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

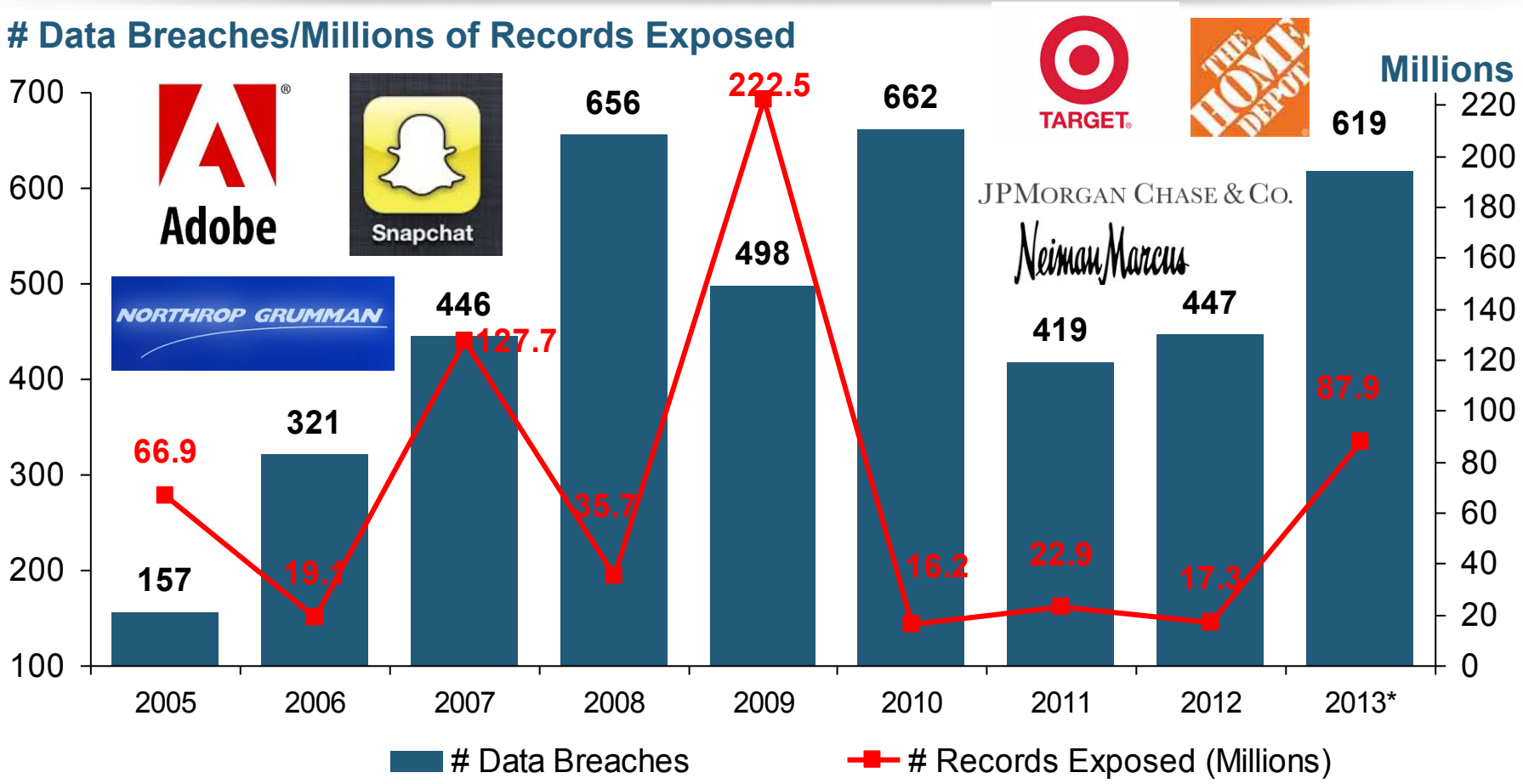
INSURANCE INFORMATION INSTITUTE

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

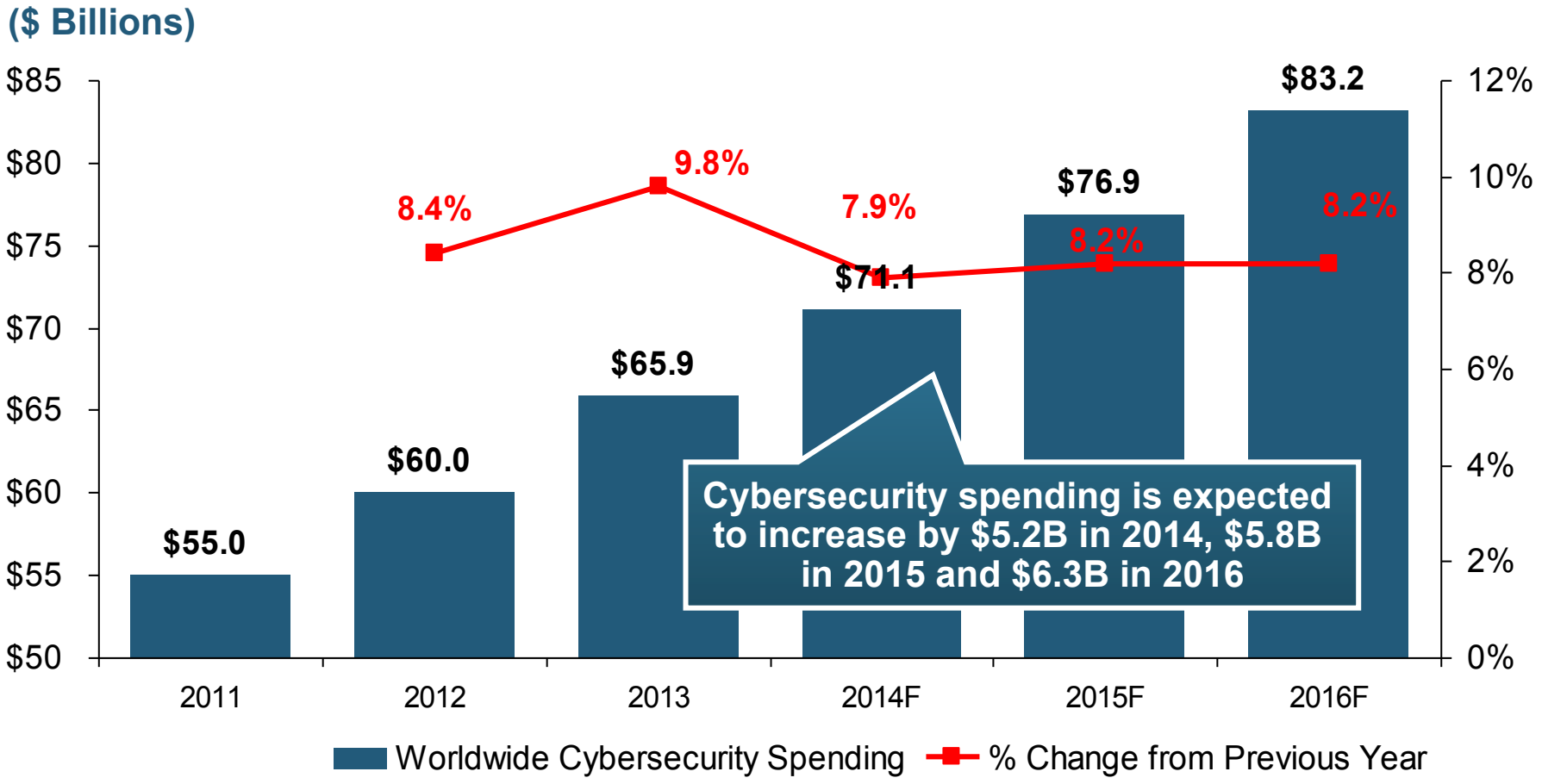
INSURANCE INFORMATION INSTITUTE



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



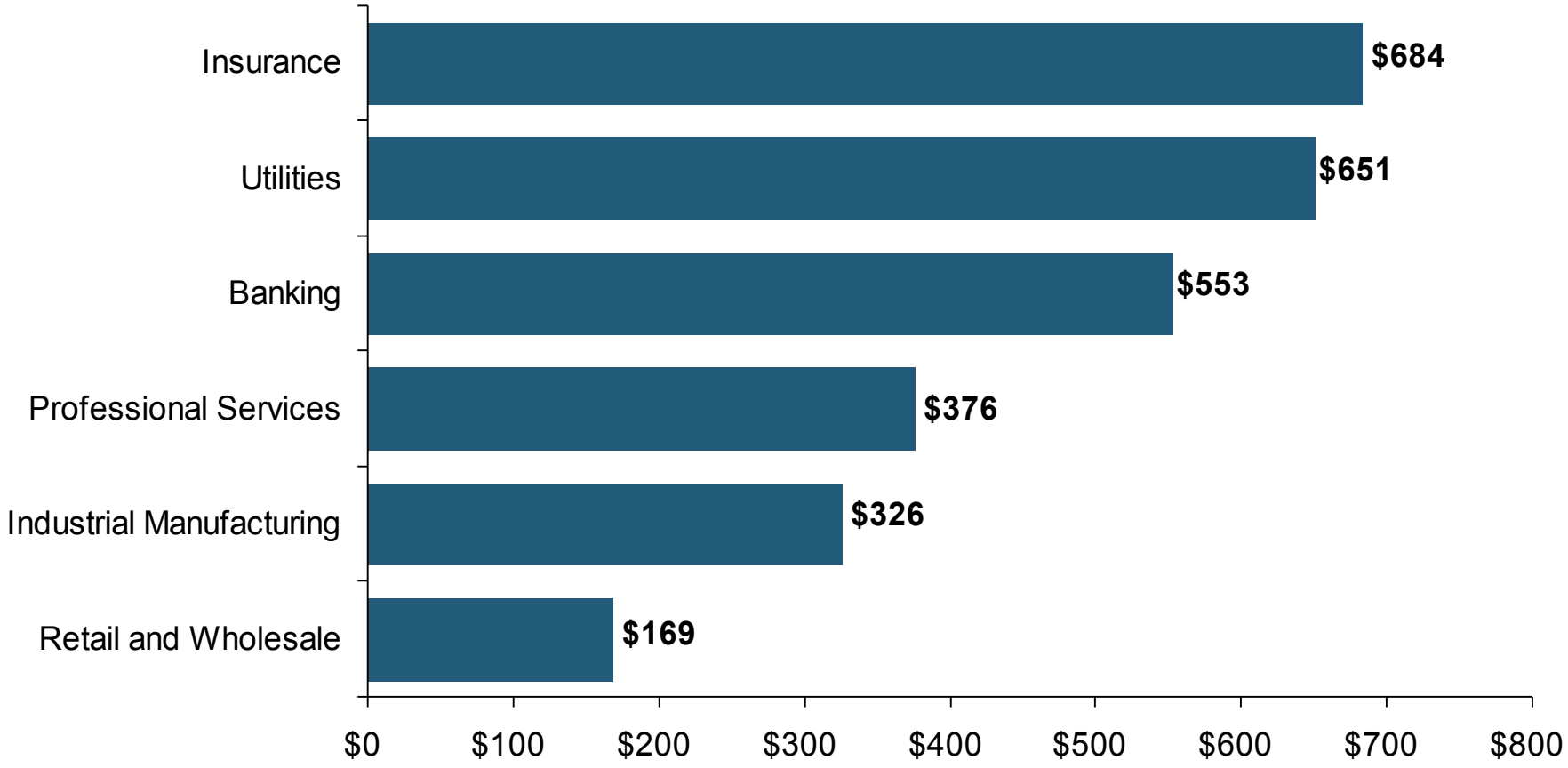
