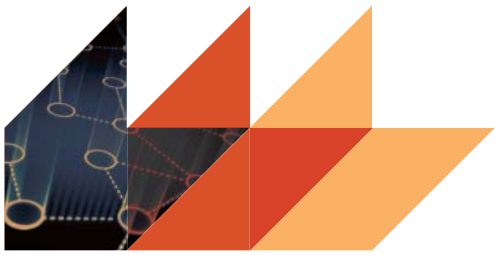
INSURANCE
INFORMATION
INSTITUTE

110 William Street, New York, NY 10038
212.346.5500
www.iii.org



Cyberrisk:
Threat and opportunity

October 2016

Robert P. Hartwig, Ph.D., CPCU
Moore School of Business, University of South Carolina;
Special Consultant, Insurance Information Institute

Claire Wilkinson
Consultant
917.459.6497
clairew@iii.org

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Interest in cyber insurance and risk continues to grow beyond expectations in 2016 in part due to high profile data breaches, but also due to awareness of the almost endless range of exposures businesses face.

- The Panama Papers global breach underscored the importance of having a robust insurance program and security strategy.
- Breaches targeting medical/healthcare providers continue apace. A ransomware attack in February against a Hollywood, California, hospital forced its computer systems offline for more than one week. While patient records were not compromised, the hospital paid a ransom to the hacker to regain control of its systems.
- Insurers are also coming under attack. Two high profile breaches in 2015 targeted health insurers Anthem and Premera Blue Cross, exposing data on 78.8 million and 11 million customers, respectively.
- The U.S. government has also been targeted by hackers. Recent breaches at the Federal Deposit Insurance Corp (FDIC) and the Internal Revenue Service follow multiple breaches in May 2015 of the Office of Personnel Management and Interior Department systems that compromised the records of 22 million current and former civilian U.S. government employees.

Attacks and breaches have grown in frequency, and loss costs are on the rise. In 2015, the number of U.S. data breaches tracked totaled 781—the second highest year on record—with 169 million records exposed. In the first half of 2016, some 507 data breach events have been publicly disclosed as of July 7, with 12.8 million records exposed. These figures do not include the many attacks that go unreported. In addition, many attacks go undetected. Despite conflicting analyses, the costs associated with these losses are increasing. McAfee and CSIS estimated the likely annual cost to the global economy from cybercrime is $445 billion a year, with a range of between $375 billion and $575 billion.

Insurers are issuing an increasing number of cyber insurance policies and becoming more skilled and experienced at underwriting and pricing this rapidly evolving risk. They are also working with catastrophe modelers to develop a standardized approach to identify, quantify and report exposure data across the industry. More than 60 carriers now offer stand-alone cyber insurance policies, and it is estimated the U.S. market is worth over $3.25 billion in gross written premiums in 2016, with some estimates suggesting it has the potential to grow to $7.5 billion.

Some observers believe that exposure is greater than the insurance industry's ability to adequately underwrite the risk. Attacks have the potential to be massive and wide-ranging due to the interconnected nature of this risk, which can make it difficult for insurers to assess their likely severity. The underreporting of attacks means that accurately evaluating exposures is challenging. Several insurers have warned that the scope of the exposures is too broad to be covered by the private sector alone, and a few observers see a need for government cover akin to the terrorism risk insurance programs in place in several countries.

I. GROWTH IN INTEREST IN CYBER LIABILITY

An explosion of data and digital technologies, combined with the increasing complexity of threats and changing regulatory expectations, is propelling the cyberrisk landscape into uncharted territory.

Economic thought leaders have warned that failing to understand and address risks related to technology, primarily the systemic cascading effects of cyberrisks or the breakdown of critical information infrastructure could have far-reaching consequences for national economics, economic sectors and global enterprises. As the Internet of Things (IoT) leads to more connections between people and machines, cyber dependency will increase, raising the odds of an attack with potential cascading effects across the cyber ecosystem.[1]

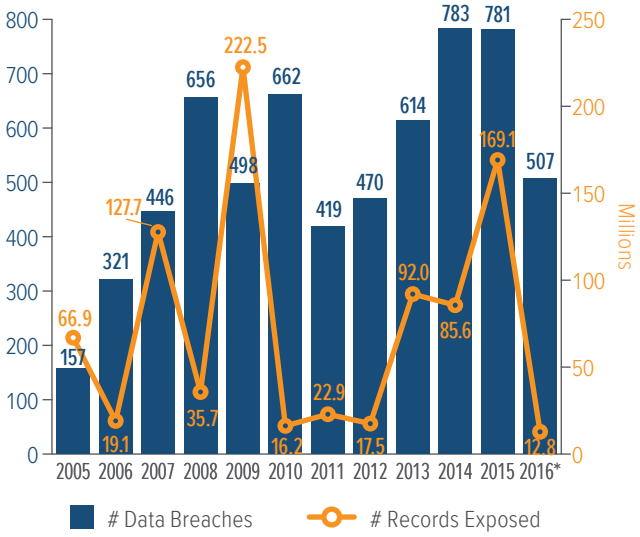
Emerging technologies such as drones, additive manufacturing (3-D printing, for example), smart city projects, internet-connected home appliances and autonomous vehicles could also disrupt established business practices and create new security threats, fundamentally changing the nature of risks.[2] Effective global governance will be critical to manage evolving security and privacy risks going forward.

Number and Impact of Data Breaches Continues to Rise

In 2015 a total of 781 U.S. data breaches were tracked, with 169 million records exposed, according to the Identity Theft Resource Center **(Fig. 1)**.[3] This represents the second highest year since the center began tracking breaches in 2005.

Fig. 1

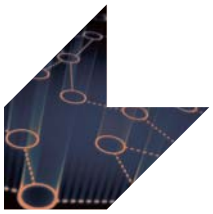
Number of Data Breaches/ Millions of Records Exposed*



*Figures as of July 7, 2016.
Source: Identity Theft Resource Center.

The ongoing trend of record high numbers of breaches continues—in the first half of 2016, some 507 data breach events had been publicly disclosed as of July 7, 2016, with 12.8 million records exposed.

A high profile global breach with massive fallout is the Panama Papers online leak targeting Panamanian law firm Mossack Fonseca. This email hack included 2.6 terabytes of data, including 4.8 million email messages and 2.2 million PDFs. The leaked information allegedly details the ways dozens of high-ranking politicians, their relatives or close associates in more than 40 countries used offshore companies to hide income and avoid paying taxes. More than 100



news organizations published reports based on the leaked information starting in early April 2016. Meanwhile, the just-disclosed 2014 Yahoo breach believed to have been the work of a state-sponsored group, compromised a record 500 million accounts. It highlights the scope of the threat and widespread impact as users scramble to reset passwords. Disclosure of the breach comes as Yahoo tries to complete its pending deal with Verizon. Both events serve as a reminder of the importance of having a robust insurance program and cybersecurity strategy.

Breaches targeting medical/healthcare providers continue apace in 2016. A ransomware attack in February against a Hollywood hospital forced its computer systems offline for more than one week. While patient records were not compromised in this attack, Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to the hacker to regain control of its systems. In July 2015, hackers accessed as many as 4.5 million patient records in UCLA Health System's computer network.

Insurers are also coming under attack. Two high profile breaches in 2015 occurred at health insurers Anthem and Premera Blue Cross. At Anthem, hackers gained access to a corporate database containing the personally identifiable information on 78.8 million current and former U.S. customers and employees. Anthem also stated that anywhere from 8.8 million to 18.8 million non-customers could have been impacted. Meanwhile, Premera Blue Cross suffered a network intrusion in March 2015 that compromised the financial and medical records of 11 million customers.

The U.S. government continues to be a target of hackers. Recent breaches at the Federal Deposit Insurance Corp (FDIC) and the IRS follow multiple breaches in May 2015 of the Office of Personnel Management and Interior Department systems, when hackers stole records on as many as 22 million current and former civilian U.S. government employees. The U.S. Federal Reserve is also reported to have been the target of multiple attacks.

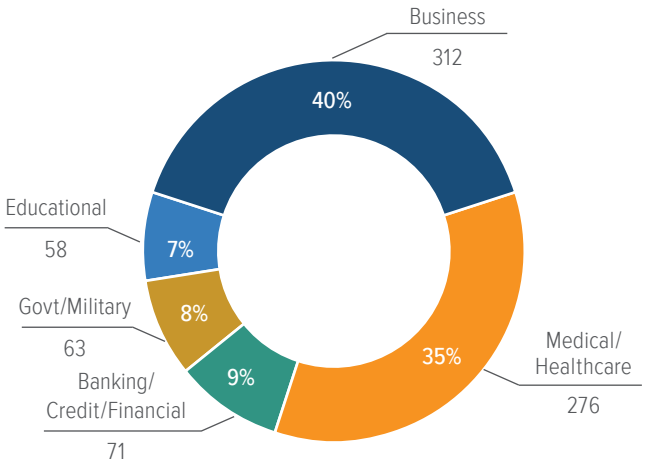
Other recent victims include well-known brands such as Wendy's, Verizon Enterprise Solutions, Ashley Madison, Sony Pictures, Staples, Home Depot, JP Morgan Chase, PF Chang's, eBay, Snapchat and Target.

Yet despite the large number reported, the actual number of breaches and exposed records is without a doubt much higher as many, if not most, attacks go unreported and undetected.

The majority of the 781 data breaches in 2015 hit business and medical/healthcare organizations, according to the Identity Theft Resource Center **(Fig. 2)**.

