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.

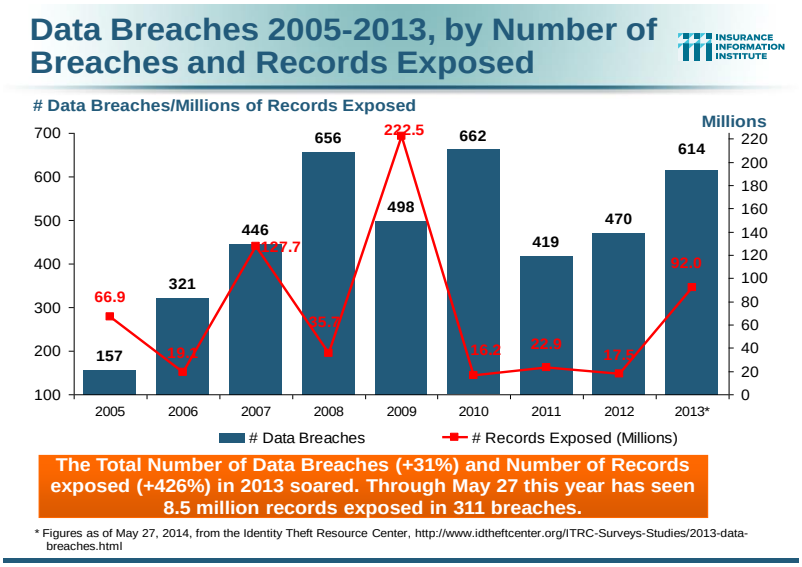
Victims of recent attacks include such well-known brands as eBay, Target, Neiman Marcus, Michaels Stores, the University of Maryland, NATO, JPMorgan Chase, Adobe, Living Social. The list goes on.

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.

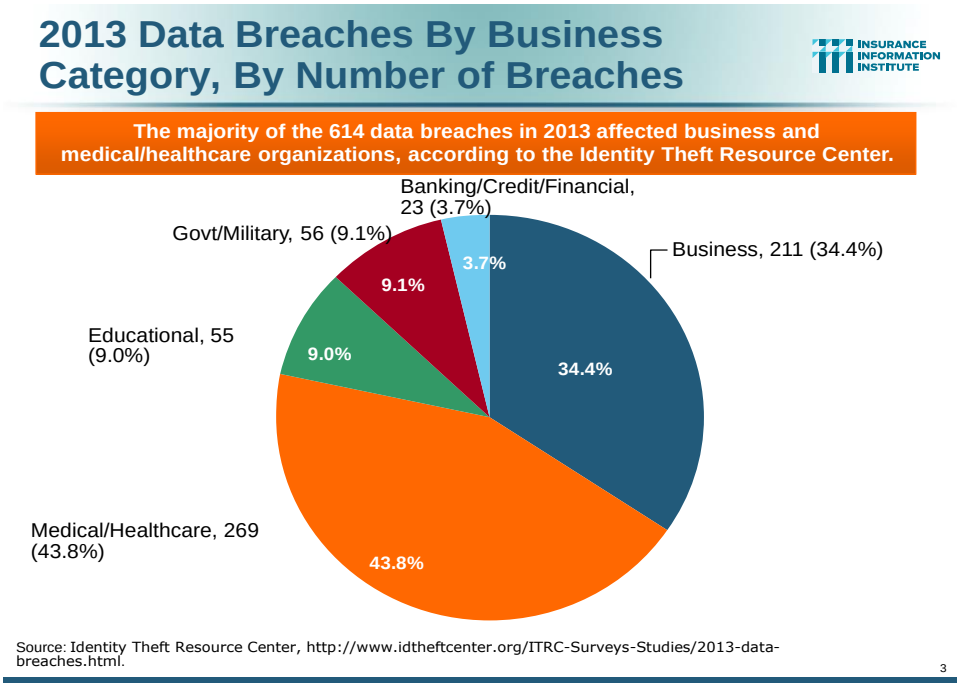
[1] Global Risks 2014, Ninth Edition, by the World Economic Forum, http://www.weforum.org/risks.
[2] Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf.

