

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



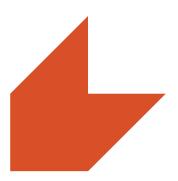
# Cyber Risk:

# Threat and opportunity

October 2015

Robert P. Hartwig, Ph.D., CPCU President & Economist 212.346.5520 bobh@iii.org

Claire Wilkinson Consultant 917.459.6497 clairew@iii.org



# EXECUTIVE SUMMARY

- Interest in cyber insurance and risk has grown beyond expectations in 2014 and 2015 as
  a result of high profile data breaches, including a massive data breach at health insurer
  Anthem that exposed data on 78.8 million customers and employees and another at
  Premera Blue Cross that compromised the records of 11 million customers. The U.S.
  government has also been targeted by hackers in two separate attacks in May 2015 that
  compromised personnel records on as many as 14 million current and former civilian
  government employees. A state-sponsored attack against Sony Pictures Entertainment,
  allegedly by North Korea, made headlines in late 2014.
- Cyber attacks and breaches have grown in frequency, and loss costs are on the rise. In 2014, the number of U.S. data breaches tracked hit a record 783, with 85.6 million records exposed. In the first half of 2015, some 400 data breach events have been publicly disclosed as of June 30, with 117.6 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. More than
  60 carriers now offer stand-alone cyber insurance policies and insurance broker Marsh
  estimates the U.S. cyber insurance market was worth over \$2 billion in gross written
  premiums in 2014, with some estimates suggesting it has the potential to grow to \$5 billion
  by 2018 and \$7.5 billion by 2020. Industry experts indicate rates are rising, especially in
  business segments hit hard by breaches over the past two years.
- Some observers believe that cyber exposure is greater than the insurance industry's ability
  to adequately underwrite the risk. Cyberattacks 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. 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 technologies, combined with the increasing complexity of cyber threats and changing regulatory expectations, is propelling the cyber risk landscape into uncharted territory.

Economic thought leaders have warned that the Internet of Things (IoT) is likely to disrupt business models and ecosystems across a range of industries.¹ While this will bring innovation, such radical change at the same time across major organizations in multiple industries also raises the potential for systemic risks, including large-scale disruption in labor markets and financial market volatility.

Meanwhile, emerging technologies such as drones, additive manufacturing (3-D printing, for example), Internet-connected home appliances and autonomous vehicles could also disrupt established business practices and create new security threats, fundamentally changing the nature of cyber risks.<sup>2</sup> Effective global governance will be critical to manage evolving cybersecurity and privacy risks going forward.

# Number and Impact of Data Breaches Continues to Rise

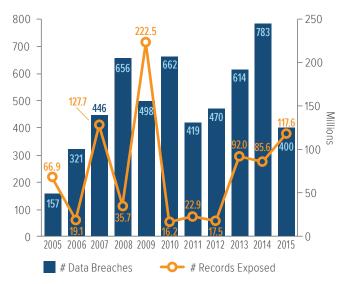
In 2014 the number of U.S. data breaches tracked hit a record high of 783, with 85.6 million records exposed, according to the Identity Theft Resource Center (Fig. 1).<sup>3</sup>

This represents a 27.5 percent jump from the 614 breaches reported in 2013 and an 18.3 percent increase over the previous high of 662 data breaches tracked in 2010.

And the trend continues—in the first half of 2015, some 400 data breach events have been publicly disclosed as of June 30, 2015, with 117.6 million records exposed.

Fig. 1

## Number of Data Breaches/ Millions of Records Exposed\*



\*Figures as of June 30, 2015. Source: Identity Theft Resource Center.

High-profile breaches include a state-sponsored attack against Sony Pictures Entertainment, allegedly sponsored by North Korea, which was the defining cyber intrusion of 2014. The hacker break-in involved the theft of unreleased motion pictures as well as more than 25 gigabytes of sensitive data on tens of thousands of Sony employees, including Social Security numbers and medical and salary information.



It caused a major shutdown of the company's computer systems. A trove of sensitive and sometimes embarrassing emails sent by senior Sony executives was also released.

Two recent incidents involved attacks on the health insurance industry. At Anthem, hackers gained access to a corporate database containing the personally identifiable information on 78.8 million of the health insurer's current and former U.S. customers and employees. Anthem has since stated that anywhere from 8.8 million to 18.8 million non-customers could have been impacted by the breach. Meanwhile, Premera Blue Cross suffered a network intrusion in March that compromised the financial and medical records of 11 million customers.