Fig. 2

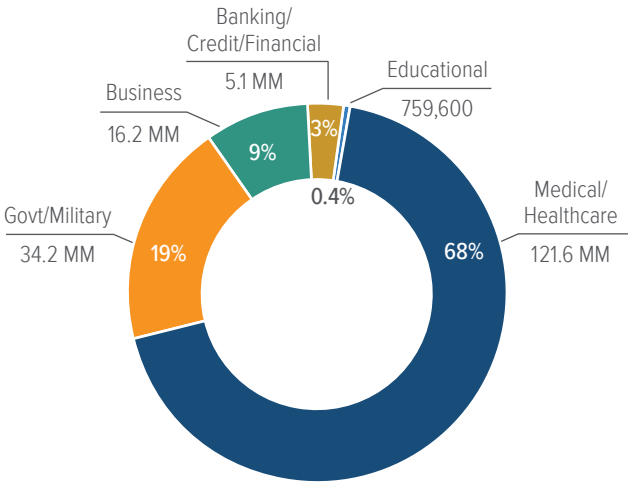
2015 Data Breaches By Business Category, By Number of Breaches



Source: Identity Theft Resource Center.
Total may not equal 100% due to rounding.

Fig. 3

Medical And Healthcare Records Were More Than Half Of All Records Stolen



Source: Identity Theft Resource Center.
Total may not equal 100% due to rounding.

Medical and healthcare organizations accounted for the majority of records exposed by data breaches in 2015 **(Fig. 3)**.

High profile breaches have triggered greater awareness of the risk and need for insurance. One legal expert described the 2013 Target data breach as "the equivalent of 10 free Super Bowl ads for insurers selling cyber policies."[4]

The fact that Target had $100 million in network security insurance was widely reported.[5] As of January 2016, Target estimated it had already accrued $291 million in expenses related to the data breach, with some $90 million expected to be offset by insurance.

Health insurer Anthem is understood to have some $150 million to $200 million in cyber insurance, including excess layers of coverage. It is also reported that Home Depot had $105 million in coverage and that insurance would cover some $27 million in recovery costs from the retailer's 2014 breach.

The Threat to Businesses

No industry sector appears to be safe. For any business or government entity that stores confidential customer and client information online, a massive data breach can leave it fighting to maintain reputation and brand value.

Cyber incidents (crime, data breaches, IT failures) moved into the top 3 global business risks in 2016, according to the fifth annual Allianz Risk Barometer Survey, climbing up to rank 3 from No. 5 **(Fig. 4)**.[6]

Cyber incidents also ranked as the top long-term risk, according to the Allianz survey, while impact of digitalization and new technology also feature among the top 10 risks identified by companies.

Other survey highlights:

- Loss of reputation (69 percent) is the main cause of economic loss after an attack, followed by business interruption (BI) (60 percent) and liability claims after a data breach (52 percent).
- The increasing sophistication of attacks is the impact of digitalization that companies fear most (52 percent), according to Allianz. Respondents also fear data fraud or theft (50 percent) and breakdown of critical infrastructure (38 percent).
- A lack of understanding (48 percent) of the complexity of the risks involved is cited as the main factor preventing companies from being better prepared to combat threats. Not having a concrete assessment of the cost of the risks involved (46 percent) ranks second, while budgetary constraints (39 percent) ranks third.

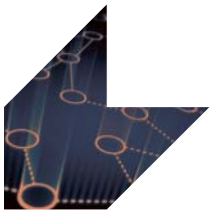
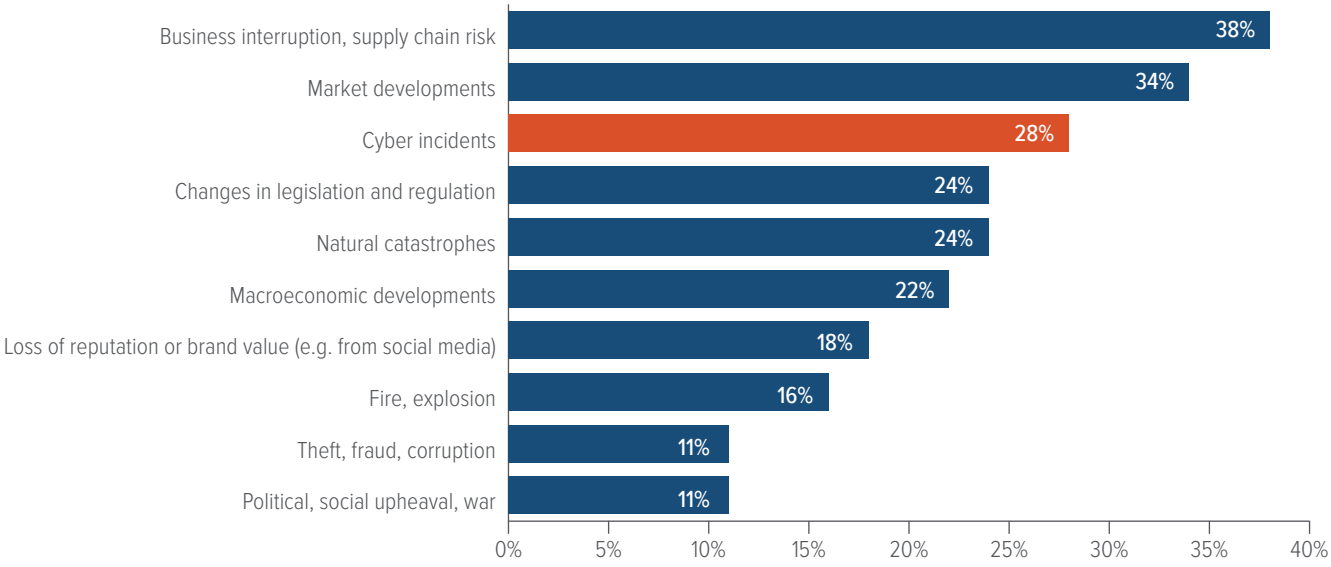


Fig. 4

In 2016 Cyber Incidents Were Ranked The No. 3 Global Business Risk



Source: Allianz Risk Barometer on Business Risks 2016.

Emerging Technology Risks

As technologies evolve, companies of all sizes are potentially exposed to even greater risks from data breaches.

The Internet of Things (IoT) means that billions of connected things, from autonomous vehicles, to smart home devices, to medical devices, to wearable devices could be vulnerable to attack and the onus is on manufacturers to prioritize security and reduce the risks.[7] Gartner forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020.[8]

Even automobiles are now vulnerable to hacking. Laptop computers are now being used to bypass key fobs and hijack electronic ignition systems to steal cars. In August 2016 two men were accused of using a laptop to steal more than 100 vehicles in the Houston area.[9] And in July 2015, Chrysler announced the recall of 1.4 million Jeep vehicles after it was demonstrated that dashboard functions, steering, transmission and braking systems could be hacked and manipulated wirelessly.[10]

Smart home devices, including smart door locks and alarms, in millions of homes are a potential target of attacks. Symantec research found multiple vulnerabilities in 50 commercially available devices.

Researchers have also discovered potentially life-threatening vulnerabilities in medical devices, such as insulin pumps, smart pacemakers and X-ray machines.[11] In January, the U.S. Food and Drug Administration issued draft guidance outlining steps medical device manufacturers should continuously take to address cyberrisks.

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.

The Cloud Security Alliance (CSA) has identified data breaches as the top cloud computing threat that companies face in 2016.[12] Because of the huge amount of data stored on cloud servers, providers have become an attractive target, the CSA report found.

A hack of Apple's iCloud service last year resulted in a collection of nearly 500 private pictures and videos of celebrities being posted online.

Mobile security and privacy is another concern. Growing numbers of mobile devices are being used to access confidential and critical information, leaving corporate networks even more vulnerable to attack.

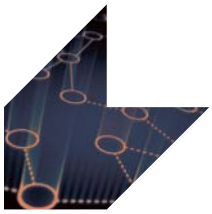
Meanwhile, the FBI's unlocking of an iPhone belonging to one of the terrorists involved in the San Bernardino shooting may have ended its legal battle with Apple, but left open the question of whether devices should be manufactured with back doors so that information can be extracted.

Ransomware and Social Engineering Risks

Ransomware and social engineering attacks are on the rise. A $16,000 ransom paid by the University of Calgary to restore data following a ransomware attack, a $500 bitcoin payment made by a NASCAR racing team after critical team data was held hostage, and a $17,000 bitcoin payment made by Hollywood Presbyterian Medical Center after a hacker gained control of its systems are just some recent attacks that have raised concerns among businesses and insurers.

Nearly 40 percent of businesses have experienced a ransomware attack in the last year, and of these, more than one-third lost revenue while one in five had to stop business completely, according to recent research.[13] More than 20 percent of attacks demanded more than $10,000 in ransom. In April, the Federal Bureau of Investigation (FBI) reported that law enforcement had seen an increase in ransomware attacks in 2015, particularly targeting organizations because the payoffs are higher. Ransomware attacks are not only proliferating, but becoming more sophisticated, the FBI warned.[14] Symantec reports that crypto-style ransomware (encrypting files) grew by 35 percent in 2015 and predicted that this extremely profitable type of attack

> For any business or government entity that stores confidential customer and client information online, a massive data breach can leave it fighting to maintain reputation and brand value.



will continue to ensnare PC users and expand to any network-connected device that can be held hostage for a profit.[15] McAfee Labs predicted that ransomware will remain a major and rapidly growing threat in 2016.[16]

A growing financial fraud—and form of social engineering—is business email compromise (BEC) fraud, also known as CEO fraud, which last year was described by the FBI as an emerging global threat.[17] These sophisticated phishing attacks occur when cyber criminals send fake email messages from company CEOs, often when a CEO is known to be out of the office, asking company accountants to transfer funds to a supplier. Instead, the funds go to a criminal account.