**Fig. 1**



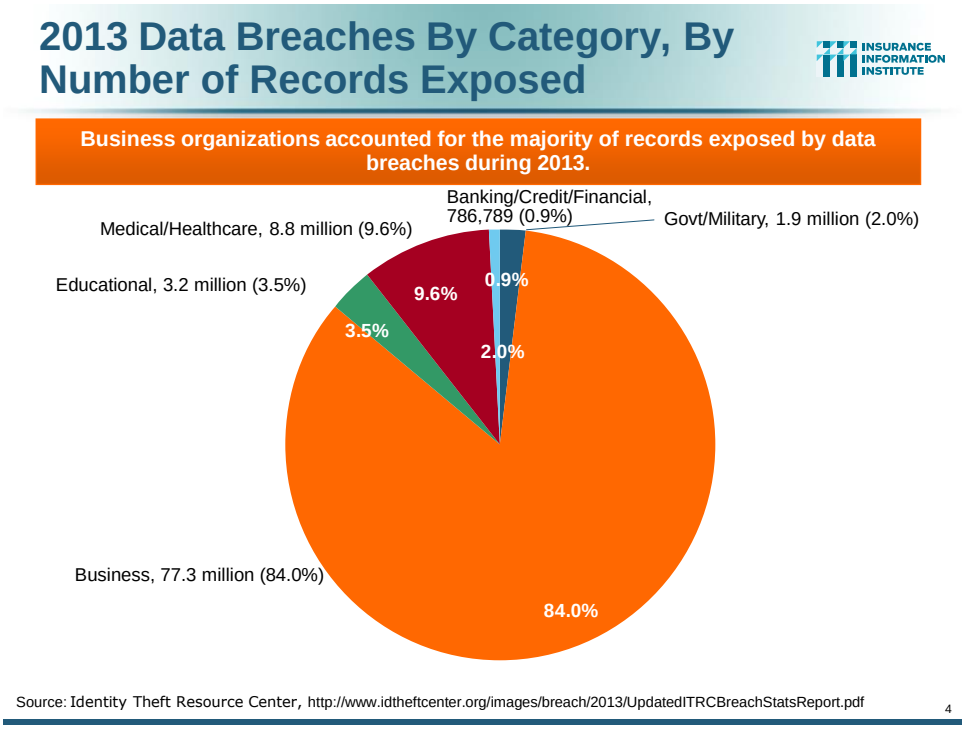

The majority of the 614 data breaches in 2013 affected business and medical/healthcare organizations, according to the Identity Theft Resource Center (Fig. 2).

**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.

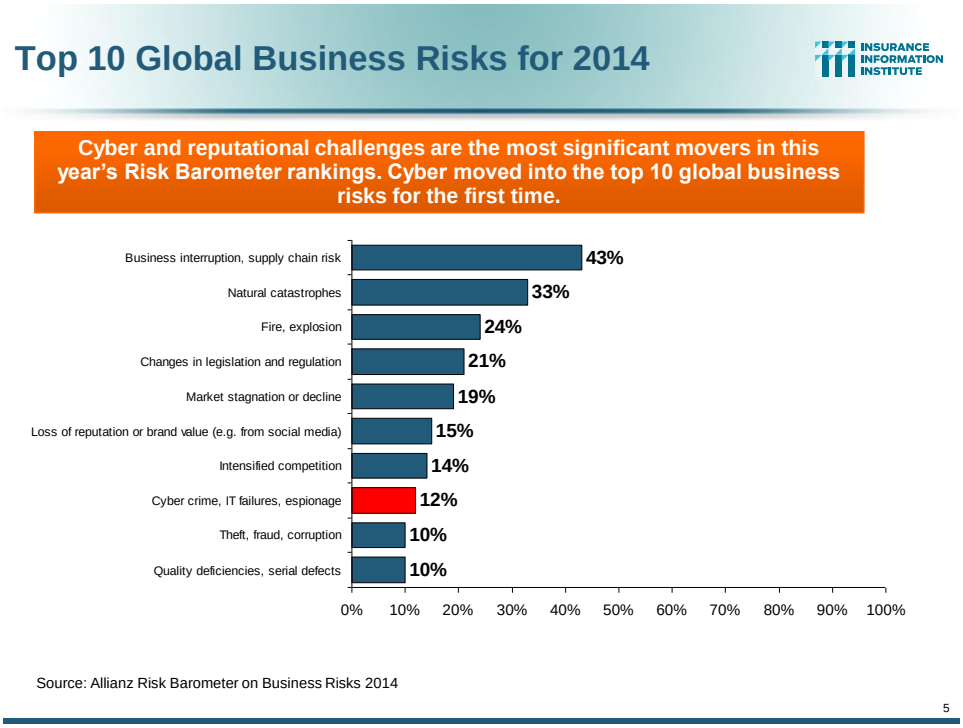
Cyber risk moved into the top 10 global business risks in 2014, according to the third annual Allianz Risk Barometer Survey, climbing up to rank 8 from 15 in last year's survey (Fig. 4).[5]