Other recent victims include well-known brands such as Staples, Home Depot, JP Morgan Chase, P.F. Chang's, eBay, Snapchat and Target.

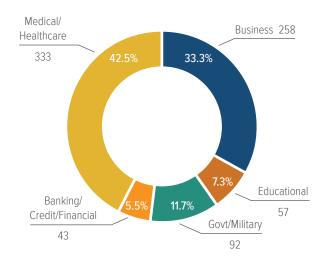
The U.S. government was targeted by hackers who broke into the Office of Personnel Management and Interior Department systems twice in May 2015, stealing records on as many as 14 million current and former civilian U.S. government employees.

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 783 data breaches in 2014 hit business and medical/healthcare organizations, according to the Identity Theft Resource Center (Fig. 2).

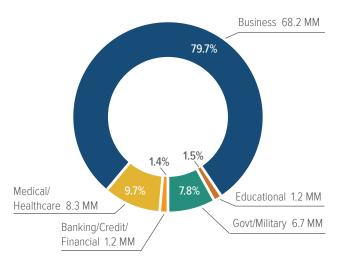
Business organizations accounted for the majority of records exposed by data breaches in 2014 (Fig. 3).

2014 Data Breaches By Business
Category, By Number of Breaches



Source: Identity Theft Resource Center.

2014 Data Breaches By Category, By Number of Records Exposed



Source: Identity Theft Resource Center.



Recent 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."

The fact that Target had \$100 million in network security insurance has been widely reported.<sup>5</sup> As of the end of January 2015, Target estimated it had already accrued \$252 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 cyber insurance coverage and that insurance would cover some

\$27 million of the retailer's breach recovery costs.
Sony Pictures had some \$60 million in cyber insurance coverage in place at the time of its latest breach, after consolidating coverage with Sony Corp. of America.

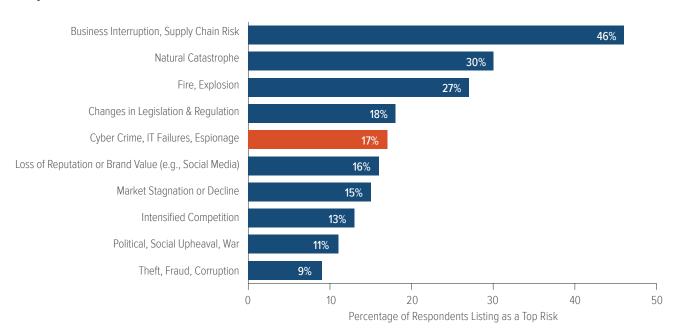
#### The Threat to Businesses

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 risk moved into the top 5 global business risks in 2015, according to the fourth annual Allianz Risk Barometer Survey, climbing up to No. 5 from No. 8 (Fig. 4).6

Fig. 4

Top 10 Global Business Risks for 2015



Source: Allianz Risk Barometer on Business Risks 2015.



All industries Allianz surveyed found cyber risks to be more of a concern than last year, with financial services, manufacturing, power and utilities and engineering sectors the most influential in ranking cyber risks higher.

### Other survey highlights:

- Loss of reputation (61 percent) is the main cause of economic loss after a cyberattack followed by business interruption (BI) (49 percent) and damages paid due to loss of customer data (45 percent).
- Data theft and manipulation (64 percent), loss of reputation (48 percent) and increased threat of persistent hacking (44 percent) are the cyber risks companies fear most.
- Cyber risks are also the most commonly underestimated risks by businesses, according to Allianz.
   Respondents' major concerns include the potential impact on a company's supply chain and the liability they could face if they are unable to deliver products on time or if they lose customer data.
- Another more recent Allianz study suggests that cyber risks are evolving far beyond privacy and reputational issues. Future threats will come from intellectual property theft, cyber extortion and the impact of business interruption following a cyberattack, or from operational or technical failure, a risk that is often underestimated.<sup>7</sup>

#### **Emerging Technology Risks**

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

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

Even automobiles are now vulnerable to hacking. 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.<sup>8</sup>

A recent survey by crowdsourced IT research company Wisegate of hundreds of its senior IT practitioner members found that Bring Your Own Devices (BYOD) and increasing adoption of cloud technology are the top risks that most impact the threat of data breaches and malware.<sup>9</sup>



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.