Since the FBI's Internet Crime Complaint Center (IC3) began tracking BEC scams in late 2013, more than 7,000 U.S. companies have been targeted by such attacks with total dollar losses exceeding $740 million. That figure is likely much higher when non-U.S. victims and unreported losses are included.

Impact on Small, Midsize Businesses

While data breaches on larger companies tend to dominate the headlines, small and medium-sized businesses are increasingly vulnerable.

Their exposure is much the same as that of larger companies, according to experts, but many do not realize they are the "soft underbelly" of cybersecurity, mistakenly believing they are too small to be attacked.[18]

Attacks are growing more common, with Travelers estimating that 62 percent of all breach victims are small to medium-sized businesses.[19]

A recent UK government report also suggested that one-third (33 percent) of small businesses have had a breach in the past 12 months, while for medium businesses that number is at just over one-half (51 percent).[20]

While concerns have grown amid increasing frequency and costs of attacks, security spending is on the rise, a recent Gartner report found. The worldwide cybersecurity market will increase to $170 billion by 2020, up from $75.4 billion in 2015.[21]

In 2015, 38 percent more security incidents were detected than in 2014, and companies of all sizes boosted their information security budgets by 24 percent in 2015, PwC found.[22] Interestingly, 46 percent of survey respondents said their board participates in information security budgets.

Large companies, meanwhile, have noticed the risks their smaller business partners and suppliers present. The massive Target data breach began when hackers gained access to the U.S. retailer's systems via its heating, ventilation and air conditioning (HVAC) vendor.

Some big companies have increased their due diligence. Many require their vendor networks to have cyber insurance and better security in place.

As a result many small and midsized companies are now buying cyber insurance because they are required to if they want to do business with other partners.[23]

> Small businesses do not realize they are the "soft underbelly" of cybersecurity.

The Threat to Government

Governments are facing an unprecedented level of attacks and threats with the potential to undermine national security and critical infrastructure.

U.S. President Obama has stated that cyber terrorism is one of the biggest threats facing the United States today, noting in his 2015 State of the Union speech:

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids.

"We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism."[24]

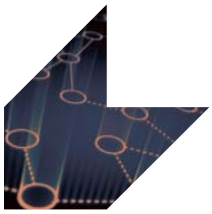
After the 2014 Sony Pictures breach, President Obama declared malicious cyberattacks a national emergency and signed an executive order April 1, 2015, establishing new sanctions to curb this "unusual and extraordinary threat to the national security, foreign policy and economy of the United States."[25]

For government the threat extends beyond dollars and cents. 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.[26]

Such attacks are the work of an evolving list of perpetrators, including:

- **State-sponsored groups:** Foreign governments are increasingly sponsoring attacks that infiltrate U.S. businesses and steal information and intelligence. Few take responsibility.
- **Criminal organizations:** Traditional organized crime groups based in a single country or loosely organized global hacker teams frequently target individuals and corporations.
- **Hacktivists:** Politically motivated groups (such as Anonymous) and lone hackers are growing in number and sophistication.
- **Insiders:** Increasing numbers of disgruntled and former employees are using their authorized access to sensitive information and computer networks to carry out attacks.
- **Terrorists:** Governments around the world are concerned about terrorists carrying out potentially wide-scale events that destroy physical and digital assets.

The rising popularity of digital currencies, such as bitcoin, has also resulted in their acceptance as payment by a growing number of establishments, despite potential risks and illegal uses. The ICT noted the technological aspects of bitcoin that make it an ideal means of fundraising for illegal activities, such as terrorism. Separately, there have also been several well-publicized hacker attacks on bitcoin exchanges, which is a growing risk for companies.



Hacks of both Democratic National Committee and Republican National Committee emails during an election year have raised concerns that groups are attempting to influence the outcome of the 2016 U.S. presidential campaign. Personal email accounts of politicians are also being targeted, as evidenced by the hacking of former secretary of state Colin Powell's Gmail account.

Theft of military and trade secrets remains a top concern. U.S. military Central Command (@Centcom) Twitter and YouTube accounts were hacked in January 2015, reportedly by Islamic state militants. No classified information was compromised.

An unprecedented external attack on the Ukraine power grid on December 23, 2015, underscores the growing threat to critical infrastructure. Reports suggest that hackers may have installed malware known as BlackEnergy on the systems of three regional power stations before launching a coordinated attack that left 225,000 homes in the Ivano-Frankivsk region of the country without electricity for several hours.[27]

> Computer sabotage coming from another country can constitute an act of war.

There were two noteworthy critical infrastructure attacks in 2014. A Russian hacker group called "Energetic Bear" launched a malware attack that caused significant disruption for U.S. energy sector companies, and an attack against a steel plant in Germany disrupted control systems, leaving operators unable to shut down a blast furnace, resulting in massive physical damage.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received reports of approximately 295 attacks on critical infrastructure control systems in the United States in fiscal year 2015 (October 2014 through September 2015), a 20 percent increase over the prior year.[28] The critical manufacturing sector saw the most reported incidents, accounting for one-third (33 percent), followed by the energy sector with 46 incidents (16 percent).

Government Fights Back

In July, the White House announced a new policy directive spelling out how the government will coordinate its response to large-scale cyber incidents. As part of this initiative a new metric designed to gauge the severity of attacks and how the government responds to them will assign a rating of 0 through 5 (with 5 being the most severe) to significant incidents.

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 risks. A year earlier President Obama issued an executive order that promoted increased information sharing about threats between government and private companies that oversee critical infrastructure such as electrical grids.

Meanwhile, incidents such as former National Security Agency contractor Edward Snowden's 2013 leaks on the U.S. intelligence community's internet surveillance

have continued to raise the profile of cyber conflict between countries.

In 2011, a report from the Pentagon concluded that computer sabotage coming from another country can constitute an act of war.[29] It noted that the Laws of 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 number of federal legislative/regulatory proposals on cybersecurity have been passed or are under consideration by Congress. At the state level, some 47 states have breach notification laws in effect.

Since October 2011 the Securities and Exchange Commission (SEC) has provided guidance for publicly traded companies to disclose significant instances of cyberrisks and events.[30] Descriptions of relevant insurance coverage were 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 of an attack. For insurers, the increasingly complex and ever evolving nature of threats and attacks presents both a challenging risk and an opportunity.

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

Two key security bills passed by the House in late April 2015 would shield from liability companies that share cyber threat information with the government.

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

Cyber Terrorism Coverage

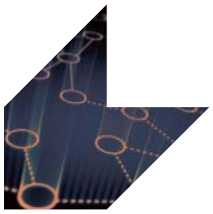
Language regarding acts of war or terrorism in cyber insurance policies is typically vague. For example, a cyberattack or data breach caused by a state-sponsored group classified by the U.S. government as a terrorist organization falls into a gray area, bringing up questions over insurance coverage.

The most recent extension of the terrorism risk insurance program [the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA)] does not explicitly or directly address cyberattacks.

The general view is that if a cyber terrorism attack resulted in damage ordinarily covered by a terrorism insurance policy such as fire or explosion, there would be coverage under the terrorism risk insurance law, so long as the event meets all the criteria set forth in the act leading to a certification of the event as an act of terrorism.[31]

For example, if a cyber terrorism attack led to a major explosion at a power plant, that damage would likely be covered by terrorism insurance. However, costs resulting from an attack such as notification to customers after a data breach, the cost of fines and penalties, the theft of confidential information and lawsuits would be far beyond the scope of the program.[32]

In response to a growing number of incidents and cyber threats targeting commercial industries that can lead to equipment failure, physical damage to property and/or injury to people, several insurers now offer expanded coverage. These products include coverage for property damage and bodily injury, specifically for companies in critical infrastructure industries, such as oil and gas, chemicals, power and utilities.



II. CYBERATTACKS: RISING FREQUENCY AND SEVERITY

Latest industry research points to the rising frequency and severity of cybercrimes and attacks.

A joint report by McAfee and the Center for Strategic and International Studies (CSIS) found that governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow.[33]

McAfee and CSIS estimated the likely annual cost to the global economy from cybercrime is $445 billion a year, with a range of between $375 billion and $575 billion. This figure is more than the national income of most countries, the report noted.

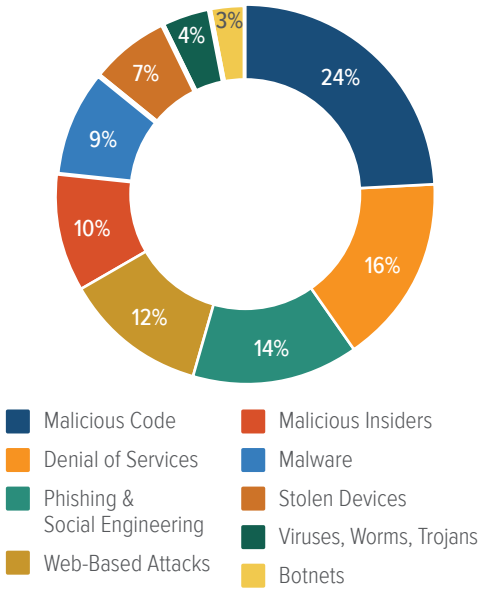
The most important cost comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation and global economic growth, according to the report.

Cybercrime remains a growth industry. CSIS research predicts that opportunities will grow as more business activities move online and more consumers around the world connect to the Internet, and as autonomous devices are connected.

Fig. 5

Malicious Code, Denial Of Service And Phishing Were The Most Costly Cyber Crimes In 2015

Percentage of Average Cost



Total may not equal 100% due to rounding.
Source: 2015 Cost of Cyber Crime: United States, Ponemon Institute.

Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it to manufacture competing goods.

The Cost of Cybercrime

The cost of the typical incident continues to grow, often into millions of dollars.