Cybersecurity Spending Is Rising Sharply, Up by About 8%+ Annually through 2016—a Projected Increase of $12.1 Billion from 2014 to 2016

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)

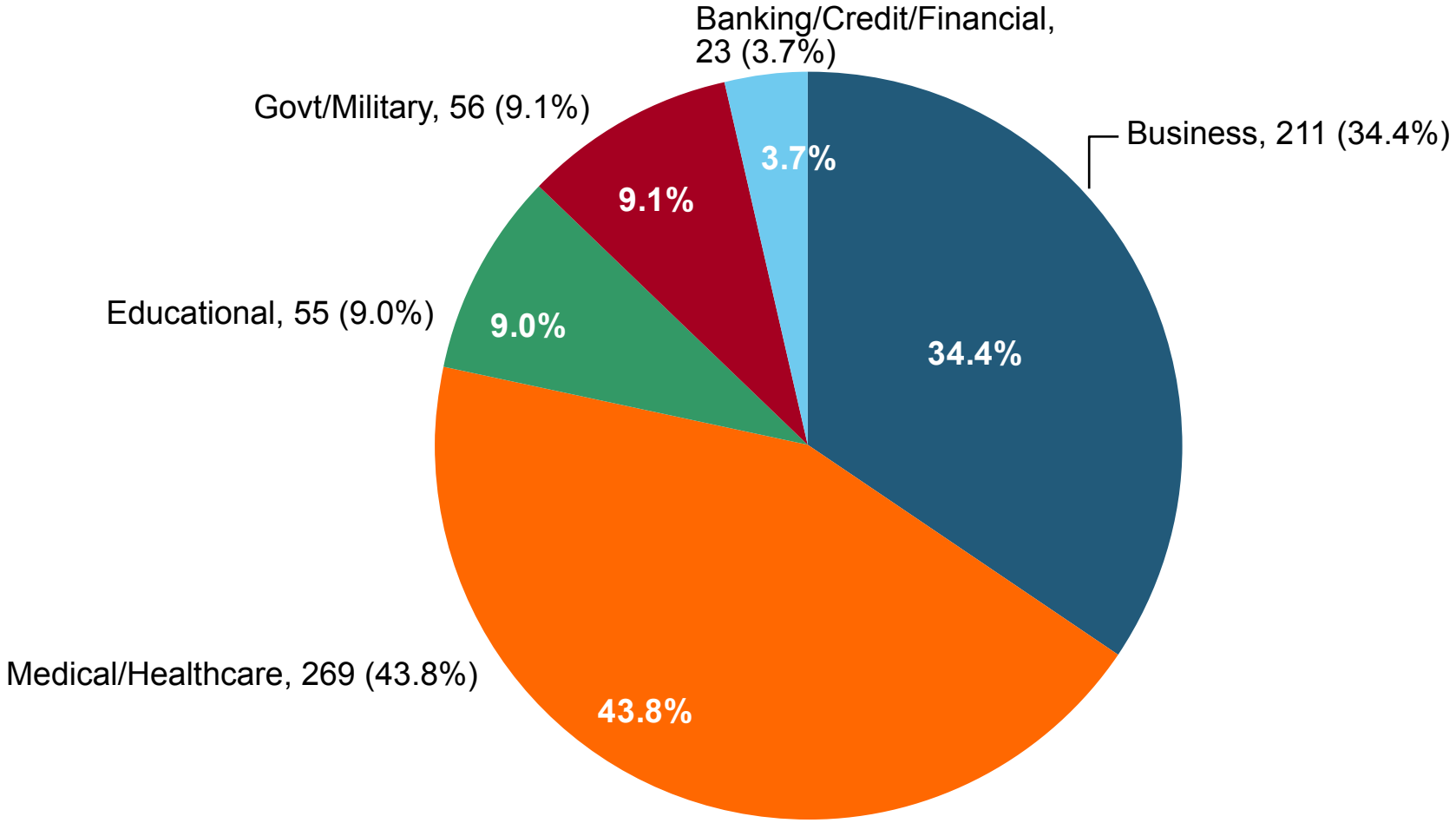


Information Security Spending by Financial Services and Critical Infrastructure Industries (e.g., Utilities) Outpaces that of Other Industries

