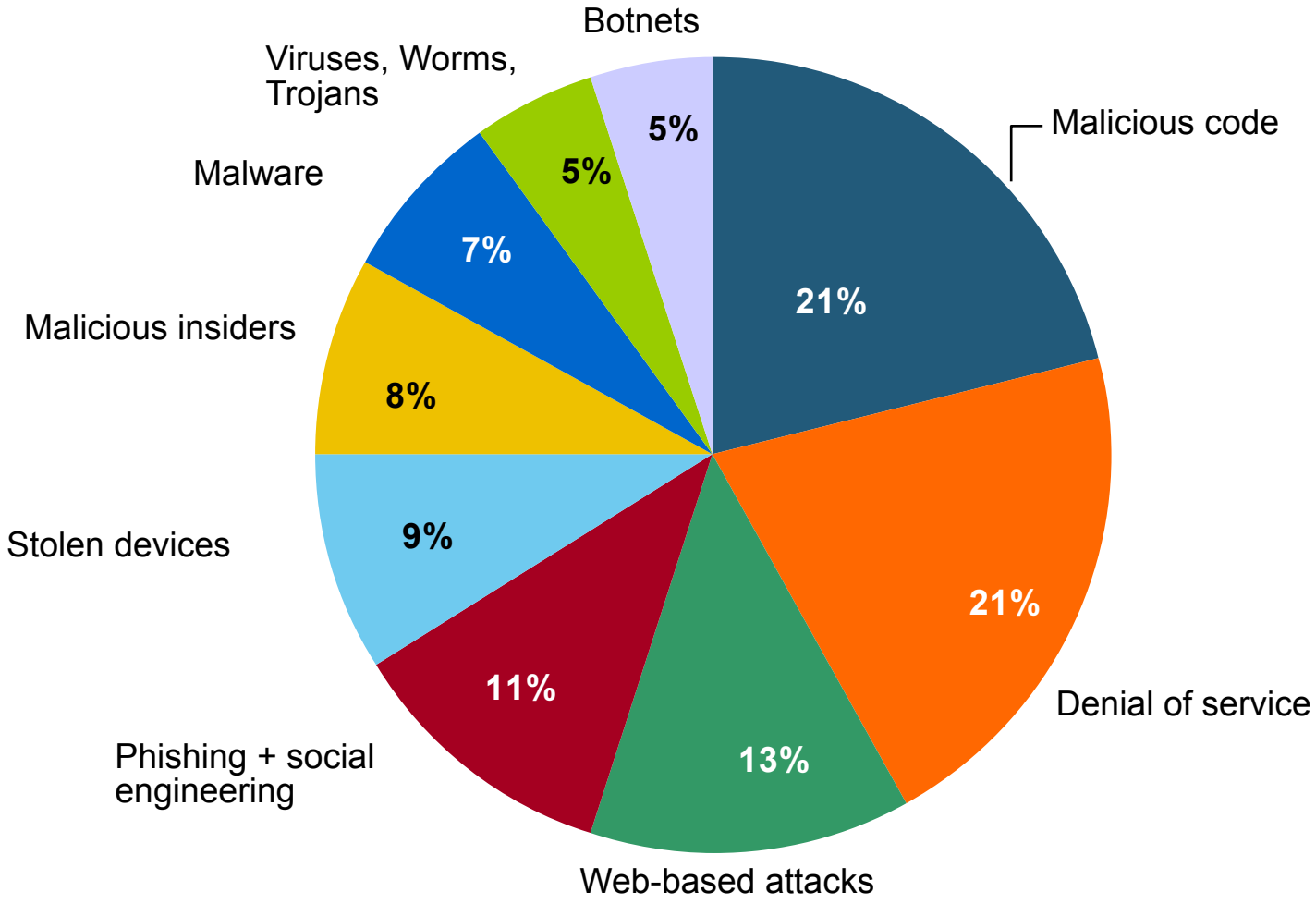



*The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Source: 2014 Cost of a Data Breach Study: Global Analysis, the Ponemon Institute, sponsored by IBM, May 2014

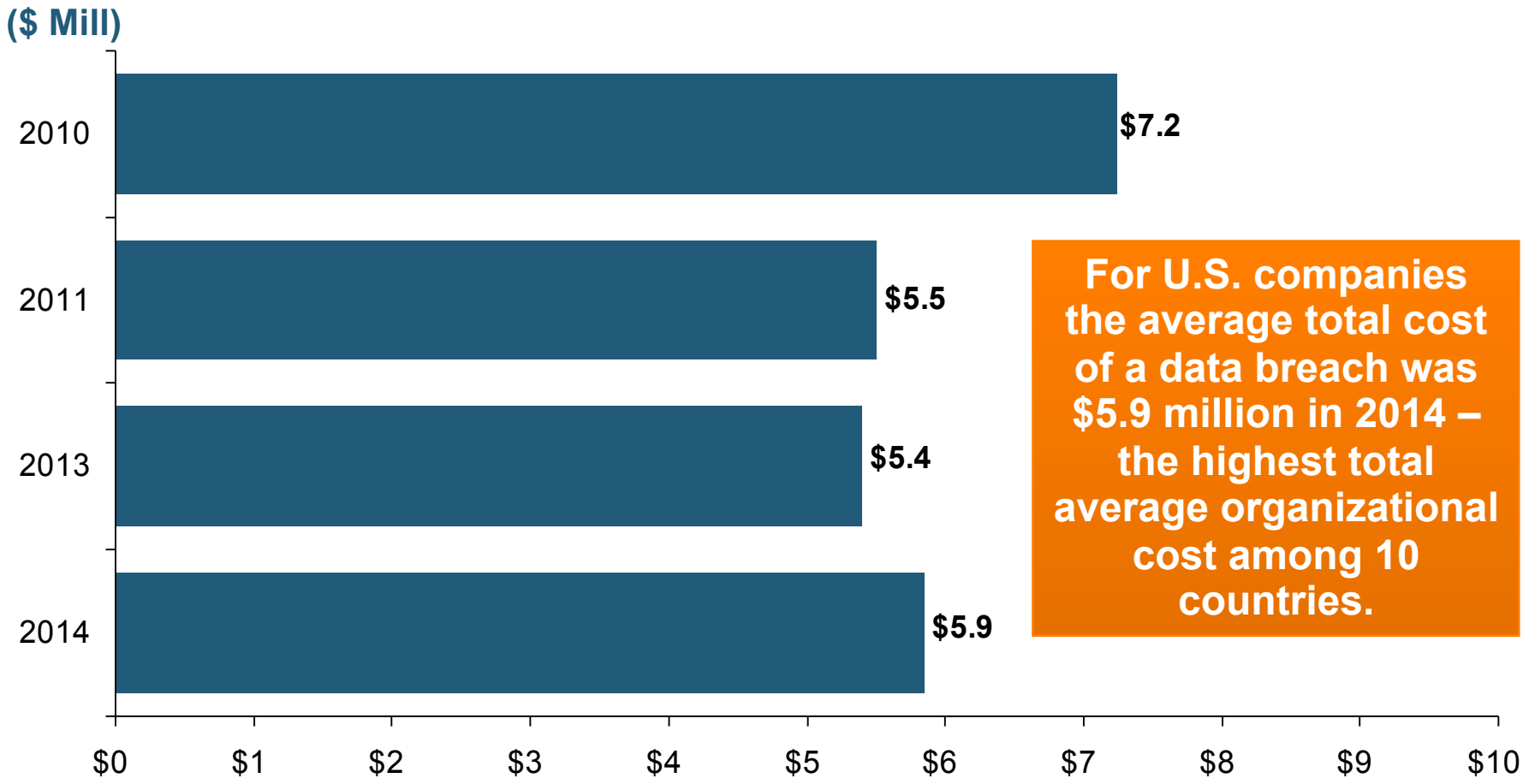
# The Most Costly Cyber Crimes, Fiscal Year 2013

**Denial of service, malicious code and web-based attacks account for more than 55 percent of all cyber costs per U.S. organization on an annual basis.**




Source: *2013 Cost of Cyber Crime: United States*, Ponemon Institute.

# U.S. Companies: Average Organizational Cost of a Data Breach, 2010-2014* ($ Millions)

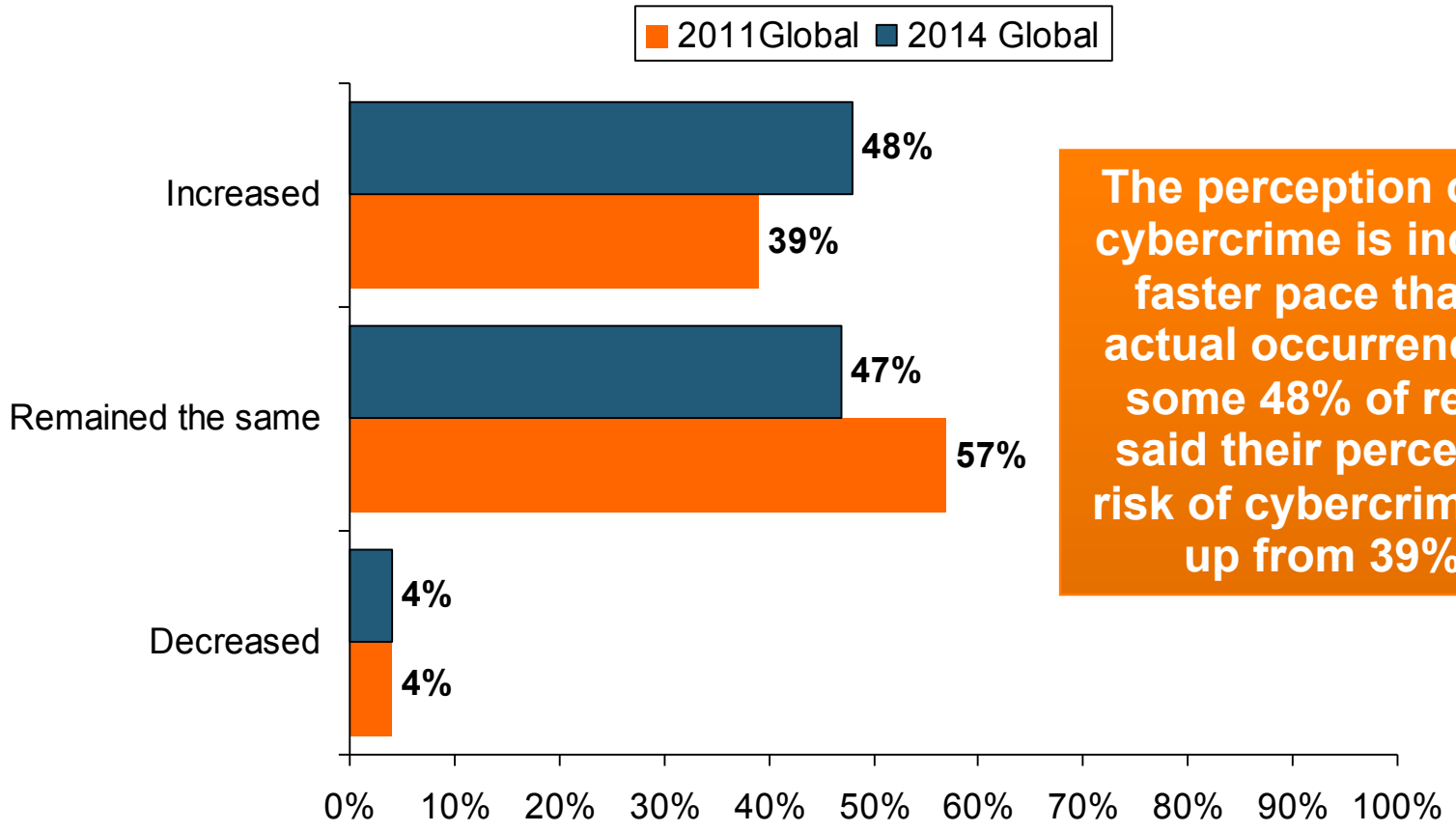



**For U.S. companies the average total cost of a data breach was $5.9 million in 2014 – the highest total average organizational cost among 10 countries.**

*The 2014 study examines the costs incurred by 314 companies across 16 industries representing 10 countries, including 61 U.S. case studies. Total breach costs include: lost business resulting from diminished trust or confidence of customers ;costs related to detection, escalation, and notification of the breach; and ex-post response activities, such as credit report monitoring.

Source: 2014 Cost of a Data Breach Study: Global Analysis, the Ponemon Institute, sponsored by IBM, May 2014

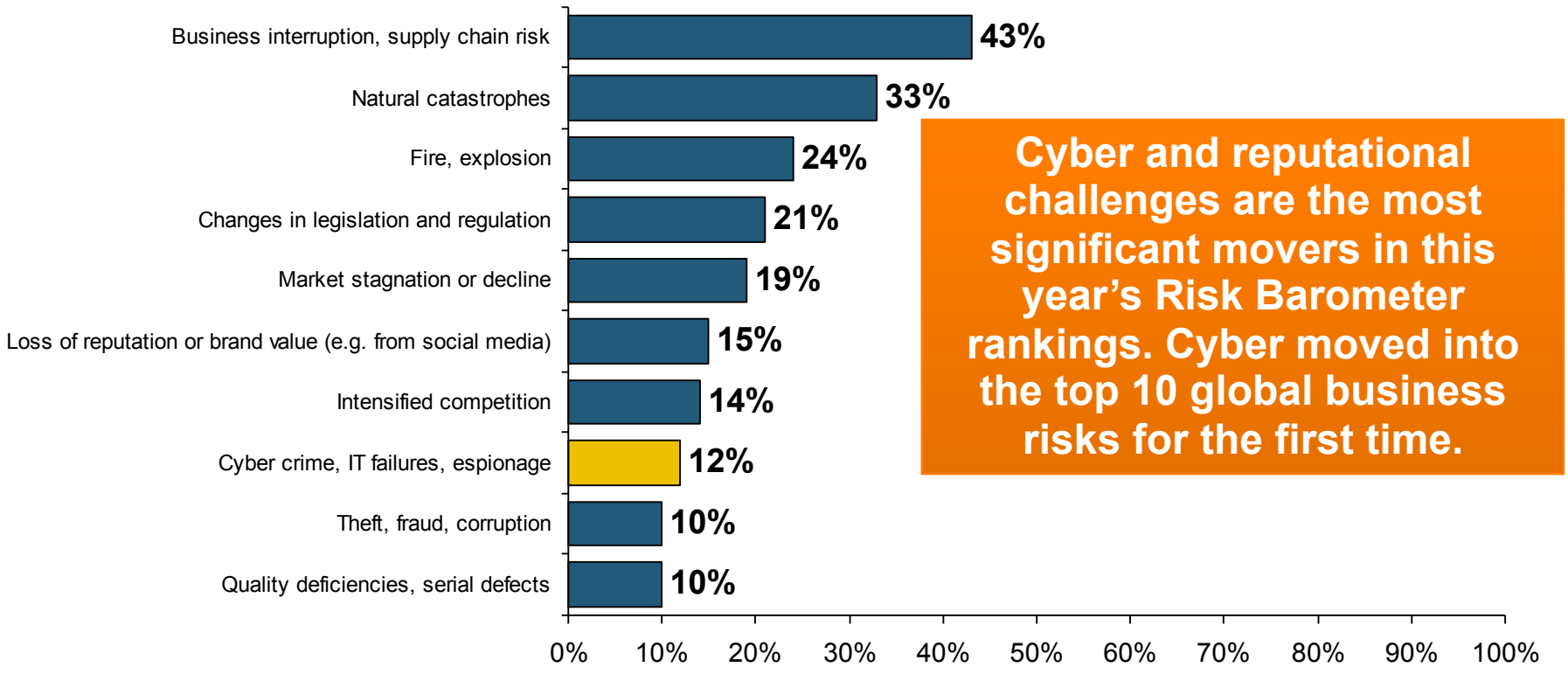
# PWC Survey: Perception of the Risk of Cybercrime




**The perception of the risk of cybercrime is increasing at a faster pace than reported actual occurrences. In 2014, some 48% of respondents said their perception of the risk of cybercrime increased, up from 39% in 2011.**

Source: 2014 Global Economic Crime Survey, PWC.

# Top 10 Global Business Risks for 2014




**Cyber and reputational challenges are the most significant movers in this year's Risk Barometer rankings. Cyber moved into the top 10 global business risks for the first time.**

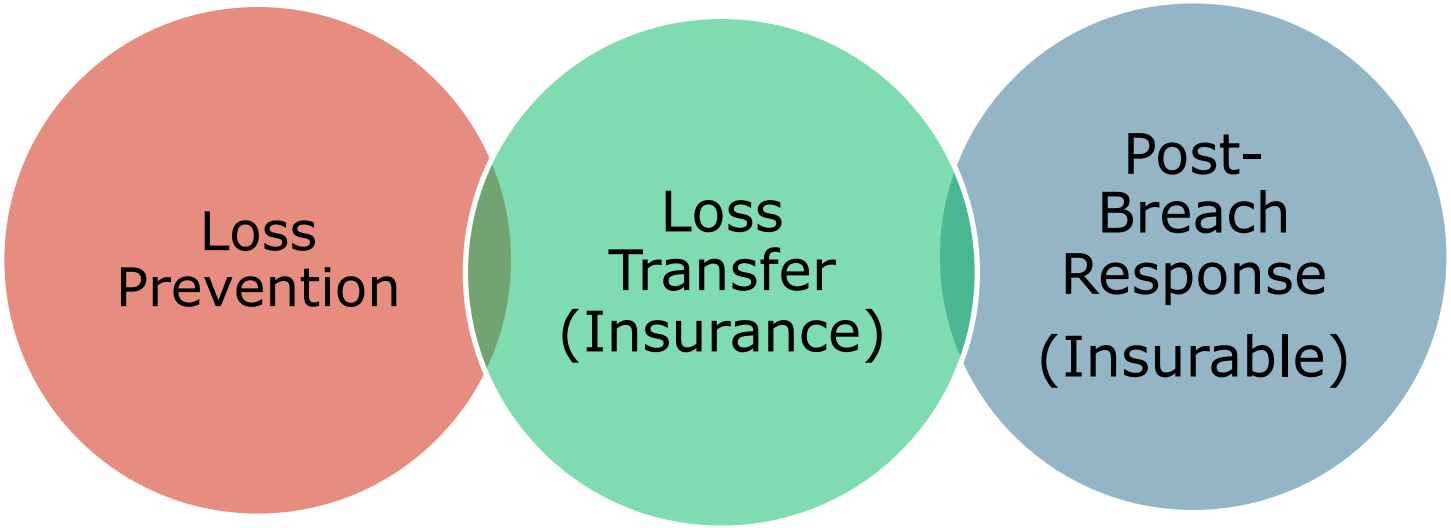
Source: Allianz Risk Barometer on Business Risks 2014

INSURANCE INFORMATION INSTITUTE

# TYPICAL STRUCTURE OF INSURER CYBER RISK PRODUCTS

## Insurers' Product Offerings Are Increasingly Designed to Provide End-to-End Cyber Risk Management Solutions

# The Three Basic Elements of Cyber Coverage: Prevention, Transfer, Response




**Cyber risk management today involves three essential components, each designed to reduce, mitigate or avoid loss. An increasing number of cyber risk products offered by insurers today provide all three.**

Source: Insurance Information Institute research.