An annual study of U.S. companies by the Ponemon Institute estimates the average annualized cost of cybercrime at $15.4 million, up 21 percent from $12.7 million per year the previous year, and an increase of 33 percent from $11.6 million two years ago.[34]

The total annualized cost for the 2015 benchmark sample of 58 organizations ranged from a low of $1.9 million to a high of $65 million each year per company.

The most costly crimes as a percentage of the average cost of cybercrime are those caused by malicious code and denial of service attacks, Ponemon said **(Fig. 5)**.

Information theft continues to represent the highest external cost, followed by costs associated with business disruption, the study revealed **(Fig. 6)**.

On an annualized basis, information theft accounted for 35 percent of total external costs (consistent with the six-year average). Costs associated with disruption to business or lost productivity accounted for 39 percent of external costs (up 4 percent from the six-year average).[35]

The cost grows if the attack is not resolved quickly. According to the study, the average time to resolve an attack was 46 days, with an average cost to participating companies of $2 million during this 46-day period. This represents a 22 percent increase from last year's estimated average cost of $1.6 million based on a 45-day resolution period. Results show that malicious insider attacks can take more than 60 days on average to contain.

International studies also show the breadth and depth of the risk, in the United States and elsewhere.

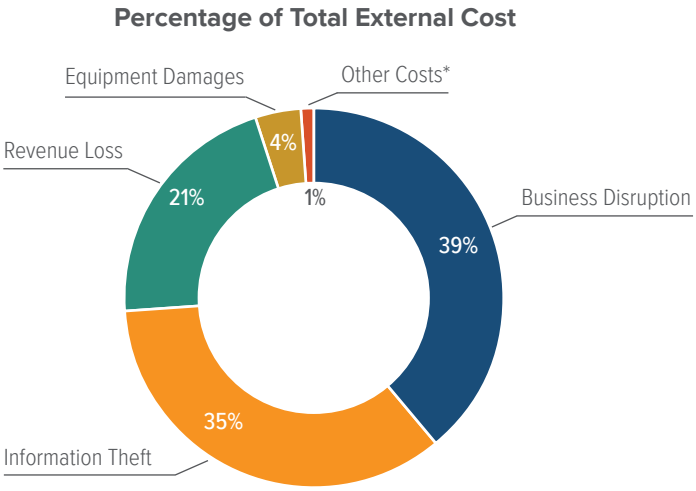
A global benchmark study by the Ponemon Institute of 383 companies representing 12 countries, including the United States, found that data breaches are becoming far more costly to manage and that U.S. companies suffered, on average, the most costly breaches.

This study did 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 breach was more than $7.0 million in 2016—the highest total average cost of the 12 countries—up 7 percent from $6.5 million in 2015 **(Fig. 7)**.[36] Germany had the next highest total average cost at $5.0 million. In contrast, samples of Indian and South African companies experienced

Fig. 6

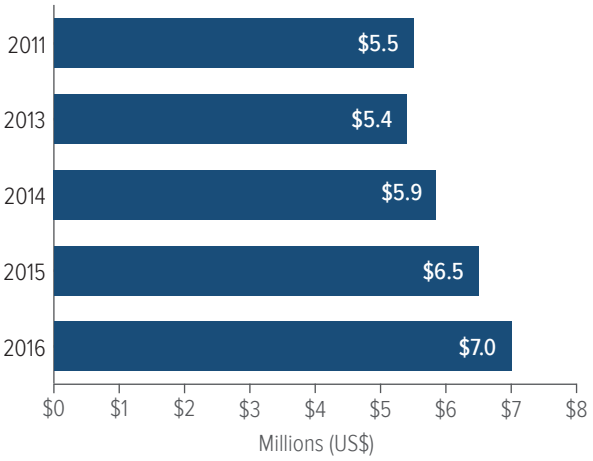
Information Theft And Business Disruption Account For The Bulk Of External Costs



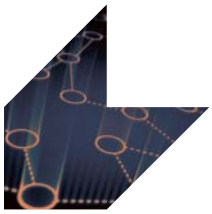
*Other costs include direct and indirect costs that could not be allocated to a main external cost category. Total may not equal 100% due to rounding.
Source: Ponemon Institute.

Fig. 7

The Average Cost Of A Breach In The U.S. Has Reached $7 Million in 2016*



*The 2016 study examines the costs incurred by 383 companies across 16 industries representing 12 countries, including 64 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.



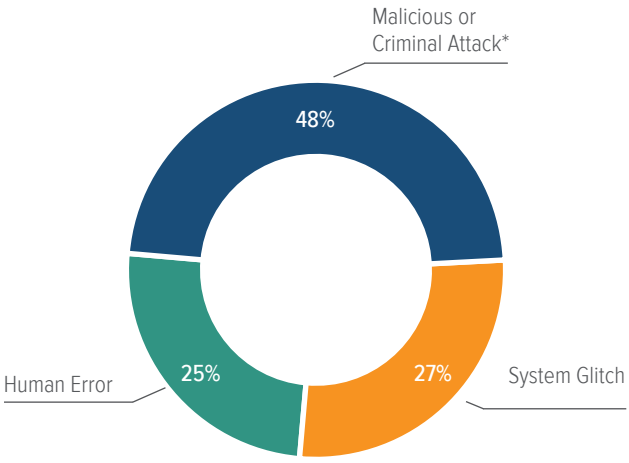
the lowest total average cost at $1.6 million and $1.9 million, respectively.

The average per capita cost of a data breach for U.S. companies was $221, compared to a $217 average cost calculated in 2015. Ponemon defines per capita cost as the total cost of data breach divided by the size of a data breach (i.e. the number of lost or stolen records). Also, on average U.S. companies had data breaches that resulted in among the greatest number of exposed or compromised records, at 29,611.

Malicious or criminal attacks are most often the cause of a data breach globally and also the most costly data breach incidents in all 12 countries, the Ponemon study found **(Fig. 8)**. U.S. companies that had a data breach due to malicious or criminal attacks experienced a cost of $236 per compromised record, significantly above the mean of $221.

Fig. 8

Malicious Or Criminal Attacks Cause Almost Half Of All Breaches



*The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.
Total may not equal 100% due to rounding.
Source: Ponemon Institute.

The Ponemon study also found that U.S. organizations have the highest lost business costs at an average of $4.0 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.

Conflicting Information on Data Breach Costs

An earlier study by Verizon suggests that these data breach cost estimates may be overstated.[37] Compared to the 2014 Ponemon estimates that breaches cost companies $201 per lost record that year, Verizon's cost-per-record estimate was just 58 cents.[38]

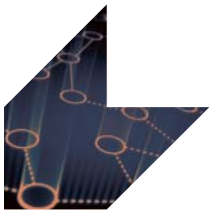
The wildly different cost estimates arise because Verizon's 2015 Data Breach Investigations Report uses only cyber liability insurance claims data from insurers to look at the data breach cost impact, rather than a broader formula that includes both direct and indirect costs.

In its analysis Verizon did acknowledge that the 58 cent cost-per-record is a very poor estimate of loss. It goes on to set out a new breach-cost model that accounts for uncertainty as the volume of records lost increases. As a result it found that a small data breach where only 100 records are lost would most likely cost an organization between $18,120 and $35,730. At the other end of the scale, a massive data breach of 100 million records would have an average cost of between $5 million and $15.6 million, Verizon said.

The 2014 Ponemon study did find 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.



III. THE INSURANCE INDUSTRY AND CYBERRISK

Historical Development of Cyber Insurance

Cyber insurance in the United States evolved as a product in the mid- to late-1990s, and the market is still seen as being in its infancy **(Fig. 9)**. Insurers have had to expand coverage for a risk that is rapidly shifting in scope and nature.

More than 60 carriers offer stand-alone policies, and Marsh, a major insurance broker, estimates the U.S. market was worth $2.75 billion in gross written premiums in 2015, up from $2 billion in 2014. Today, market experts suggest gross written premiums have increased to $3.25 billion.[39]

Fig. 9

Historical Development of Cyber (Re)Insurance

Evolution of the U.S. Product

1996
- Cyber insurance first emerged as a product.

2003
- Privacy breach notice laws enacted in California, furthering demand for cyber products.

2000s
- Following California's example, 47 of the 50 states have enacted compulsory breach notification legislation, driving the cyber market in the U.S.

2006
- Cyber becomes privacy issue.

2014
- Cyber is underwritten by over 60 insurers and produces over $1 billion a year in premium income.

Evolution of the European Product

1995
- Data Protection Directive in the EU.
- Established data protection as a right for EU citizens.

Mid 2000s
- Increased reliance on IT and high-profile hacking scandals lead to increase in inquiries for cyber insurance in Europe.

2012
- Reform of Data Protection Legislation released by the EU. These detailed compulsory breach notification rules increase fines to be enforced and other requirements for data protection.

2013
- EU announced the Cyber Security Directive, which will impose minimum security measures on businesses.

2013/14
- Insurers develop international offerings. 25-30 markets in London.

2015
- Expected implementation of the Reform of Data Protection Legislation. (However, this date is a moving target).

Source: *Historical Development of Cyber (Re)Insurance*, GCCapitalIdeas.com, October 23, 2014.

Estimates also project the European market at between €700 million and €900 million by 2018 (US$765 million to US$983 million).[40] Industry experts say the European market is likely to get a boost from expected reform of European Union (EU) data protection rules that would force companies to disclose breaches of customer data.

PwC estimates the global market could grow to at least $7.5 billion in annual premiums by the end of the decade. Insurers need to move quickly to innovate before a disruptor such as Google enters the market.

The Lloyd's insurance market estimates that the growing global market will be worth $85 billion and is positioning itself to be a global hub for coverage.[41]

Why Reliance on Traditional Policies Is Not Enough

While traditional insurance policies typically have not handled the emerging risk, limited coverage under traditional policies may be available.