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

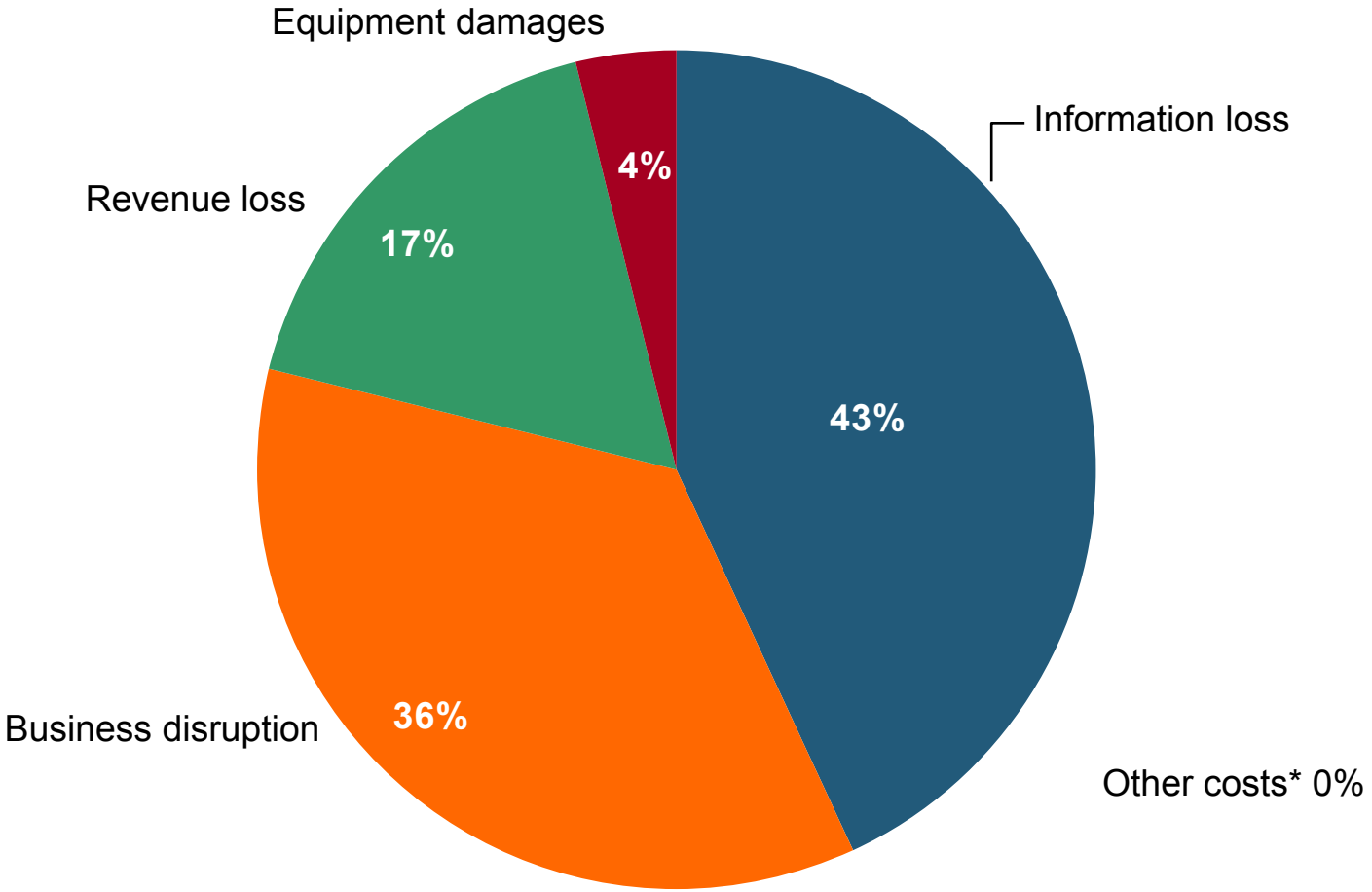
The majority of the 614 data breaches in 2013 affected business and medical/ healthcare organizations, according to the Identity Theft Resource Center.



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

External Cyber Crime Costs: Fiscal Year 2013

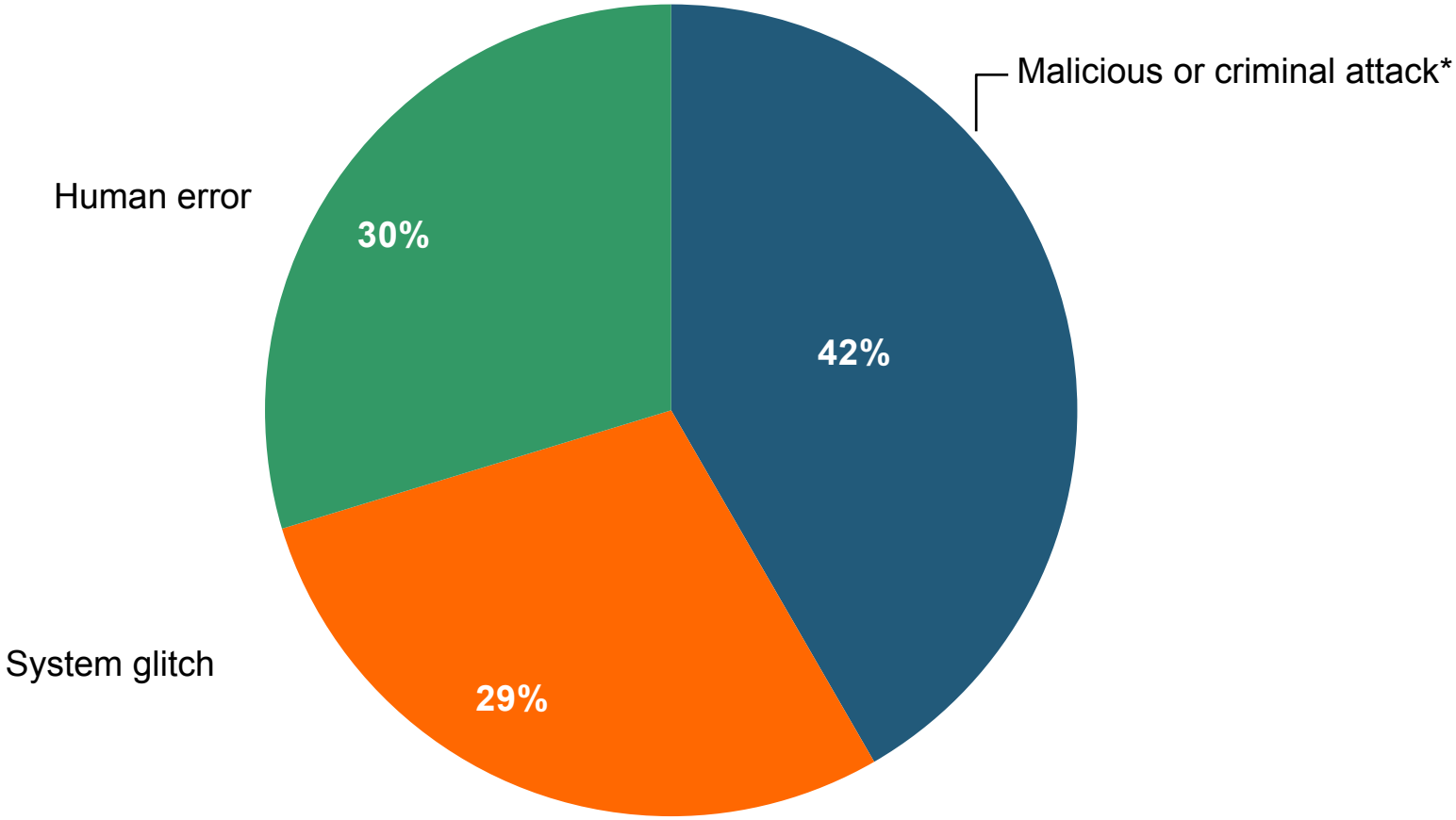
Information loss (43%) and business disruption or lost productivity (36%) account for the majority of external costs due to cyber crime.



* 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).