#### 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. Yet many do not realize they are the "soft underbelly" of cybersecurity, mistakenly believing they are too small to be attacked. Should an attack occur, they may not have adequate security.<sup>10</sup>



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

While concerns have grown, spending has not kept pace, a recent PwC report found, even as the frequency and costs of security incidents continue to rise. Smaller companies, in particular, are not spending on security, the report found.<sup>11</sup>

Companies with annual revenues less than \$100 million reduced their security spending by 20 percent in 2014, PwC noted, while medium-size organizations (revenues of \$100 million to \$1 billion) and large companies (revenues greater than \$1 billion) increased security investments by a modest 5 percent.

The study also found that midsize companies detected 64 percent more cybersecurity incidents in 2014, compared to 2013.

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. Still, PwC reports that big companies often make little effort to monitor the security of their partners, suppliers and supply chains.

#### The Threat to Government

Governments are facing an unprecedented level of cyberattacks 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." <sup>12</sup>

After the Sony 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."<sup>13</sup>

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 against cyberattack.<sup>14</sup>

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

- State-sponsored groups: Foreign governments are increasingly sponsoring cyberattacks 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 Bitcoinmake 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.

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

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 245 cyberattacks on critical infrastructure control systems in the United States between October 2013 to September 2014. The energy sector saw the most reported incidents (32 percent), while attacks against critical manufacturing comprised 27 percent).<sup>15</sup>

## Government Fights Back

In February 2014, the National Institute of Standards and Technology (NIST) released a new framework for improving critical infrastructure cybersecurity. The framework gathers existing global standards and practices to help organizations understand, communicate and manage their cyber risks. A year earlier President Obama issued an executive order that promoted increased information sharing about cyber 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.<sup>16</sup> 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 cyber risks and events.<sup>17</sup> 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 a cyberattack. For insurers, the increasingly complex and ever evolving nature of cyber 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 cybersecurity measures at the national level.

Two key cybersecurity 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 are included in the Appendices.



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

## 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 grey 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) 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.<sup>18</sup>



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, damages resulting from a cyberattack 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.<sup>19</sup>

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 cyber insurers now offer expanded cyber 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.<sup>20</sup>

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 of cybercrime comes from its damage to company performance and to national economies. Cybercrime damages

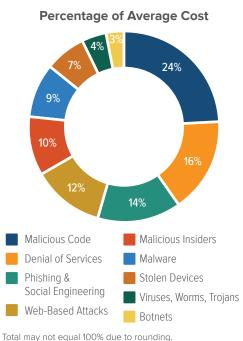
trade, competitiveness, innovation and global economic growth, according to the report.

CSIS research predicts that the opportunities for cybercrime will grow as more business activities move online and more consumers around the world connect to the Internet, and as autonomous devices are connected.

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.

#### Fig. 5

# The Most Costly Cybercrimes in the U.S., Fiscal Year 2015



Total may not equal 100% due to rounding. Source: Ponemon Institute.

# 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 million per year, an increase of \$2.3 million (19 percent) in mean value from \$12.7 million the previous year.<sup>21</sup>

The total annualized cost of cybercrime 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 cybercrimes

as a percentage of the average cost of cybercrime are those caused by malicious code, denial of services and phishing and social engineering, Ponemon said (Fig. 5).



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

On an annualized basis, information loss accounted for 42 percent of total external costs. Costs associated with disruption to business or lost productivity accounted for 36 percent of external costs (up 4 percent from the six-year average).<sup>22</sup>

The cost grows if the attack is not resolved quickly. According to the study, the average time to resolve a cyberattack 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 68 days on average to contain.

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

An earlier study by PwC also found that U.S. organizations are more at risk of suffering financial losses in excess of \$1 million due to cybercrime (Fig. 7).<sup>23</sup>

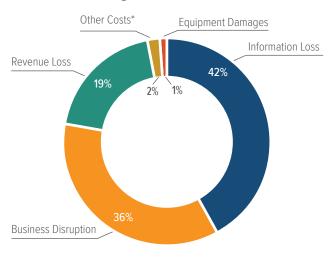
According to the study, some 7 percent of U.S. companies lost \$1 million or more, compared to just 3 percent of global organizations. In addition, 19 percent of U.S. organizations lost \$50,000 to \$1 million, compared to 8 percent of global respondents.

A global benchmark study by the Ponemon Institute of 314 companies representing 10 countries, including the United States, found that data breaches are becoming far more costly to manage and that U.S. companies suffered, on average, the most costly breaches.

