INSURANCE INFORMATION INSTITUTE

CYBER RISKS: THE GROWING THREAT

APRIL 2013

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

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

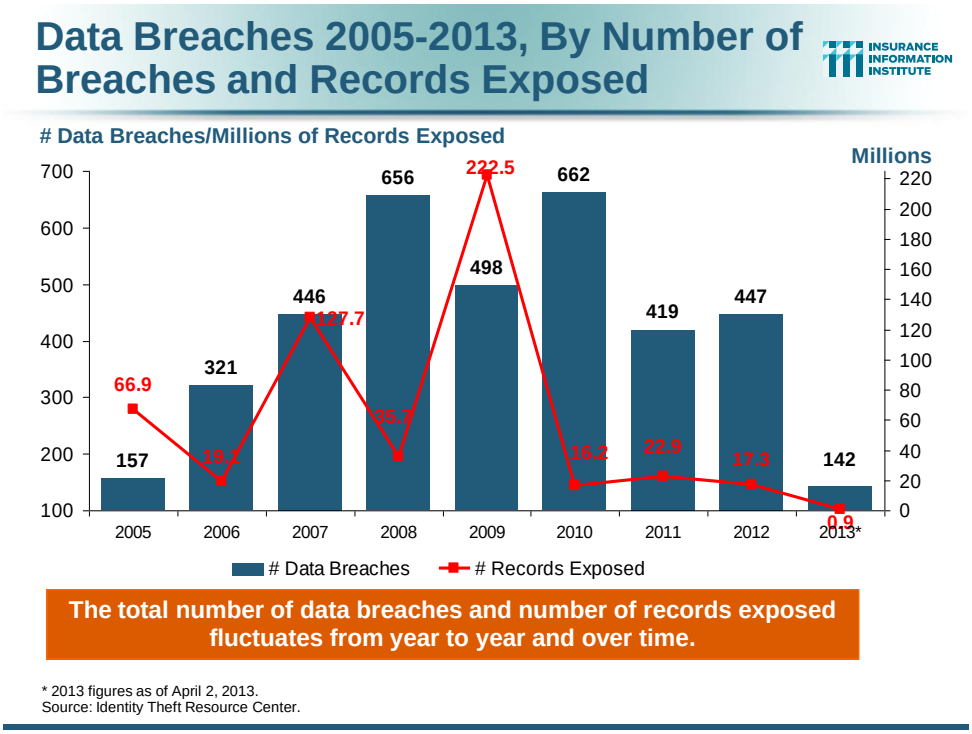
Cyber Risks: An Evolving Threat

INTRODUCTION

Businesses across major industry sectors face a growing risk from cyber attacks. Targets of recent attacks have ranged from large U.S. financial institutions, to energy facilities, to media and technology companies, as well as online social networking service providers. Media reports suggest that a number of these high profile attacks have been traced to hackers in China and Iran.

The total number of data breaches and number of records exposed fluctuates from year to year and over time (Fig. 1). Some 447 organizations across business, financial, educational, government and healthcare sectors, had publicly disclosed data breaches in 2012 as of December 26, according to the Identity Theft Resource Center.[1] This compares to 419 publicly disclosed data breaches during 2011, and 662 publicly disclosed data breaches in 2010. Through April 2, 2013, some 142 data breach events have been publicly disclosed, exposing nearly one million records.

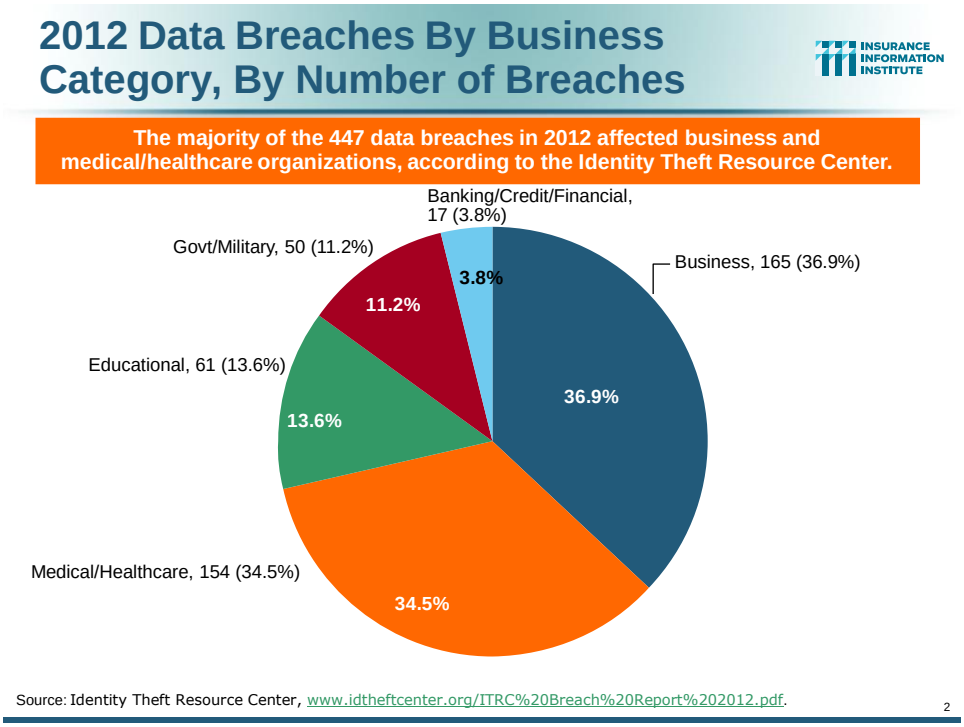
Fig. 1



[1] Identity Theft Resource Center, www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf.