# COMPONENT 1: Loss Prevention, Mitigation & Avoidance

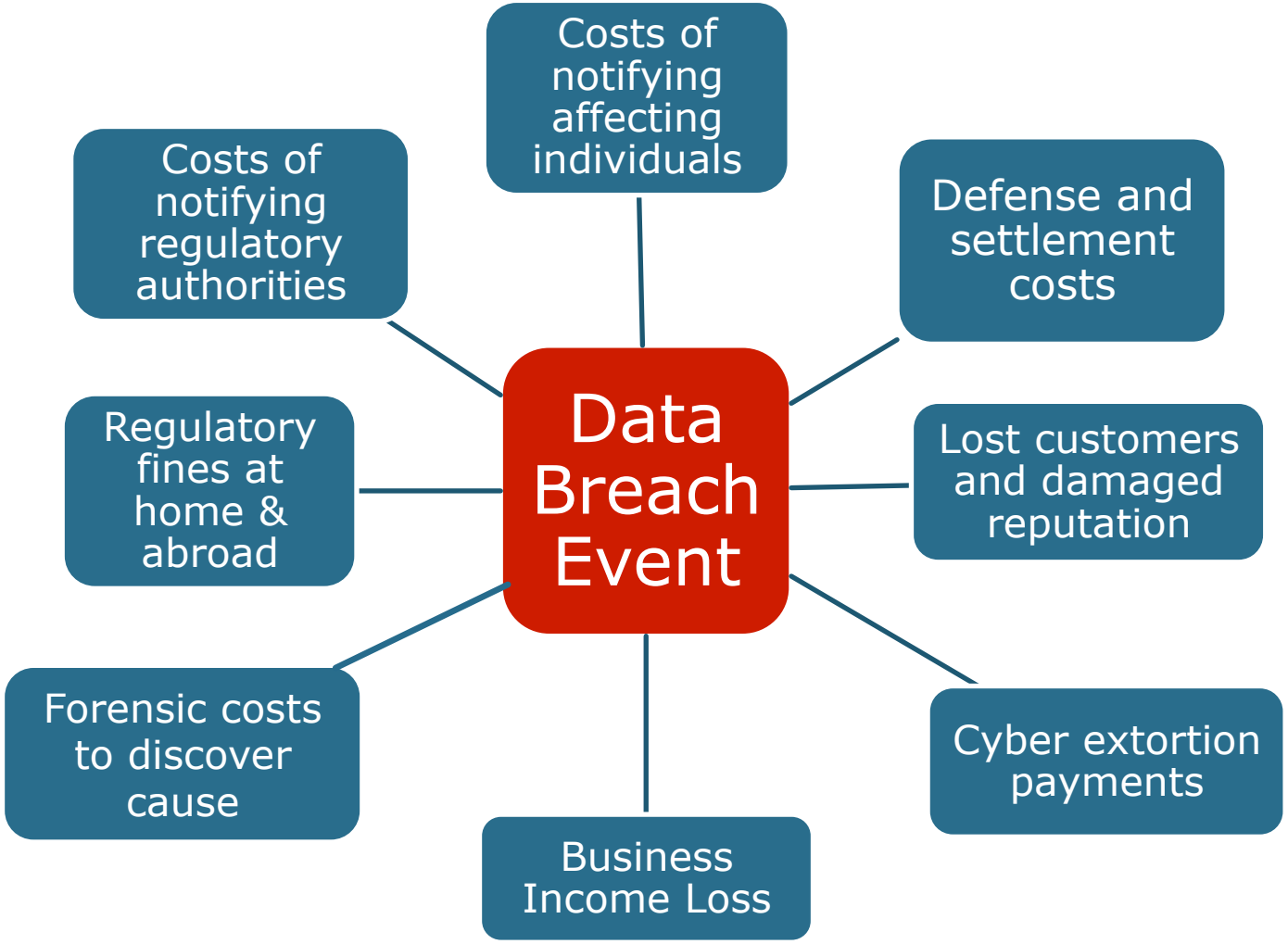
INSURANCE INFORMATION INSTITUTE

- **IT Systems Security Assessment**
- **Expert Advice**
- **Training Assistance for Staff**
- **Education**
- ***Hardware/Software to Enhance Defenses***

# COMPONENT 2: Loss Transfer (Insurance)

- 3rd–Party Liability Due to Breach
- Direct 1st –Party Breach Response Costs
- Directors & Officers, Errors & Omission and Fiduciary Liabilities
- Legal and Defense Costs

# Data/Privacy Breach: Many Potential Costs Can Be Insured




Source: Zurich Insurance; Insurance Information Institute

# COMPONENT 3: Post-Breach Response and Recovery (Frequently Insurable)

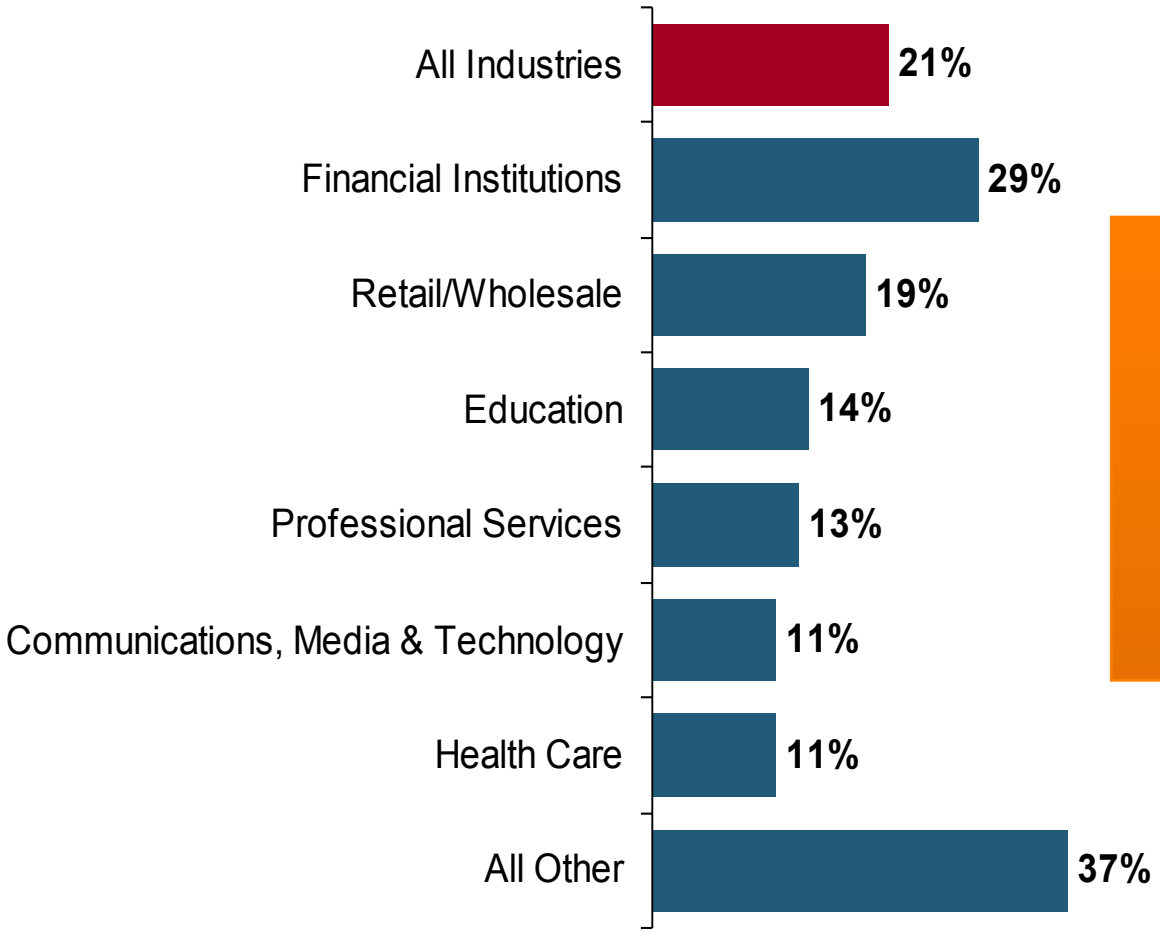
- Forensic Investigation Costs
- Notification Expenses
  - Affected individuals/businesses
  - Regulators
- Public Relations Expenses
- Legal Expenses
- Civil Fines and Penalties
- Business Income (Direct and Dependent) and Extra Expenses
- Cyber Extortion, Reward Payments

INSURANCE INFORMATION INSTITUTE

# CYBER RISK INSURANCE MARKETS

## Coverage Limits, Purchase Decisions & Pricing

# Increase in Purchase of Cyber Insurance Among U.S. Companies, 2013



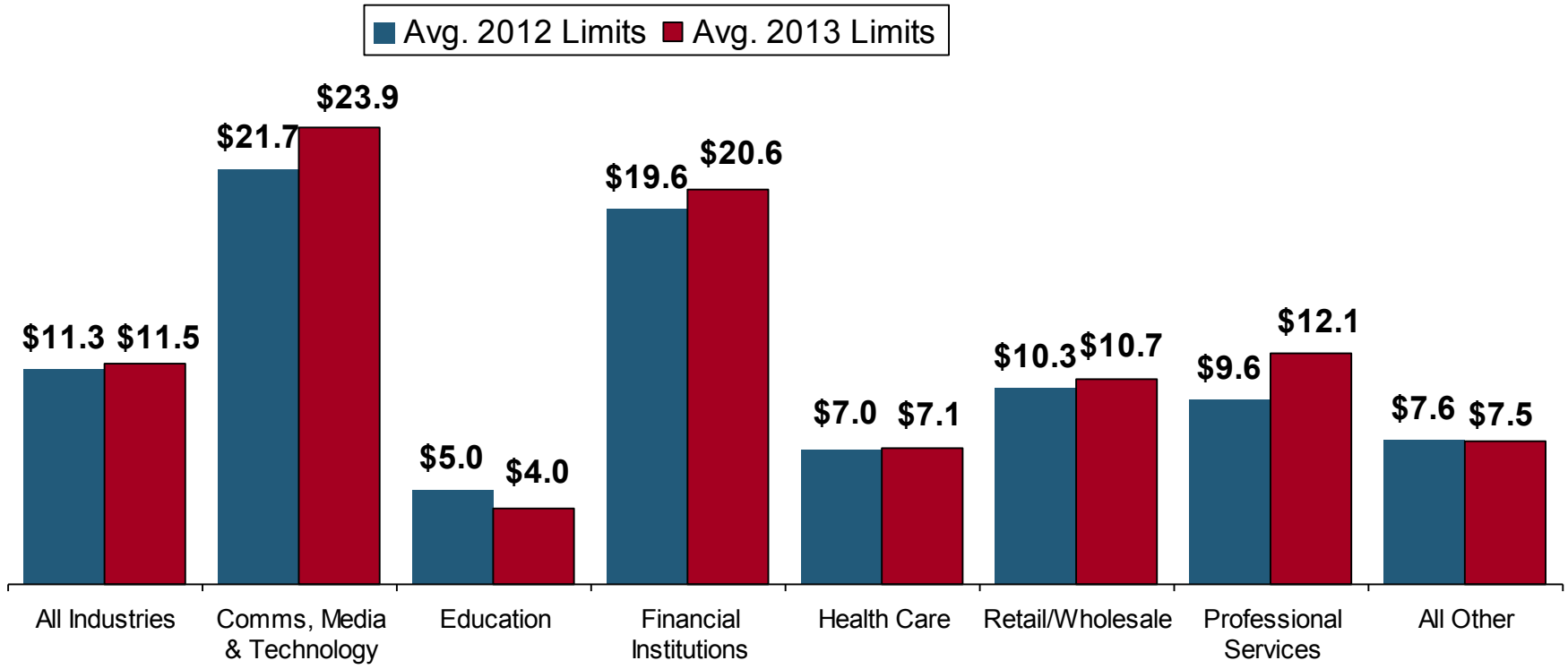

**Interest in cyber insurance continues to climb. The number of companies purchasing cyber insurance increased 21 percent from 2012 to 2013.**

Source: *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh Risk Management Research Briefing, April 2014

# Marsh: Total Limits Purchased, By Industry – Cyber Liability, All Revenue Size

**Average limits purchased for cyber risk rose to $11.5 million for all industries and all company sizes in 2013, a slight increase over the average of $11.3 million in 2012.**

($ Millions)

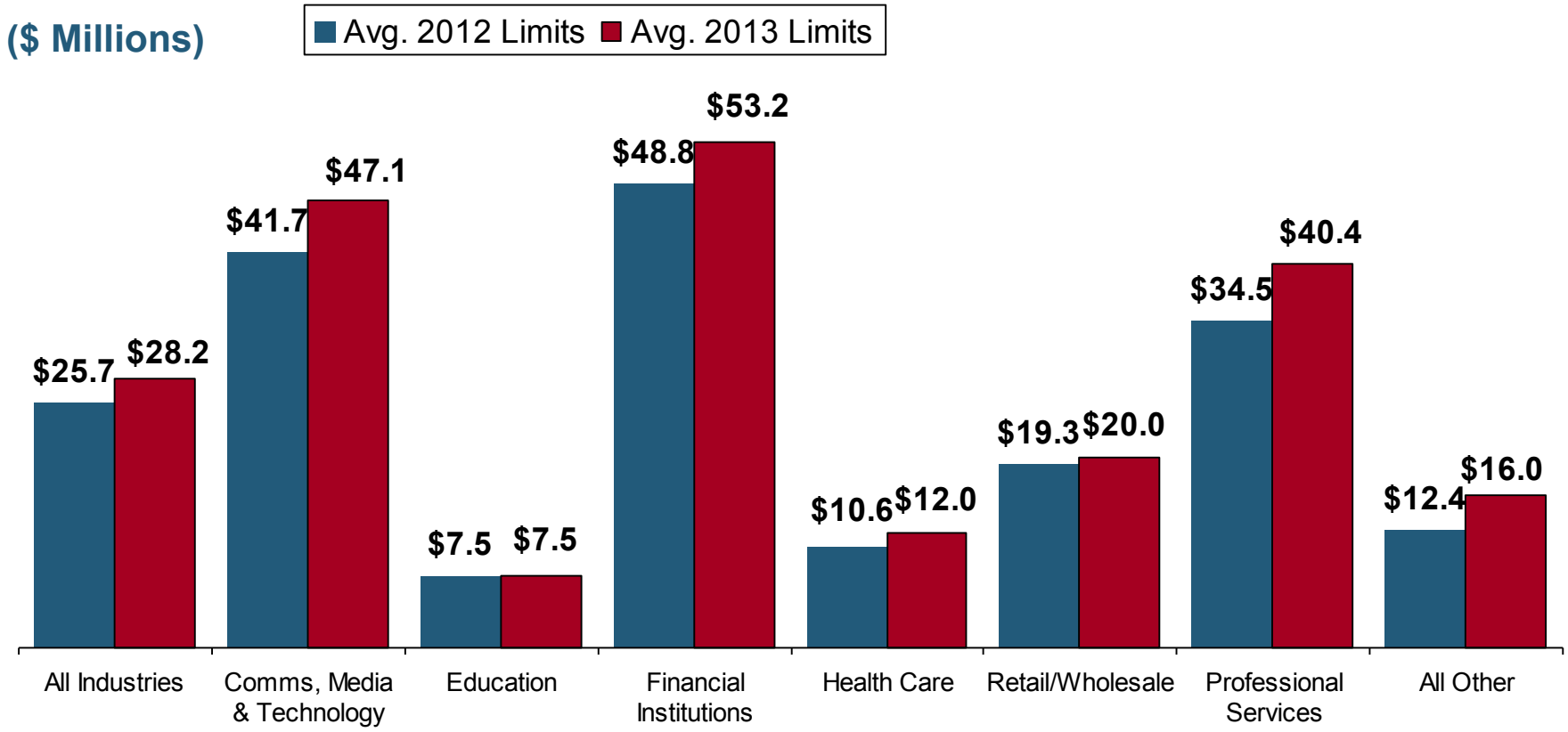



Source: *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh Risk Management Research Briefing, April 2014

# Marsh: Total Limits Purchased, By Industry – Cyber Liability, Revenue $1 Billion+

INSURANCE INFORMATION INSTITUTE

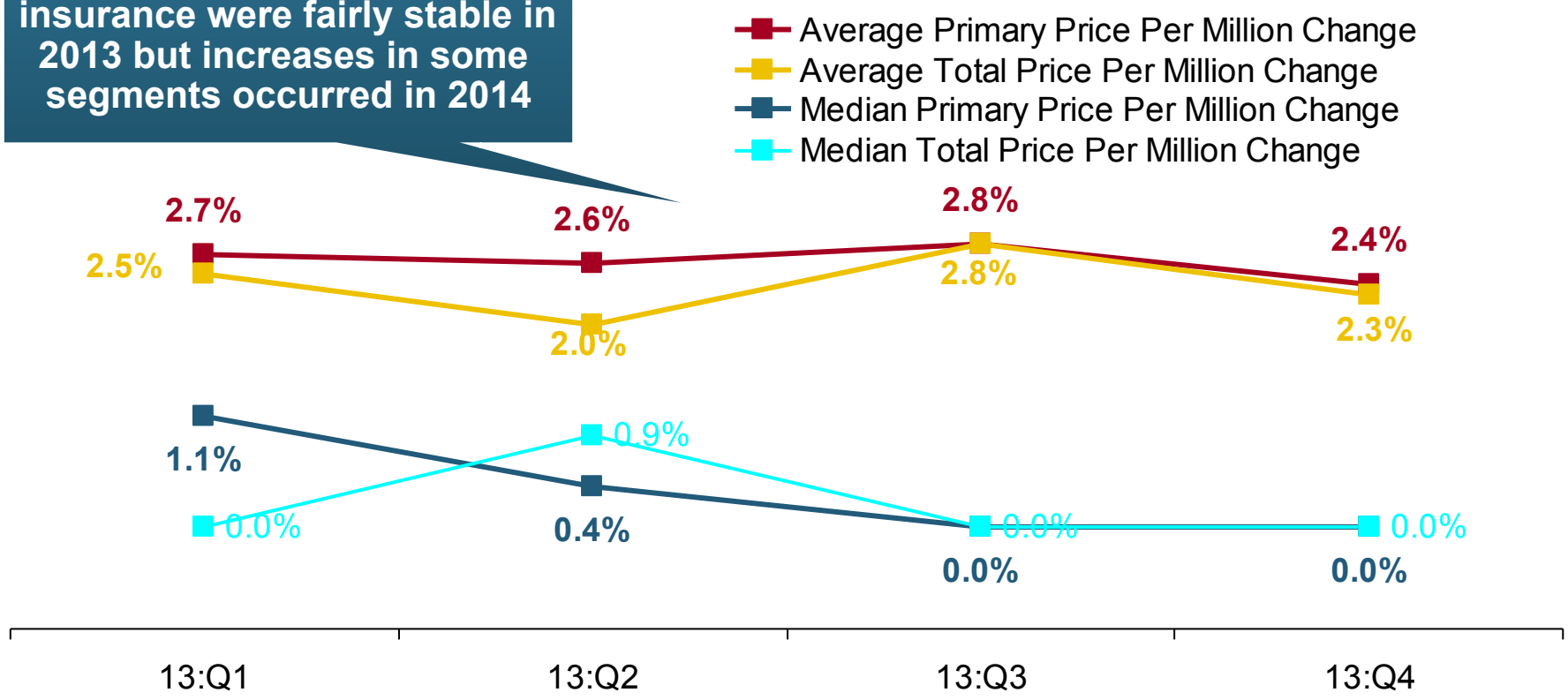
**Among larger companies, average cyber insurance limits purchased increased by 10 percent to $28.2 million in 2013, from $25.7 million in 2012.**




Source: *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh Risk Management Research Briefing, April 2014

# Cyber Liability: Historical Rate Changes (price per million)

**Overall, rates for cyber insurance were fairly stable in 2013 but increases in some segments occurred in 2014**




Source: *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh Risk Management Research Briefing, April 2014

INSURANCE INFORMATION INSTITUTE

## Insurance Information Institute Online:

# www.iii.org

***Thank you for your time and your attention!***

***Twitter: twitter.com/bob_hartwig***

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

# Corporate Governance and Compliance Considerations

Charles White | *Director, PricewaterhouseCoopers*
Lori Anne Czepiel, Esq. | *Partner, Lewis Brisbois Bisgaard & Smith LLP*

# Concerning Risk

- ✓What is the risk to our organization?
- ✓What are we doing about the risk?
- ✓Are we doing enough?

# Evolving Threats

| | |
|---|---|
| State Sponsored Groups | • Foreign government sponsored<br>• Sophisticated and **well-funded** |
| Organized Cyber Criminals | • Traditional organized crime groups<br>• Loosely organized **global** hacker crews |
| Hacktivists | • **Politically-motivated** hackers<br>• Increasing capabilities |
| Insiders | • Easy access to sensitive information<br>• Difficult to detect |
| Terrorists | • **Destruction** of physical and digital assets |

# Digital Duties and Obligations

- ✓ Does the organization understand its digital duties and obligations?
  - Contractual, Regulatory and Statutory
- ✓ Addressing these concerns forms the foundation of a security program.
  - The most comprehensive area today concerns data privacy.
- ✓ Is the security program **reasonable**?
  - What is reasonable for one organization may be different for another.
- ✓ Organizations must be able to demonstrate they are **Good Corporate Citizens**—Were it not for the criminal acts of some group, the organization's **procedures and protocols were reasonable.**

# Cyber Governance

- ✓ Does the organization's governance model identify the senior officer within the organization responsible for breach detection, remediation, escalation and notification?
  - Establishment of the governance model *ex-post-facto* to be avoided. Investigators and/or regulators may be present.