For example, there may be coverage under a traditional property insurance policy if an incident resulted in a covered cause of loss, such as a fire or explosion, which 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 (up to a specified limit).

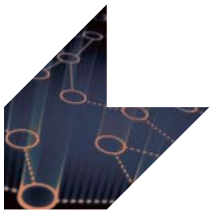
If electronic data is destroyed or damaged as the result of a covered cause of loss, the insurer will pay the cost to replace or restore it. Causes of loss that apply to this coverage include a computer virus, harmful code or other harmful instructions entered into a computer system or network to which it is connected. There is no coverage, however, for loss or damage caused by the actions of any employee.

Forms now allow insurers to tailor coverage for small and midsize businesses. Optional endorsements to the standard BOP cover data breaches, data replacement and restoration, cyber extortion and business interruption.[42]

Most traditional commercial general liability policies do not cover cyberrisks, however.[43] In the United States, Insurance Services Office (ISO), a subsidiary of Verisk Analytics, is a key supplier of statistical, actuarial and underwriting claims information for property/casualty insurers. ISO also develops standard insurance policy forms. ISO's revisions to its general liability policy form in 2014 and 2013 consist primarily of a mandatory exclusion of coverage for personal and advertising injury claims arising from access or disclosure of confidential information.

Reliance on traditional insurance policies is therefore not enough, so specialized policies have been developed by insurers.

The Lloyd's insurance market estimates that the growing global cyber insurance market will be worth $85 billion and is positioning itself to be a global hub for coverage.



Stand-Alone Cyber Coverage

Specialized cyberrisk 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.

Coverages 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 on 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 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 cyberrisks, 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. An insured's ransom payment following a ransomware attack is typically covered, subject to individual policy terms and conditions.

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 as 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 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.

Depending on the individual policy, specialized coverage can apply to both internally and externally launched 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.

New Areas of Development

As quickly as insurers develop cyber policies, new exposures are emerging.

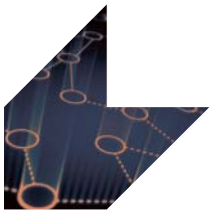
Individual Risks: Insurers are starting to offer cyber insurance programs for individuals. Such programs typically bundle coverages previously available only to businesses, but increasingly important to individuals as they access and store data online. Coverage can be added to homeowners or renters policies and may include coverage and services for computer attacks, cyber extortion, online fraud and the breach of personal information involving smart phones, computers and connected home devices.

Individuals seek 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 is also evolving. 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.

Deceptive Funds Transfer (Social Engineering Coverage): Coverage for theft losses resulting from deceptive funds transfer (sometimes known as social engineering coverage) is in demand in response to the rise in losses from business email compromise (BEC) scams. A number of cyber insurers have started offering cyber crime policies that provide coverage for losses due to funds transfer fraud and cyber deception.

Property Damage and Bodily Injury: Several insurers have started offering limited coverage that addresses property damage and bodily injury from a cyberattack. These products have been developed in response to the increasing incidence and threats of attacks targeting commercial industries that can lead to equipment failure, physical damage to property and physical harm to people. Companies in critical infrastructure industries, such as oil and gas, chemicals, power and utility, and transportation have a growing need for this type of cover. Products typically address coverage gaps in a customer's existing commercial lines program.



Social Media/Networking: Insurers have developed products that can be added to cyber policies to cover a company's media and/or social networking activities. Some policies now provide coverage for certain social media liability exposures such as online defamation, advertising, libel and slander. Intellectual property rights may also be covered.

Cyber Insurance: Legal Environment

In its *sigma* publication Swiss Re noted that the recent rise in cyber-related litigation is only expected to increase.[44] There have been several recent legal developments in the cyber arena.

Data Breach Liability

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 actions 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 in 2014 upheld the power of the Federal Trade Commission (FTC) to sue companies that fail to protect their customers' data.[45] 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 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.[46]

For example, over 70 class actions lawsuits alone were filed against Target following its 2013 breach. According to one legal expert, for some plaintiffs' lawyers this was "the Black Friday door buster to end all others."[47] And an April 2011 hacking of Sony's PlayStation online services led to the filing of more than 50 class action complaints in the United States.

> 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.

Plaintiffs 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 as well as punitive damages. Target and other companies may also face class actions from banks and credit unions seeking damages for administrative expenses, lost interest, transaction fees and lost customers.

Settlements can be huge. In March 2015, a federal judge gave preliminary approval to a $10 million settlement in just one Target class action.[48] In August 2015, Target agreed to pay up to $67 million to settle with Visa Inc. on behalf of banks and other firms that issue credit and debit cards. The amount would compensate card issuers for the costs of issuing new cards, adding more call center staff to handle customer queries and the costs of the actual fraud. In December 2015, Target also agreed to a $39 million settlement with several U.S. banks that service MasterCard.

As of January 2016, Target estimated it had already accrued $291 million in expenses related to the data breach, with some $90 million expected to be offset by insurance. That estimate was based on the prospect of settling many lawsuits.

A total of 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—one of the costliest data breaches of all time. 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.

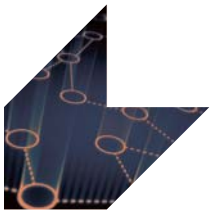
Data Breach Insurance Coverage

Companies that have suffered a data breach look to their insurance policies for coverage to help mitigate some of the enormous costs. The increasing uptake of cyber liability policies and rising claims makes it inevitable that coverage disputes will arise. The fact that there is no standard cyber insurance form means that individual policy terms and conditions may vary greatly.

In one of the first decisions interpreting a cyber insurance policy, the U.S. District Court in Arizona on May 31, 2016, held that a cyber insurance policy issued by Federal Insurance Co. (Chubb) does not cover liabilities to credit card issuers arising from a 2014 data breach at P.F. Chang's China Bistro.

When a stolen credit card number is fraudulently used, the bank that issued the credit card is financially responsible for paying the fraudulent charge. It also incurs the cost of delivering a new credit card to the consumer. If a retailer's data breach was behind the fraud, the bank has legal agreements that let it indirectly recover its costs from the retailer responsible for the breach. One such agreement left P.F. Chang with an assessment of just under $2 million. The restaurant chain filed a claim against its cyber insurance policy.

P.F. Chang lost. The court found that losses arising from these assessments are not covered losses, at least not under this specific insurance policy. It's important to note that in reaching its decision, the court turned to cases analyzing commercial general liability (CGL) policies for guidance because cyber policies are relatively new to the market, but the fundamental principles are the same. Also of note is the fact that Federal Insurance did pay approximately $1.7 million for P.F. Chang's damages related to forensic and defense costs. These damages were not at issue under the policy.[49]



Despite the fact that most traditional CGL policies are not designed to cover cyberrisks, there have been various legal actions and differing opinions on the application of standard form CGL policies to data breach incidents. However, many insurers have adopted ISO's May 2014 cyber exclusions for CGL policies, which has reduced the chances of insureds finding coverage under traditional policies.

One high profile case followed the April 2011 data breach involving tens of millions of Sony PlayStation Network users. A New York trial court had ruled that Zurich American Insurance Co. owed no defense coverage to Sony Corp. or Sony Computer Entertainment America LLC. In his February 2014 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.[50] However, in early May 2015, it was reported that Sony and Zurich had reached a settlement, though terms were not disclosed. As a result, legal experts say the precedential value of Judge Oing's opinion will be diminished, as it should remain an outlier trial court decision.[51]

Changes in Cyber Insurance Pricing and Capacity

While the market is growing rapidly, the exact number of companies in the United States and elsewhere that have a policy has been difficult to determine. But new reporting requirements developed by the National Association of Insurance Commissioners (NAIC) give us a first glimpse of the cyber insurance policies issued in the U.S. marketplace.

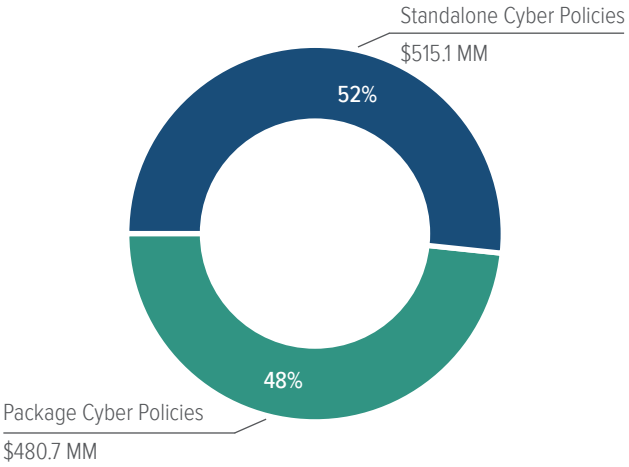
Based on the NAIC Cybersecurity and Identity Theft Coverage Supplement for insurer financial statements, a total of 117 U.S. insurers reported writing some cyber insurance premiums in 2015. Direct premiums written were $993 million in 2015, while the number of in-force policies totaled 1.5 million.[52]

Aon Benfield reports that 48 insurers wrote more than $1 million in cyber premiums in 2015. Only seven insurers reported written premiums over $50 million. The top five accounted for 61 percent of premiums, and the top 10 accounted for 80 percent. As the market expands, premiums for the smaller insurers are expected to expand as well, broadening the distribution of premium in the market.

Cyber insurance was profitable in 2015, with a 49.0 percent average loss ratio across all insurers, though individual insurer results deviated greatly. Loss ratios among the top 20 underwriters varied between zero

Fig. 10

Package Policies Make Up Just More Than Half Of All Cyber Insurance Premium



Source: NAIC Cybersecurity and Identity Theft Coverage Supplement, 2015.

percent at the low end to 161 percent at the high end, according to Aon's analysis.