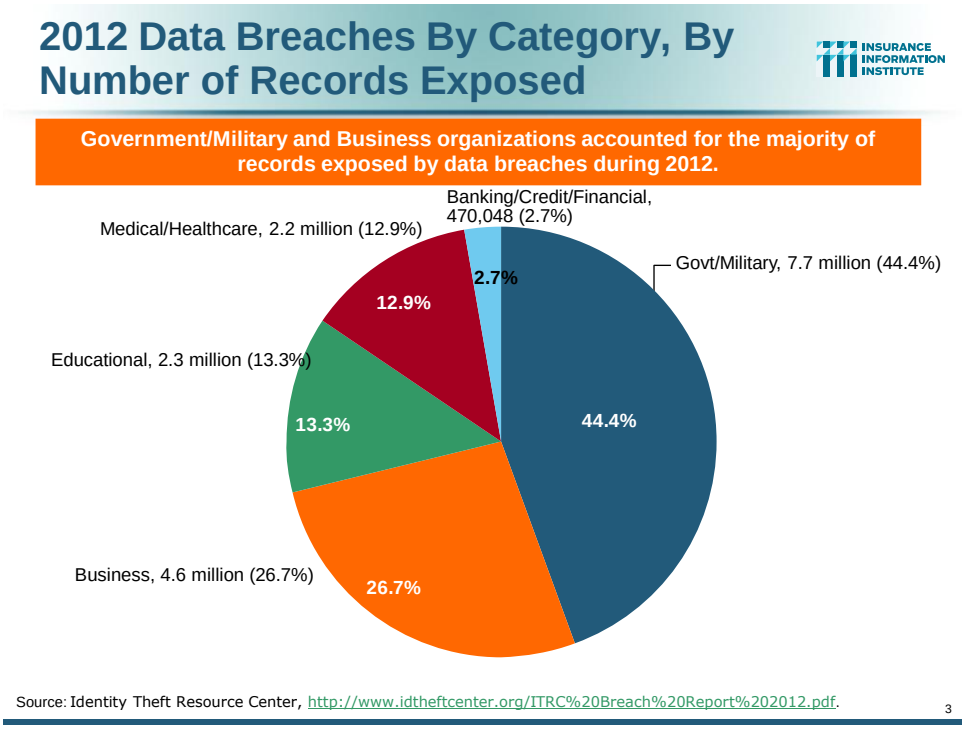
The majority of the 447 data breaches in 2012 affected business and medical/healthcare organizations, according to the Identity Theft Resource Center (Fig. 2).

Fig. 2



Government/military and business organizations accounted for the majority of records exposed by data breaches in 2012 (Fig. 3).

Fig. 3



U.S. Homeland Security Secretary Janet Napolitano recently warned that a major cyber attack is a looming threat that could have the same type of impact as superstorm Sandy, knocking out power to a large swath of the Northeast.

Napolitano said a "cyber 9/11" could happen imminently and noted that critical infrastructure—including water, electricity and gas—is very vulnerable to such a strike (see later section on cyber terrorism).[2]

In recent months high profile U.S. media outlets, including The Wall Street Journal and The New York Times, have confirmed sophisticated hacking attacks on their computer systems, reportedly traced to China.

Large U.S. banks, including Bank of America, PNC Bank, Wells Fargo, Citigroup, HSBC and SunTrust, have also been targeted by a rising number of so-called distributed denial of service (DDOS) attacks that have disrupted their websites. Reports attribute these attacks to Iranian government hackers.

[2] *Napolitano warns of risk of major cyber attack*, Newsday, January 24, 2013.

Meanwhile, the online social networking service Twitter announced in early February 2013 that it had been breached in a sophisticated attack that left data for 250,000 Twitter users vulnerable. According to reports, this attack has been traced to hackers in China.

A hacker group known as Anonymous has also drawn the attention of the FBI and other federal investigators after much-hyped cyber threats, announced in video messages on YouTube or via Twitter, some of which have crashed the websites of governments and financial institutions.

Amid this evolving risk landscape, 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.

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 an 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. The move comes in response to rising complaints about theft of military and corporate secrets.[4]

On February 12, 2013, President Obama issued a cybersecurity executive order that promotes increased information sharing about cyber threats between government and private companies that oversee critical infrastructure systems such as electrical grids. The executive order also calls for the National Institute of Standards (NIST) to develop a new cybersecurity framework to reduce cyber risks to critical infrastructure.

Meanwhile, a number of federal legislative/regulatory proposals on cybersecurity are under consideration by Congress. At the state level, some 46 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**.

[3] www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[4] *U.S. Ups Ante for Spying on Firms*, The Wall Street Journal, February 21, 2013.