- ✓ Does the organization understand its **Enterprise Technical Debt**?
  - Vast majority of breaches originate from vulnerabilities the organization knew about, or should have known about.

- ✓ Does the Enterprise Risk Plan properly reflect the cybersecurity risk?
  - The most recent SEC flash report unambiguously states all registrants' enterprise risk registers should reflect cybersecurity risk. Many of investigations have shown that organizations consider cybersecurity an IT risk vs. an enterprise risk.

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

# Corporate Governance and Compliance Considerations: *Summary Checklist of Key Issues for Cyber Risk Oversight and Planning*

**November 18, 2014**

Lori Anne Czepiel, Esq. | Partner, Lewis Brisbois Bisgaard & Smith

LoriAnne.Czepiel@LewisBrisbois.com / 646-239-5008 / 213-281-5225

# Key Issues for Cyber Risk Oversight and Planning

- ***Directors can be liable*** for a failure of board oversight to monitor risk where there is sustained or systemic failure of the board to exercise oversight, such as ***where they****:*

  - *Utterly* ***fail to implement any reporting or information systems or controls, or***

  - *Having implemented such a system or controls, consciously* ***fail to monitor or oversee*** *its operations* thus disabling themselves from being informed of risks or problems requiring their attention.

*[In re Caremark International Derivative Litigation (1996), Stone v. Ritter (1996). Also Palkon v. Holmes (2014) (re: Wyndham hotels data breach)]*

# Key Issues for Cyber Risk Oversight and Planning

- ***In the absence of "red flags"*** the manner in which a company evaluates the risks involved with a given business decision is protected by the business judgment rule and ***will not be second-guessed*** *by courts*.

  *[For example, In re Citigroup Inc. Shareholder Derivative Litigation (2009), Goldman Sachs Group Inc. Shareholder Litigation (2011)]*

# Key Issues for Cyber Risk Oversight and Planning

- **Board-Level Attention to IT Governance/Cyber Security**
  - ✓ Board education
  - ✓ Recruit director with relevant expertise
  - ✓ Board committee focused on cyber risk
  - ✓ Work with outside experts
  - ✓ Regular briefing on privacy and cyber developments, specific risks and protocols

# Key Issues for Cyber Risk Oversight and Planning

- **Board-Level Attention to IT Governance/Cyber Security (cont.)**
  - ✓ Understand legal and fiduciary duty requirements, and Board's role in connection with response to cyber incidents
  - ✓ Attention to staffing/budget for management and outside consultants
  - ✓ Monitor performance through sufficient reporting systems, and oversee internal investigations
  - ✓ Keep current with best practice guidance, including from governance organizations and proxy advisory firms
  - ✓ Develop corporate culture aligned with cyber risk management priorities

# Key Issues for Cyber Risk Oversight and Planning

## ➢ Management Focus on Cyber Security

- ✓ Appoint dedicated senior executive for cyber security, regularly reporting to Board
- ✓ Appoint executive committee of internal management and business division stakeholders, to assess, oversee and report to Board on privacy and cyber issues
- ✓ Assess prior and current practices in light of regulatory and disclosure issues/requirements, including SOX
- ✓ Develop cyber risk management framework, policies and controls in consultation with Board

# Key Issues for Cyber Risk Oversight and Planning

## ➢ Assess and Develop Risk Management Framework

- ❑ Risk Assessment
  - ✓ Inventory data required to be protected, scope of privacy obligations
  - ✓ Assess controls, risk profile and tolerance (external and internal risk)
  - ✓ Determine risks to avoid, accept, mitigate or transfer through insurance, and value of potential losses and insurance coverage/ needs; review at least annually
  - ✓ Assess D&O liability coverage, other protections and exculpations; determine any changes needed

# Key Issues for Cyber Risk Oversight and Planning

- **Assess and Develop Risk Management Framework (cont.)**
  - Legal Assessment
    - ✓ Assess and understand compliance/regulatory and disclosure requirements, fiduciary duties; reconcile conflicts of laws and other requirements
    - ✓ Discuss/consider when to notify law enforcement, and related issues
    - ✓ Assess company contracts for response requirements and issues; determine any changes needed (vendor/supplier contracts, and contracts/templates for company customers)

# Key Issues for Cyber Risk Oversight and Planning

- **Assess and Develop Risk Management Framework (cont.)**
  - Additional Legal Assessment
    - ✓ Assess counterparty risk from third-party service providers and their subcontractors; address notification/disclosure and other desired protections in contracts
    - ✓ Understand issues and requirements (including notice and disclosure, restoring confidence) for markets, lenders, vendors, suppliers, customers, employees, proxy advisory services, etc.
    - ✓ Consult outside experts to audit/review current controls and policies, and examine/understand best practice protocols

# Key Issues for Cyber Risk Oversight and Planning

- **Assess and Develop Risk Management Framework (cont.)**

  - Engage Outside Advisors with Cyber Security Expertise
    - ✓ IT/Security
    - ✓ Legal – data security/cyber response, governance, specific industry and other regulatory compliance issues, white collar criminal
    - ✓ Forensic
    - ✓ Insurance
    - ✓ PR/Crisis Communications

  - Develop Your Crisis Management Plan
    - ✓ Appoint incident response team, and assign roles/responsibilities and chain of command
    - ✓ Develop written incident response plan

# Key Issues for Cyber Risk Oversight and Planning

- **Assess and Develop Risk Management Framework (cont.)**
  - Focus on Company Culture
    - ✓ Develop general security standards, and policies for reporting incidents upstream
    - ✓ Conduct related training programs for entire organization
    - ✓ Align risk management and exec comp, business opportunities (including M&A)

# Key Issues for Cyber Risk Oversight and Planning

- **Assess and Develop Risk Management Framework (cont.)**
  - Actively Monitor Performance, Plan and Developments, Before and After Breaches
    - ✓ Maintain sufficient reporting systems as the business evolves
    - ✓ Track history of breaches and attacks, responses
    - ✓ Test often - assess gaps and effectiveness of controls, policies, plans and training; investigate and adjust accordingly
    - ✓ Stay current – follow changing threats, laws and practices

# Key Issues for Cyber Risk Oversight and Planning

*For questions and additional information, please contact:*


Lori Anne Czepiel | Partner, Lewis Brisbois Bisgaard & Smith

LoriAnne.Czepiel@LewisBrisbois.com

646-239-5008 | 213-281-5225

https://www.linkedin.com/in/lorianneczepiel

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

# Developing Incident Response Plans

John Mullen, Esq. | *Partner, Lewis Brisbois Bisgaard & Smith LLP*
Charles White | *Director, PricewaterhouseCoopers*

# What Threats?

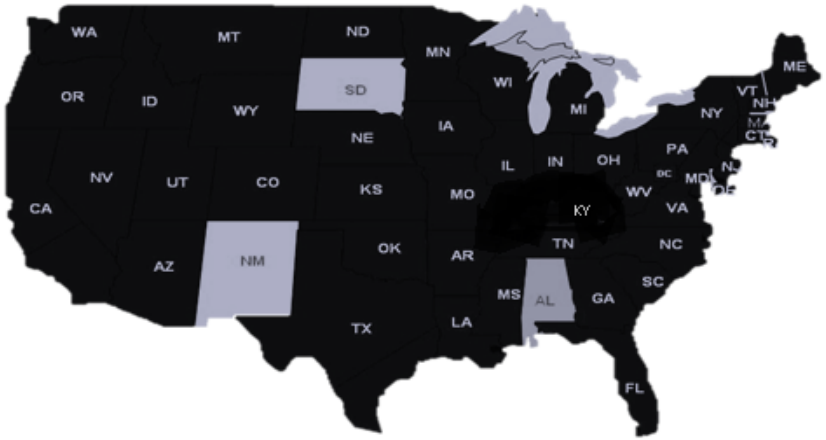
- **Malicious attack**
  - Hackers in network, Malware and viruses, Phishing scams, Physical theft of hardware and paper
  - Rogue employees
- **Employees**
  - Negligence related to use and storage of data, failure to follow or learn policies and procedures, loss of portable devices, mis-mailing of paper, unencrypted emails to the wrong recipients
- **Business partners**
  - Any of the above can occur to a business partner with whom data is shared

# Are You At Risk? Ask Your Team:

| | |
|---|---|
| • Has your firm ever experienced a data breach or system attack event? | *Studies show 80-100% of execs admitted to a recent breach incident* |
| • Does your organization collect, store or transact any personal, financial or health data? | |
| • Do you outsource any part of computer network operations to a third-party service provider? | *Your security is only as good as their practices and you are still responsible to your customers* |
| • Do you allow outside contractors to manage your data or network in any way? | *The contractor is often the responsible party for data breach events* |
| • Do you partner with entities and does this alliance involve the sharing or handling of data? | *You may be liable for a future breach of your business partners* |
| • Does your posted Privacy Policy align with your actual data management practices? | *If not you may be facing a deceptive trade practice allegation* |
| • Has your organization had a recent cyber risk assessment of security/ privacy practices to ensure that they are reasonable and prudent and measure up with your peers? | *Doing nothing is a plaintiff lawyer's dream.* |

# State Regulatory Exposures

State level breach notice: 47 states (plus Puerto Rico, Wash. D.C., Virgin Islands) require notice to customers after unauthorized access to PII/PHI.




- Require firms that conduct business in state to notify resident consumers of security breaches of unencrypted computerized personal information
- Many require notification of state attorney general, state consumer protection agencies, and credit monitoring agencies
- Some states allow private right of action for violations
- Data-at-rest (disc level) encryption often a safe harbor

# Evolving Exposures

**VERMONT**

- Notice to affected individuals within 45 days of breach discovery
- Notice to VT AG within 14 days of breach discovery or affected individual notice (whichever is sooner)

**CONNECTICUT**

- Department licensees and registrants to notify Department [Commissioner] as soon as incident affecting Connecticut residents is discovered, but no later than 5 calendar days after
- Notice to CT AG no later than time when notice provided to Connecticut residents

**TEXAS**

- Notice to affected individuals pursuant to law of individual's state of residence or, if none, then pursuant to TX

**CALIFORNIA**

- Notice (electronic) to CA AG if more than 500 California residents affected
- HIPAA provisions augmented
- Notice to California Department of Health and affected individuals within 5 business days (15 days as of 1/1/2015)
- Statutory damages/fines, private cause of action
- 12 months of identity theft prevention and mitigation services at no cost to affected individual

**MASSACHUSETTS**

- "Written information security plan" for businesses storing MA resident personal information

**NEVADA**

- Data collectors doing business in NV to comply with PCI-DSS

# Examples of Federal Regulatory Exposures

- HIPAA/ HITECH
  - Covered Entities and their Business Associates
  - Notice within 60 days (to HHS and Media if more than 500)
- FTC
  - FTC Act protecting against “unfair and deceptive trade practices” enables FTC to investigate and fine entities suffering data breaches.
- SEC
  - 2011 Guidance *suggests* disclosure of material cyber risks

# More Federal & Other Regulations

- FERPA (Family Educational Records Protection Act)
  - federal funding can be (but never has been) cut off following violations.
- SOX (Sarbanes Oxley)
  - Requires security controls, and auditors will require disclosure if such controls are inadequate.
- GLB (Gramm-Leach-Bliley - for financial institutions)
  - Privacy Rule suggests notification; Safeguards rule suggests written security plan.
- FACTA (Regulates entities that use credit reporting)
  - Red Flags Rule requires procedures to detect and prevent identity theft
- International
  - EU and 45 other countries have data protection or privacy laws

# Payment Card Industry (PCI)

- Payment Card Industry Security Standards Council (Visa, Mastercard, AmEx, Discover, JCB International)
- Requires merchants and service providers to abide by certain protocols to protect customers' credit card information
- Imposes "fines" and "penalties" on offending merchants and service providers (can be millions)
- Violations of PCI DSS have multiple consequences
- Impact on standard of care – industry investigations, outside lawsuits
- Small minority of states have incorporated PCI-DSS requirements into data protection laws

# Regulator/Compliance Costs

Breach Costs

- Forensics vendor
- Notification vendor
- Call centers
- PR vendor
- ID theft insurance
- Credit monitoring
- ID restoration
- Attorney oversight

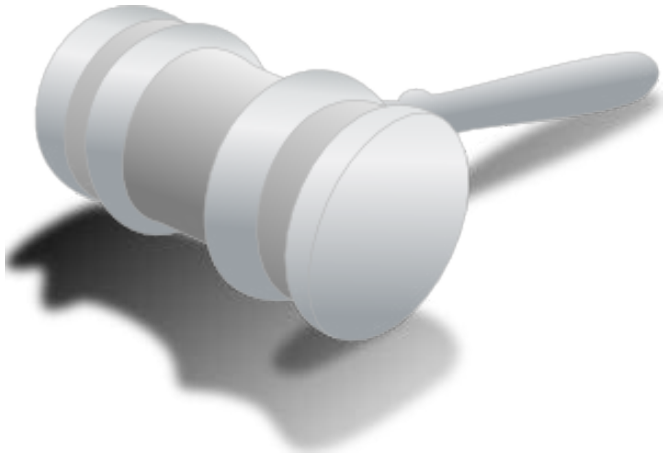
Planning and Data Management

- Breach planning (Mass.)
- ID Theft monitoring (Red Flags)
- PCI DSS (Nevada and merchants)
- HIPAA

# Litigation Trends

- Single Plaintiff
  - Identity theft
  - Privacy
- Government Action
  - **Attorney General**
  - **FTC**
  - **HHS**
- Banks
  - Cost of replacing credit cards
  - Reimbursement of fraudulent charges
  - Business interruption

- Class Action
  - Failure to protect data
  - Failure to properly notify
  - Failure to mitigate
  - NO VERDICTS. . . *YET*



# Regulator Actions - AGs

## California

- Kaiser Foundation Health Plan Inc. (2014)
  - Breach exposed over 20,0000 employees' SSN, dates of birth, addresses and other PII for spouses and children
  - Breach allegedly occurred in December 2011 but notice was not provided until March 2012
  - Settlement requires notification on a rolling basis, meaning "as soon as reasonably possible after identifying a portion of the total individuals affected by a breach, even if the investigation is ongoing[,]" with notification continuing throughout and until Kaiser competes its investigation
  - Kaiser Permanent paid $150,000 in penalties and attorneys' fees

# Regulator Actions - AGs

**Massachusetts**

- Women & Infants Hospital of Rhode Island (WIH) (2014)
  - $150,000 settlement  for a data breach involving 12,000 patients in Massachusetts that exposed patients' names, dates of birth Social Security numbers, dates of exams, physicians' names and ultrasound images
  - WIH discovered 19 unencrypted backup tapes were missing in April 2012 after they were supposedly shipped in the summer of 2011
  - WIH did not provide notice to consumers and regulators until the fall of 2012

**Indiana**

- WellPoint (2011)
  - Records (including SS#s, health and financial info) of over 32,000 Indiana residents were potentially accessible on an unsecured website (Involved 645,000 nationally)
  - Settlement includes $100,000 fine to the state, up to two years of credit protection to affected state residents, and reimbursement of up to $50,000 for any losses

# Shareholder Derivative Actions

Target

- Allegations: Failure to prevent breach and to timely report accurate information about the breach causing severe damage to the Company
- Claims: Breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control
- Relief Sought: Monetary damages and injunctive relief "by way of significant corporate and managerial reforms to prevent future harm to the Company by disloyal directors and officers."

Wyndham Worldwide Corporation

- Allegations: Company affected by 3 breaches between April 2008 and January 2010; Company failed "to take reasonable steps to maintain customers' personal and financial information in a secure manner"
- Claims: Breaches of fiduciary duty, waste of corporate assets and unjust enrichment
- Relief Sought: Recovery of the damages the Company allegedly suffered, remedial action with respect to corporate governance and internal procedures and disgorgement of profits and compensation

# Shareholder Derivative Actions

## TJ Maxx

- Claims: Breach of fiduciary duties, and gross mismanagement
- Relief sought: Injunctive relief to improve security and prevent data breaches
- In anticipation of their soon to be released SEC Disclosure Guidance, TJ Maxx settled the suit the same day it was filed
  - Board to oversee computer security through 2015
  - Company agreed to maintain the toll free number to handle questions about card cancellations, credit theft, etc. for extra 6 months
  - Company to pay up to $595,000 in plaintiffs' attorneys fees

# Best Practices

- Identify all potentially private information
- Define internal written policies
  - Network usage
  - Social networking
  - Data handling
- Computer network sophistication and security
  - Backup, backup, backup
  - Encryption
  - Competent IT Professionals
  - Firewalls/IDS
  - Assess/Insure

# Best Practices

**Vendor compliance**

- Non-disclosure agreements (“NDA”)
- Cyber
- Certificates of Insurance (Cyber)

**Employee training**

- Awareness, training
- Enforcement

**Incident-response planning**

- First response
- Business continuity
- Disaster recovery
- Lessons learned
- Policies and procedures updated, trained, enforced

# Concerning Data

- Where is our Data?
- Who has access to it?

# Key Messages

| | |
|---|---|
| **The global business ecosystem has changed the risk landscape** | Business models have evolved creating a dynamic environment that is increasingly interconnected, integrated, and interdependent, but security strategies and investment have not kept pace. |
| **Focus on securing high value information and protecting what matters most** | Rather than treating everything equally, companies must now identify and protect their "crown jewels"—those business assets that are critical to future cash flows. |
| **Know your adversary – motives, means, and methods** | Sophisticated adversaries are actively exploiting cyber weaknesses in the business ecosystem for economic, monetary, and political gain, among other things. |
| **Embed cybersecurity into board and executive level decision making** | An integrated cybersecurity strategy that is aligned with business objectives requires commitment and consideration from the highest executive levels of the organization. |

# Assemble an Incident Response Team

**The makeup of the team will generally include:**

- An executive with decision making authority
- Team leader responsible for response coordination, contacting outside counsel and the forensics team, press inquiries
- “First Responder” security and IT personnel with access to systems and permissions
- Representatives from key departments, to include IT, Legal, Human Resources, Customer Relations, Risk Management, Communications/ Public Relations, Operations (for physical breaches) and/or Finance (for breaches involving loss of company financial information)
- CIO, CISO, and other C-level stakeholders

# Outside Subject Matter Experts

- Outside Counsel specializing in cyber breach
- Cyber Security Experts and Forensic Examiners
- Public Relations Firm
- Initiate contact with law enforcement

# Create a Plan

***"Plans are of little importance, but planning is essential."***

***– Winston Churchill***

- Draft a cyber response plan.
- The plan should be effective, simple and scalable.
- The plan should be drafted **together** with the Incident Response Team.
- The senior officer/executive responsible for breaches should lead the Incident Response Team in occasional dry-run or table-top exercises.
- Plan for the worst case scenario.

# Questions?

# LORI ANNE CZEPIEL

*Partner*
**Lewis Brisbois**

LoriAnne.Czepiel@lewisbrisbois.com
646.239.5008

**Los Angeles**
221 North Figueroa Street
Suite 1200
Los Angeles, CA 90012
Tel: 213.281.5225

**New York**
77 Water Street
Suite 2100
New York, NY 10005
Tel: 212.232.1307

Lori Anne Czepiel leads the business/corporate practice at Lewis Brisbois. She has over twenty-five years of experience counseling middle market, public and early stage companies and their boards, executives, owners and investors on fiduciary duty, governance, risk management and corporate securities matters. She has served as acting General Counsel for a Fortune 500 public company.

Ms. Czepiel also advises clients in complex domestic, international and multi-jurisdictional strategic and financial matters. She regularly leads and manages large interdisciplinary teams in:

- Strategic and corporate governance matters, including all manner of M&A transactions;
- Related corporate finance, securities and other capital raising matters, including private equity, venture capital and similar investments;
- International and cross-border business matters;
- Distressed and bankruptcy matters and restructurings; and
- Commercial and other business litigation and dispute resolution matters.

A substantial portion of Ms. Czepiel's practice involves general corporate counseling, providing practical business law advice on commercial, contract, and risk management issues in close collaboration with lawyers in other firm practices (such as IP/ technology, real estate, employment/labor, benefits, environmental, litigation, data privacy, healthcare, entertainment, insurance, banking, and finance).