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]

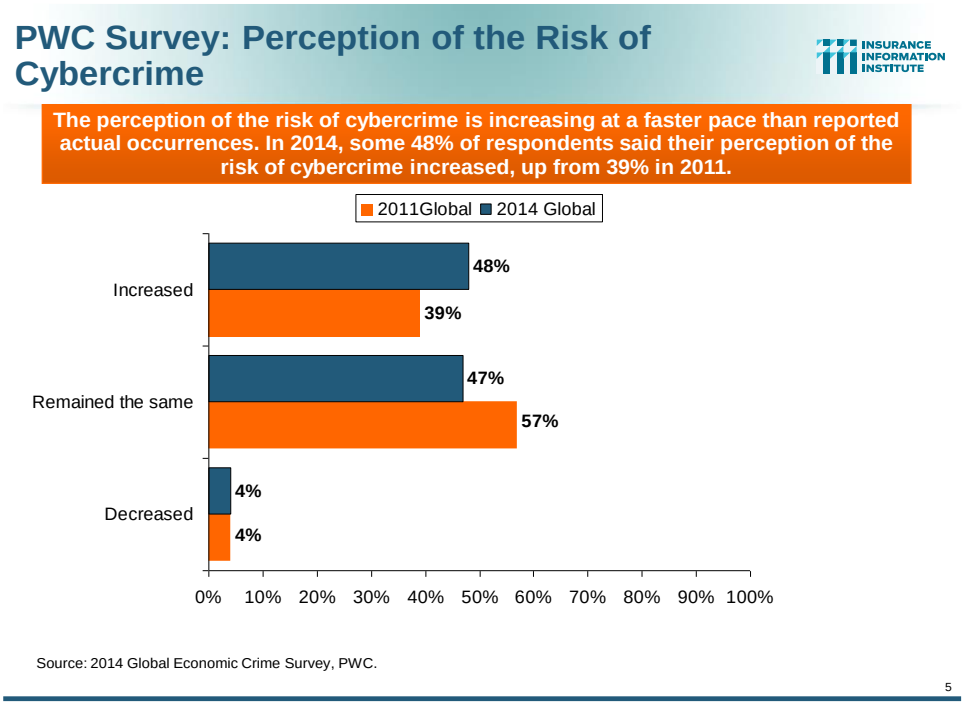
In a sign that organizations are taking this threat more seriously, the PWC survey found that the perception of the risk of cybercrime is increasing at a faster pace than that of reported actual occurrences.

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.