Of the $993 million in total premium reported in 2015, packaged cybersecurity policies accounted for $515.1 million, or 52 percent, while stand-alone cybersecurity policies accounted for $480.7 million, or 48 percent **(Fig. 10)**.

Since a significant amount of the coverage is written via Lloyd's and other international insurance markets that do not report to the NAIC, actual U.S. premiums are likely considerably higher.

Whatever the precise number of U.S. companies buying cyber insurance may be, Swiss Re estimates that by 2025 cyber coverage will be included in every retail, commercial and industrial insurance policy.[53]

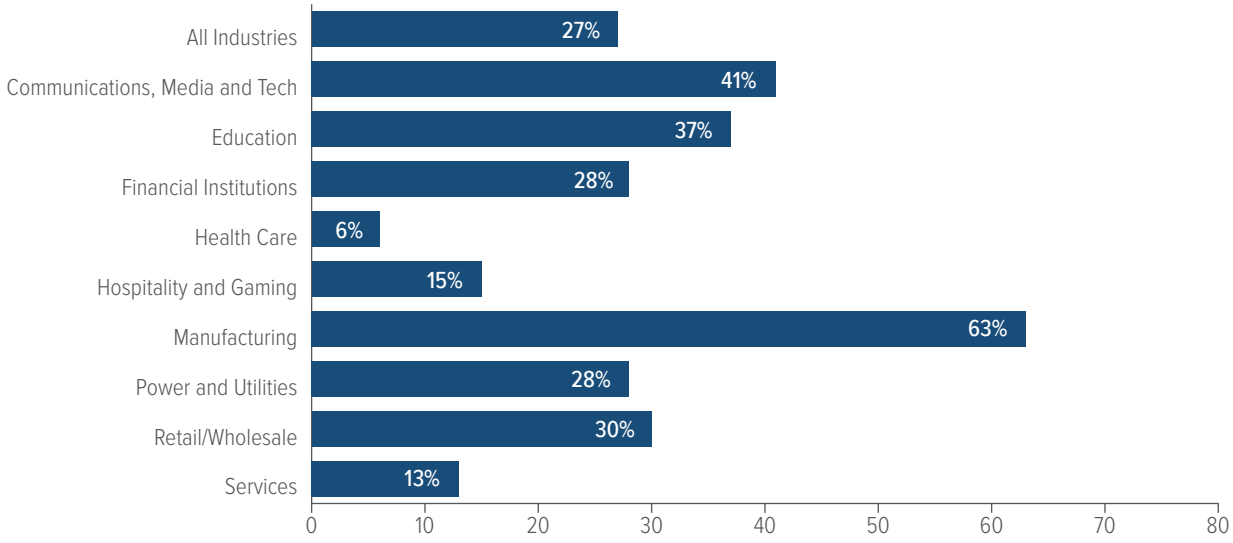
Latest market analysis indicates a continued pattern of strong growth in cyber insurance purchasing.[54] A March 2016 market briefing from broker Marsh notes an increasing awareness and appreciation of the risk, from the boardroom to the data center. In the face of an evolving risk landscape and an aggressive regulatory environment, organizations no longer treat cyber as a problem to be fixed, but rather as a risk to be managed, Marsh said.

In 2015, the number of Marsh clients purchasing stand-alone cyber insurance increased by 27 percent over 2014 **(Fig. 11)**. Critical infrastructure industries—including chemical, communications, energy, health care, and transportation—show more interest in the coverage, particularly related to business interruption losses. After the 2015 blackout caused by a cyberattack on an electricity provider in Ukraine, the power and utilities sector showed notable growth in the purchase of cyber insurance, with a 28 percent increase in the number of Marsh clients purchasing coverage in 2015 over 2014.

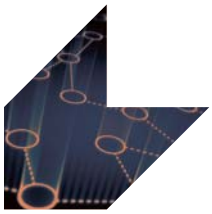
Companies are also buying higher limits. Cyber insurance limits purchased in 2015 averaged $16.9 million across all industries and all company

Fig. 11

Stand-alone Policies Grew By More Than 25 Percent Among Marsh Clients



Source: *Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise*, Marsh Risk Management Research Briefing, March 2015.



sizes, a 15 percent increase over the average of $14.7 million in 2014, Marsh says **(Fig. 12)**.

Among larger companies, which tend to have greater exposure to cyberrisk, average limits purchased were $39.2 million, up 15 percent from an average of $34.2 million in 2014 **(Fig. 13)**.

Large communications, media and technology organizations purchased the highest average limits—$86.7 million—of any industry. Large financial institutions witnessed an 18 percent increase in average limits purchased in 2015 over 2014.

Companies may not be buying enough cover, however. An earlier study by Marsh based on the data output of its proprietary statistical model—the Cyber IDEAL—found that the exposure facing many organizations eclipses the risk transfer programs they have implemented.[55] For example, retailers with revenues between $5 billion and $20 billion on average will buy an aggregate limit of $23 million. However, a hypothetical retailer in that bracket may have a much higher exposure than that average limit **(Fig. 14)**.

For a retailer with $12 billion in annual revenues that holds a maximum 75 million records, Cyber IDEAL indicates that a one-in-100 data breach event could result in the exposure of more than 21 million records with costs exceeding $340 million, or nearly 12 times the average limits purchased. Such an event could potentially create an enterprise-threatening risk, before even accounting for the risk to reputation, Marsh said.

As for rates, during 2015 markets remained challenging for certain industries—notably retail and health care—and for insureds with significant losses. Insurer competition remains strong for business outside of high-exposure classes, however. Average rate increases at renewal for both primary layers and total programs—as measured by average annual changes in the year-over-year price per million of limits—were lower in the latter half of the year than in the first half of 2015. The average primary rate per million rose at 18.5 percent in the first quarter of 2015, dropping to 12.1 percent in the fourth quarter **(Fig. 15)**.

Marsh reports that the market was challenged by a growing recognition that organizations increasingly rely upon technology for essential operations, and are thus looking for coverage beyond indemnification for privacy breach costs.

Market capacity remained abundant at more than $500 million, but total program size varied by industry as well as the types of coverage options elected. Most large towers comprise between $200 million and $400 million in limits, Marsh noted. No insurers of significant size entered the market in the last quarter of 2015, but individual insurer appetites continued to develop, with carriers differentiating around such areas as attachment points, deployed limits and followed coverages.

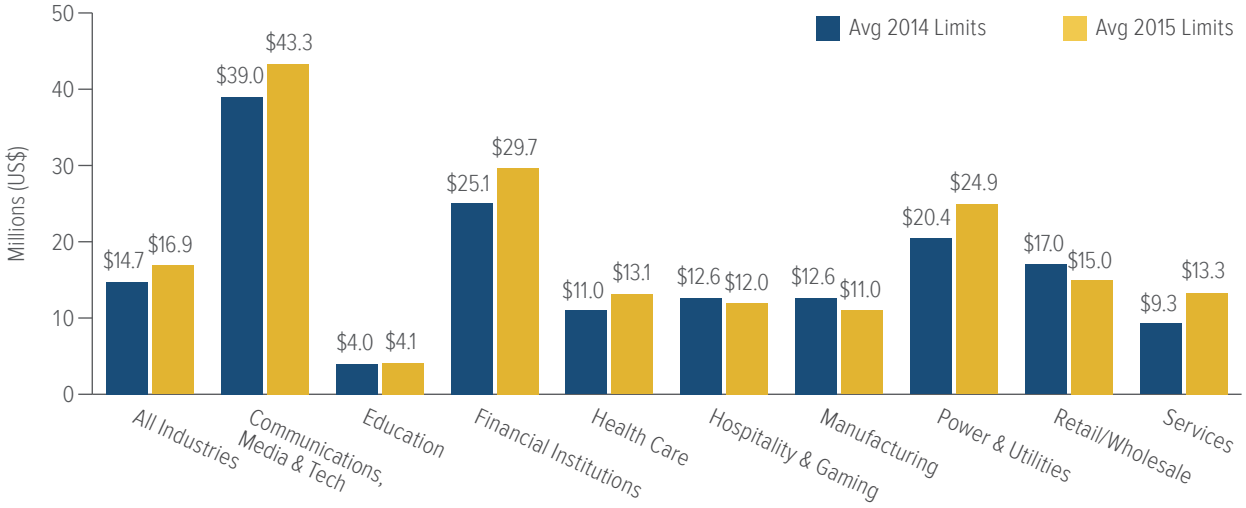
Obstacles to Writing Cyber Coverage

Cyberrisk remains difficult for insurance underwriters to quantify for a number of reasons, including:

- **Complexity of Risk:** The definition of cyber risk is rapidly evolving and expanding. Attacks are increasing sophisticated. The range of perpetrators, targets and exposures at stake ever broadens. It is a constant challenge for C-suite executives, boards of directors, cybersecurity experts, IT professionals, law enforcement, governments and insurers to keep pace. In addition to damaged or lost assets and business interruption, attacks can result in costly investigations, litigation and settlements as well as