Fig. 6

# External Cybercrime Costs: Fiscal Year 2015

#### **Percentage of Total External Cost**

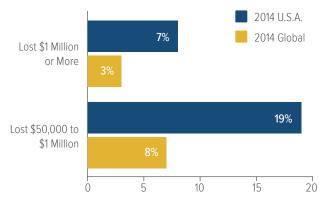


\*Other costs include direct and indirect costs that could not be allocated to a main external cost category.

Total may not equal 100% due to rounding. Source: Ponemon Institute.

Fig. 7

# **PwC Survey: Cybercrime Costs Greater** for U.S. Companies



Source: PricewaterhouseCoopers, 2014 Global Economic Crime Survey, February 2014.



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 \$5.85 million in 2014—the highest total average cost of the 10 countries—up 8 percent from \$5.4 million in 2013 (Fig. 8).<sup>24</sup> Germany had the next highest total average cost, at \$4.74 million. In contrast, samples of Brazilian and Indian companies experienced the lowest total average cost, at \$1.61 million and \$1.37 million, respectively.

The average per capita cost of a data breach for U.S. companies was \$201, compared to a \$188 average cost calculated last year. (Ponemon defines per capita cost as the total cost of data breach divided by the

breaches that resulted in the greatest number of exposed or compromised records, at 29,087.

Malicious or criminal attacks are most often the cause

size of a data breach (i.e. the number of lost or stolen

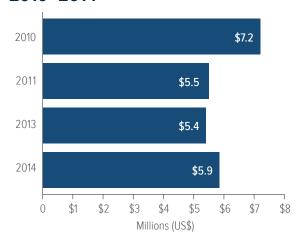
records). Also, on average U.S. companies had data

Malicious or criminal attacks are most often the cause of a data breach globally and also the most costly data breach incidents in all 10 countries, the Ponemon study found (Fig. 9). U.S. companies experience the most expensive data breach incidents, at \$246 per compromised record.

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

Fig. 8

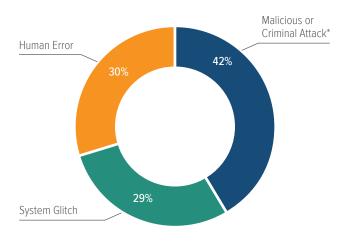
U.S. Companies: Average Organizational Cost of a Data Breach, 2010–2014



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

Fig. 9

## Main Causes of Data Breach Globally



\*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.



#### **Conflicting Information on Data Breach Costs**

A more recent study by Verizon suggests that these data breach cost estimates may be overstated.<sup>25</sup> While the Ponemon report estimates that breaches cost companies \$201 per lost record in 2014, Verizon's cost-per-record estimate is just 58 cents.

The wildly different cost estimates arise because Verizon's 2015 Data Breach Investigations Report uses only cyber liability insurance claims data from cyber 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 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 CYBER RISK

# Historical Development of Cyber Insurance

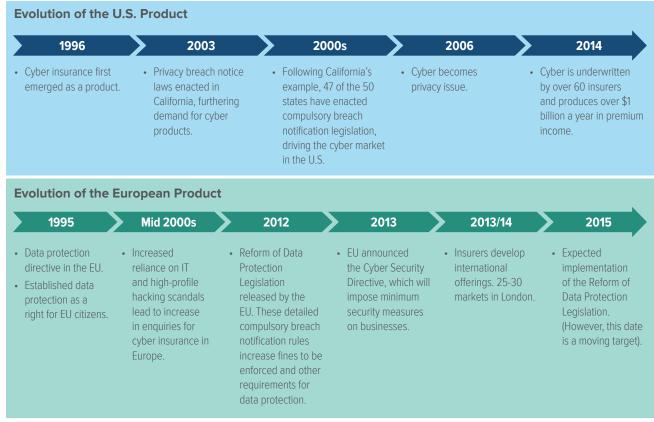
Cyber insurance in the United States evolved as a product in the mid- to late-1990s, and the market is still seen as being in its infancy (Fig. 10). Insurers have had to expand coverage for a risk that is rapidly shifting in scope and nature.

More than 60 carriers offer stand-alone cyber insurance policies, and Marsh, a major insurance broker, estimates the U.S. cyber insurance market was worth over \$2 billion in gross written premiums in 2014.

A PricewaterhouseCoopers study reported the market could grow to \$5 billion by 2018 and \$7.5 billion by 2020.