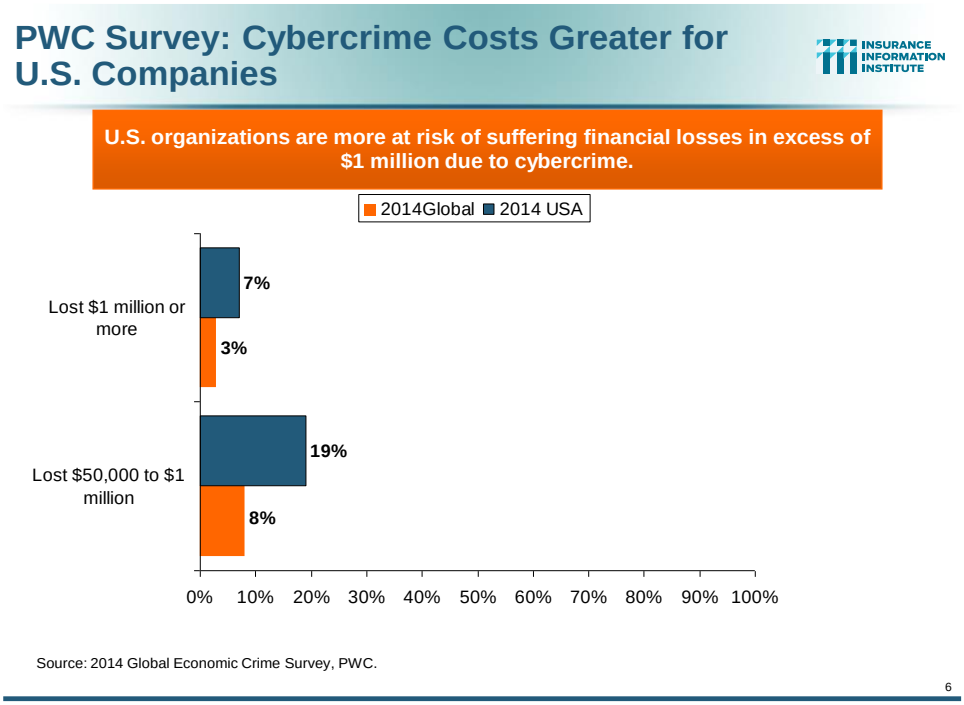
Also, some 71 percent of U.S. respondents indicated their perception of the risks of cybercrime increased over the past 24 months, rising 10 percent since 2011.

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**



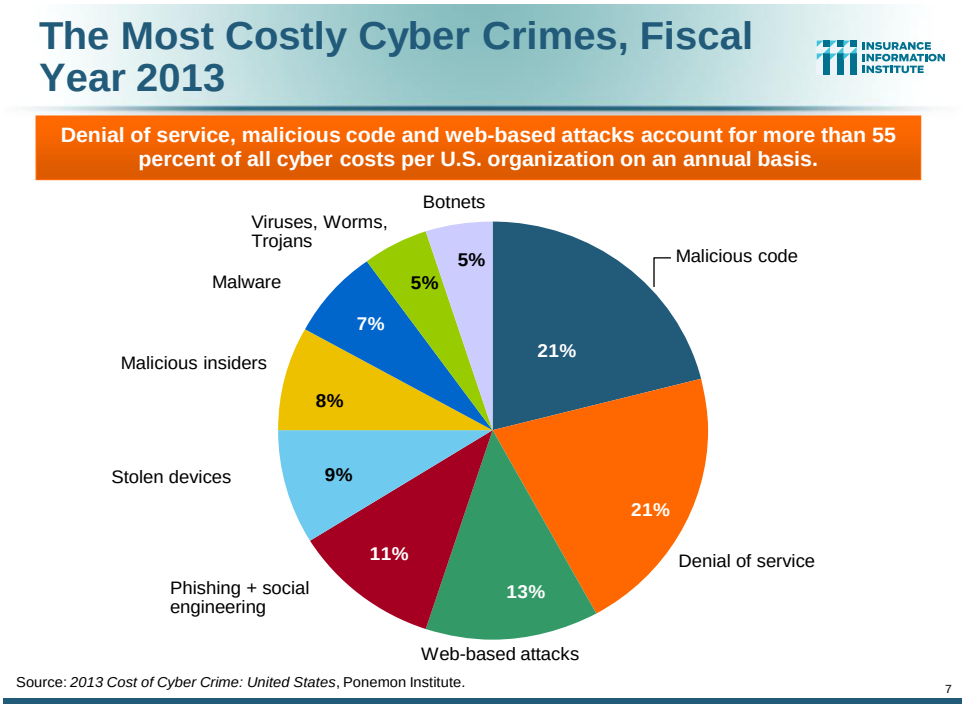

Cyber attacks continue to be very costly for organizations and those costs are rising.[7]

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).