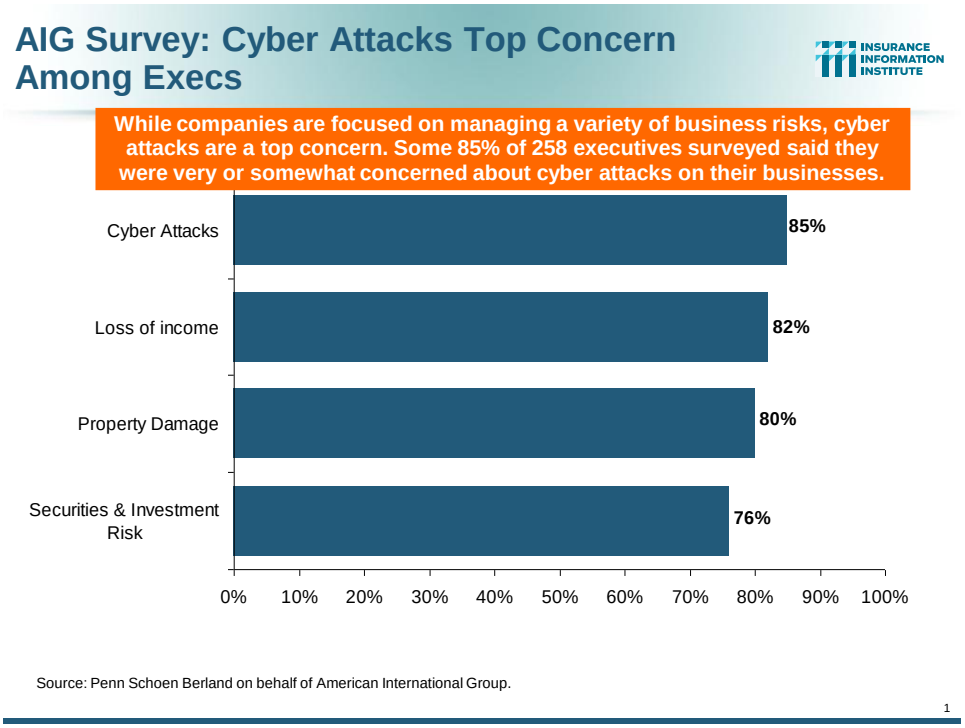
CYBER SECURITY

Cyber security and losses from cyber crimes are a growing concern among businesses today.

While companies are focused on managing a variety of business risks, their top concern appears to be cyber attacks, according to a recent survey conducted by Penn Schoen Berland on behalf of American International Group (AIG).[5]

Some 85 percent of the 258 executives surveyed said they were very or somewhat concerned about cyber attacks on their businesses. That compares with 82 percent of executives concerned about loss of income, 80 percent concerned with property damage and 76 percent with securities and investment risk (Fig. 4).

Fig. 4



AIG also reported that more than 69 percent of the executives believe that the reputational risk from a cyber attack is far greater to a company than the financial risk, while 75 percent of corporate leaders say legal compliance issues are causing their companies to think more about cyber risks.

[5] www.aig.com/press-releases_3171_438003.html.

An earlier study by Symantec also found cyber attacks to be a top concern of businesses—more so than natural disasters or terrorism.

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

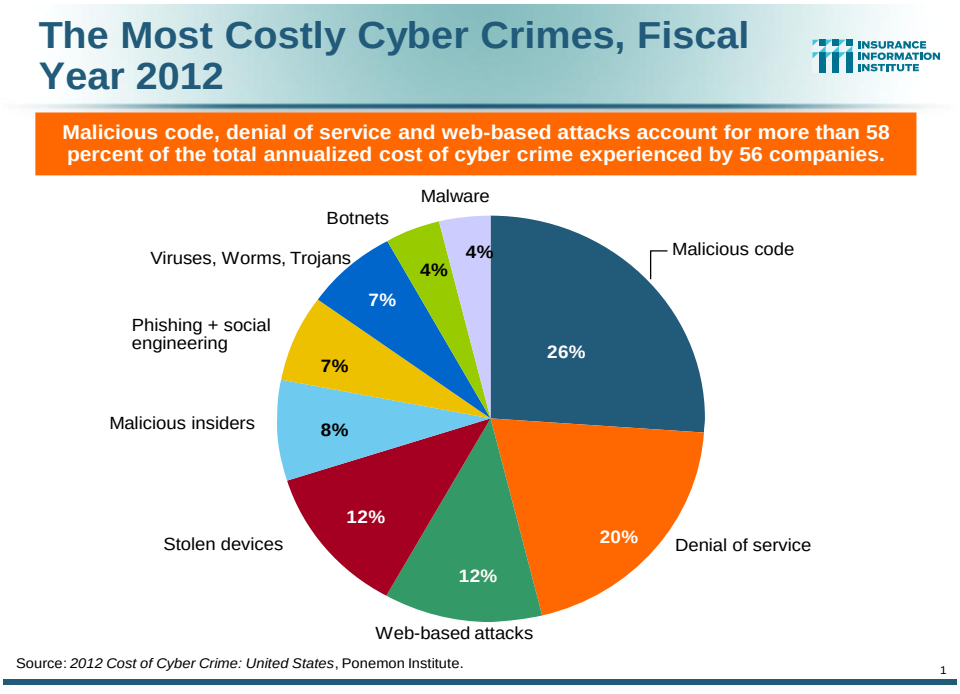
An October 2012 report by the Ponemon Institute found that not only have cyber attacks become common occurrences, but they continue to be very costly for organizations.[6]

The companies participating in the Ponemon study experienced 102 successful attacks per week (compared to 72 successful attacks per week the prior year) – or 1.8 successful attacks per organization. This represents a 42 percent increase on the previous year's successful attack experience.