Fig. 10

## Historical Development of Cyber (Re)Insurance



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).<sup>26</sup> Industry experts say the European cyber insurance 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 cyber insurance market could grow to at least \$7.5 billion in annual premiums by the end of the decade.<sup>27</sup> 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 cyber insurance market will be worth \$85 billion and is positioning itself to be a global hub for coverage.<sup>28</sup>

#### Why Reliance on Traditional Policies Is Not Enough

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

For example, there may be coverage under a traditional property insurance policy if a cyber 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.

Cyber insurance 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.<sup>29</sup>

Most traditional commercial general liability policies do not cover cyber risks, however.<sup>30</sup> 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.<sup>31</sup>

Reliance on traditional insurance policies is therefore not enough, so specialized cyber insurance policies have been developed by insurers to help businesses and individuals protect themselves from an everevolving range of risks.



## Stand-Alone Cyber Coverage

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

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 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 as the cost of providing credit monitoring or other remediation services in the event of a covered incident.



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.



**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 cyber risk coverage can apply to both internally and externally launched cyberattacks, 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:** 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.

Property Damage and Bodily Injury: Several insurers have started offering limited cyber 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 cyberattacks 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 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.

## Cyber Insurance: Legal Environment

In its publication sigma Swiss Re noted that the recent rise in cyber-related litigation is only expected to increase.<sup>32</sup> 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 theories may be pursued, including allegations of negligence, breach of fiduciary duty and breach of contract.

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

Act have requirements to safeguard the privacy of personal information.

A federal court in New Jersey recently upheld the power of the Federal Trade Commission (FTC) to sue companies that fail to protect their customers' data.<sup>33</sup> 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.<sup>34</sup>

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." 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.

Plaintiffs typically allege that businesses failed to adequately safeguard consumer information and gave insufficient and untimely notice of the breach. In the



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.



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.<sup>36</sup> 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. Target is negotiating a similar agreement with MasterCard.

As of the end of January 2015, Target estimated it had already accrued \$252 million in expenses related to the breach. That estimate was based on the prospect of settling many lawsuits, Target said. It expected the amount to be partly offset by a \$90 million insurance payout.

A total of 25 class action lawsuits were settled in the wake of the 2007 T.J.Maxx data breach involving the theft of data related to over 45 million credit and debit cards. The settlement included: up to \$1 million to customers without receipts; up to \$10 million to customers with receipts (\$30 per claimant); \$6.5 million in plaintiffs' attorneys fees; and three free years of credit monitoring, reported to cost \$177 million.

#### **Data Breach Insurance Coverage**

Companies that have suffered a data breach look to their insurance policies for coverage to help mitigate some of the enormous costs, despite the fact that most traditional commercial general liability (CGL) policies do not cover cyber risks. The application of

standard form commercial general liability policies to data breach incidents has led to various legal actions and differing opinions.

One recent high profile case followed the April 2011 data breach 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.<sup>37</sup> However, in early May 2015, it was reported that Sony and Zurich have now reached a settlement, though terms have not been 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.38

Another high profile lawsuit between restaurant chain P.F. Chang's and its insurer Travelers Indemnity Co. of Connecticut is expected to further define how much, if any, cyber liability coverage is included in a company's CGL policy.<sup>39</sup> P.F. Chang's confirmed in June 2014 that it had suffered a data breach in which data from credit and debit cards used at its restaurants was stolen

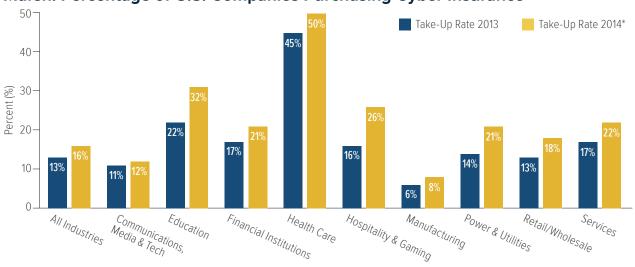
# Changes in Cyber Insurance Pricing and Capacity

Though the market is clearly growing, the exact number of companies in the United States and elsewhere that have a cyber insurance policy is difficult to determine given that individual surveys poll different numbers and types of respondents, often from a varied distribution of industry groups.



Fig. 11

Marsh: Percentage of U.S. Companies Purchasing Cyber Insurance



\*Take-up rate refers to the overall percentage of clients that purchased standalone cyber insurance.