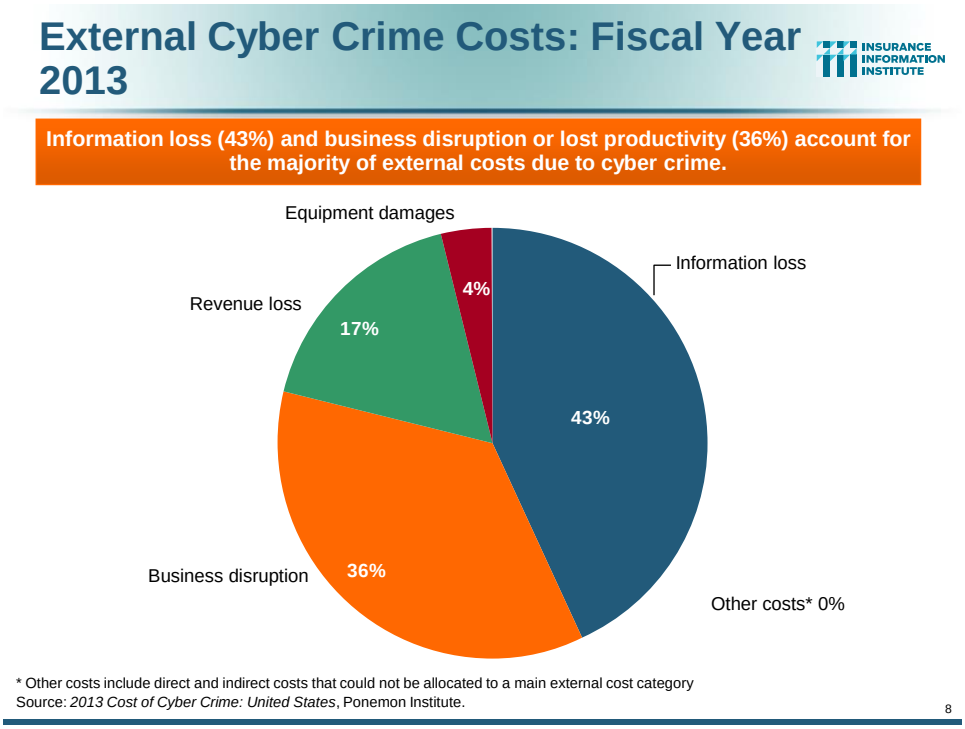
[7] *2013 Cost of Cyber Crime Study: United States*, Ponemon Institute, October 2013

**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.

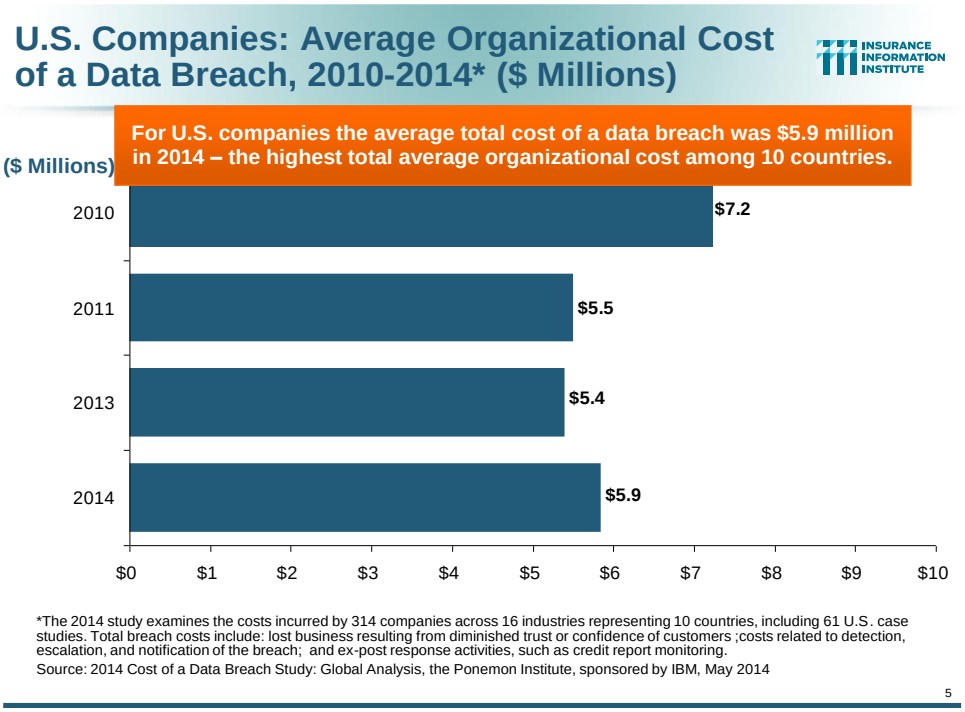
The Ponemon research does not include catastrophic or mega data breaches of more than approximately 100,000 compromised records because these are not typical of the breaches most organizations experience.