The costs of cyber crime are also rising. The Ponemon study found that the average annualized cost for 56 benchmarked organizations is $8.9 million per year, an increase of 6 percent from $8.4 million the previous year, with a range from $1.4 million to $46 million each year per company.

The most costly cyber crimes are those caused by malicious code, denial of service, and web-based attacks, Ponemon said (Fig. 5).

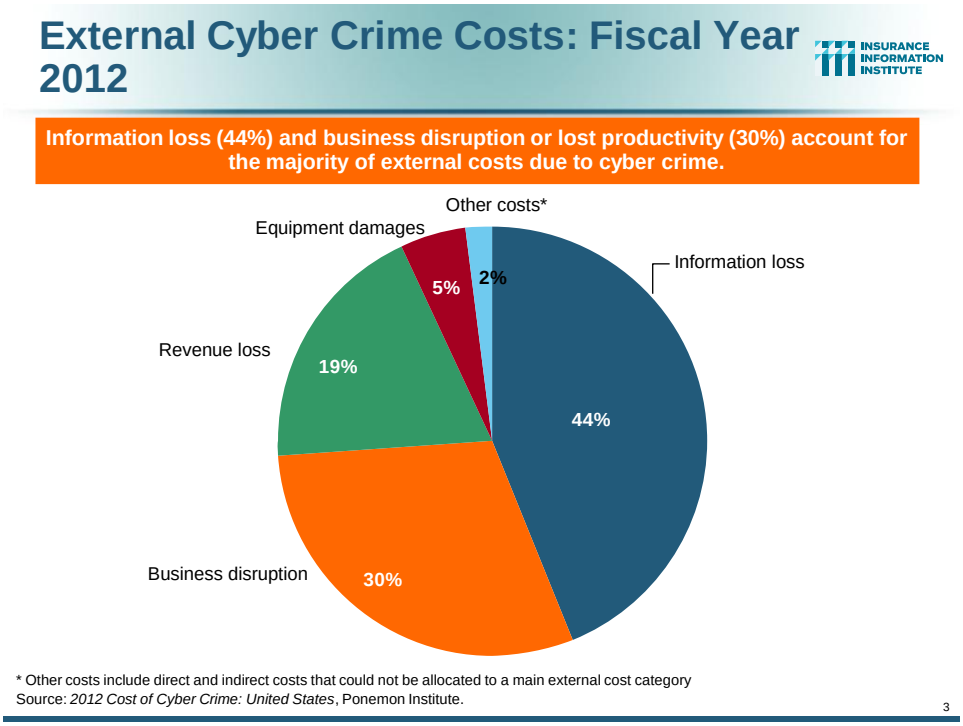
Fig. 5



[6] *2012 Cost of Cyber Crime Study: United States*, Ponemon Institute, October 2012

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. 6). On an annualized basis, information theft accounts for 44 percent of total external costs (up 4 percent from 2011). Costs associated with disruption to business or lost productivity account for 30 percent of external costs (up 1 percent from 2011). 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. 6



Cyber attacks can also become costly if not resolved quickly. According to the study results, the average time to resolve a cyber attack was 24 days, with an average cost to participating companies of $591,780 during this 24-day period. This represents a 42 percent increase from the prior year's estimated average cost of $415,748 based on an 18-day resolution period. Results show that malicious insider attacks can take more than 50 days on average to contain.

Investigating cyber attacks is also becoming a business for law firms—and not only because of the increasing number of attacks and more stringent disclosure requirements from the Securities and Exchange Commission. Law firms are touting

that hiring them provides attorney-client privilege that would not exist if the firm suffering the breach went straight to an investigative firm.[7]

THE CYBER TERRORISM THREAT

The threat both to national security and the economy posed by cyber terrorism is a growing concern for governments and businesses around the world, with critical infrastructure, such as nuclear power plants, transportation, and utilities at risk.

U.S. Homeland Security Secretary Janet Napolitano recently warned that a major cyber attack is a looming threat that could have the same type of impact as superstorm Sandy, knocking out power to a large swath of the Northeast.

Napolitano said a "cyber 9/11" could happen imminently and noted that critical infrastructure—including water, electricity and gas—is very vulnerable to such a strike.[8]

Earlier, in an October 2012 speech U.S. Defense Secretary Leon Panetta warned that the United States was facing a possible "cyber Pearl Harbor" scenario, and increasingly vulnerable to foreign cyber attacks on its critical infrastructure networks.

Such attacks are targeting the computer control systems that operate chemical, electricity and water plants and transportation networks, Panetta said:

> "An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals.
>
> They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country."

Panetta's speech came in the wake of a cyber attack in August 2012 on state oil company Saudi Aramco, which infected and rendered useless more than 30,000 computers.

The Department of Homeland Security received reports of some 198 attacks on critical infrastructure systems in the U.S. in 2012, a 52 percent increase on 2011.[9]

In 2011, a report from the Pentagon concluded that computer sabotage coming from another country can constitute an act of war.[10] It noted that the Laws of

[7] *Law Firms Tout Cybersecurity Cred,* The Wall Street Journal, April 1, 2013.
[8] *Napolitano warns of risk of major cyber attack,* Newsday, January 24, 2013.
[9] *As Hacking Against U.S. Rises, Experts Try to Pin Down Motive*, The New York Times, March 3, 2013.
[10] *Cyber Combat: Act of War,* by Siobhan Gorman and Julian E. Barnes, the Wall Street Journal, May 30, 2011.