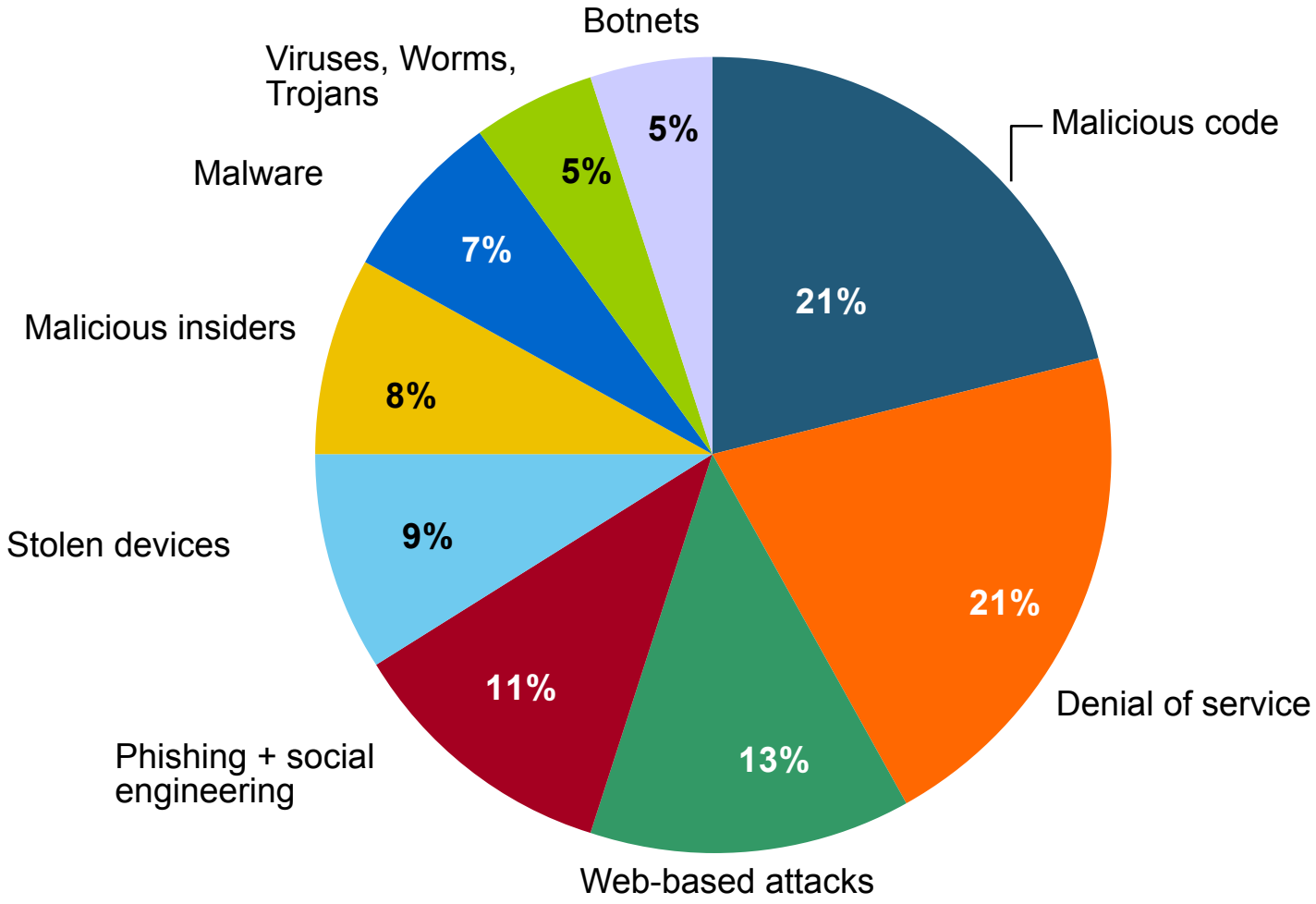


*The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

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

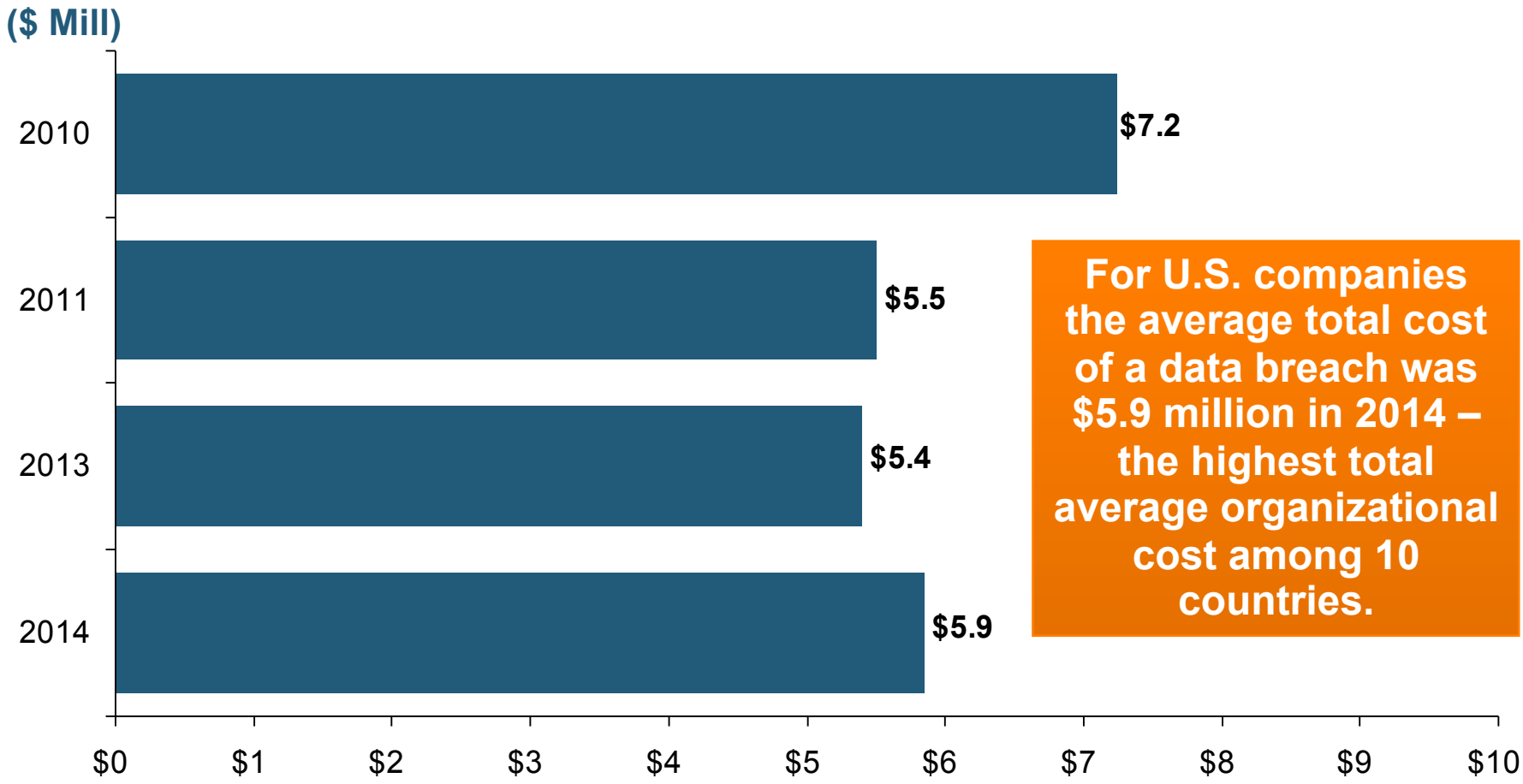
The Most Costly Cyber Crimes, Fiscal Year 2013

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)