Ms. Czepiel handles matters with values ranging from a few million to billions of dollars for middle-market and larger companies, start-ups/emerging companies, investors and their financial advisors. She has substantial experience representing clients in industries such as technology; energy/infrastructure; real estate; healthcare; insurance; financial services; funds; entertainment/media; gaming; manufacturing; mining; food and beverage; and retail/consumer products. She has particular experience with issues relating to regulated businesses. She also works regularly with nonprofits.

# LORI ANNE CZEPIEL (cont.)

Ms. Czepiel is frequently invited to speak and write about corporate, governance, securities, professionalism topics. She has addressed and written for programs by or before organizations such as the American Management Association, Standard & Poors, *Mergers and Acquisitions* magazine, Northwestern University, Prentice Hall Law & Business, Practising Law Institute, the American Bar Association, the International Bar Association, the State Commission for Restructuring the Economic Systems of the People's Republic of China, the U.S.-Mexico Chamber of Commerce, Houlihan Lokey, UBS, GE Commercial Finance, Merrill Lynch and others. She was selected to serve on NY City Bar M&A committee for nine years, and she also has been recognized by her peers as a Super Lawyer and a Law Dragon finalist.

Ms. Czepiel received her J.D. *cum laude* from Boston University School of Law and her B.A. from Northwestern University. She also attended the Northwestern University Kellogg School of Management's director development program, and has served as a director on the boards of several large international non-profit organizations.

Additional information about Ms. Czepiel and her practice is available on the Firm's website at http://www.lewisbrisbois.com/attorneys/czepiel_lori_anne. LinkedIn: www.linkedin.com/in/lorianneczepiel

# JOHN MULLEN

*Partner*
**Lewis Brisbois**

550 E. Swedesford Rd., Suite 270
Wayne, PA 19087
John.Mullen@lewisbrisbois.com
215.977.4056

John F. Mullen is the Managing Partner of the Philadelphia Regional Office and Chair of the US Data Privacy and Network Security Group with Lewis Brisbois Bisgaard & Smith. Mr. Mullen concentrates his practice on first- and third-party privacy and data security matters, and (with his team) serves as a data breach coach/legal counsel for entities coping with data privacy issues. Mr. Mullen is well-versed in the complex state, federal, and international rules and laws governing data collection, storage and security practices and breach response obligations. Mr. Mullen has been on the forefront of developing the cyber market in the insurance industry, and continues to assist insurers, brokers, risks managers, underwriters, product specialists and professional claims personnel in navigating this rapidly-developing territory.

Mr. Mullen holds a B.S. from Pennsylvania State University (1987) and a J.D. from Arizona State University, College of Law (1991).

Additional information about Mr. Mullen and his practice is available on the Firm's website at http://lewisbrisbois.com/attorneys/mullen_john-f.

# ROBERT P. HARTWIG

*President & Economist*
**Insurance Information Institute**

110 William Street
New York, NY 10038
bobh@iii.org
212.346.5520

Robert P. Hartwig is president of the Insurance Information Institute. Since joining the I.I.I. in 1998 as an economist and becoming chief economist in 1999, Dr. Hartwig has focused his work on improving the understanding of key insurance issues across all industry stakeholders including media, consumers, insurers, producers, regulators, legislators and investors.

Presently, the I.I.I. provides assistance on thousands of stories annually and covers all aspects of print, television, radio and new media while also responding to thousands of requests from I.I.I. member companies and other constituencies. The Institute is generally recognized to be the most credible and frequently used single source of information and referral for the widely diverse insurance industry. Its Board of Directors represents companies from all areas of the industry, including life insurers. In addition, some 20 other insurance organizations contract with I.I.I. for media services.

The I.I.I. is involved in products and services as varied as original research and publications with the National Bureau of Economic Research and The Wharton School, through widely used consumer publications and Fact Books, to maintaining the National Insurance Consumer Helpline on behalf of the entire U.S. property/casualty industry. Each year the Institute's staff makes more than 100 presentations worldwide on behalf of member organizations. The Institute also develops software and apps designed to improve policyholder preparedness in the event of a routine claim or major natural catastrophe.

Dr. Hartwig previously served as director of economic research and senior economist with the National Council on Compensation Insurance (NCCI) in Boca Raton, Florida, where he performed rate of return and cost of capital modeling and testified at workers' compensation rate hearings in many states. He has also worked as senior economist for the Swiss Reinsurance Group in New York and as senior statistician for the United States Consumer Product Safety Commission in Washington, D.C. He is a member of the American Economic Association, the American Risk and Insurance Association, the National Association of Business Economics and the CPCU Society. In 2005 and 2006 Dr. Hartwig served on the State of Florida's Task Force for Long-Term Homeowners Insurance Solutions. He has also served on the boards of directors of the American Risk and Insurance Association and the Independent Insurance Agents and Brokers Association of New York. Currently, Dr. Hartwig serves on the board of trustees for the Griffith Foundation for Insurance Education and is a member of the National Board of the Insurance Industry Charitable Foundation.

# ROBERT P. HARTWIG (cont.)

Dr. Hartwig received his Ph.D. and Master of Science degrees in economics from the University of Illinois at Urbana-Champaign. He also received a Bachelor of Arts degree in economics *cum laude* from the University of Massachusetts at Amherst. He has served as an instructor at the University of Illinois and at Florida Atlantic University. Dr. Hartwig also holds the Chartered Property Casualty Underwriter (CPCU) credential.

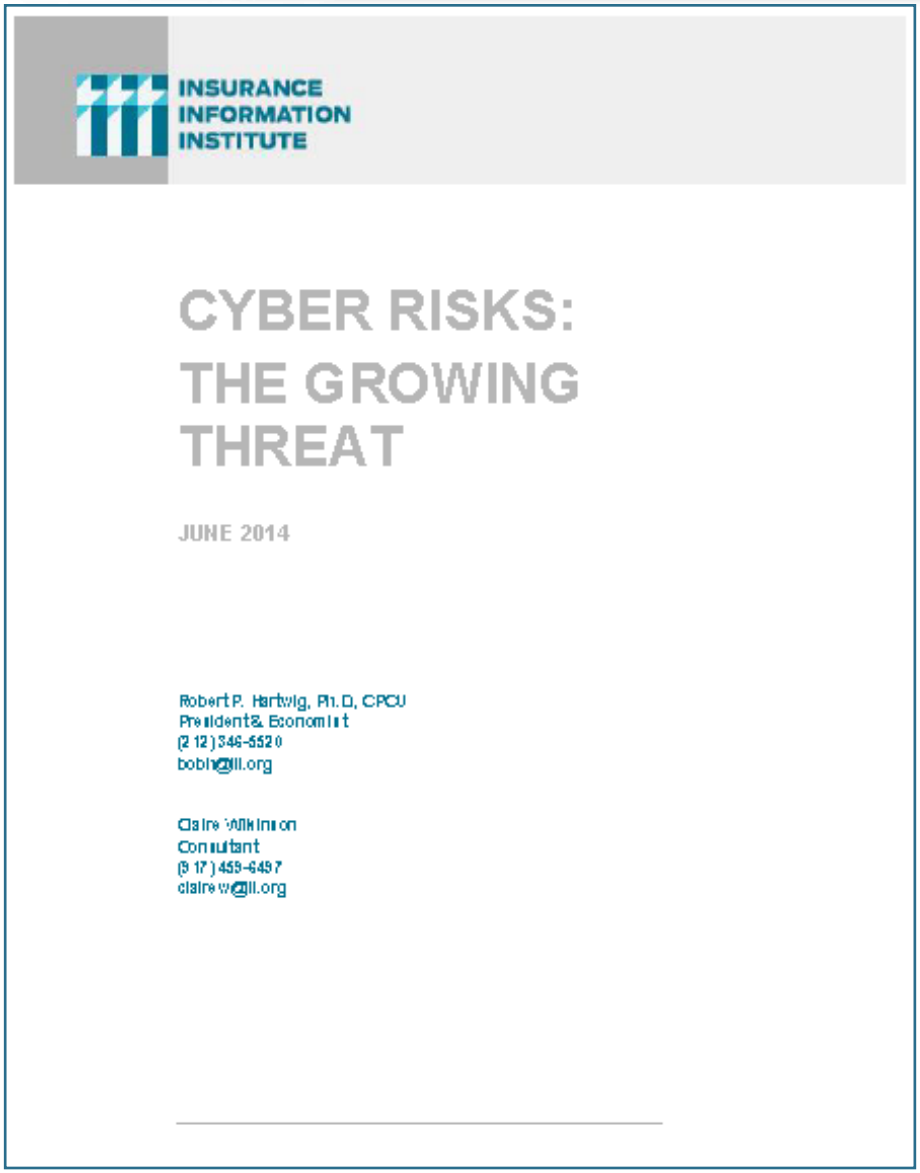
Dr. Hartwig has authored and co-authored papers that have appeared in numerous publications, including the Journal of Health Economics, the Proceedings of the Casualty Actuarial Society, the John Liner Review, Dossiers et Etudes (Geneva Association), the Journal of Workers' Compensation, the Journal of Insurance Operations, Global Reinsurance, Risk & Insurance, Insurance Day, Compensation and Benefits Review. He is also a regular contributor to National Underwriter and many other industry trade publications.

In 2011, Dr. Hartwig was awarded the National Association of Mutual Insurance Companies (NAMIC) Chairman's Award. In 2010, he was a recipient of a research award from the U.S. Chamber of Commerce Institute for Legal Reform in the area of torts and tort reform.

Dr. Hartwig makes frequent presentations to industry associations, company management, industry executives, analysts and clients and speaks internationally on a wide range of insurance issues. He has testified before numerous state and federal regulatory and legislative bodies, including the U.S. Senate Judiciary Committee, the Senate Banking, Housing and Urban Affairs Committee, the House Financial Services Subcommittee on Capital Markets, Insurance and Government Sponsored Enterprises and the House Financial Services Subcommittee on Oversight and Investigations and the House Committee on Transportation and Infrastructure.

Dr. Hartwig serves as a media spokesperson for the property/casualty insurance industry, and is quoted frequently in leading publications such as The Wall Street Journal, The New York Times, USA Today, Washington Post, Los Angeles Times, Financial Times, BusinessWeek, Newsweek, U.S. News & World Report, CFO, Fortune, Forbes, The Economist and many others throughout the world. Dr. Hartwig also appears regularly on television, including programs on ABC, CBS, NBC, CNN, CNBC, Fox, PBS and the BBC.

# I.I.I.'s 2014 Cyber Report: *Cyber Risk: The Growing Threat*


INSURANCE INFORMATION INSTITUTE

CYBER RISKS: THE GROWING THREAT

JUNE 2014

Robert P. Hartwig, Ph.D, CPCU
President & Economist
(212) 346-5520
bobh@iii.org

Claire Wilkinson
Consultant
(917) 459-6457
clairew@iii.org

- Provides information on cyber threats and insurance market solutions
- Global cyber risk overview
  - Quantification of threats by type and industry
- Cyber security and cost of attacks
- Cyber terrorism
- Cyber liability
- Insurance market for cyber risk
- *http://www.iii.org/white-paper/cyber-risks-the-growing-threat-062714*

# CHARLES WHITE

*Director*
**PricewaterhouseCoopers**

Three Embarcadero Center
San Francisco, California 94111
charles.white@us.pwc.com
415.498.5352

Charles White is a director in the PricewaterhouseCoopers forensics practice, based in San Francisco. He specializes in assisting clients with their IT, physical and human capital security challenges. He has deep experience working with organizations to both prepare for and respond to significant security events such as cyber breach incidents. Charles has a breadth of experience working cybercrime investigations on a global scale.

Prior to joining PwC in 2013, Charles had a distinguished 27 year career with the U.S. Secret Service. Among his assignments with the Secret Service, Charles served two tours at the White House as part of the Presidential Protective Division, the second tour as Assistant Special Agent in Charge. Charles also served two international assignments. Among his responsibilities overseas, he was selected to establish the Secret Service presence in Russia. He served as the agency representative to the former Soviet Union for 5 years. During this time he directed numerous global financial crimes investigations spanning both Eastern and Western Europe and the United States.

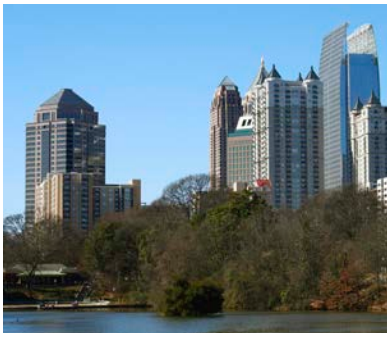
Charles' most recent assignment was at the San Francisco Field Office, where he directed agency operations in Central and Northern California. Charles served on the steering committee for the San Francisco Electronic Crimes Task Force, a Secret Service led effort to combat electronic crimes comprised of over 700 members from law enforcement, private industry, and academia.

Charles has a Bachelor's degree in Economics from the University of California at Los Angeles and speaks French, German and Russian.


LEWIS
BRISBOIS
BISGAARD
& SMITH LLP
ATTORNEYS

# Firm Overview

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS



Established in 1979, Lewis Brisbois Bisgaard & Smith LLP is a national, full-service law firm with more than 900 attorneys and 32 offices, in 18 states and the District of Columbia. Our national practice is sophisticated, multi-faceted and well-versed in current legal trends, while our individual state practices provide vast resources and knowledge of procedural and legal nuances.

Lewis Brisbois offers legal practice in more than 40 specialties, and a multitude of sub-specialties associated with each practice area. Our attorneys have broad knowledge, expertise, and sensitivity to their clients' unique needs. Through interaction among its practices, Lewis Brisbois provides a wide range of legal services to each client with a continuity of representation over multiple disciplines. We have built longstanding relationships with corporate and institutional clients based on our ability to provide comprehensive service on a national scale.

The combination of Lewis Brisbois' nationwide presence, our focus on efficiency and our broad ranging legal practice makes us a leading choice for companies that want a full-service law firm that delivers value and results. With more than 900 attorneys in 32 offices from coast to coast, Lewis Brisbois offers our clients the complete legal package.

At Lewis Brisbois, diversity is an integral part of our firm culture and our daily life. We have a Diversity and Inclusion Committee whose mission is to promote and advance diversity and inclusion within the firm. The success of the firm's diversity initiatives is reflected in the fact that Lewis Brisbois has repeatedly received national recognition for its commitment to embracing diversity. In 2012 we were ranked #1 by American Lawyer Media as the nation's most diverse law firm. Lewis Brisbois has consistently ranked in the top 10 in recognized diversity surveys since 2005. The diversity of the firm's client base is matched by the diversity of our attorneys. With offices from Los Angeles to New York, our attorneys reflect the communities in which they live. We are also committed to supporting diversity through new and ongoing relationships with minority and women-owned businesses.

For more about Lewis Brisbois, please visit us at LewisBrisbois.com.

LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS

# Nationwide Locations

**ATLANTA**
1180 Peachtree Street NE
Suite 2900
Atlanta, Georgia 30309
T: 404.348.8585
F: 404.467.8845

**BALTIMORE**
400 East Pratt Street
8th Floor
Baltimore, Maryland 21202
T: 410.858.4420
F: 410.779.3910

**BEAUMONT**
550 Fannin Street, Suite 800
Beaumont, Texas 77701
T: 409.838.6767
F: 409.838.6950

**BOSTON**
One International Place, 3rd Floor
Boston, MA 02110
T: 857.313.3950
F: 857.313.3951

**CHARLESTON**
209 Capital Street, Third Floor
Charleston, West Virginia 25301
T: 304.553.0166
F: 304.343.1805

**CHICAGO**
550 West Adams Street, Suite 300
Chicago, Illinois 60661
T: 312.345.1718
F: 312.345.1778

**DALLAS**
2100 Ross Avenue, Suite 2000
Dallas, TX 75201
T: 214.347.4508
F: 972.638.8664

**DENVER**
1700 Lincoln Street
Suite 4000
Denver, Colorado 80203
T: 303.861.7760
F: 303.861.7767

**FORT LAUDERDALE**
110 SE 6th Street
Suite 2600
Fort Lauderdale, Florida 33301
T: 954.728.1280
F: 954.728.1282

**HARTFORD**
100 Pearl Street
Suite 1438
Hartford, Connecticut 06103
Tel: 860.748.4806
Fax: 860.748.4857

**HOUSTON**
Weslayan Tower, Suite 1400
24 East Greenway Plaza
Houston, Texas 77046
T: 713.659.6767
F: 713.759.6830

**LA QUINTA, CA**
78075 Main Street
Suite 203
La Quinta, California 92253
T: 760.771.6363
F: 760.771.6373

**LAFAYETTE**
100 E. Vermilion Street
Suite 300
Lafayette, Louisiana 70501
T: 337.326.5777
F: 337.504.3341

**LAS VEGAS**
6385 South Rainbow Blvd.
Suite 600
Las Vegas, Nevada 89118
T: 702.893.3383
F: 702.893.3789

**LOS ANGELES**
221 North Figueroa Street
Suite 1200
Los Angeles, California 90012
T: 213.250.1800
F: 213.250.7900

**MADISON COUNTY, IL**
Mark Twain Plaza II
103 W. Vandalia Street
Suite 300
Edwardsville, Illinois 62025
T: 618.307.7290
F: 618.692.6099

**NEWARK**
One Riverfront Plaza
Suite 350
Newark, New Jersey 07102
T: 973.577.6260
F: 973.577.6261

**NEW ORLEANS**
400 Poydras Street
Suite 1320
New Orleans, Louisiana 70130
T: 504.322.4100
F: 504.754.7569

**NEW YORK**
77 Water Street
Suite 2100
New York, New York 10005
T: 212.232.1300
F: 212.232.1399

**ORANGE COUNTY**
650 Town Center Drive
Suite 1400
Costa Mesa, California 92626
T: 714.545.9200
F: 714.850.1030

**PHILADELPHIA**
550 E. Swedesford Road
Suite 270
Wayne, Pennsylvania 19087
T: 215.977.4100
F: 215.977.4101

**PHOENIX**
Phoenix Plaza Tower II
2929 North Central Avenue
Suite 1700
Phoenix, Arizona 85012
T: 602.385.1040
F: 602.385.1051

**PROVIDENCE**
10 Dorrance Street
Suite 700
Providence, Rhode Island 02903
Tel: 401.406.3310
Fax: 401.406.3312

**SACRAMENTO**
2850 Gateway Oaks Drive
Suite 450
Sacramento, California 95833
T: 916.564.5400
F: 916.564.5444

**SAN BERNARDINO**
650 East Hospitality Lane
Suite 600
San Bernardino, California 92408
T: 909.387.1130
F: 909.387.1138

**SAN DIEGO**
701 B Street, Suite 1900
San Diego, California 92101
T: 619.233.1006
F: 619.233.8627

**SAN FRANCISCO**
333 Bush Street, Suite 1100
San Francisco, California 94104
T: 415.362.2580
F: 415.434.0882

**SEATTLE**
2101 Fourth Avenue, Suite 700
Seattle, Washington 98121
T: 206.436.2020
F: 206.436.2030

**TAMPA**
3812 Coconut Palm Drive
Suite 200
Tampa, Florida 33619
T: 813.739.1900
F: 813.739.1919

**TEMECULA**
One Ridgegate Drive, Suite 245
Temecula, California 92590
T: 951.252.6150
F: 951.252.6151

**TUCSON**
One South Church Avenue
Suite 2100
Tucson, Arizona 85701
T: 520.399.6990
F: 520.838.8618

**WASHINGTON, D.C.**
601 Pennsylvania Avenue, NW
Suite 900, South Building
Washington, D.C. 20004
T: 202.220.3165
F: 202.400.2288

# SELECTED PRACTICE AREAS OF NOTE

## Corporate

Our Corporate Practice is well positioned to serve our clients' transactional and governance needs in a comprehensive, coordinated and efficient manner. Our resources include many former general counsel and other in-house experts. Our Corporate Practice may also serve as your outside General Counsel, to coordinate and handle all non-litigation legal aspects of your business, bringing in specialized experts as needed—not just responding to problems as they arise; but also spotting future issues and implications in advance, and treating them pro-actively with cost effective solutions.

## Data Privacy & Network Security

We provide legal services designed to navigate the complex patchwork of federal, state and foreign law, including disclosure and notification requirements. We work closely with a client's management team, the client's in-house and outside cyber-security experts, law enforcement and government regulators. When necessary, we are well equipped to defend litigation, including multi-district national consumer class action litigation. Where appropriate, we also appreciate the need to work with crisis management consultants to accomplish accurate and timely public reporting to assure customers and investors.