Armed Conflict—which 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.[11]

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 about 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.

DATA BREACHES: RISING COSTS AND LIABILITY EXPOSURE

Businesses that store confidential customer and client information online are exposed to increasing liabilities and costs as a result of data breaches.

Some 447 organizations across business, financial, educational, government and healthcare sectors, had publicly disclosed data breaches in 2012 as of December 26, according to the Identity Theft Resource Center.[12] This compares to 419 publicly disclosed data breaches during 2011, and 662 publicly disclosed data breaches in 2010. Some 142 data breach events were publicly disclosed through April 2, 2013.

Recent high profile data breach incidents include a massive data breach at online business networking site LinkedIn in June 2012 that compromised some 6.5 million user passwords.

And another massive data breach at credit card processor Global Payments in March 2012 exposed some 1.5 million consumer payment card numbers (Fig. 7).

[11] Tenable Network Security survey, February 2013.
[12] Identity Theft Resource Center, www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf.

Fig. 7

High Profile Data Breaches, 2012-2013

Date	Company	Description of Breach
Mar 2013*	South Korean banks, media cos	Cyber attack causes computers to crash at South Korean banks and media companies, paralyzing bank machines across the country. No immediate reports of records compromised.
July 2012	Yahoo	Security breach at Yahoo in which some 450,000 passwords lifted and posted to the Internet.
July 2012	eHarmony	Online dating site eHarmony confirms security breach in which some 1.5 million user names and passwords compromised.
July 2012	LinkedIn	Social networking site LinkedIn reportedly targeted in hacker attack that saw 6.5 million hacked passwords posted to the Internet.
April 2012	Utah Dept of Technology Services	Utah Department of Technology notifies of a March 30 breach of a server containing personal data including social security numbers for about 780,000 Medicaid patient claims. Breach traced to Eastern Europe hackers.
Mar 2012	Global Payments	Credit card processor Global Payments confirms hacker attack has compromised the payment card numbers of around 1.5 million cardholders.
Mar 2012	CA Dept of Child Support Services	Officials announce that four computer storage devices containing personal information for about 800,000 adults and children in California's child support system were lost by IBM and Iron Mountain Inc.
Jan 2012	Zappos	Online shoe retailer Zappos announces that information, such as names, addresses and passwords of as many as 24 million customers illegally accessed.
Jan 2012	NY State Electric + Gas Co	Security breach at NYSEG that allowed unauthorized access to NYSEG customer data, containing social security numbers, dates of birth and bank account numbers, exposing 1.8 million records.

*March 2013 South Korean attack is not part of ITRC research.

Sources: Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf; 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.

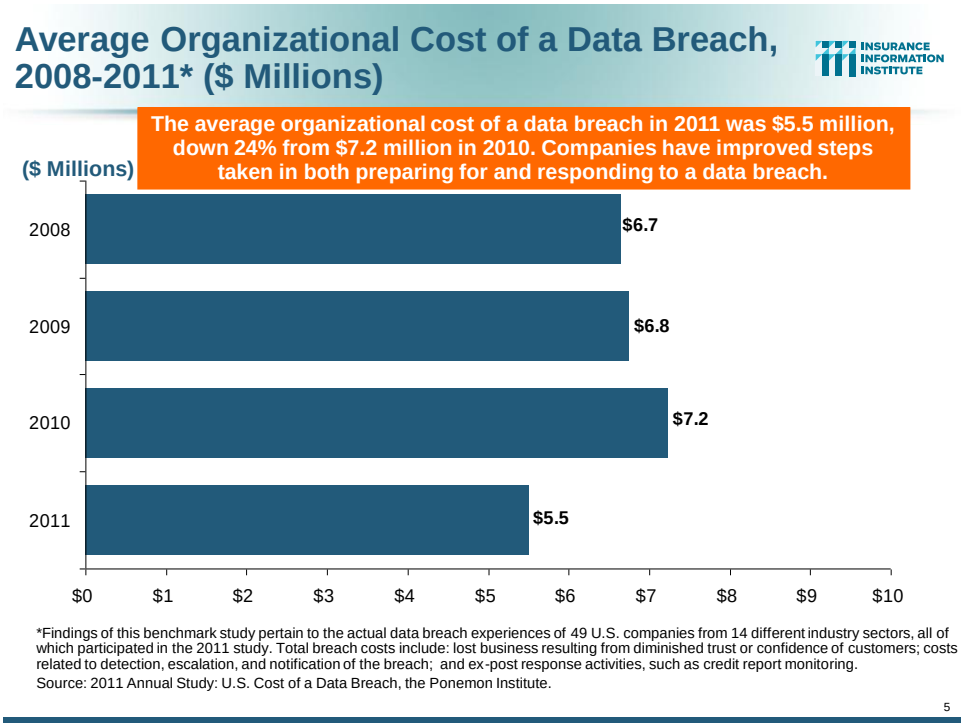
A benchmark study of 49 U.S. companies by the Ponemon Institute found that while data breaches continue to have serious financial consequences for organizations, there is evidence that companies are becoming better at managing the costs incurred to respond and resolve a data breach incident.