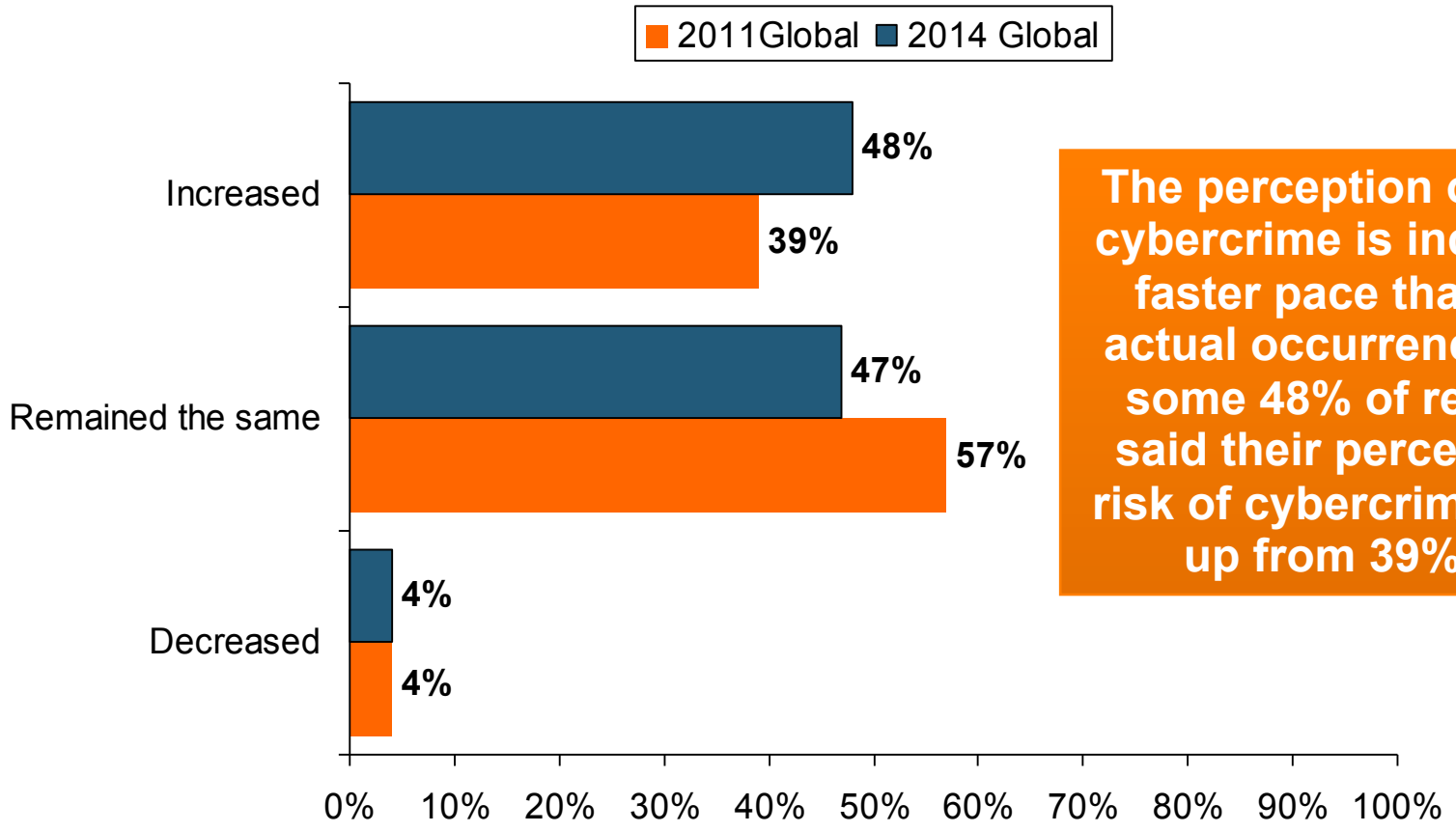


For U.S. companies the average total cost of a data breach was $5.9 million in 2014 – the highest total average organizational cost among 10 countries.

*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

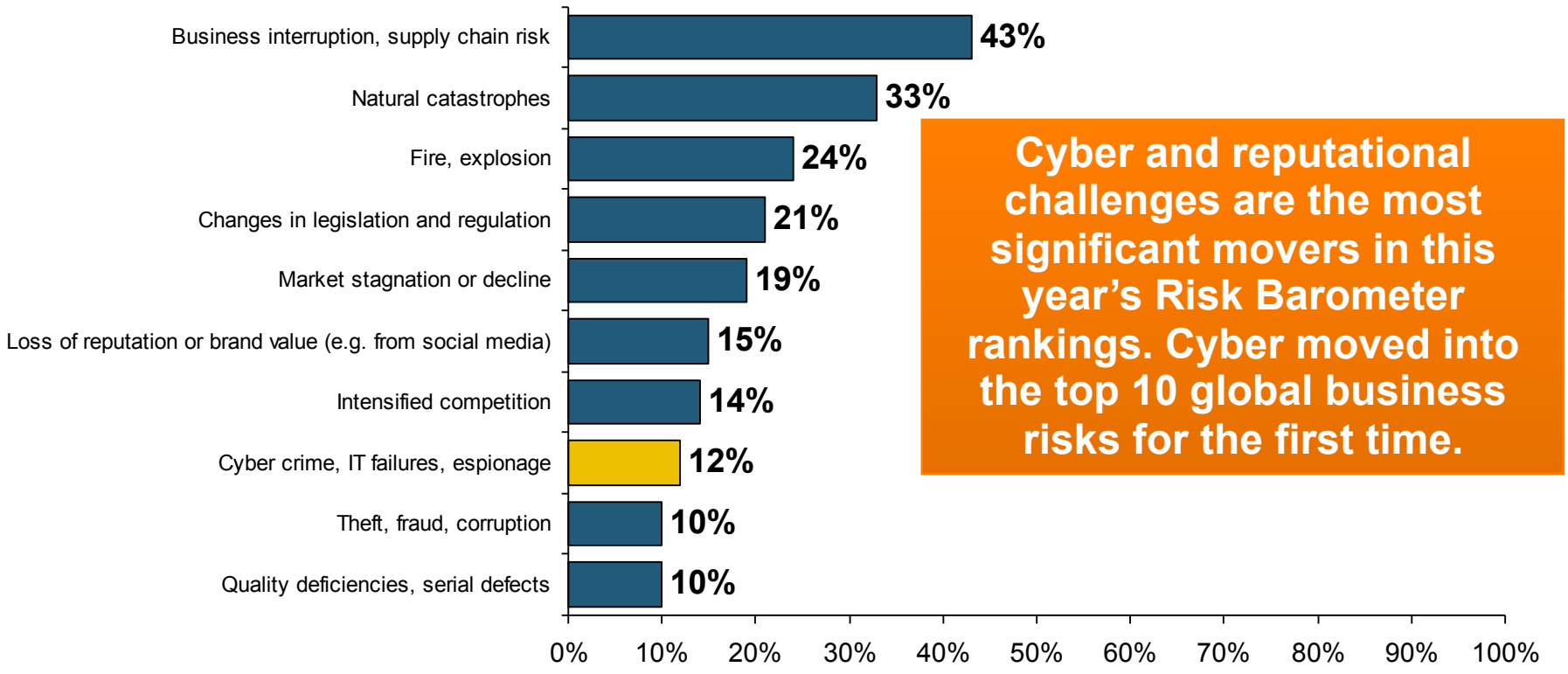
PWC Survey: Perception of the Risk of Cybercrime



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.

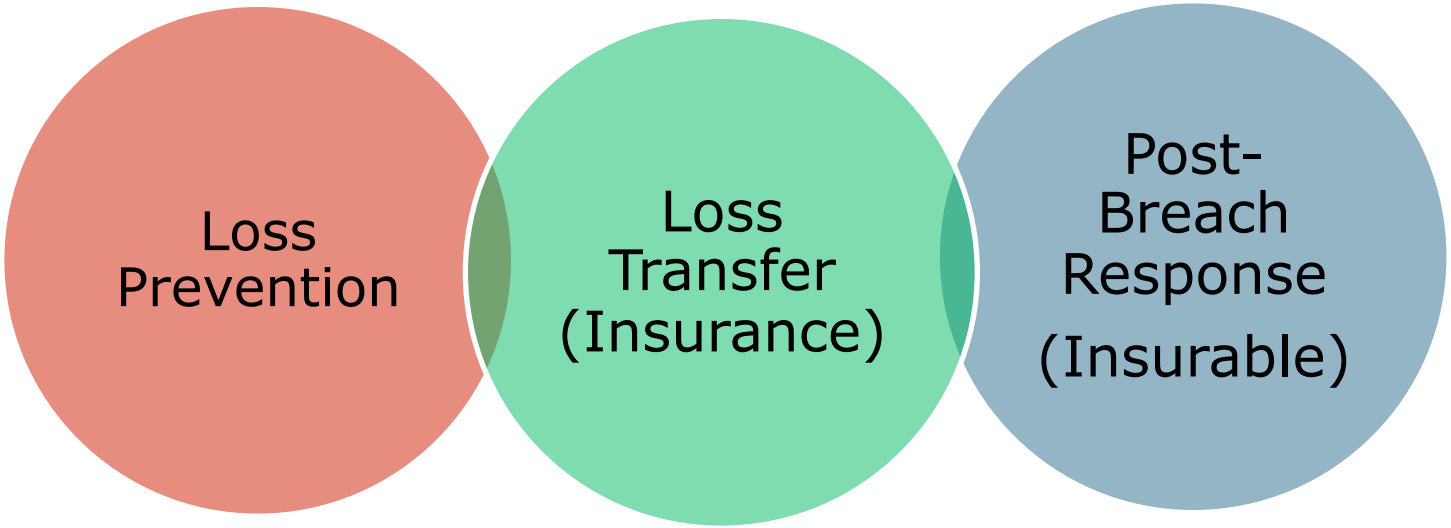
Source: Allianz Risk Barometer on Business Risks 2014