## Directors & Officers

Since its inception, Lewis Brisbois has had a Directors and Officers Practice specializing in this unique and complex area of law. This long-standing practice has resulted in Lewis Brisbois being involved in virtually every significant development in the area. Throughout our history, we have represented major insurers providing D&O insurance across the country. In our capacity as coverage counsel, we work closely with directors, officers, corporations, and their defense counsel in order to achieve resolutions mutually favorable to both insurers and insureds. By creating a cooperative environment and providing our experience and expertise in dealing with plaintiffs and their counsel, we can be instrumental in finding creative solutions to complex and potentially catastrophic lawsuits.

## White Collar Criminal Defense

The White Collar Criminal Defense and Government Investigations Practice represents individuals and corporations in state and federal investigations, grand jury investigations, administrative enforcement proceedings, and civil and criminal trials. Frequently, white collar criminal investigations and government enforcement activities are not mutually exclusive. These matters are often complicated by derivative civil actions or other governmental investigations. With a staff of accomplished and experienced former prosecutors and other attorneys, we work together in fields such as antitrust, healthcare, food and drugs, financial institutions, tax, corporate, and environmental law to provide an efficient and comprehensive defense.

## Insurance Regulatory & Reinsurance

The attorneys of our Insurance Regulatory and Reinsurance Practice represent insurance, reinsurance, technology, manufacturing, and other businesses in a wide array of litigation, transactional, regulatory, and corporate matters. Our attorneys have experience in both the private and public sectors, having served as corporate general counsel and counsel with regulatory agencies.

# ADDITIONAL FIRMWIDE PRACTICES

## BUSINESS/TRANSACTIONAL:

## Employment & Labor

Comprising a nationwide network of experienced attorneys, Lewis Brisbois' Employment and Labor Practice represents clients in all phases and types of employment litigation, counseling, training and collective bargaining. Our team of employment experts provides clients with sound counsel in dozens of jurisdictions. Our size and geographic coverage allow us to provide our employment clients with consistent representation throughout the nation.

## Energy & Environment

The attorneys in Lewis Brisbois' Energy and Environment Practice manage a broad portfolio of legal services related to both traditional and alternative energy projects as well as providing advice and assistance to public and private entities, and environmental and community groups involved in natural resources and environmental law issues. Our attorneys offer advice and assistance to private and public entities involved in the energy sector, with particular emphasis on renewable energy, energy efficiency and waste-to-energy matters. Our counseling includes representation before administrative and public agencies, as well as subsequent litigation in federal and state courts. Because Lewis Brisbois has represented both project applicants, opponents and public agencies processing permits, we have a broad perspective allowing us to fashion effective approaches to resolving development and environment-related disputes.

## Finance & banking

Our attorneys have relevant experience stretching back to the savings-and-loan crisis, and forward to the challenges of today. What is needed to adapt to and overcome such challenges is experience and creativity, and that is exactly what our bakning and finance team offers to our clients.

## Governmental Relations

The Government Relations Practice offers services to professional associations, businesses, trade associations, other non-profit organizations, local governments, political organizations, and individuals. Frequently, our clients are confronted by enforcement actions that deal with complex compliance standards established for each activity, and subject to licensure or regulation. Our attorneys possess the depth and breadth of knowledge required to provide effective and cost-efficient representation. From time to time, resolution of complex issues requires legislative direction. The firm's attorneys draft and interpret bill and regulation language, and actively engage with legislators and other elected or appointed officials, to tackle issues facing the firm's clients.

## Insolvency & Bankruptcy

The attorneys of our Bankruptcy and Insolvency Practice assist businesses and individuals in formulating and carrying out problem-solving strategies when they are faced with insolvency. We represent diverse companies and individuals, bankruptcy trustees, plan disbursing agents, lenders, landlords, and acquirers of assets from bankruptcy estates. We have represented clients in all aspects of contested matters and adversary proceedings, including fraudulent conveyances, preferences, relief from stay motions, non-dischargeability actions, trustee motions, and the entire range of litigation matters that arise in bankruptcy cases, including appeals. In addition, we assist our insurance clients in all insolvency-related matters.

## Intellectual Property

Our Intellectual Property Practice is a leader in the acquisition and protection of intellectual property rights. We represent national companies in such matters as web site management, licensing, e-commerce, domain name issues, media content, and protection of all intellectual property assets. Our attorneys are authors, speakers, and experts in all aspects of intellectual property including, copyright, trademark, trade dress, unfair competition, licensing and rights acquisitions. In today's challenging market place, our clients demand and have come to expect prompt, comprehensive, and cost effective solutions to intellectual property issues. Our attorneys are recognized leaders in crafting creative solutions to our client's legal needs assuring that each client's goals are carefully discussed and observed.

## Life, Health, Disability & Erisa

We are well positioned to advise on life, health, disability, annuity and ERISA benefits and fiduciary breach claims. We also have expertise in all aspects of litigation and arbitration proceedings encompassing both group and individual plans, including COBRA litigation and HIPAA issues, claims, and benefits litigation arising out of commercial, Medicare and Medicaid contracts. Additionally, we are experienced in issues arising out of the business practices of the health care industry, such as bundling, unbundling, downcoding and falsified claims. We have expertise in representing annuity issuers and their registered representatives. We offer extensive insurance and medical malpractice expertise, enhancing our ability to determine the most effective and efficient approach to advance our clients' interests.

## Real Estate

The Real Estate Practice represents shopping center developers, owners and operators; commercial and industrial real estate developers, owners, and operators; financial institutions; public agencies; national/regional/local tenants; and other business organizations in real estate transactions, including acquisitions; sales and tax-deferred exchanges; retail, office and industrial leasing transactions; and construction transactions.

### Sustainable Development & Green Technology

The attorneys in the firm's Sustainable Development Practice advise clients on issues relating to renewable energy, government regulations, land and water use, environmental impact, real estate development, and intellectual property. They each have a personal commitment to sustainable development, and several have obtained their LEED (Leadership in Energy and Environmental Design) accreditation. Our attorneys have represented clients on issues that run the gamut from financing and business expansion for energy and utilities companies, government regulatory compliance, real estate transactions, waste management, and environmental and construction litigation; to patent and trademark protection for green building, wind power, and solar products, professional liability litigation, government tax credits, and various corporate transactions.

## LITIGATION:

### Appellate

Although most lawsuits are resolved at the trial court level, some proceed to judgment and then are litigated on appeal. Appellate advocacy requires special skills in areas such as writing briefs, analyzing and framing legal issues, legal research, and presentation of oral argument. The members of Lewis Brisbois' Appellate Practice have these skills. We handle matters on appeal originating from lawyers within our firm, from trial court matters originating outside the firm, and as amicus counsel. The members of the Appellate Practice have handled thousands of appeals and extraordinary writ proceedings that have gone to decision. Of these, over 400 have resulted in published opinions, shaping the law.

### Asbestos Litigation

Lewis Brisbois represents asbestos defendants in state and federal courts throughout the country acting as national coordinating counsel, regional counsel and local counsel in various jurisdictions. We have represented clients in virtually every sector of the asbestos industry including manufacturers, distributors, contractors and premises owners, shipyards, refineries, power plants, schools, home construction or remodel, industrial sites, and home and commercial garages and auto repair shops. Lewis Brisbois' success in California Courts in mass tort cases has transcended to a national level as demonstrated by the number of jury trial verdicts we have achieved on behalf of our asbestos clients in more than 14 venues across the country.

### Commercial Litigation

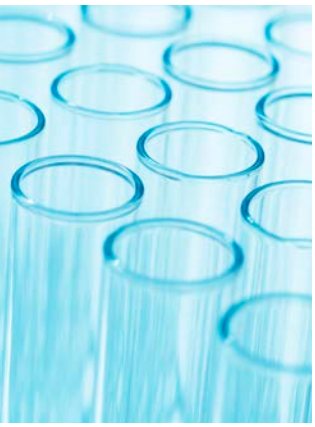
The issues handled by our Commercial Litigation Practice go to the heart of a company's bottom-line, and clients must exercise sound business judgment to obtain the best possible legal solution when confronted with litigation. Our commercial litigation attorneys constantly re-evaluate the clients' risks and benefits during the course of litigation, providing the clients with timely and accurate information. By keeping our clients currently advised on the status of any case, they are able to develop and maintain clear commercial objectives. Clients are involved in all phases of strategic planning and are provided with detailed litigation plans and budgets in order to appropriately manage and control the litigation.

### Consumer Litigation & Financial Services

Our attorneys represent banking, mortgage lending and consumer financial institutions in a wide variety of matters, including unfair and predatorial lending practices, fidelity bond litigation and judicial foreclosures. Our attorneys participated in the litigation of the largest fidelity bond claim in history. They have represented banks, mortgage banks, mortgage loan service providers, and other consumer financial service institutions in putative national classes, and state and multi-state classes. We have handled litigation in both state and federal courts through trial and on appeal. Our attorneys are licensed to practice in multiple state and federal jurisdictions and also represent professionals in administrative proceedings before the N.A.S.D. and many different state agencies.

### Electronic Discovery, Information Management & Compliance

The Electronic Discovery, Information Management and Privacy Practice is directly involved with issues relating to information management and privacy issues, because the procedural rules governing electronic discovery directly implicate our clients' information management policies, hardware and software infrastructures. Our attorneys have represented clients during the course of numerous class actions and multi-district litigation proceedings involving E-Discovery disputes. In particular, our attorneys have developed significant expertise in limiting the scope of subpoenas and document requests in order to limit the scope of production or shift the cost of responding to the requesting parties.



### Life Sciences Litigation

Lewis Brisbois has established a strong reputation in its representation of healthcare providers including hospitals, physicians, nurses, technicians, therapists, mental healthcare counselors, pharmacists, dentists, podiatrists, hospitals, clinics, convalescent homes and other healthcare providers in state and federal courts. Lewis Brisbois also handles medical malpractice actions in numerous areas including obstetrics, emergency medicine, surgery, cardiology, general practice, pulmonary medicine, nursing, orthopedics, neurology, oncology, plastic surgery, ophthalmology, genetics testing, radiology, dentistry and podiatry. We regularly appear on behalf of healthcare providers before the Medical Board on licensing and disciplinary matters.

### Products Liability

Lewis Brisbois is proud to have developed one of the nation's strongest and most diversified products liability practices. We serve a wide range of products liability needs for our clients with an emphasis on acting as trial counsel in federal and state courts, and serving as regional or national coordinating counsel. We manage an extensive case load of civil litigation involving products liability matters. Our attorneys handle both catastrophic injury and routine products liability litigation in state and federal courts. We have an experienced team of lawyers who have achieved a remarkable level of success at trial. Our trial counsel are provided superb support by Lewis Brisbois' Appellate Practice with its cadre of appellate attorneys.

### Securities Litigation & FINRA

We represent securities brokers and broker dealers in connection with errors and omissions claims made by investors in NYSE arbitration matters, and in federal and state courts involving issues of unsuitability, due diligence, Rule 144k exchanges, elder abuse, supervision in the sale of securities, variable life insurance policies, and variable annuities. Lewis Brisbois specializes in representing individual securities brokers on claims involving churning, unsuitability, negligence, and misrepresentation, pertaining to investments in equities, mutual funds, limited partnerships, real estate and retirement planning. We also specialize in representing broker dealers on claims involving negligent failure to supervise and defense of class action securities fraud cases.

### Toxic Tort & Environmental Litigation

For over two decades Lewis Brisbois has had one of the preeminent environmental law practices in the country with experience and expertise in a wide range of litigation and counseling services, including toxic tort, Federal and State Superfund, California Environmental Quality Act ("CEQA"), Proposition 65 and related matters. We have assembled an impressive team of experienced attorneys who are intimately familiar with environmental law, and the defense of toxic tort lawsuits. In addition, we provide a full range of environmental and product counseling services for our clients.

## SELECTED INDUSTRY-FOCUSED PRACTICES:

### Aviation

Aviation law cases require high-level expertise in many aspects of aviation, not solely legal expertise. Our team produces cost-effective results for clients, given their knowledge of the subject matter and sophisticated skills at developing aviation-related cases. We provide aviation and transportation clients nationwide with the kind of skilled representation that comes from an in-depth comprehension of the specific legal issues facing the industry. Our attorneys have both the professional and personal experience to assist our aviation clients— at the scene of accident sites shortly after the accident occurs. We have litigated many aviation-related cases and have the resources to try the most complex and sophisticated aviation cases to produce favorable, cost-effective verdicts or settlements.

### Entertainment Law

Our attorneys provide services in all phases of motion picture, television, video, music and mult-imedia development, production and distribution. We represent actors, directors, film producers, film composers, screenwriters, motion picture sales agents, record labels, record producers, recording artists, songwriters, promoters, models, authors, and others. Representing clients in all facets of entertainment, we offer both litigation and transactional expertise. We have litigated copyright infringement actions involving major motion pictures, disputes between actors and studios or networks, disputes between production companies and distributors, disputes between artists and managers, disputes between record labels, band dissolutions and disputes between recording artists and labels.

### Gaming Law, Sweepstakes & Contests

Lewis Brisbois' Gaming Law, Sweepstakes and Contests Practice represents major casino hotel resorts in Las Vegas and New Jersey, the Sovereign Indian Nations in California, and riverboat and land-based operations across the county. Our lawyers are well-versed in all facets of casino development and casino operations. Our lawyers are also uniquely experienced in emerging subject areas such as internet gaming, social media, mobile gaming, and data security.

### Healthcare Regulatory & Compliance

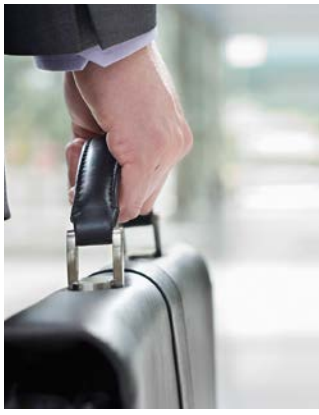
State and federal regulation of medical and long-term care has a profound impact on the industry. Regulatory and enforcement actions by the Centers for Medicare and Medicaid Services, state Departments of Public Health, the Departments of Social Services, the Department of Justice, medical and nursing boards and countless other federal and state agencies can impose significant risk, significant costs, foreclose promising business opportunities, and at times threaten the existence of the entity. A thorough understanding of the legal principles concerning government regulation and conduct is critical to a successful challenge to an adverse agency action or the successful advocacy for—or defense of—a favorable agency decision. The knowledge and experience that goes with both negotiation and litigation is invaluable to achieving the best outcome.

### Transportation

Our nationwide Transportation Practice is extensively involved in the defense of the trucking industry. Our clients include freight carriers, truck insurers, public entities, and waste management groups engaged in both intra-state and interstate transportation. The Transportation Practice is actively involved in an array of organizations such as ABOTA (American Board of Trial Advocates), Trucking Industry Defense Association (TIDA), Defense Research Institute, California Trucking Association (CTA), and the Transportation Lawyers Association. The Transportation Practice is committed to continuing education and keeping abreast of developments that affect large fleets, small fleets, and owner operators.

### Wineries & Vineyards

Lewis Brisbois' Wineries and Vineyards Practice offers a cross-disciplinary approach to meeting the needs of its wine industry clients. Our attorneys have experience in wine consulting, alcoholic beverage regulation, and hold leadership positions in wine industry organizations. Our team approach brings together members from our Corporate, Employment, Real Estate, Intellectual Property, and Commercial Litigation and Dispute Resolution practices to provide focused advice in a cost-effective manner. Among other things, we offer advice on the acquisition and sales of facilities, regulatory matters, water and environmental issues, packaging/labeling and intellectual property issues. We also provide commercial litigation and alternative dispute resolution services to our clients.



## INTERNATIONAL PRACTICE GROUPS:

### Chinese Business & Litigation

Our Chinese Business and Litigation Practice assists clients to successfully navigate the United States legal system. Our client list includes major Chinese insurers, state-owned and privately held companies, Fortune 500 corporations and small to medium sized businesses. We advise and represent our clients on many matters including products liability, intellectual property and technology, international trade disputes, cross-border transactions, marine and admiralty, banking and finance, employment and labor, energy projects, environmental compliance and real estate law.

### Japanese Business & Litigation Practice

Lewis Brisbois' Japanese Business and Litigation Practice provides legal services that are personalized and tailored for the unique needs of our Japanese clients. Our clients include major Japanese insurers, Fortune 100 corporations, publicly traded and privately-held corporations, and small to mid-sized businesses. With an understanding of the strong presence of Japanese businesses in the United States, our team is staffed by exceptional attorneys who have years of knowledge and experience in their fields. They include both Japanese and Japanese American attorneys who are fluent in Japanese and understand Japan's cultural nuances. Our attorneys have extensive experience working closely with Japanese businesses and are attuned to the cultural intricacies and sensitivities unique to Japanese businesses.

### Korean Business & Litigation

In order to better serve the growing needs of the Korean and the Korean-American Communities, Lewis Brisbois has formed the Korean Business and Litigation Group. With a number of highly qualified Korean-American attorneys strategically located throughout the firm's different offices who are bilingual, bi-cultural and experts in a multitude of practice areas, Lewis Brisbois is well suited to handle the unique challenges associated with assisting Korean and Korean-American clients. Our team of exceptional Korean-American attorneys will work closely with other members of the firm to maximize results as well as efficiency for our clients.

### London Market Group

Lewis Brisbois' London Market Group serves the specialized needs of London-based insurers, brokers and their international clients by offering a unique combination of proven Market experience and a nationwide team of top tier business, litigation and coverage attorneys. Our practice leaders have worked in and with the London Insurance Market for many years, gaining an appreciation of its history, needs and breadth.

LEWIS
BRISBOIS
BISGAARD
& SMITH LLP

ATTORNEYS

INSURANCE INFORMATION INSTITUTE

# CYBER RISKS: THE GROWING THREAT

JUNE 2014

**Robert P. Hartwig, Ph.D., CPCU**
**President & Economist**
**(212) 346-5520**
**bobh@iii.org**

**Claire Wilkinson**
**Consultant**
**(917) 459-6497**
**clairew@iii.org**

## INTRODUCTION

The cyber risk landscape is evolving rapidly in a multitude of areas. Governments are facing an unprecedented level of cyber attacks and threats with the potential to undermine national security and critical infrastructure, while businesses that store confidential customer and client information online are fighting to maintain their reputations in the wake of massive data breaches.

The potential economic fallout from the cyber threat cannot be underestimated. Economic thought leaders have warned of a digital disintegration, a scenario in which cyberspace could be completely undermined due to strengthening attacks where the Internet is no longer a trusted medium for communication or commerce, at a huge cost to economies and societies.[1]

Businesses across a wide range of industry sectors are exposed to potentially enormous physical losses as well as liabilities and costs as a result of cyber attacks and data breaches.

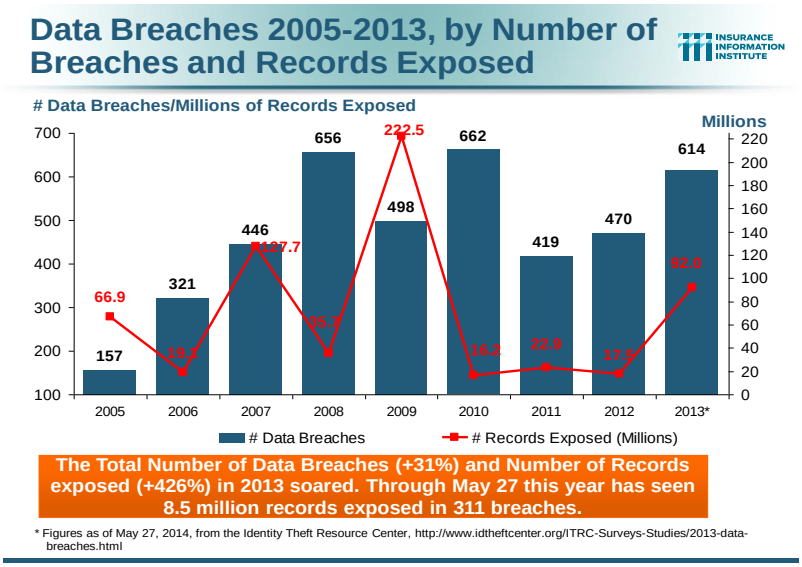
Victims of recent attacks include such well-known brands as eBay, Target, Neiman Marcus, Michaels Stores, the University of Maryland, NATO, JPMorgan Chase, Adobe, Living Social. The list goes on.