Fig. 12

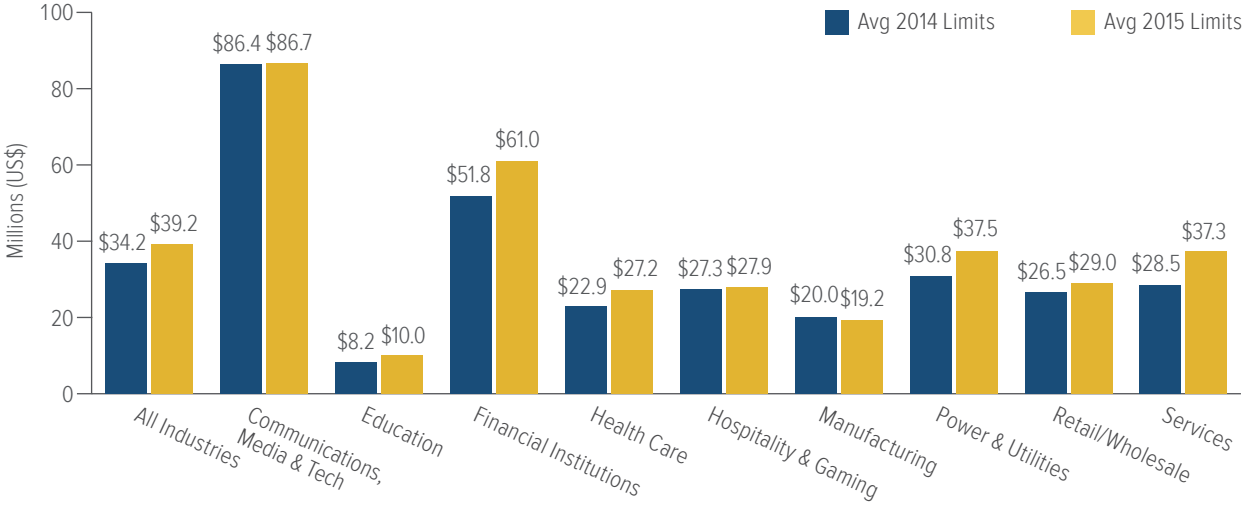
The Average Limit Purchased For Cyber Liability Insurance Rose to $16.9 Million in 2015



Source: *Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases*, Marsh Global Analytics, March 2016.

Fig. 13

Among Larger Companies The Average Total Limit Purchased Grew To $39.2 Million In 2015.



Source: *Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases*, Marsh Global Analytics, March 2016.

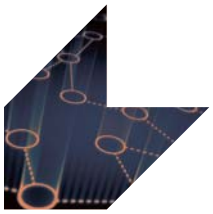
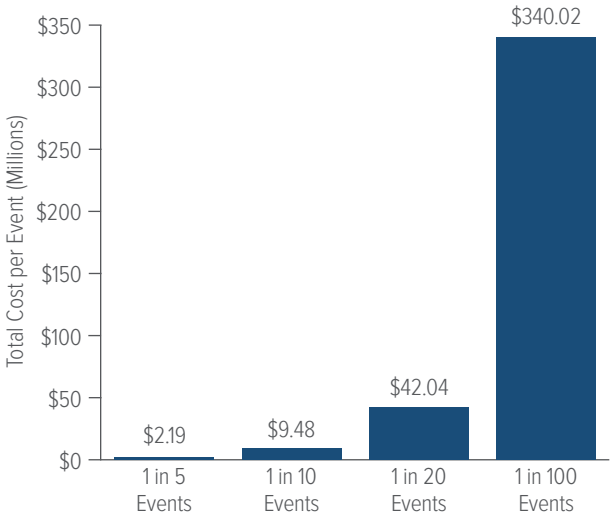


Fig. 14

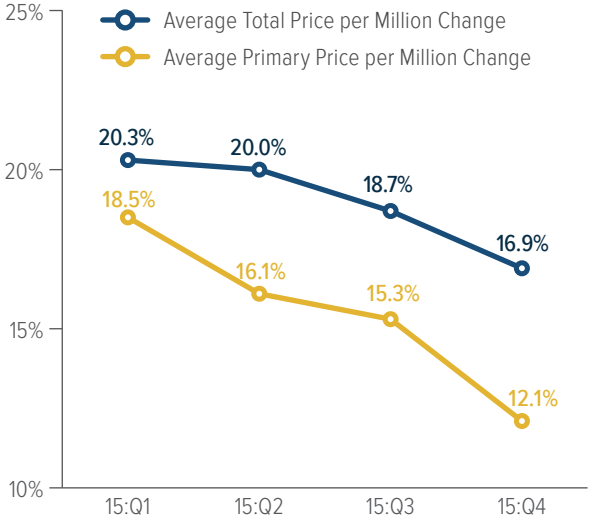
A One-In-100 Data Breach Could Cost $340 Million



Source: *A Cybersecurity Call to Action*, Marsh & McLennan Cos, The Chertoff Group, November 2014

Fig. 15

Rates For Cyber Cover Rose In 2015 For Both Primary And Excess Layers, But At A Declining Rate

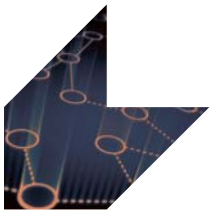


Source: *Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases*, Marsh Global Analytics, March 2016.

reputation damage, with the potential knock-on effect on a company's customer base, stock price and earnings. Insurance industry leaders have acknowledged that there could be inescapable limitations on the capacity of the market to handle the demand for cyber insurance for both public and private sectors.[56]

- **Lack of Historical Data:** Although many costly events have occurred, there is a lack of historical data for cyberrisk, making it difficult for insurers to write and price policies appropriately. While there is no standard form for the coverage, catastrophe modelers and insurers are working together to develop common data standards for use in risk models. Earlier this year Lloyd's and the Lloyd's Market Association teamed up with catastrophe modelers AIR Worldwide and RMS along with the Cambridge Center for Risk Studies, to develop a set of common core data requirements.[57] The goal is to develop a standardized approach to identify, quantify and report cyber exposure data across the insurance industry. Several catastrophe modelers and brokers have launched tools and models to manage cyberrisks.[58] Aggregation and accumulation risk is a particular focus of modelers. Guy Carpenter recently formed a strategic alliance with cybersecurity specialist Symantec to create a cyber aggregation model.[59] Surveys can help identify and track trends, but they do not provide an adequate basis for actuarial analysis. Last year ratings agency A.M. Best[60] noted: "The quantifying of risks and rewards to insureds has not reached a reliable level of actuarial data and consequence-oriented analytics, which is needed for accurate pricing of the premiums and establishing appropriate reserves." This lack of actuarial data is holding back the growth in market capacity, industry players say.[61]

- **Risk Accumulation and Aggregation Uncertainty:** Cyberattacks have the potential to be massive and wide-ranging. Risk accumulation—in which a single event spans multiple risks affecting companies, countries, industries and lines of business—is a growing concern and creates the potential for catastrophic risk.[62] A "cyber hurricane" event, in which tens or hundreds of thousands of systems are compromised by a common event could result in potentially catastrophic numbers of insurance claims.[63] The Heartbleed security flaw, disclosed in April 2014, is just one example of this type of vulnerability. Another source of concern is cloud computing. The breach of a cloud service provider could affect many customers around the world, many of whom might share the same insurer. Several insurers have warned that the scope of the exposures is too broad to be covered by the private sector alone.[64] At least one has described cyber as a "systemic risk" and proposed government cover akin to the terrorism risk insurance programs in place in several countries.[65]



CONCLUSION

A proliferation of high profile attacks and data breaches ensures that businesses, governments, law enforcement, security experts and consumers around the world are paying close attention to the risks of cyberspace and developing a corresponding response.

As technologies evolve, companies of all sizes are potentially exposed to even greater risks. The Internet of Things means that billions of connected things could be vulnerable to attack, and the onus is on manufacturers to prioritize security and reduce the risks. This level of awareness and scrutiny has put increased pressure on government leaders, legislators and regulators to address the risk.

As information-sharing of attacks in the United States becomes tied to limiting liability in the corporate world, the question of how to balance privacy with transparency remains a major challenge. Still, companies need to demonstrate that the information provided by their customers and clients is properly safeguarded.

There is greater acceptance that insurance has an important role to play in mitigating some of the costs that arise from data breaches and attacks. However, insurance is not a fail-safe.

Cyberrisks remain challenging for insurers to underwrite for a number of reasons.

- The complex and rapidly shifting nature of cyberrisk means there is a constantly changing range of perpetrators, targets and exposure values at stake;
- A lack of historical actuarial data makes it difficult for insurers to write and price policies appropriately, though a more consistent approach to capture data and model risk is now underway;
- The interconnected nature of cyberspace creates considerable uncertainty around risk accumulation and aggregation, making it difficult for insurers to assess the likely severity of attacks.

How insurers manage these risks while creating products for this multi-billion dollar market opportunity as the legal and regulatory landscape becomes more defined will determine how best we all are protected from cyberrisks in the years to come.

Appendix I

Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities

Source: The White House, Office of the Press Secretary

On April 1, 2015, President Obama issued an executive order which enables U.S. government agencies to block the assets of any foreign person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in or to have directly or indirectly engaged in malicious cyber-enabled activities.

These activities encompass those that originated from or were directed by persons located, in whole or in substantial part, outside the U.S. that are reasonably likely to result in, or have materially contributed to, a significant threat to U.S. national security, foreign policy or economic health or financial stability and that have the purpose or effect of:

- Harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
- Significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
- Causing a significant disruption to the availability of a computer or network of computers; or
- Causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

The Cyber-Security Executive Order

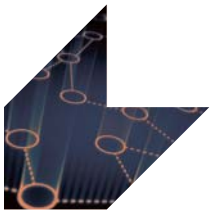
Source: Mayer Brown Legal Update, February 13, 2013

On February 12, 2013, President Obama issued a cyber security 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 June 2016.

Cyber Act of War Act (H.R. 5220 and S. 2905)

Summary: Would require the administration to develop a policy to determine when a cyberattack rises to the level of warfare.

Protecting Cyber Networks Act (H.R. 1560)

Passed House 4/22/2015

Summary: Amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal or local governments; and (2) the sharing of imminent or ongoing cyber security threats with such entities to prevent or mitigate adverse impacts. Provides liability protections, if the following activities are conducted in accordance with this title, to: (1) private entities that monitor information systems; or (2) non-federal entities that share, receive, or fail, in good faith, to act upon shared indicators or defensive measures.