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

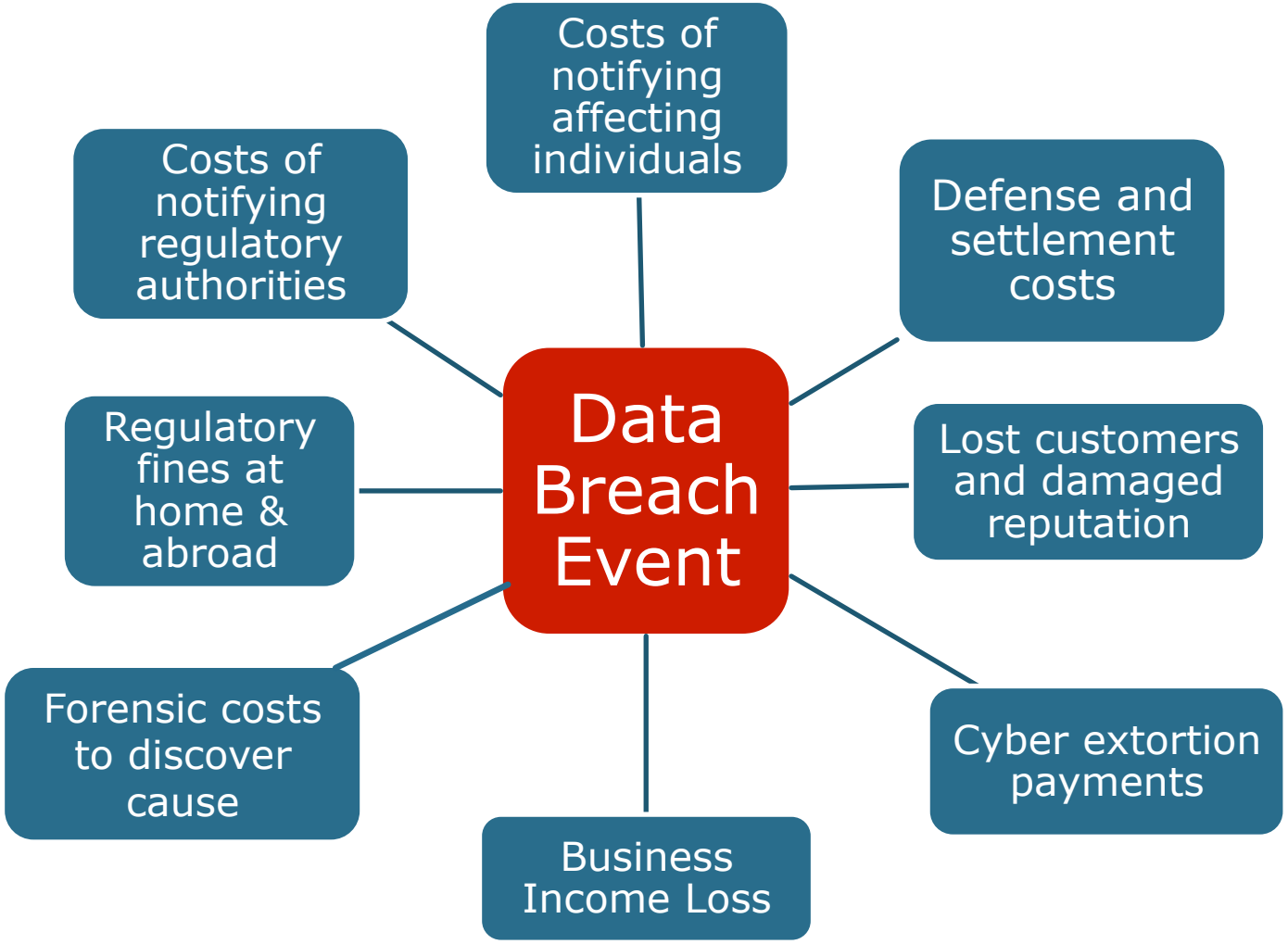
INSURANCE INFORMATION INSTITUTE

- **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)

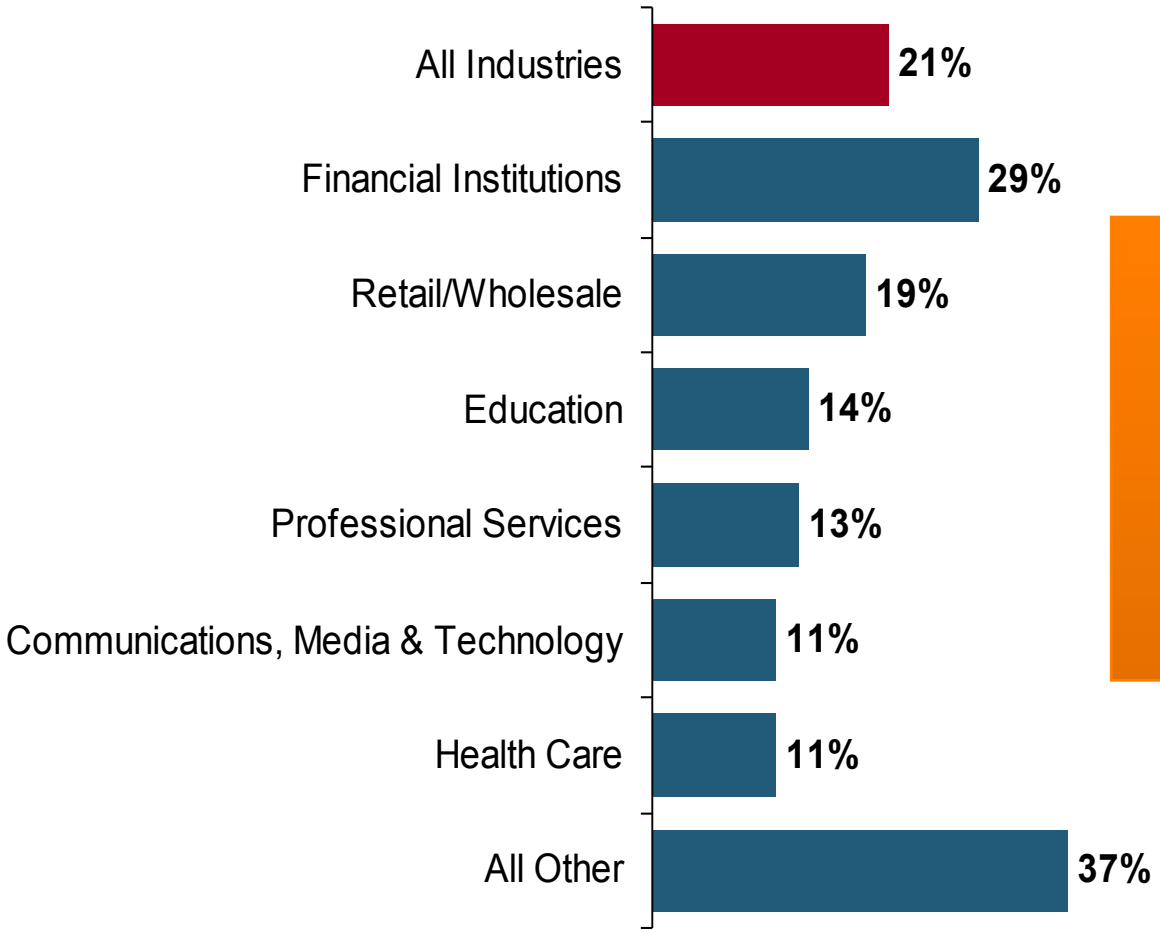
- Forensic Investigation Costs
- Notification Expenses
  - Affected individuals/businesses
  - Regulators
- Public Relations Expenses
- Legal Expenses
- Civil Fines and Penalties
- Business Income (Direct and Dependent) and Extra Expenses
- Cyber Extortion, Reward Payments