And then came the April 2014 disclosure of the Heartbleed bug which undermines the popular OpenSSL encryption technology. Many companies have said they were affected by Heartbleed and it remains to be seen how many companies will disclose data breaches as a result of this security flaw.

The total number of data breaches and number of records exposed fluctuates from year to year and over time, but in 2013 the numbers soared (Fig. 1). Some 614 organizations across the business, financial, educational, government and healthcare sectors, have publicly disclosed data breaches in 2013 exposing close to 92 million records, according to the Identity Theft Resource Center.[2] This compares to 449 publicly disclosed data breaches during 2012, 419 during 2011, and 662 publicly disclosed data breaches in 2010. So far in 2014, some 311 data breach events have been publicly disclosed as of May 27, with 8.5 million records exposed. Yet despite the large number of reported breaches, the actual number of breaches and exposed records is without a doubt much higher as many, if not most, attacks go unreported.

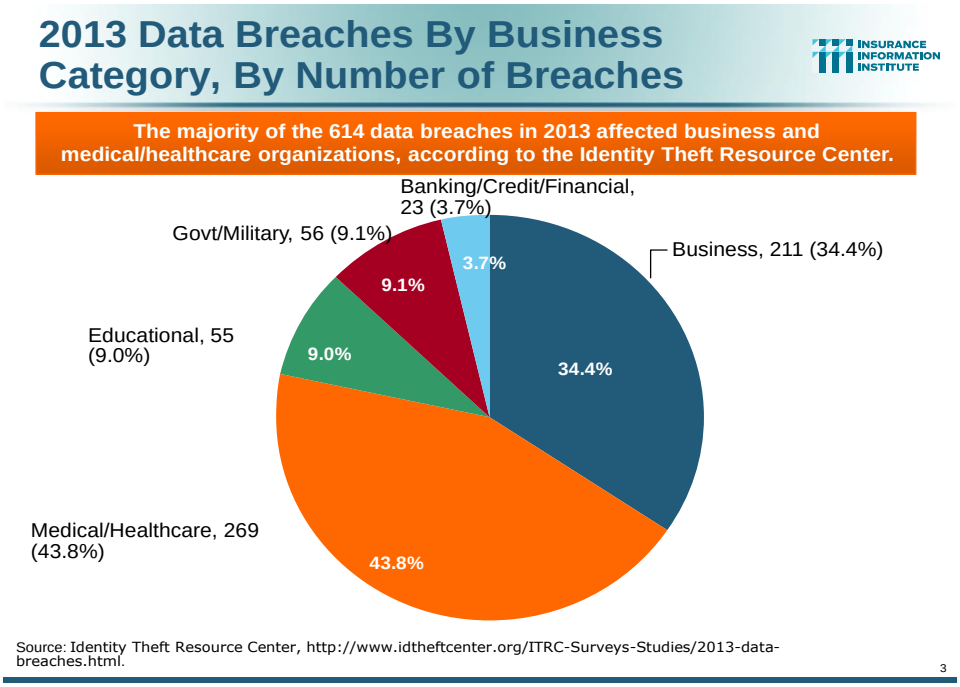
[1] Global Risks 2014, Ninth Edition, by the World Economic Forum, http://www.weforum.org/risks.
[2] Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf.

**Fig. 1**



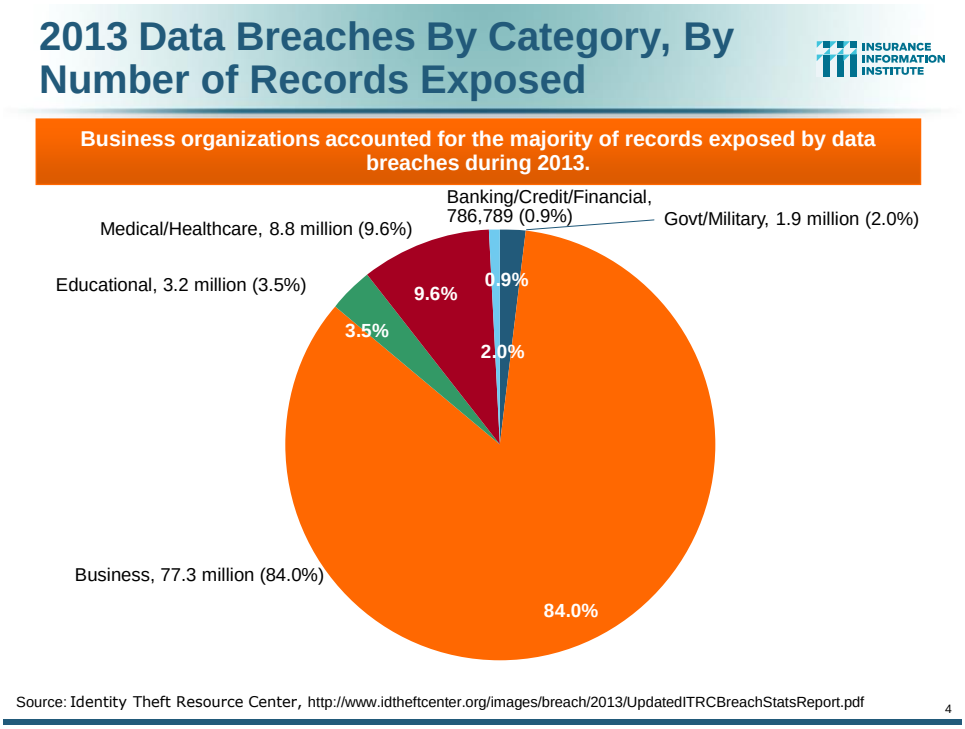

The majority of the 614 data breaches in 2013 affected business and medical/healthcare organizations, according to the Identity Theft Resource Center (Fig. 2).

**Fig. 2**



Business organizations accounted for the majority of records exposed by data breaches in 2013 (Fig. 3).

**Fig. 3**




In October 2011 the Securities and Exchange Commission (SEC) issued guidance urging publicly traded companies to disclose significant instances of cyber risks and events.[3] Description of relevant insurance coverage was included in the SEC's list of appropriate disclosures.

This raises the important question of whether and how adequately businesses are protected by insurance coverage in the event they suffer a loss due to a cyber attack.

The rising incidence of cyber crime targeting major U.S. companies has led to increasing momentum among government and legislative leaders to introduce substantive cybersecurity measures at the national level.

Theft of military and trade secrets remains a top concern, with the U.S. in May 2014 indicting five members of the Chinese military with hacking into U.S. computer networks and engaging in cyber espionage for a foreign government. Nuclear technology developer Westinghouse was one of the entities targeted in the attack, according to the Department of Justice.

[3] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Meanwhile, the fallout continues in the wake of former NSA contractor Edward Snowden's leaks in 2013 regarding the extent of the U.S. intelligence community's Internet surveillance.

And the hacker groups known as Anonymous continue their politically motivated cyber attacks around the world, against targets in Arab countries and in the United States, in response to publications regarding activities by the National Security Agency (NSA), drawing the attention of the FBI and other federal investigators.

In February 2014, the National Institute of Standards and Technology (NIST) released a new framework for improving critical infrastructure cybersecurity. The framework gathers existing global standards and practices to help organizations understand, communicate and manage their cyber risks. The NIST release followed an executive order issued by President Obama a year earlier that promotes increased information sharing about cyber threats between government and private companies that oversee critical infrastructure systems such as electrical grids.

The Department of Homeland Security received reports of some 257 cyber attacks on critical infrastructure systems in the U.S. in 2013, a 30 percent increase from the 197 incidents reported in 2012.[4]

A number of federal legislative/regulatory proposals on cybersecurity are under consideration by Congress. At the state level, some 47 states also have breach notification laws in effect.

A summary of the executive order as well as a summary of the various legislative bills in Congress is included in Appendix 1.

## CYBER SECURITY: RISING CONCERNS AND COSTS

Cyber security and losses from cyber crimes are a growing concern among businesses today, as highlighted in latest industry research.

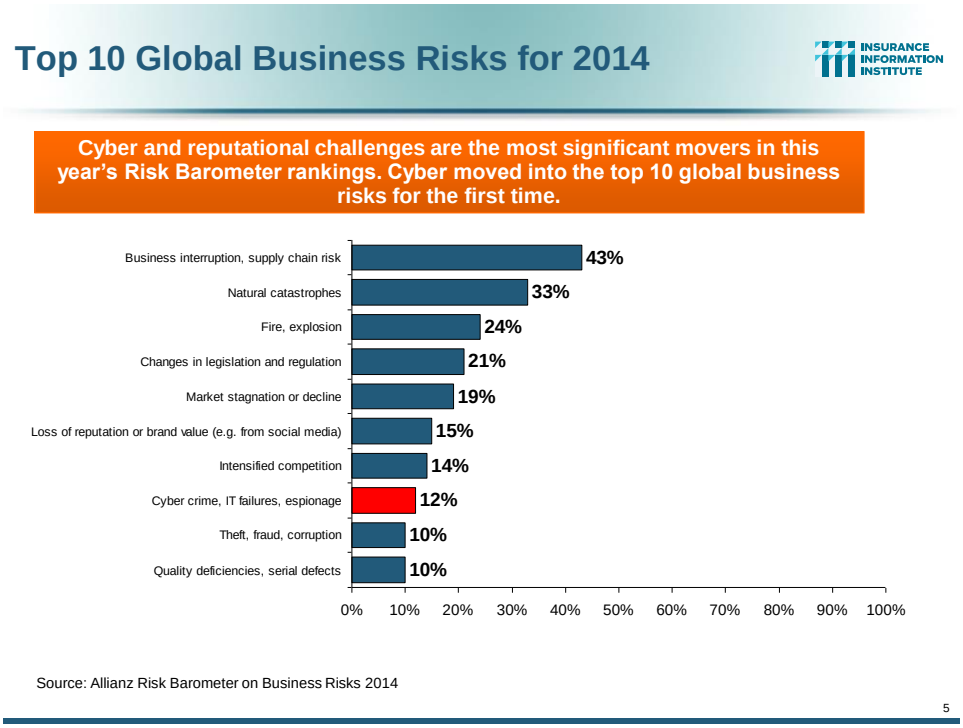
Cyber risk moved into the top 10 global business risks in 2014, according to the third annual Allianz Risk Barometer Survey, climbing up to rank 8 from 15 in last year's survey (Fig. 4).[5]

The Risk Barometer, which surveyed more than 400 corporate insurance experts from 33 countries, found other interlinked emerging risks, such as loss of reputation issues and changes in legislation, were also at the forefront.

Allianz noted that companies increasingly face new exposures to first- and third-party liability and business interruption from cyber attacks or disruptions, with loss of personal data and theft of intellectual property being major concerns.

[4] ICS-CERT Year in Review 2013, Department of Homeland Security.
[5] Allianz Risk Barometer 2014, January 2014, http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf.

**Fig. 4**




Similarly, a May 2014 report by PWC found that while companies are focused on managing a variety of business risks, cyber crimes are considered a high-level threat globally.[6]

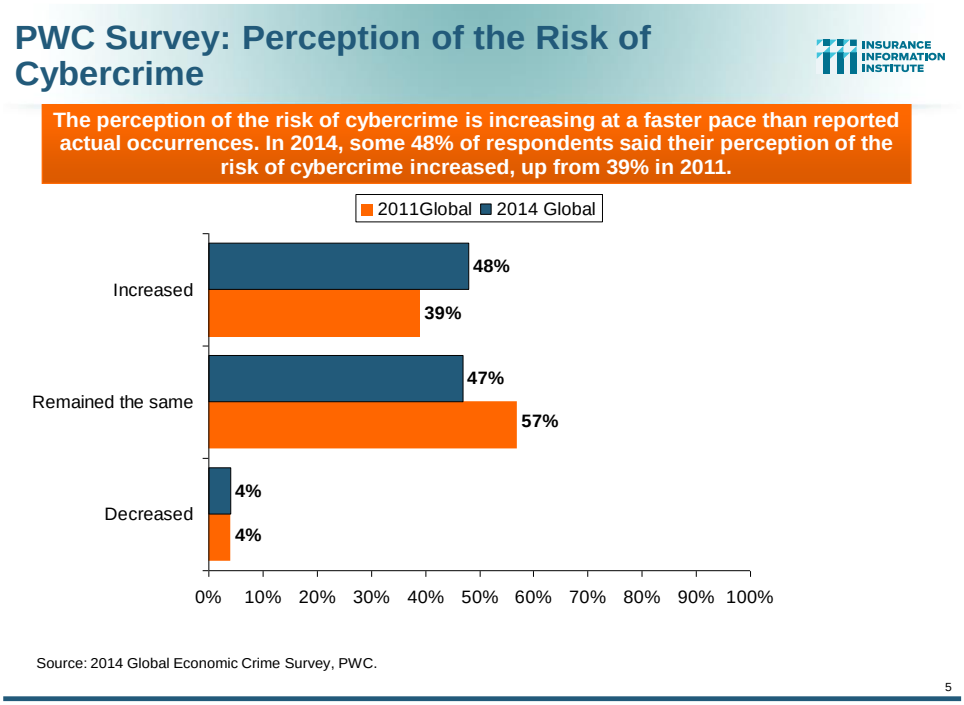
In a sign that organizations are taking this threat more seriously, the PWC survey found that the perception of the risk of cybercrime is increasing at a faster pace than that of reported actual occurrences.

Some 48 percent of respondents said their perception of cybercrime risk at their organization increased in 2014, up from 39 percent in 2011 (Fig. 5).

Reinforcing this evidence, PWC noted that an identical percentage (48 percent) of CEOs in its latest Global CEO Survey said they were concerned about cyber threats, including the lack of data security.

[6] 2014 Global Economic Crime Survey, PWC, http://www.pwc.com/crimesurvey

**Fig. 5**




Overall, U.S. companies appear to have a greater understanding of the risk of cybercrime than their global peers, the survey found. PWC noted that U.S. organizations' perception of the risks of cybercrime exceeded the global average by 23 percent.

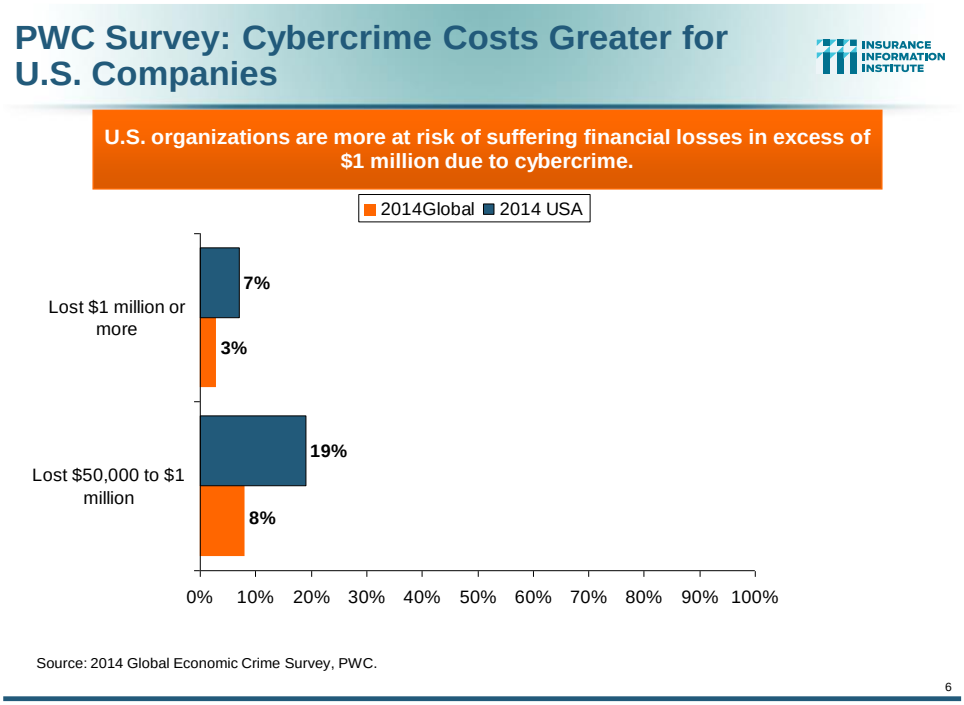
Also, some 71 percent of U.S. respondents indicated their perception of the risks of cybercrime increased over the past 24 months, rising 10 percent since 2011.

Cyber attacks have also become more frequent and increasingly costly for companies to resolve.

PWC's findings suggest that U.S. organizations are more at risk of suffering financial losses in excess of $1 million due to cybercrime (Fig. 6).

According to the study, some 7 percent of U.S. companies lost $1 million or more, compared to just 3 percent of global organizations. In addition, 19 percent of U.S. organizations lost $50,000 to $1 million, compared to 8 percent of global respondents.

**Fig. 6**



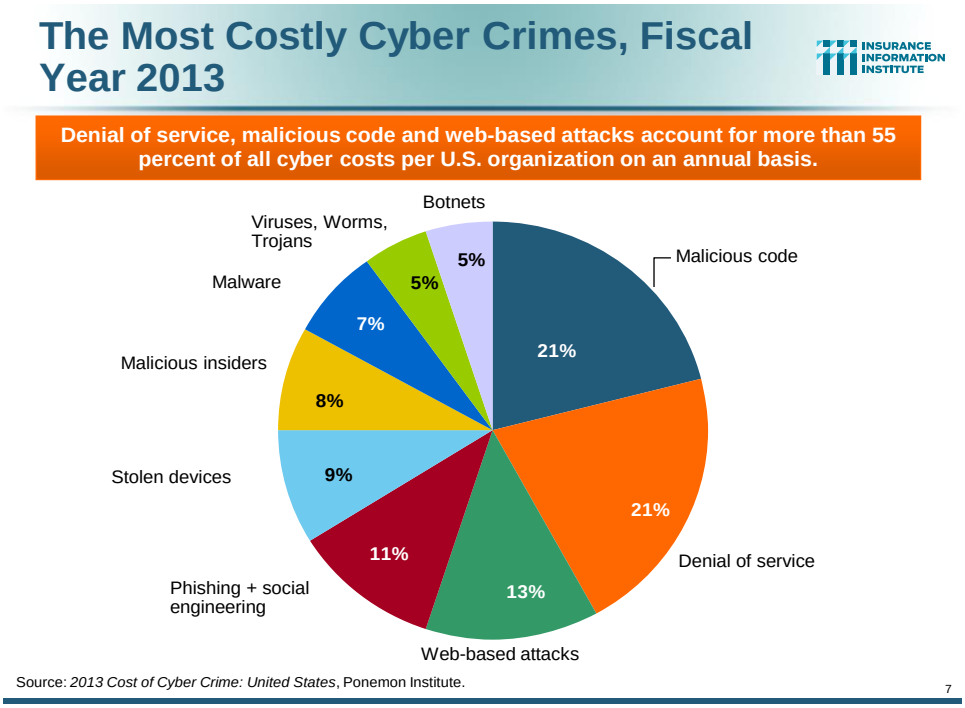

Cyber attacks continue to be very costly for organizations and those costs are rising.[7]

An annual study of U.S. companies by the Ponemon Institute estimates the average annualized cost of cyber crime at $11.6 million per year, an increase of 30 percent from $8.9 million the previous year. The total annualized cost of cyber crime for the 2013 benchmark sample of 60 organizations ranges from a low of $1.3 million to a high of $58 million.

The most costly cyber crimes are those caused by denial of service, malicious insiders and web-based attacks, Ponemon said (Fig. 7).