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.

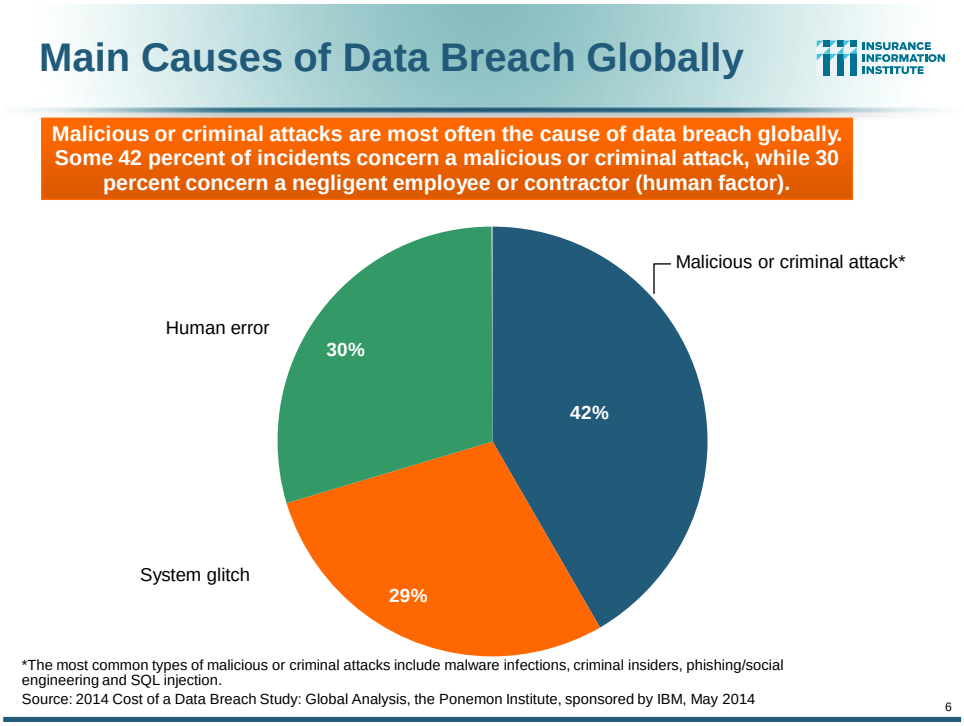
[12] *2014 Cost of a Data Breach Study: Global Analysis*, research by the Ponemon Institute, sponsored by IBM, May 2014.