INSURANCE INFORMATION INSTITUTE

CYBER RISK INSURANCE MARKETS

Coverage Limits, Purchase Decisions & Pricing

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



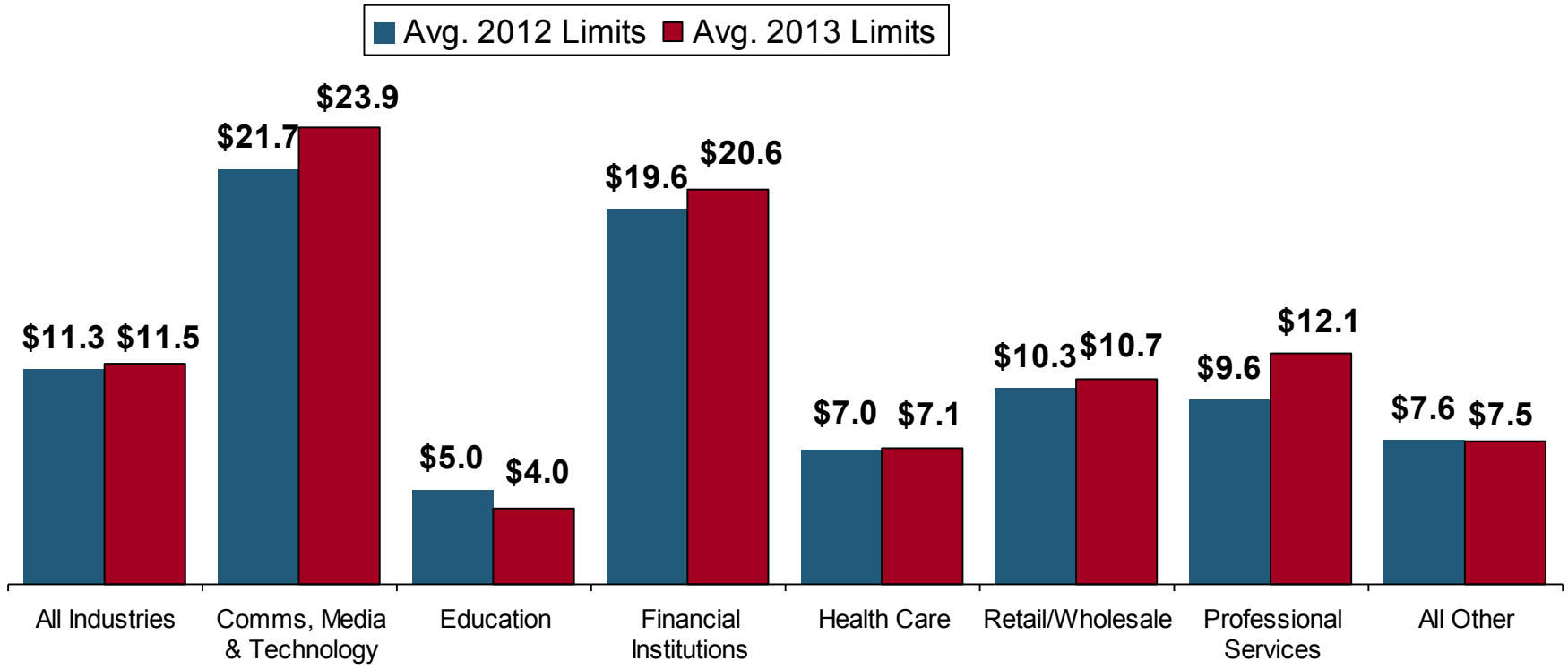
Interest in cyber insurance continues to climb. The number of companies purchasing cyber insurance increased 21 percent from 2012 to 2013.

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)

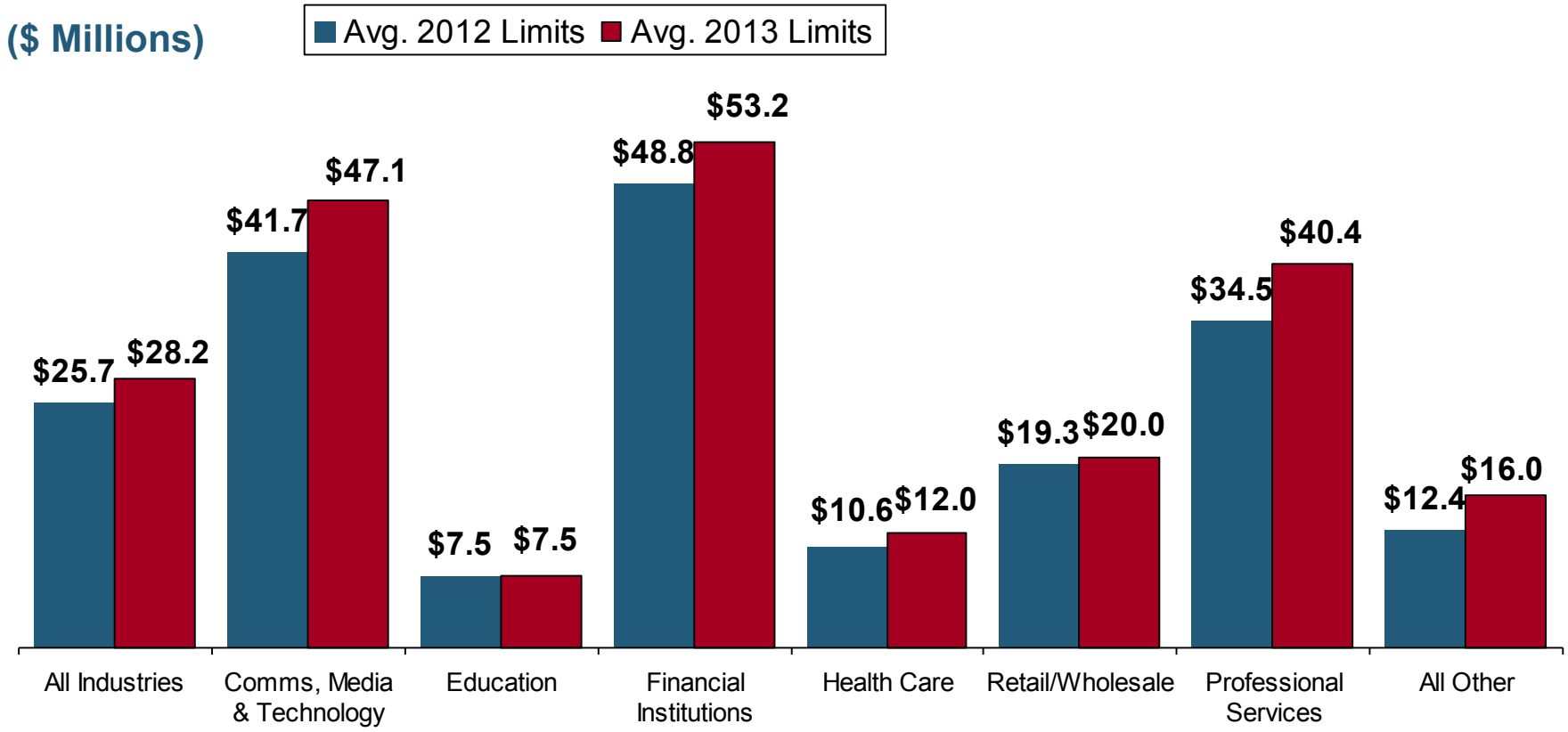


Source: *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, Marsh Risk Management Research Briefing, April 2014