The average cost of a data breach was $5.5 million in 2011, down 24 percent from $7.2 million in 2010 (Fig. 8).[13] The average breach cost companies $194 per compromised record also down from $214 in 2010, it found.

This is the first time in seven years that both the organization cost of a data breach and the cost per lost or stolen record have declined.

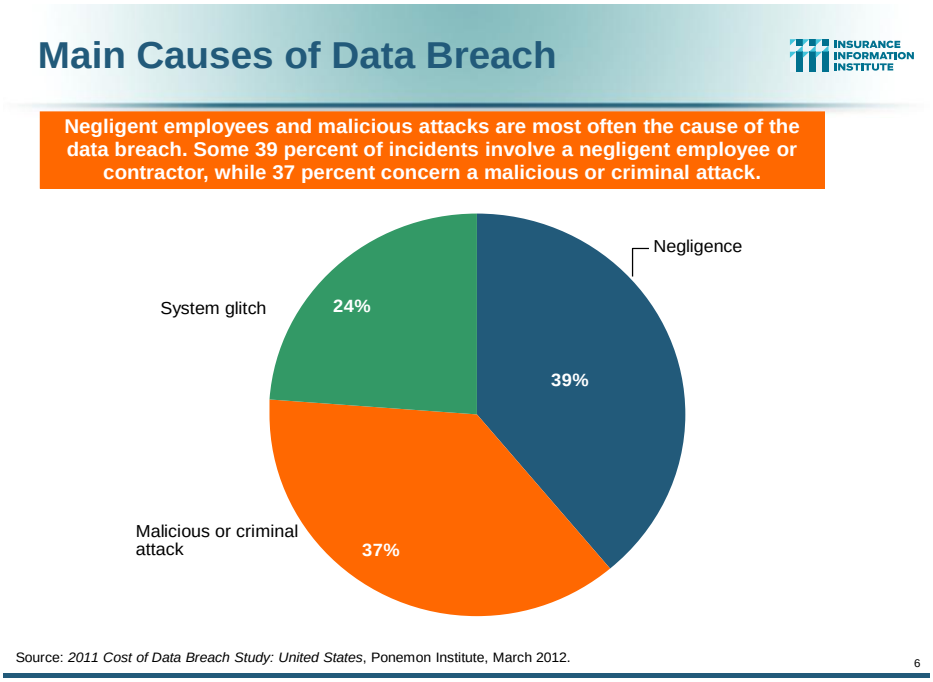
[13] *2011 Cost of a Data Breach: United States*, research by the Ponemon Institute, sponsored by Symantec, March 2012, www.ponemon.org/library/2011-cost-of-data-breach-united-states.

Fig. 8



Negligent insiders and malicious attacks are the main causes of data breach. For the first time, malicious or criminal attacks accounted for more than a third (37 percent) of the total breaches reported in the study (Fig. 9). Since 2007, they have also been the most costly.

Fig. 9



The Ponemon study also found that lost business costs declined sharply from $4.54 million in 2010 to $3.01 million in 2011. These costs refer to 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 highest cost for lost business during the seven years is $4.59 million, which occurred in 2008.

The study noted that certain organizational factors can reduce the overall cost of a data breach. If the company has a chief information security officer (CISO) with overall responsibility for enterprise data protection, the average cost of a data breach can be reduced as much as $80 per compromised record. Hiring an outside consultant to assist with breach response can also save as much as $41 per record.

However, specific attributes or factors of the data breach can also increase the overall cost. For example, the study found that companies that had their first ever data breach spent an average $37 more per record. Those that responded and notified customers too quickly without thoroughly assessing the data breach, also paid an average of $33 more per record. Data breaches caused by third parties or a lost or stolen device increased the cost by $26 and $22, respectively.

As new technologies continue to evolve, companies are exposed potentially 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 Intel found that 28 percent of IT professionals whose companies have adopted some kind of public cloud computing have experienced a security breach. Regardless of the number of breaches seen, some 65 percent of IT professionals whose companies have had a breach in the public cloud say this number is higher than what they experience with their traditional IT infrastructure, Intel found.[14]

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 damage arising from a covered cause of loss, such as a fire that caused damage to insured property.

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 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 specialist cyber insurance policies have been developed by insurers to help businesses and individuals protect themselves from an ever-evolving range of risks.

A recent survey sponsored by Zurich, and conducted by Harvard Business Review Analytic Services found that while a growing number of private and public sector organizations express concerns about information security and privacy, less than 20 percent currently purchase cyber risk insurance.[15]

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

[14] *Cloud Security Survey*, Intel, May 2012.
[15] *Meeting the Cyber Risk Challenge*, by Harvard Business Review Analytic Services, sponsored by Zurich Insurance Group and the Federation of European Risk Management Associations (FERMA), January 2013.

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 the 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 and specially tailored D&O products that include 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. 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.