Data Breach Notification and Punishing Cyber Criminals Act of 2015 (S. 1027)

Summary: Would require notification of information security breaches and enhance penalties for cyber criminals.

National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731)

Passed House 4/23/2015

Summary: Amends the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cyber security risks and strengthen privacy and civil liberties protections, and for other purposes. Provides liability protections to companies acting in accordance with the Act that: (1) conduct network awareness; or (2) share indicators or defensive measures or fail to act based on such sharing.

Cybersecurity Information Sharing Act of 2015 (S. 754)

Passed Senate October 2015, Signed into law December 2015

Summary: Requires the Director of National Intelligence (DNI), the Department of Homeland Security (DHS), the Department of Defense (DOD) and the Department of Justice (DOJ) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal or local governments; (2) the sharing of unclassified indicators with the public; and (3) the sharing of cyber security threats with entities to prevent or mitigate adverse effects. Provides liability protections to entities acting in accordance with the Act.

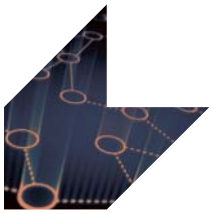
Cyber Privacy Fortification Act of 2015 (H.R. 104)

Summary: Would amend the Federal criminal code to provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information. Requires a person who owns or possesses data in electronic form containing a means of identification and who has knowledge of a major security breach of the system containing such data to provide prompt notice to the U.S. Secret Service of the Federal Bureau of Investigation.

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).

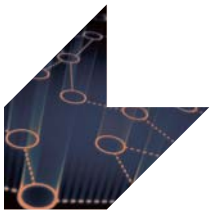
In 2016, at least 25 states introduced legislation expanding the scope of laws, setting additional requirements related to notification or changing penalties for those responsible for breaches.



Sources and Endnotes

1. World Economic Forum, *Global Risks 2016, 11th Edition*.
2. ESADEgeo (Center for Global Economy and Geopolitics) and Zurich, *Global cyber governance: preparing for new business risks*, Risk Nexus, April 2015.
3. Current statistics found at Identity Theft Resource Center.
4. Randy Maniloff, White and Williams LLP, "There Aren't As Many Cos. With Cyberinsurance As You Think," *Law360.com*, February 24, 2014.
5. Craig A. Newman, "Target's Cyber Insurance: A $100 Million Policy vs. $300 Million (So Far) In Costs," *The Data Security Law Blog of Patterson Belknap Webb & Tyler LLP*, April 7, 2016.
6. Allianz Risk Barometer 2016, January 2016.
7. Symantec, 2016 Internet Security Threat Report, Volume 21, April 2016.
8. Gartner, press release, November 10, 2015.
9. "Two arrested for stealing Jeeps—using laptops", *USA Today* and *KHOU-TV,* August 4, 2016.
10. Andy Greenberg, "After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix," *Wired*, July 24, 2015.
11. Kim Zetter, "Medical Devices That Are Vulnerable To Life-Threatening Hacks," *Wired*, November 24, 2015.
12. Cloud Security Alliance, *The Treacherous 12: Cloud Computing Top Threats in 2016*, February 29, 2016.
13. Malwarebytes™, "Major International Study Finds Nearly 40 Percent of Enterprises Hit By Ransomware in the Last Year," press release, August 3, 2016.
14. Federal Bureau of Investigation, *Incidents of Ransomware on the Rise*, April 29, 2016.
15. Symantec, *2016 Internet Security Threat Report*, Volume 21, April 2016.
16. McAfee Labs, *2016 Threats Predictions*, November 2015.
17. Federal Bureau of Investigation, *Business Email Compromise: An Emerging Global Threat,* August, 28, 2015.
18. Rick Betterley, editor of the *Betterley Report*, interviewed on WRIN.tv, February 20, 2015.
19. Rosalie Donlon, "Small, mid-sized businesses hit by 62% of all cyber attacks," *Propertycasualty360.com*, May 27, 2015.
20. Oliver Ralph, "Cyber Villains Pose Greater Threats to Smaller Companies," *The Financial Times*, June 1, 2016.
21. Steve Morgan, "CyberSecurity Market Reaches $75 billion in 2015; Expected to Reach $170 Billion By 2020," *Forbes*, December 20, 2015.
22. PwC, *The Global State of Information Security Survey 2016*.
23. Richard Betterley, "Cyber/Privacy Insurance Market Survey—2016," *The Betterley Report,* June 2016.
24. Damian Paletta, "Obama Calls For Tough Legislation to Combat Cyber-Attacks," *The Wall Street Journal*, January 20, 2015.

25. Statement by the President on Executive Order *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*.
26. International Institute for Counter-Terrorism (ICT), Cyber-Terrorism Activities, Report No. 14, July–September 2015, and Report No. 10, July-September 2014.
27. International Institute for Counter-Terrorism (ICT), Alert (IR-ALERT-H-16-056-01), Cyber Attack Against Ukrainian Critical Infrastructure, February 25, 2016.
28. ICS-CERT Monitor, November/December 2015.
29. Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, May 30, 2011.
30. Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 – Cybersecurity, October 13, 2011.
31. Robert Hartwig, interview by Kenneth Simon, WRIN.tv, April 13, 2015. At the time, Dr. Hartwig was president of the Insurance Information Institute.
32. Matthew Sturdevant, "When Terrorists Attack Online, Is Cyber-Insurance Enough?," *Hartford Courant*, January 26, 2015.
33. McAfee and the Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II*, June 2014.
34. Ponemon Institute, *2015 Cost of Cyber Crime Study: United States*, October 2015.
35. In the context of the Ponemon study, an external cost is one that is created by external factors such as fines, litigation of marketability of stolen intellectual properties.
36. Ponemon Institute (research sponsored by IBM), *2016 Cost of a Data Breach Study: Global Analysis*, June 2016.
37. Verizon, *2015 Data Breach Investigations Report*, April 2015.
38. Ponemon Institute (research sponsored by IBM), *2014 Cost of a Data Breach Study: Global Analysis*, May 2014.
39. Richard Betterley, "Cyber/Privacy Insurance Market Survey—2016," *The Betterley Report*, June 2016.
40. Allianz Global Corporate & Specialty, press release, July 10, 2013.
41. Stuart Poole-Robb, "Here's why the cyber insurance industry is worth £55.6 billion," *ITProPortal.com,* February 7, 2015.
42. "New ISO Cyber Endorsements for Small, Medium Businesses Now Available," *Insurance Journal,* March 4, 2015.
43. *Cybersecurity Brief,* National Association of Insurance Commissioners, updated February 13, 2015.
44. "Liability Claims Trends: Emerging Risks And Rebounding Economic Drivers," Swiss Re *sigma* No. 4/2014.
45. "Court Upholds FTC's Power to Sue Hacked Companies," *National Journal Online*, April 7, 2014.



46. *Trends in Data Breach Cybersecurity Regulation, Legislation and Litigation*, Mayer Brown, April 17, 2014.
47. Randy J. Maniloff, "Measuring the Bull's-Eye on Target's Back: Lessons From the T.J. Maxx Data Breach Class Actions," *Coverage Opinions*, January 15, 2014.
48. Hiroko Tabuchi, "$10 Million Settlement in Target Data Breach Gets Preliminary Approval," *The New York Times*, March 19, 2015.
49. Tressler LLP, "The Future is Now: Court Finds No Coverage Under Cyber Policy For P.F. Chang's Data Breach," *Privacy Risk Report,* June 9, 2016.
50. Young Ha, "N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation," *Insurance Journal*, March 17, 2014.
51. Young Ha, "Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York," *Insurance Journal*, May 1, 2015.
52. *Cyber Update: 2015 Cyber Insurance Profits and Performance,* May 2016, Aon Benfield Analytics.
53. Michel M. Lies, "How Do You Insure Against Cybercrime?," *The Experts* (blog)*, The Wall Street Journal*, April 21, 2015. Lies is group chief executive of Swiss Re.
54. "Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases," *Marsh Risk Management Research Briefing*, March 2016.
55. *A Cybersecurity Call to Action*, Marsh & McLennan Cos., The Chertoff Group, November 2014.
56. Mark Hollmer, "Cyber Attacks Increasing on Public-Sector and Non-Profit Targets," *Carrier Management*, March 12, 2015.
57. "Lloyd's Develops Standardized Data Requirements for Cyber Risks," *Insurance Journal*, January 19, 2016.
58. Robert Lenihan, "Modeling Firms Take First Look at Cyber Risks," *Business Insurance,* May 29, 2016.
59. Guy Carpenter, Guy Carpenter Forms Strategic Alliance to Develop Cyber Aggregation Model, press release, May 17, 2016.
60. A.M. Best, "Cyber Security Presents Challenging Landscape for Insurers and Insureds," *Best's Special Report*, Issue Review, December 5, 2014.
61. Ben Beeson, vice president, Cyber Security and Privacy, Lockton Cos, testimony before the U.S. Senate Commerce Committee Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security Hearing: *Examining the Evolving Cyber Insurance Marketplace*, March 19, 2015.
62. "Liability Claims Trends: Emerging Risks And Rebounding Economic Drivers," *Swiss Re sigma* No. 4/2014.
63. *The Betterley Report*, "'Maybe Next Year' Turns Into 'I Need It Now,'" Cyber Privacy/Insurance Market Survey – 2014, June 2014.
64. Catherine Mulligan, senior vice president, Management Solutions Group, Zurich, testimony before the U.S. Senate Commerce Committee Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security Hearing: *Examining the Evolving Cyber Insurance Marketplace*, March 19, 2015.
65. Alistair Gray, "Cyber risks too big to cover, says Lloyd's insurer," *The Financial Times,* February 5, 2015.