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

INSURANCE INFORMATION INSTITUTE

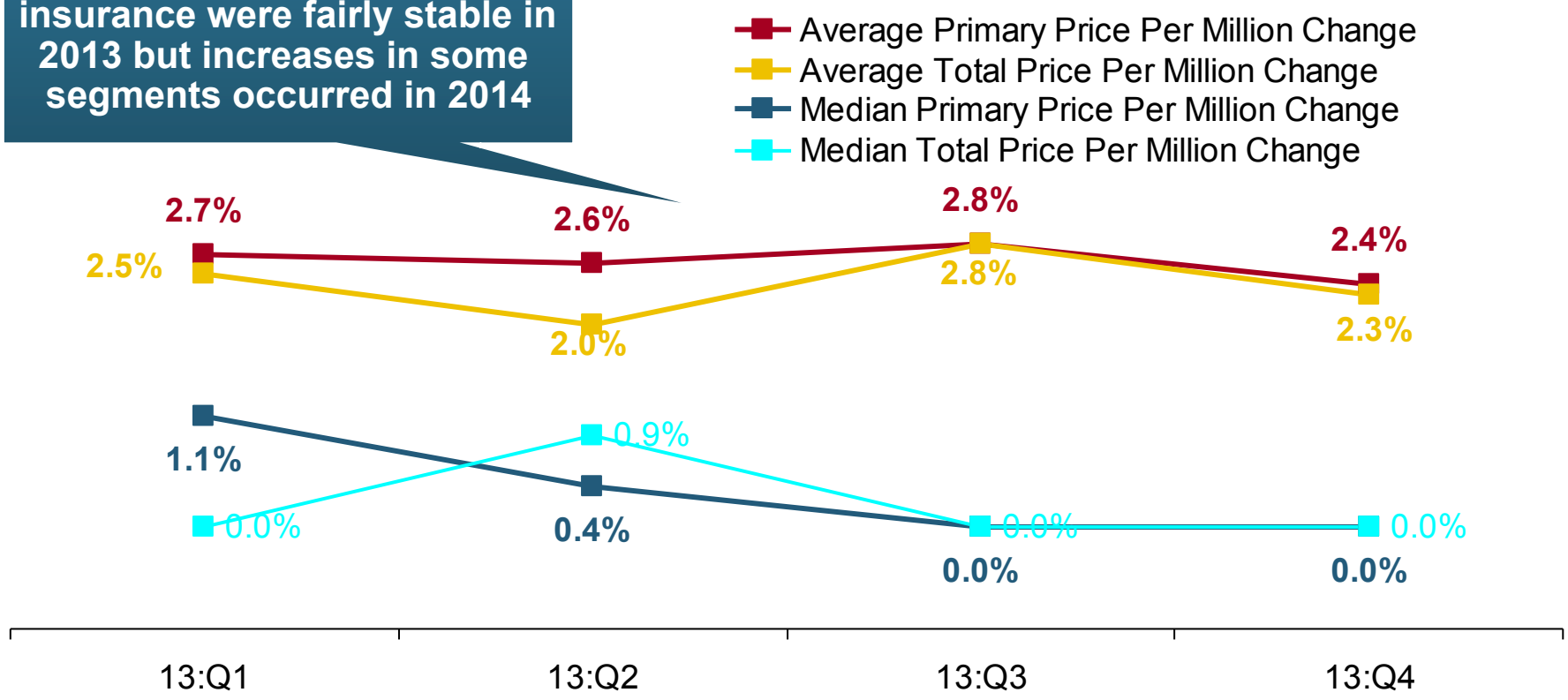
Among larger companies, average cyber insurance limits purchased increased by 10 percent to $28.2 million in 2013, from $25.7 million in 2012.



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 • Sophisticated and **well-funded**
Organized Cyber Criminals	• Traditional organized crime groups • Loosely organized **global** hacker crews
Hacktivists	• **Politically-motivated** hackers • Increasing capabilities
Insiders	• Easy access to sensitive information • 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?

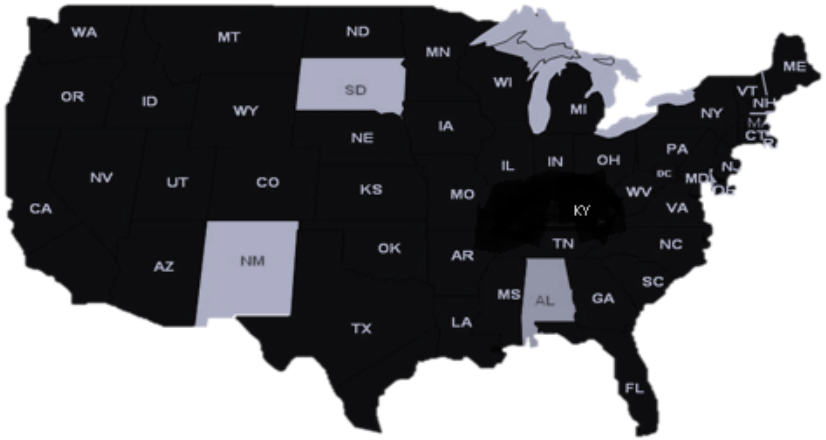
- **Malicious attack**
  - Hackers in network, Malware and viruses, Phishing scams, Physical theft of hardware and paper
  - Rogue employees
- **Employees**
  - Negligence related to use and storage of data, failure to follow or learn policies and procedures, loss of portable devices, mis-mailing of 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

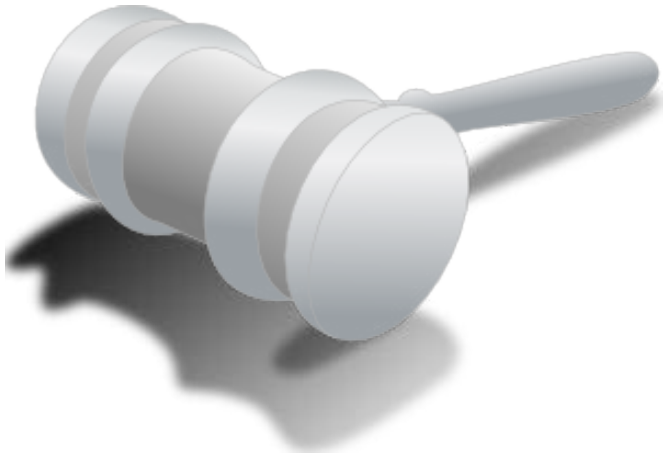
Planning and Data Management

- 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.

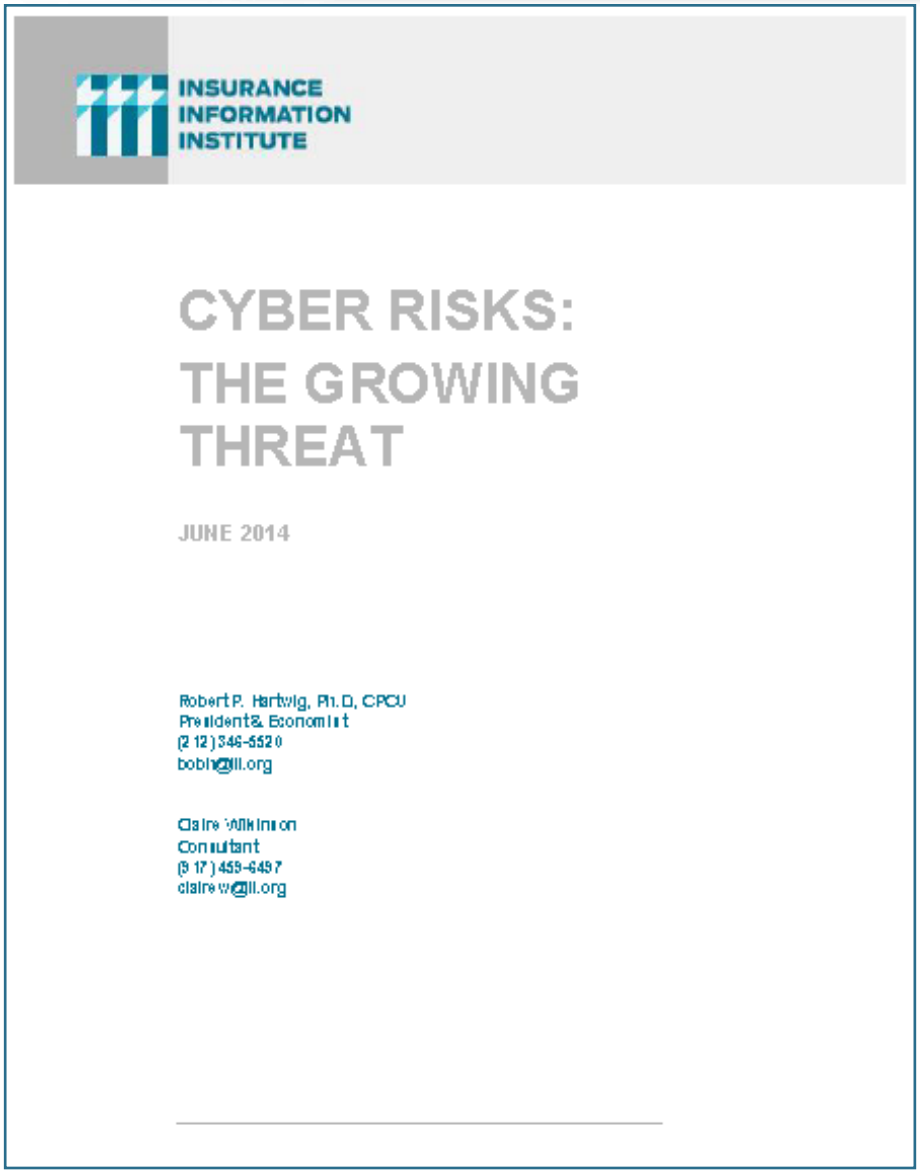
Dr. Hartwig has authored and co-authored papers that have appeared in numerous publications, including the Journal of Health Economics, the Proceedings of the Casualty Actuarial Society, the John Liner Review, Dossiers et Etudes (Geneva Association), the Journal of Workers' Compensation, the Journal 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