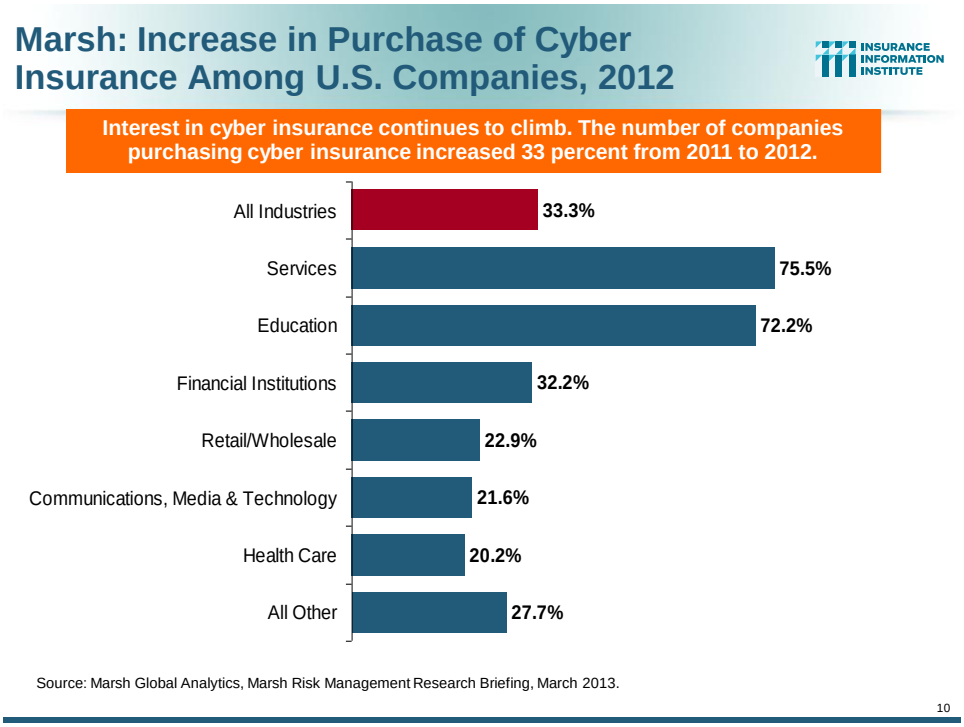
CURRENT MARKET CONDITIONS FOR CYBER INSURANCE

The latest market analysis suggests that as awareness of cyber insurance continues to grow, there has been a substantial increase in the number of companies now purchasing cyber insurance.

A March 2013 market briefing from broker Marsh notes that the number of clients purchasing cyber insurance increased by 33 percent from 2011 to 2012. This trend

was seen across most industries, with the services (professional, business, legal, accounting and personal) and education sectors leading the way (Fig. 10).

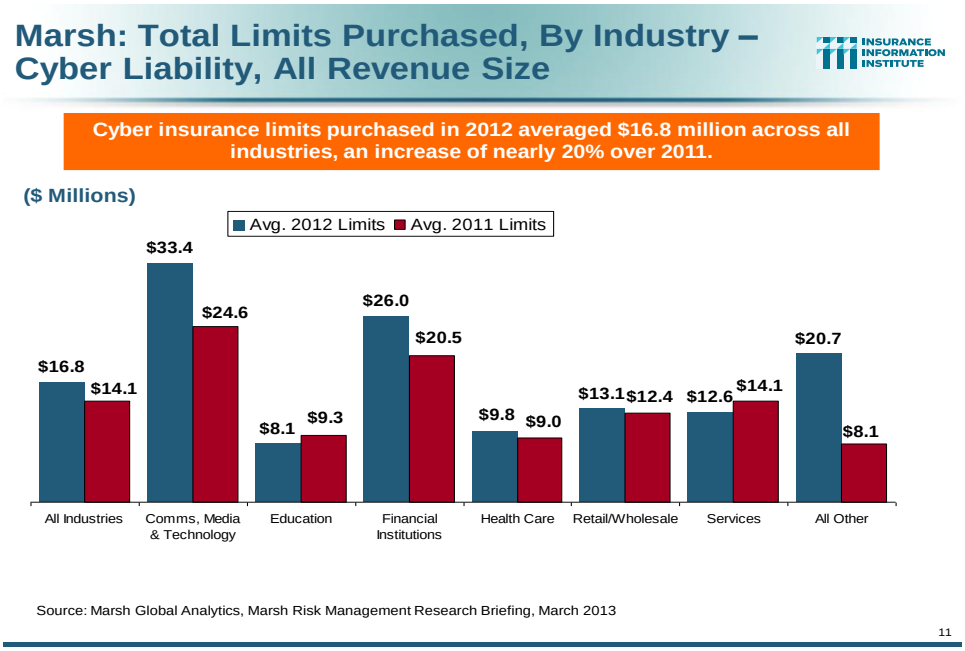
Fig. 10



Those companies purchasing cyber insurance are also buying higher limits. Cyber insurance limits purchased in 2012 averaged $16.8 million across all industries, an increase of nearly 20 percent over 2011, Marsh says (Fig. 11).