**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]

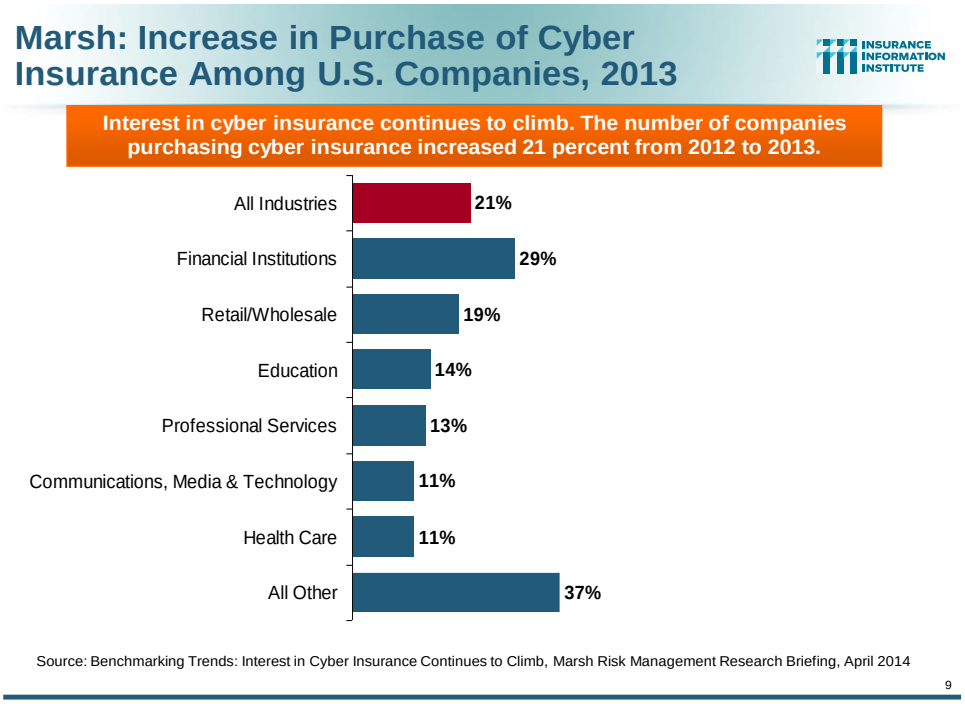
The fact that Target did have $100 million in network security insurance has been widely reported in the news.[22] As of February 1, Target said of the $61 million in expenses related to the data breach during the fourth quarter 2013, some $44 million was offset by insurance.

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.

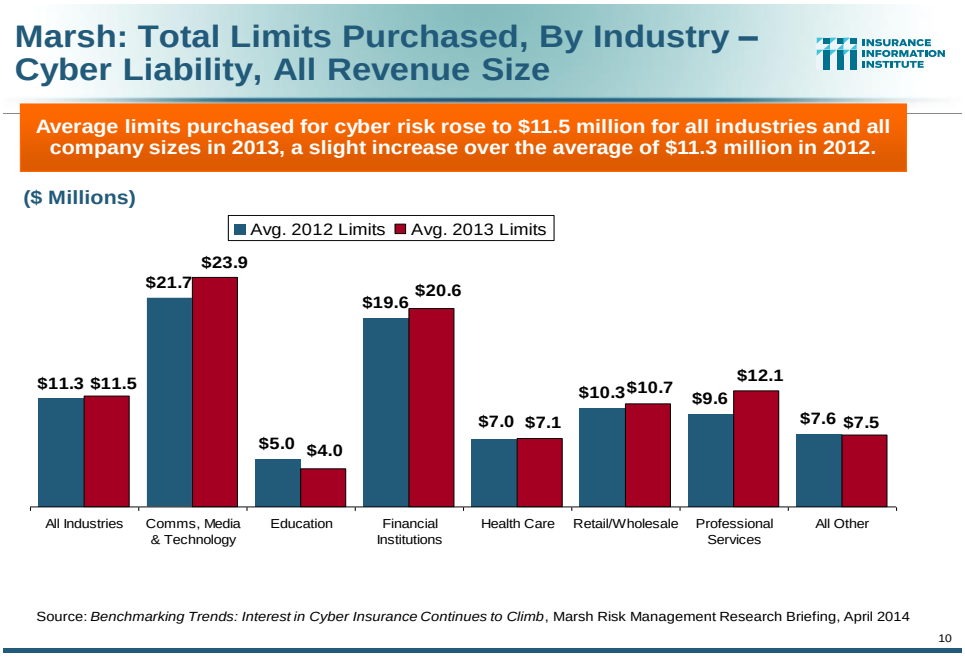
**Fig. 12**




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).