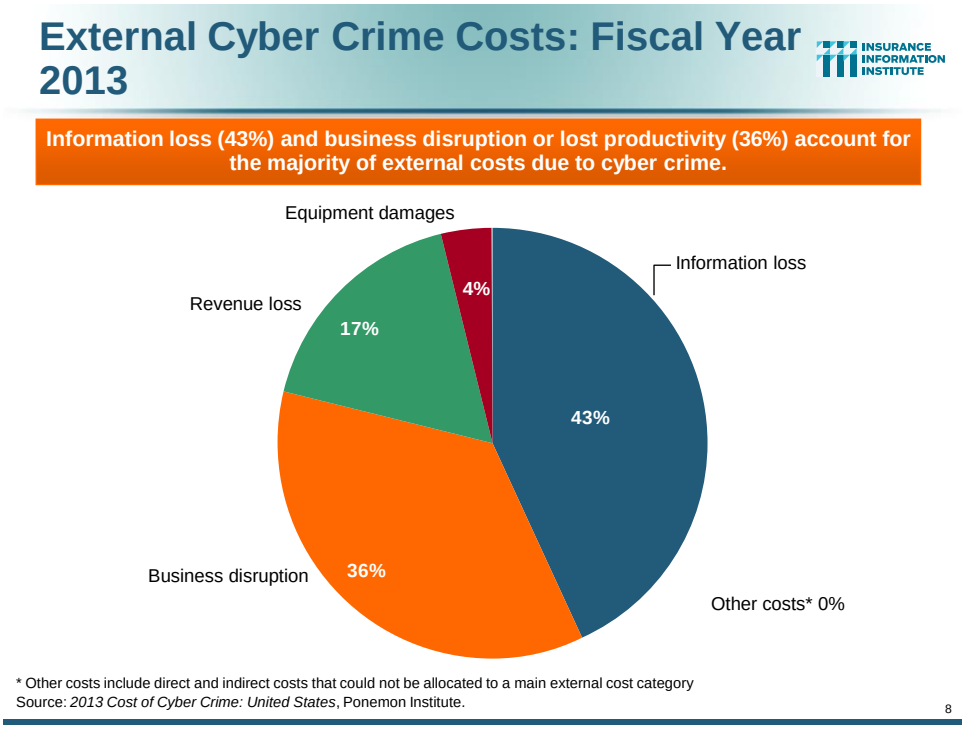
[7] *2013 Cost of Cyber Crime Study: United States*, Ponemon Institute, October 2013

**Fig. 7**




Information theft continues to represent the highest external cost for companies that experience a cyber attack, followed by costs associated with business disruption, the Ponemon study revealed (Fig. 8). On an annualized basis, information theft accounts for 43 percent of total external costs (down 2 percent from 2012). Costs associated with disruption to business or lost productivity account for 36 percent of external costs (up 18 percent from 2012). In the context of the Ponemon study, an external cost is one that is created by external factors such as fines, litigation, marketability of stolen intellectual properties and more.

**Fig. 8**




Cyber attacks can also become costly if not resolved quickly. According to the study results, the average time to resolve a cyber attack was 32 days, with an average cost to participating companies of just over $1 million during this 32-day period. This represents a 55 percent increase from last year's estimated average cost of $591,780 based on a 24-day resolution period. Results show that malicious insider attacks can take more than 65 days on average to contain.

## THE CYBER CRIME AND CYBER TERRORISM THREAT

The threat both to national security and the economy posed by cyber crime and cyber terrorism is a growing concern for governments and businesses around the world

The International Institute for Counter Terrorism (ICT) reports that global jihad groups and other terrorist organizations are increasingly venturing into cyberspace, engaging in what they call "electronic jihad," attacking the enemy by sabotaging its online infrastructure, using the information available to them from the virtual world to cause mayhem in the real world, and developing their own defensive capabilities against cyber-attack. [8]

In recent years there have also been an increasing number of cyber attacks on political targets, critical infrastructure (including water, electricity and gas), and the

[8] Cyber-Terrorism Activities, Report No. 6, October-November 2013, International Institute for Counter-Terrorism (ICT).

websites of commercial corporations. According to the ICT, these attacks are perpetrated by states (which do not take responsibility for them), groups of hackers (such as Anonymous), criminal organizations and lone hackers.

The ICT highlights a number of recent developments, including: the increasing popularity of digital currency, such as Bitcoin, that has resulted in its acceptance as payment by an increasing number of establishments, despite the potential risks and illegal uses; continued politically motivated attacks around the world by the Anonymous hacker groups against targets in Arab countries and in the United States, in response to publications regarding activities by the National Security Agency (NSA); and activities by members of the Syrian Electronic Army hackers, targeting President Obama.

In 2011, a report from the Pentagon concluded that computer sabotage coming from another country can constitute an act of war.[9] It noted that the Laws of Armed Conflict—that guide traditional wars and are derived from various international treaties such as the Geneva Convention—apply in cyberspace as in traditional warfare.

A recent survey conducted by Tenable Network Security found that the majority of Americans fear that cyber warfare is imminent and that the country will attack or be attacked in the next decade.[10]

An overwhelming 93 percent of respondents to the survey believe that U.S. corporations and businesses are at least somewhat vulnerable to state-sponsored attacks. And 95 percent believe U.S. government agencies themselves are at least somewhat to very vulnerable to cyber attacks.

Some 94 percent of survey respondents also say they support the President having the same level of authority to react to cyber attacks as he has to respond to physical attacks on the country.

The survey also revealed conflicting results as to whether the public or private sector should be held accountable for protecting corporate networks.

Some 66 percent of respondents believe corporations should be held responsible for cyber breaches when they occur. But an almost equal number of Americans—62 percent—say government should be responsible for protecting U.S. businesses from cyber attacks.

[9] *Cyber Combat: Act of War*, by Siobhan Gorman and Julian E. Barnes, the Wall Street Journal, May 30, 2011.
[10] Tenable Network Security survey, February 2013.

## DATA BREACHES: RISING COSTS AND LIABILITY EXPOSURE

Businesses across a wide range of industry sectors are exposed to potentially enormous physical losses as well as liabilities and costs as a result of cyber attacks and data breaches.

Victims of recent attacks include such well-known brands as eBay, Target, Neiman Marcus, Michaels Stores, the University of Maryland, JPMorgan Chase, Adobe, Living Social. The list goes on.

And then came the April 2014 disclosure of the Heartbleed bug which undermines the popular OpenSSL encryption technology. Many companies have said they were affected by Heartbleed and it remains to be seen how many companies will disclose data breaches as a result of this security flaw.

In 2013 some 614 organizations across business, financial, educational, government and healthcare sectors, publicly disclosed data breaches exposing close to 92 million records, according to the Identity Theft Resource Center.[11] This compares to 449 publicly disclosed data breaches during 2012, 419 during 2011, and 662 publicly disclosed data breaches in 2010.

So far in 2014, some 311 data breach events have been publicly disclosed as of May 27, with 8.5 million records exposed.

Recent high profile data breach incidents include a massive data breach at online marketplace EBay in May 2014 that exposed personal records of the site's 233 million customers.

Another huge data breach at retailer Michaels Stores, revealed by the company in January 2014, may have affected some 2.6 million customer payment cards (Fig. 9).

And in January 2014 Neiman Marcus announced that 1.1 million customer credit cards may have been compromised in a data breach that occurred in late 2013.

Meanwhile, the massive data breach at Target during holiday season 2013 exposed the personal and financial information of up to 110 million consumers.

[11] Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf

**Fig. 9**

## High Profile Data Breaches, 2013-2014

| Date | Company | Description of Breach |
|---|---|---|
| May 2014 | EBay | Massive data breach exposed records of site's 233 million customers, including names, email addresses, physical addresses, phone numbers and birthdates. |
| Feb 2014 | Michaels Stores | Possible fraudulent activity on some U.S. payment cards used at Michaels stores suggests it may have experienced data security attack, exposing 2.6 million records. |
| Jan 2014 | Neiman Marcus | Hacker break-in exposed unknown number of customer cards, compromising estimated 1.1 million records. |
| Dec 2013 | JPMorgan Chase | Hackers attacked banking giant's network, compromising some personal information of 465,000 card holders. |
| Nov/Dec 2013 | Target | Malware stored on Target's checkout registers led to theft of data from about 40 million credit and debit card accounts and the personal information of up to 70 million customers. |
| October 2013 | CA-based AHMC Hospitals | Two unencrypted laptops stolen compromising patient information, including names, social security numbers, and diagnostic codes, jeopardizing 729,000 patients. |
| Aug/Sept 2013 | Adobe | Hackers stole encrypted customer credit card information and other data for 38 million users. |
| July 2013 | Dept of Energy | Leak of over 104,000 employees' and contractors' personal information, including name, social security number, date of birth. Attack leveraged flaw in Adobe product. |
| April 2013 | Living Social | Hackers stole personal data, including names, emails, birthdates and encrypted passwords of more than 50 million users. |
| Jan 2013 | New York Times | Chinese hackers infiltrated New York Times computer systems for a period of four months, getting passwords for its reporters and employees. |
| Dec 2012 | Google, Facebook, LinkedIn, Twitter, Yahoo and ADP | Cybercriminals stole 2 million passwords and user names with a botnet known as 'Pony' from Google, Facebook, Twitter and Yahoo. Nearly 100 countries hit. |

Sources: Identity Theft Resource Center; Insurance Information Institute (I.I.I.) research.

These high profile data breach incidents have served to increase both public and government scrutiny of cyber security practices.

A benchmark study by the Ponemon Institute of 314 companies representing 10 countries, including the United States, found that data breaches are becoming far more costly to manage.

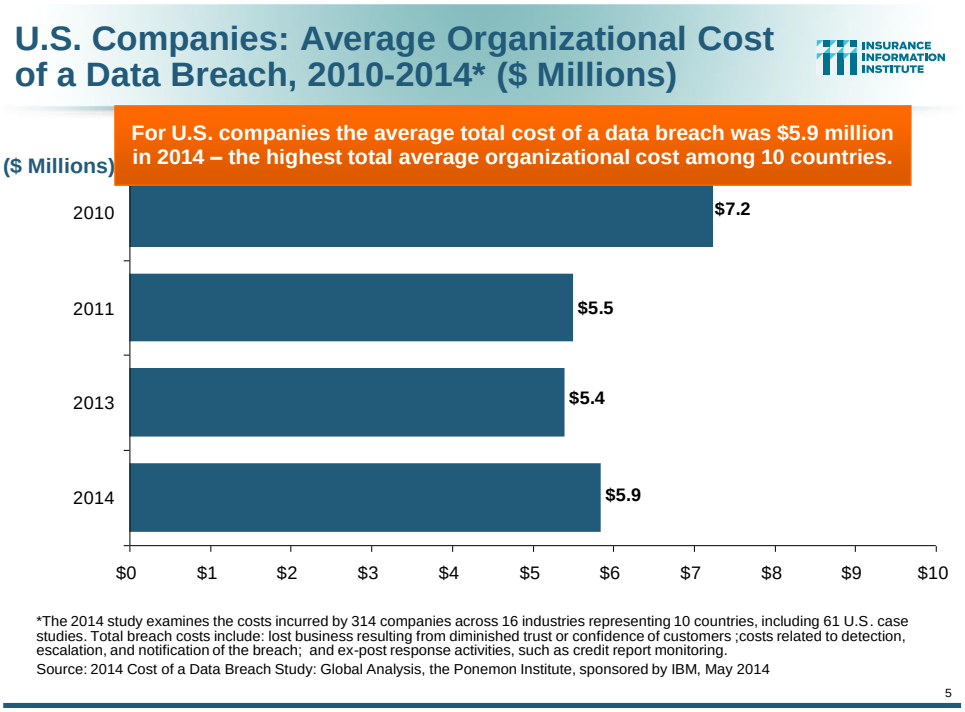
The Ponemon research does not include catastrophic or mega data breaches of more than approximately 100,000 compromised records because these are not typical of the breaches most organizations experience.

For the U.S. companies participating in this research the average total cost of a data breach was more than $5.85 million in 2014—the highest total average cost of the 10 countries—up 8 percent from $5.4 million in 2013 (Fig. 10).[12] The average per capita cost of a data breach for U.S. companies was $201, compared to a $188 average cost calculated last year.

Also, on average U.S. companies had data breaches that resulted in the greatest number of exposed or compromised records, at 29,087.

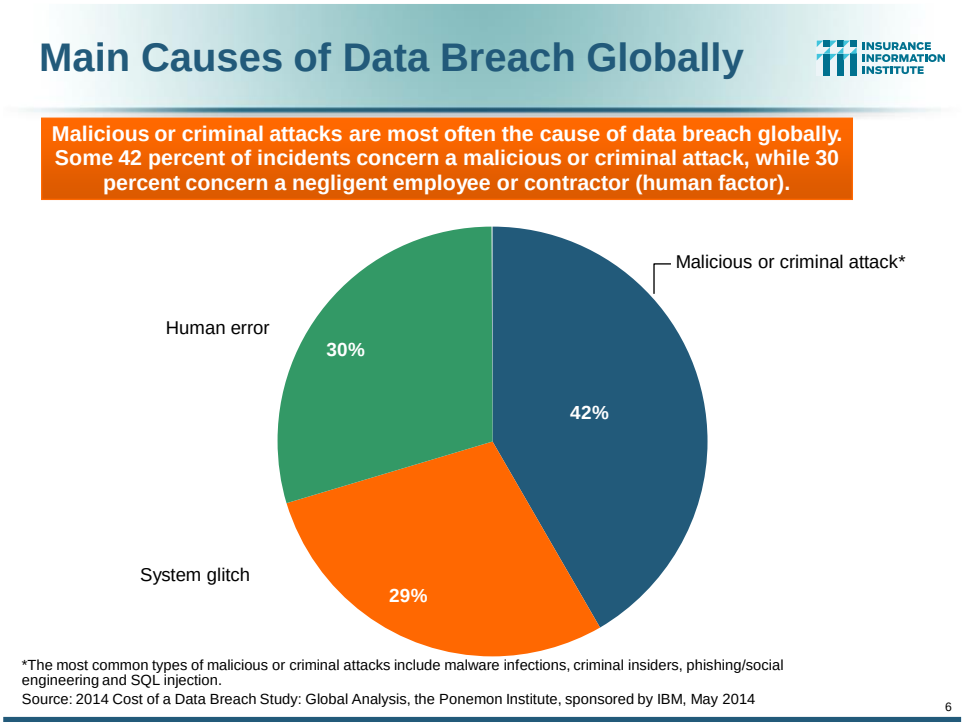
[12] *2014 Cost of a Data Breach Study: Global Analysis*, research by the Ponemon Institute, sponsored by IBM, May 2014.

**Fig. 10**




Malicious or criminal attacks are most often the cause of a data breach globally and also the most costly data breach incidents in all 10 countries (Fig. 11). U.S. companies experience the most expensive data breach incidents, at $246 per compromised record.

**Fig. 11**




The Ponemon study also found that U.S. organizations have the highest lost business costs at an average of $3.3 million. These costs include abnormal turnover of customers (a higher than average loss of customers for the industry or organization), increased customer acquisition activities, reputation losses and diminished goodwill.

The study noted that certain organizational factors can reduce the overall cost of a data breach. Companies that had a strong security posture at the time of the data breach could reduce the average cost per record by $14.14 to $131.86 – the greatest decrease in cost. Companies that had an incident response plan in place also reduced the average cost per record by $12.77.

However, the specific attributes or factors of a data breach can also increase the overall cost. For example, the study found that if the data breach involved lost or stolen devices the cost per record could increase by $16.10 to $161.10. Third party involvement in the breach incident also increases the per capita cost of a data breach by $14.80.

As new technologies continue to evolve, companies are potentially exposed to even greater risks from data security breaches. For example, security concerns surround the adoption of cloud computing—the use of a network of remote servers over the Internet to store, manage and process data, rather than a local server—by both companies and government agencies.

A recent survey by InformationWeek of business technology professionals at 446 companies with 50 or more employees asked respondents to identify three cloud computing concerns from among 10 options. The top three cloud risks cited by respondents were all security related, as follows: 51 percent cited security defects in the technology itself; 45 percent cited unauthorized access to or leak of proprietary information; and 40 percent cited unauthorized access to or leak of customers' information.[13]

## LEGAL DEVELOPMENTS

The cyber risk landscape is fast-evolving and companies face growing potential liabilities in this area.

Some of the recent legal developments include:

**Data Breach Liability:** Litigation surrounding data and privacy protection continues to evolve amid a growing number of high profile data breaches. An organization may be found liable if a breach resulting from a systems failure or lax security compromises the security of customer personal information or data. A variety of legal theories may be pursued, including allegations of negligence, breach of fiduciary duty and breach of contract.

Increased regulation at both the Federal and state level related to information security and breach notification is expanding the legal avenues that may be pursued. Many states have enacted laws requiring companies to notify consumers of breaches of personal data. Federal laws, such as the HIPAA, the Gramm Leach Bliley Act and the Fair Credit Reporting Act have requirements to safeguard the privacy of personal information.

A federal court in New Jersey recently upheld the power of the Federal Trade Commission (FTC) to sue companies that fail to protect their customers' data.[14] The ruling rebuffed a challenge from Wyndham hotels, which argued that the FTC overstepped its authority with a 2012 lawsuit against the global hotel chain.

**Class Action Lawsuits:** Mega data breaches have prompted class action lawsuits to be filed against companies seeking damages collectively on behalf of individuals whose personal information was lost or stolen. Legal experts note that the scope and number of data breach class actions is unprecedented, with more cases being filed in the aftermath of recent massive data breaches.[15]

For example, over 70 class actions lawsuits alone have been filed against Target by its customers following its 2013 holiday season data breach that compromised up to 110 million customer accounts. According to one legal expert, for some plaintiffs'

[13] *2013 InformationWeek State of Cloud Computing Survey,* February 2013.
[14] *Court Upholds FTC's Power to Sue Hacked Companies*, National Journal Online, April 7, 2014.
[15] Trends in Data Breach Cybersecurity Regulation, Legislation and Litigation, Mayer Brown, April 17, 2014.

lawyers this was "the Black Friday door buster to end all others."[16] Plaintiffs in data breach class actions typically allege that businesses failed to adequately safeguard consumer information and gave insufficient and untimely notice of the breach. In the Target class actions some of the plaintiffs are even seeking damages for emotional distress and punitive damages. Target and other companies can also face class actions from banks and credit unions seeking damages for administrative expenses, lost interest, transaction fees and lost customers.

Settlements of data breach class actions can be huge. For example, 25 class action lawsuits were settled in the wake of the 2007 TJ Maxx data breach involving the theft of data related to over 45 million credit and debit cards. The settlement included: up to $1 million to customers without receipts; up to $10 million to customers with receipts ($30 per claimant); $6.5 million in plaintiffs' attorneys fees; and three free years of credit monitoring, reported to cost $177 million.

**Data Breach Insurance Coverage:** Companies that have suffered a data breach look to their insurance policies for coverage to help mitigate some of the enormous costs. The application of standard form commercial general liability (CGL) policies to data breach incidents has led to various legal actions and differing opinions. One recent high profile case followed the April 2011 data breach at Sony Corp. in which hackers stole personal information from tens of millions of Sony PlayStation Network users. A New York trial court ruled that Zurich American Insurance Co. owed no defense coverage to Sony Corp. or Sony Computer Entertainment America LLC. In his ruling, New York Supreme Court Justice Jeffrey K. Oing said acts by third-party hackers do not constitute "oral or written publication in any manner of the material that violates a person's right of privacy" in the Coverage B (personal and advertising injury coverage) under the CGL policy issued by Zurich.[17]

## CYBER SECURITY AND INSURANCE

While traditional insurance policies typically have not handled these emerging risks, limited coverage under traditional policies may be available. For example, in general there would be coverage under a traditional property insurance policy if a cyber incident resulted in a covered cause of loss such as a fire that caused property damage.

Traditional property insurance policies often contain express provisions covering damage or disruption to electronic data. The package policy known as the Business Owners Policy (BOP) that is often purchased by medium and smaller-sized businesses includes coverage for electronic data loss.

This means that in the event electronic data is destroyed or damaged as the result of a covered cause of loss, the insurer will pay the cost to replace or restore it. Causes of loss that apply to this coverage include a computer virus, harmful code or other

[16] *Measuring the Bull's-Eye on Target's Back: Lessons From the T.J. Maxx Data Breach Class Actions*, by Randy J. Maniloff, Coverage Opinions, January 15, 2014.
[17] *N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation*, by Young Ha, Insurance Journal, March 17, 2014.

harmful instructions entered into a computer system or network to which it is connected. There is no coverage, however, for loss or damage caused by the actions of any employee.

Reliance on traditional insurance policies is not enough, however, so specialized cyber insurance policies have been developed by insurers to help businesses and individuals protect themselves from an ever-evolving range of risks. Recent market intelligence suggests that the types of specialized cyber coverage being offered by insurers are expanding in response to this fast-growing market need.

Specialized cyber risk coverage is available primarily as a stand-alone policy. Each policy is tailored to the specific needs of a company, depending on the technology being used and the level of risk involved. Both first- and third-party coverages are available.