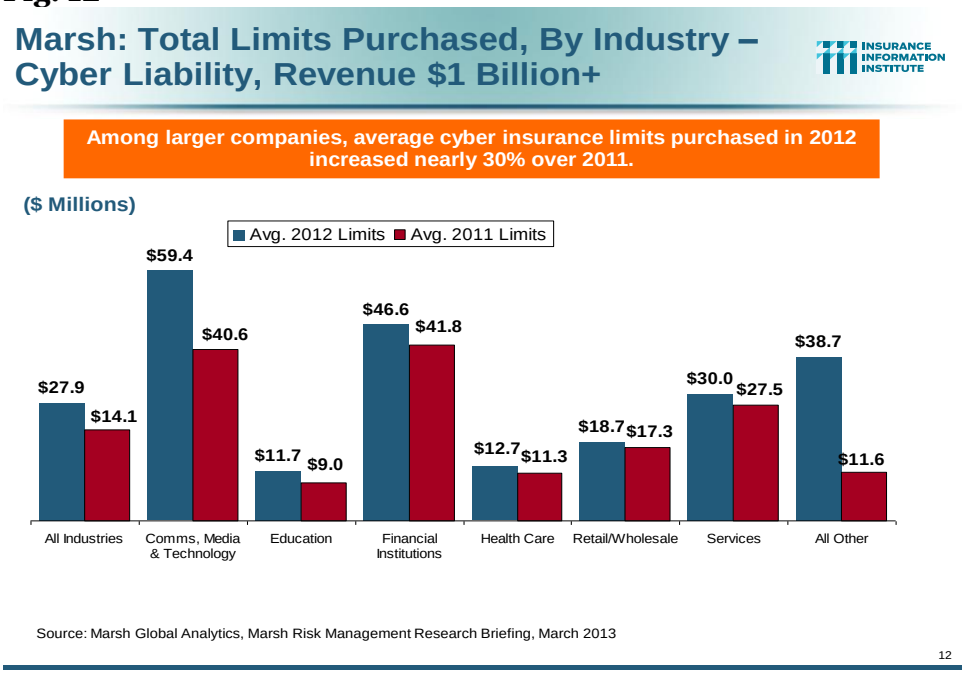
Communications, media, and technology led all industries, both by average limits purchased ($33.4 million) and the rate of increase over 2011 (nearly 36 percent).

Fig. 11



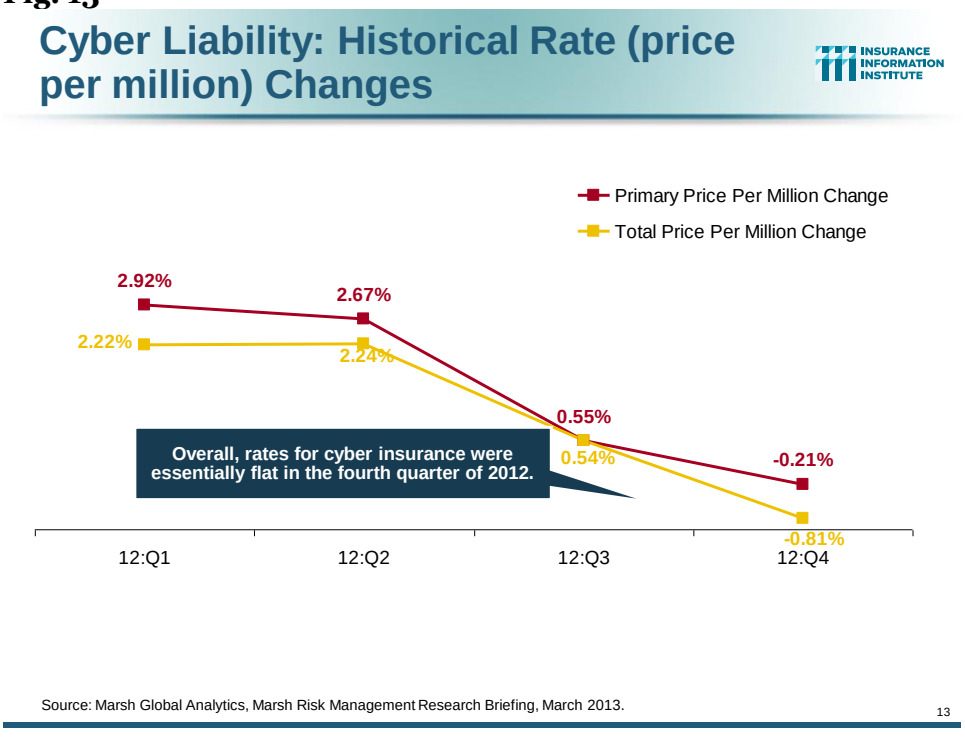
Among larger companies, which tend to have greater exposure to cyber risk, average limits purchased increased by nearly 30 percent over 2011 (Fig. 12).

Fig. 12



Rates for cyber insurance appeared flat in the fourth quarter of 2012, but market conditions varied significantly by company size (Fig. 13).

Fig. 13



CONCLUSION

Amid a rising number of high profile cyber attacks—most recently at Twitter, LinkedIn and Yahoo—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 an executive order issued by President Obama on February 12, 2013. While this is a voluntary initiative, the goal is to improve cyber security of critical infrastructure in the United States and promote sharing of information about cyber threats between government and private companies.

Despite the fact that cyber risks and cyber security are widely acknowledged to be a serious threat, a majority of companies today still do not purchase cyber risk insurance, though this is changing. Recent industry analysis suggests that more companies are now purchasing cyber coverage 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.

Data shows that companies are learning from past cyber attacks and breaches. There is evidence companies are becoming better at managing the costs incurred to resolve a data breach incident. For the first time in seven years both the organization cost of a data breach and the cost per lost or stolen record declined in 2011, the Ponemon Institute found.

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 February 2013.

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.

State Legislative Developments:
Since 2002, some 46 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, according to the National Conference of State Legislatures (NCSL).

In 2012, at least 13 states have introduced legislation expanding the scope of laws, setting additional requirements related to notification, or changing penalties for those responsible for breaches.