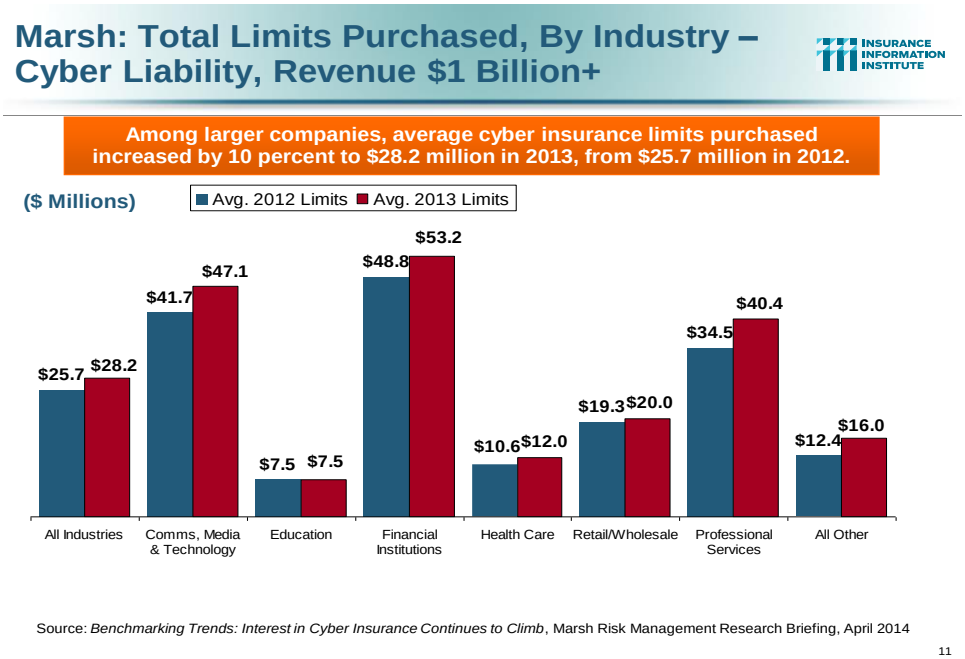
Communications, media, and technology continued to purchase the highest limits, with $23.9 million in 2013, up from $21.7 million in 2012.

**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).

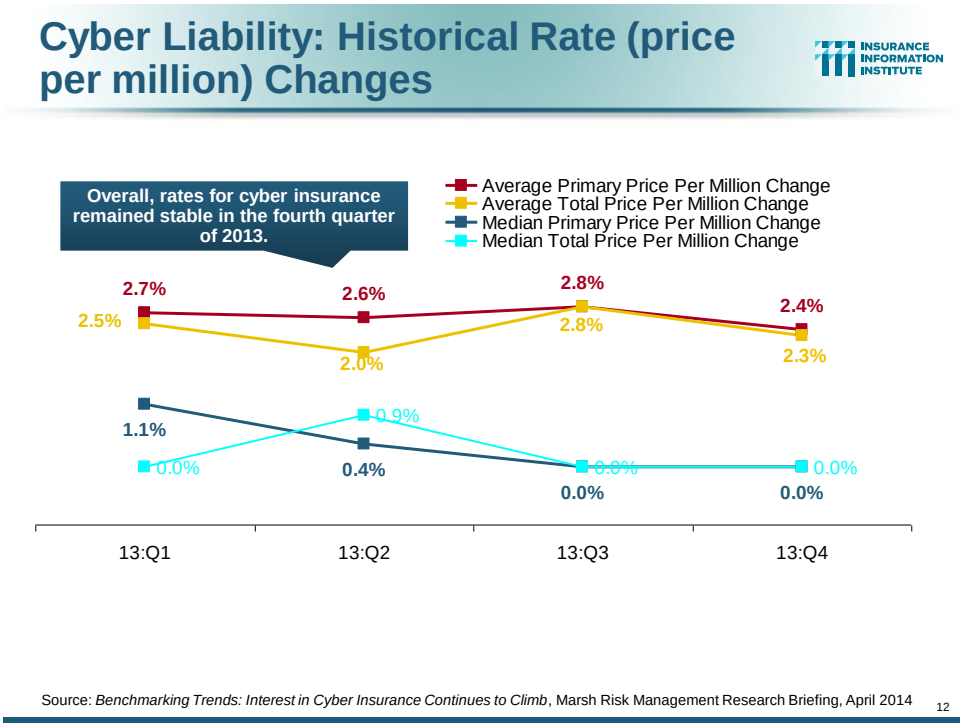
**Fig. 14**



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.