Types of cyber risk coverage include:

**Loss/Corruption of Data** – Covers damage to, or destruction of, valuable information assets as a result of viruses, malicious code and Trojan horses.

**Business Interruption** – Covers loss of business income as a result of an attack on a company's network that limits its ability to conduct business, such as a denial-of-service computer attack. Coverage also includes extra expenses, forensic expenses and dependent business interruption.

**Liability** – Covers defense costs, settlements, judgments and, sometimes, punitive damages incurred by a company as a result of:

- Breach of privacy due to theft of data (such as credit cards, financial or health related data);
- Transmission of a computer virus or other liabilities resulting from a computer attack, which causes financial loss to third parties;
- Failure of security which causes network systems to be unavailable to third parties; rendering of Internet Professional Services;
- Allegations of copyright or trademark infringement, libel, slander, defamation or other "media" activities in the company's website, such as postings by visitors on bulletin boards and in chat rooms. This also covers liabilities associated with banner ads for other businesses located on the site.

**D&O/Management Liability –** Newly developed tailored D&O products provide broad all risks coverage, meaning that the risk is covered unless specifically excluded. All liability risks faced by directors, including cyber risks, are covered.

**Cyber Extortion** – Covers the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.

**Crisis Management** – Covers the costs to retain public relations assistance or advertising to rebuild a company's reputation after an incident. Coverage is also available for the cost of notifying consumers of a release of private information, as well the cost of providing credit-monitoring or other remediation services in the event of a covered incident.

**Criminal Rewards** – Covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of a cyber criminal who has attacked a company's computer systems.

**Data Breach** – Covers the expenses and legal liability resulting from a data breach. Policies may also provide access to services helping business owners to comply with regulatory requirements and to address customer concerns.

**Identity Theft** – Provides access to an identity theft call center in the event of stolen customer or employee personal information.

**Social Media/Networking** – Insurers are looking to develop products that cover a company's social networking activities under one policy. Some cyber policies now provide coverage for certain social media liability exposures such as online defamation, advertising, libel and slander.

Depending on the individual policy, specialized cyber risk coverage can apply to both internally and externally launched cyber attacks, as well as to viruses that are specifically targeted against the insured or widely distributed across the Internet. Premiums can range from a few thousand dollars for base coverage for small businesses (less than $10 million in revenue) to several hundred thousand dollars for major corporations desiring comprehensive coverage.

As part of the application process, some insurers offer an online and/or on-site security assessment free of charge regardless of whether the applicant purchases the coverage. This is helpful to the underwriting process and also provides extremely valuable analysis and information to the company's chief technology officer, risk manager and other senior executives.

Individuals are also seeking to better protect themselves from the risks created by their participation in social media. While traditional homeowners insurance policies include liability protection that covers the insured against lawsuits for bodily injury or property damage, coverage may be limited and individual policies may differ by company and by state. Case law in this area is also evolving and still uncertain. However, umbrella or excess liability policies provide broader protection, including claims against the insured for libel and slander, as well as higher liability limits.

Specialized insurance products that protect an individual from social media-related risks are under development.

**Cloud Computing** – Insurers are developing products to provide coverage for cloud providers and the businesses that utilize them. Recruiting new business can be challenging for cloud providers as businesses have concerns over data security. Traditional cyber liability policies typically exclude losses incurred by a third party such as a cloud provider. The cloud coverage being developed by insurers would apply to loss, theft and liability of the data stored within the cloud, whether the loss occurs from hacking, a virus or a subsequent liability event.

## CYBER INSURANCE: BUYING TRENDS AND MARKET OVERVIEW

The exact number of U.S. companies that have a cyber insurance policy is difficult to determine given that individual surveys poll different numbers and types of respondents, often from a varied distribution of industry groups.

Here are some examples of recent findings/research in this area:

- A 2013 annual survey jointly produced by Advisen and Zurich found that 52 percent of companies claim to purchase cyber liability insurance.[18] Of those companies that do purchase coverage, some 72 percent have done so for more than three years, a 10-point increase from 2012. Some 329 risk managers, insurance buyers and other risk professionals participated in the survey, which was conducted in September 2013.

- A 2013 report sponsored by Experian and conducted by the Ponemon Institute stated that 31 percent of U.S. companies have a cyber security insurance policy.[19] As well as reducing the potential financial liability of a breach or security exploit, companies' security posture becomes stronger with the purchase of cyber insurance, the survey found. Some 62 percent of respondents said their companies' ability to deal with security threats improved after the purchase of the policy. The findings are based on 638 surveys completed by experienced individuals involved in their companies' cyber security risk mitigation and risk management activities in various-sized organizations in the United States

[18] *2013 Information Security, Cyber Liability & Risk Management*, by Advisen, sponsored by Zurich, October 2013.
[19] *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, conducted by the Ponemon Institute, sponsored by Experian, August 2013.

- Two 2013 reports by Willis surveyed the U.S. listed Fortune 500 and Fortune 501-1,000 firms.[20] In both reports, only 6 percent of companies disclosed that they purchase insurance to cover cyber risks. The earlier Willis Fortune 500 Cyber Disclosure Report reviewed the 10-Ks or annual reports filed by the Fortune 500 in 2012, tracking organizations' response to SEC Guidance issued in October 2011 that asked U.S. listed companies to provide extensive disclosure on their cyber exposures. The Willis Fortune 1,000 Cyber Disclosure Report asks the same questions of the wider pool of companies and highlights industry groups.

Whatever the precise number of U.S. companies buying cyber insurance may be, there is growing evidence that in the wake of the Target data breach and other high profile breaches, the number of policies is increasing, with one legal expert describing the Target data breach as "the equivalent of 10 free Super Bowl ads for insurers selling cyber policies."[21]

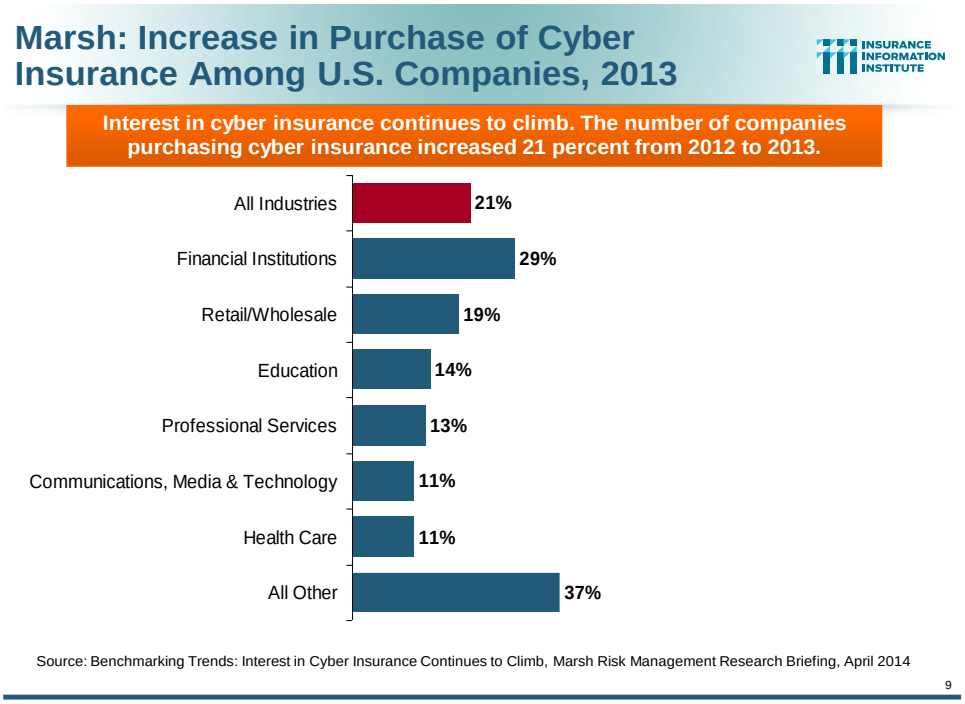
The fact that Target did have $100 million in network security insurance has been widely reported in the news.[22] As of February 1, Target said of the $61 million in expenses related to the data breach during the fourth quarter 2013, some $44 million was offset by insurance.

Latest market analysis indicates that the trend to purchase cyber insurance is not just continuing but accelerating.[23] An April 2014 market briefing from broker Marsh notes that recent high-profile data breaches, growing board-level concern, and the increasing vulnerability of operations to failure of technology appear to be influencing purchasing decisions.

The number of Marsh clients purchasing cyber insurance increased by 21 percent from 2012 to 2013. Data-rich sectors, including financial institutions, retail/wholesale, and professional services, saw the number of buyers increase more than 13 percent (Fig. 12). Industries representing emerging sectors for cyber purchasing, such as manufacturing, power and utilities, and hospitality added to that trend.

[20] Willis Fortune 1000 Cyber Disclosure Report, August 2013; and Willis Fortune 500 Cyber Disclosure Report, 2012.
[21] *There Aren't As Many Cos. With Cyberinsurance As You Think*, Law360.com, by Randy Maniloff, White and Williams LLP, February 24, 2014.
[22] *Target SEC filing details insurance coverage and outlines costs of data breach*, by Judy Greenwald, Business Insurance, March 30, 2014.
[23] Benchmarking Trends: Interest in Cyber Insurance Continues to Climb, Marsh Risk Management Research Briefing, April 2014.

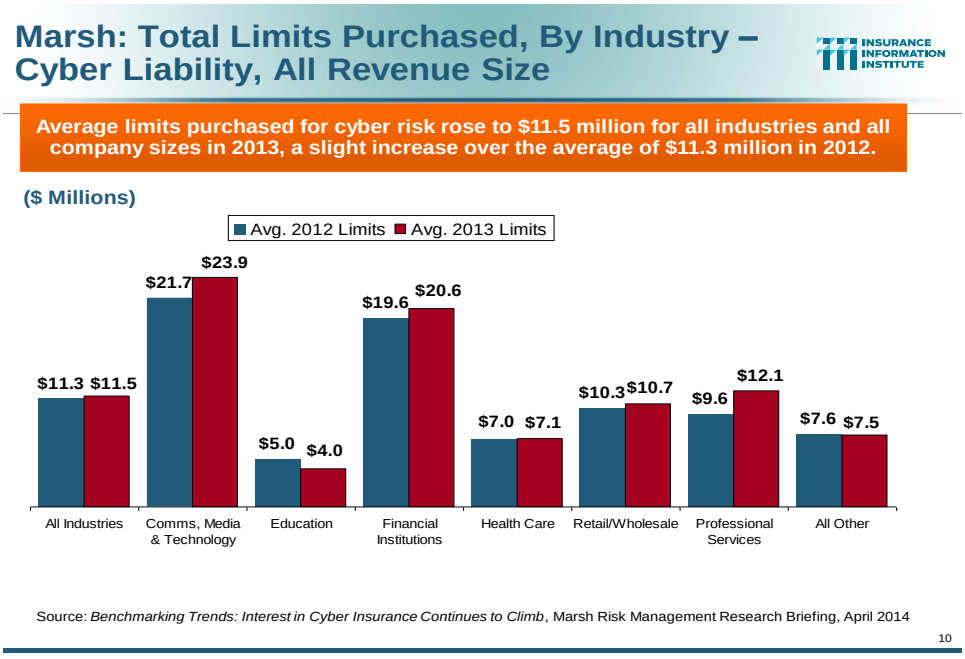
**Fig. 12**




Those companies purchasing cyber insurance are also buying higher limits. Cyber insurance limits purchased in 2013 averaged $11.5 million across all industries and all company sizes, a slight increase over the average of $11.3 million in 2012, Marsh says (Fig. 13).

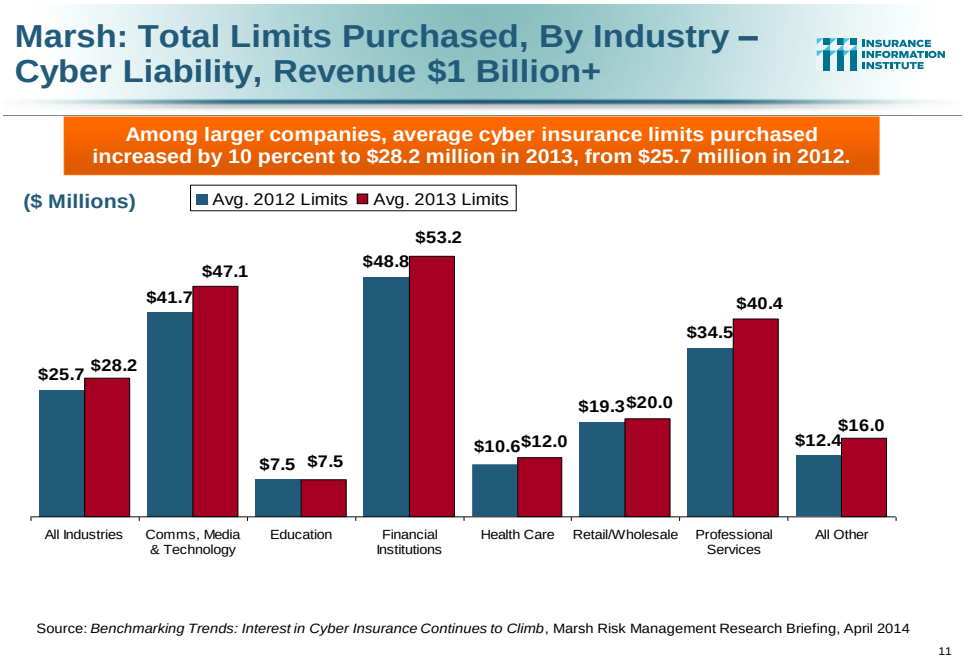
Communications, media, and technology continued to purchase the highest limits, with $23.9 million in 2013, up from $21.7 million in 2012.

**Fig. 13**




Among larger companies, which tend to have greater exposure to cyber risk, average limits purchased increased by 10 percent over 2012 (Fig. 14).

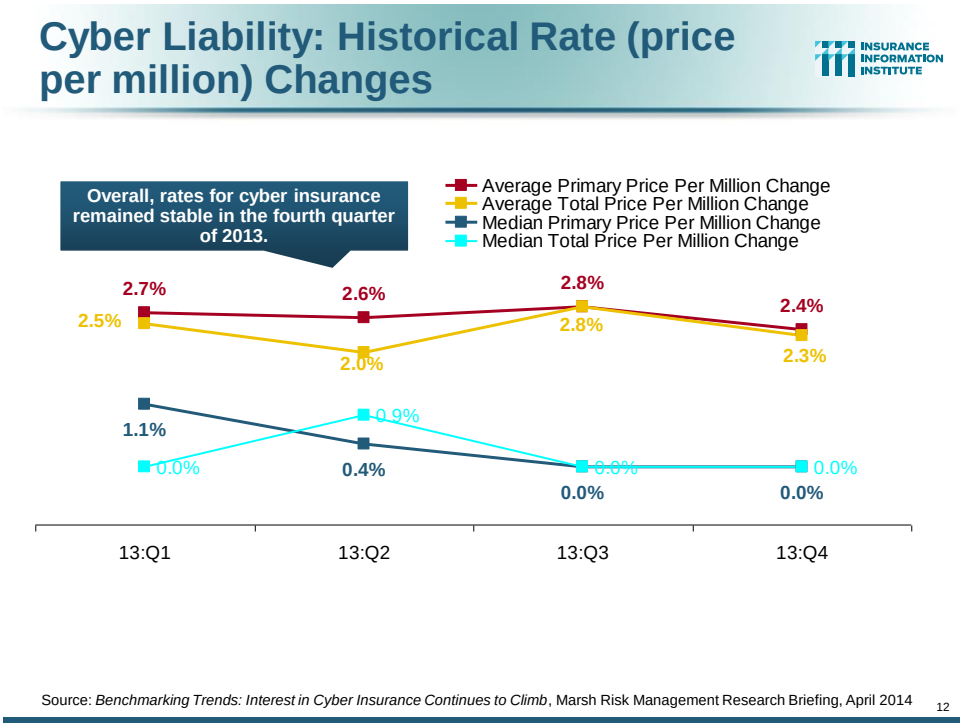
**Fig. 14**



During 2013, renewal rates for cyber liability coverage—as measured by average and median annual changes in the year-over-year price per million of limits—remained generally stable for both primary layers and total programs (Fig. 15). Marsh reports that average increases were typically small, ranging between 2 percent and 3 percent compared to pricing in the prior year.

While 2013 saw fewer new entrants into the market than in prior years, only marginally tamping down rates, Marsh notes that both new buyers and renewals benefited from increased competition among existing markets. However, the December 2013 retail breaches caused several insurers to reassess their appetite for certain industries and the retentions at which they would attach on such risks.

**Fig. 15**




Source: *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh Risk Management Research Briefing, April 2014 12

## CONCLUSION

Amid a rising number of high profile mega data breaches—most recently at eBay, Target and Neiman Marcus—government is stepping up its scrutiny of cyber security. This is leading to increased calls for legislation and regulation, placing the burden on companies to demonstrate that the information provided by customers and clients is properly safeguarded online.

One notable advance in this area is a new framework for improving critical infrastructure cybersecurity released by the National Institute of Standards and Technology (NIST) in February 2014. The framework gathers existing global standards and practices to help organizations understand, communicate and manage their cyber risks. The NIST release followed an executive order issued by President Obama a year earlier that promotes increased information sharing about cyber threats between government and private companies that oversee critical infrastructure systems such as electrical grids.

Despite the fact that cyber risks and cyber security are widely acknowledged to be a serious threat, many companies today still do not purchase cyber risk insurance. However, this is changing. Recent legal developments underscore the fact that reliance on traditional insurance policies is not enough, as companies face growing liabilities in this fast-evolving area. For example, over 70 class actions lawsuits alone have been filed against Target by its customers following its 2013 holiday season data breach that compromised up to 110 million customer accounts.

Settlements of data breach class actions can be huge. For example, 25 class action lawsuits were settled in the wake of the 2007 TJ Maxx data breach involving the theft of data related to over 45 million credit and debit cards. The retailer ultimately paid out several hundred million dollars.

Specialist cyber insurance policies have been developed by insurers to help businesses and individuals protect themselves from the cyber threat. Market intelligence suggests that the types of specialized cyber coverage being offered by insurers are expanding in response to this fast-growing market need.

There is also growing evidence that in the wake of the Target data breach and other high profile breaches, the number of policies is increasing, and that insurance has a key role to play as companies and individuals look to better manage and reduce their potential financial losses from cyber risks in future.

**Appendix 1**

**The Cyber-Security Executive Order**
**Source:** Mayer Brown Legal Update, February 13, 2013

On February 12, 2013, President Obama issued a cybersecurity executive order to improve the cyber security of critical infrastructure in the United States and to promote information sharing about cyber threats between government and private companies that oversee such critical infrastructure systems.

The Order will have an impact on private companies that oversee critical infrastructure, including transportation systems, dams, electrical grids and financial institutions.

The definition of critical infrastructure is broad and includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

While this order is currently voluntary, the Secretary of Commerce will be designing "incentives" to encourage owners and operators of critical infrastructure to participate in the program.

**Summary of Major Cybersecurity Legislative Proposals**
Source: I.I.I. research and National Conference of State Legislatures (NCSL), as of May 2014.

**Cybersecurity and American Cyber Competitiveness Act of 2013** (S. 21)
**Summary:** Would secure the United States against cyber attack, improve communication and collaboration between the private sector and the federal government, enhance the competitiveness of the U.S. and create jobs in the information technology industry, and protect the identities and sensitive information of U.S. citizens and businesses.

**Cyber Intelligence Sharing and Protection Act** (H.R. 624)
**Summary:** Would provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes.

**Cyber Economic Espionage Accountability Act** (H.R. 2281 and S. 1111)
**Summary**: Would make cyber espionage a priority and directs the United States to intensify diplomatic efforts to address the harm to international economic order by cyber espionage and increase efforts to bring economic espionage criminal cases against foreign actors.

**Deter Cyber Theft Act of 2014** (S. 884)
**Summary:** Requires Director of National Intelligence (DNI) to report annually to specified congressional committees on foreign countries that engage in economic and industrial espionage in cyberspace with respect to U.S. trade secrets or proprietary information.

**State Legislative Developments:**

Some 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information, according to the National Conference of State Legislatures (NCSL).

In 2014, at least 19 states have introduced legislation expanding the scope of laws, setting additional requirements related to notification, or changing penalties for those responsible for breaches.