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

#### Some examples:

- A 2015 report jointly published by the U.K. government and Marsh found that despite the growing concern among U.K. companies about the threat of cyberattacks, fewer than 10 percent have cyber insurance protection even though 52 percent of CEOs believe that their companies have some form of coverage in place.<sup>40</sup>
- A 2014 annual survey jointly produced by Advisen and Zurich found that 52 percent of companies claimed to purchase cyber liability insurance, the same percentage as in 2013.<sup>41</sup>
- A 2013 report sponsored by Experian and conducted by the Ponemon Institute stated that 31 percent of U.S. companies have a cyber security insurance policy.<sup>42</sup>
- Two 2013 reports by Willis surveyed the U.S. listed Fortune 500 and Fortune 501–1,000 firms.<sup>43</sup> In both reports, only 6 percent of companies disclosed that they purchase insurance to cover cyber risks.

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.<sup>44</sup>

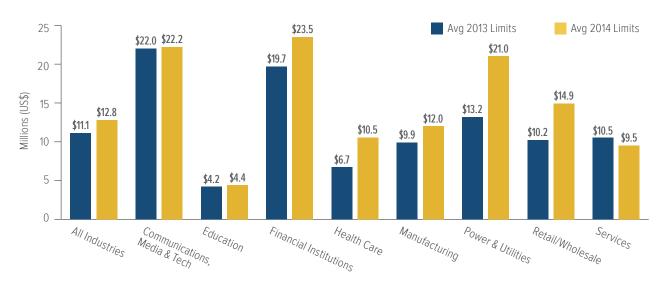
Latest market analysis indicates that the trend to purchase cyber insurance is not just continuing but accelerating.<sup>45</sup> An April 2015 market briefing from broker Marsh notes that recent high-profile data breaches, growing board-level concern, and the increasing vulnerability of operations to failure of technology appear to be influencing purchasing decisions.

In 2014, the number of Marsh clients purchasing standalone cyber insurance increased by 32 percent over 2013. The take-up rate—the percentage of Marsh financial and professional liability clients that purchased cyber insurance—rose to 16 percent (Fig. 11). Early evidence in 2015 shows continued acceleration in demand, Marsh said.



Fig. 12

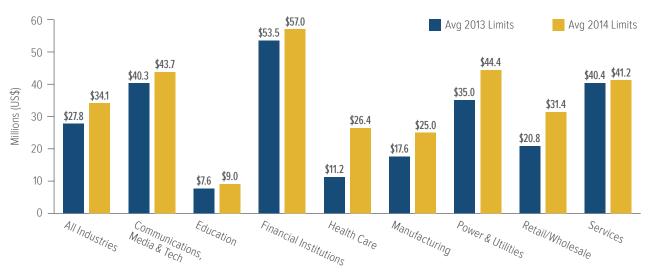
Marsh: Total Limits Purchased, By Industry – Cyber Liability, All Revenue Size



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

Fig. 13

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



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



Health care and education clients had the highest take-up rates in 2014 at 50 percent and 32 percent, respectively, followed by hospitality and gaming (26 percent) and services (22 percent).

Universities and schools continue to be targets due to the vast array of personal information they hold. This underscores the fact that the growing need for cyber insurance goes across both private and public sector entities.

Companies are also buying higher limits. Cyber insurance limits purchased in 2014 averaged \$12.8 million across all industries and all company sizes, a 15 percent increase over the average of \$11.1 million in 2013, Marsh says (Fig. 12).

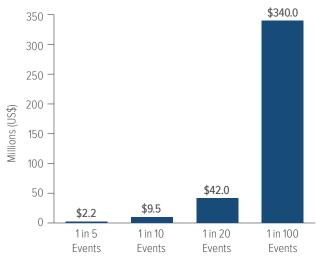
Among larger companies, which tend to have greater exposure to cyber risk, average limits purchased increased by 22 percent over 2013 (Fig. 13).

Companies may not be buying enough cover, however. Another study by Marsh based on the data output of its proprietary statistical model—the Cyber IDEAL—found that the cyber exposure facing many organizations eclipses the risk transfer programs they have implemented. 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).

As for rates, during 2014 increases in the frequency and severity of losses and near-constant headlines about attacks and outages kept premiums volatile. 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 fourth quarter than in the first quarter (Fig. 15). Industry experts point to a

Fig. 14

# Marsh: Retail Exposure for a 1-in-100 Data Breach Event\*



\*Assumptions for Retail Exposure: hypothetical retailer with annual revenues of \$12 billion, holding a maximum 75 million credit and debit card records. Source: *A Cybersecurity Call to Action*, Marsh & McLennan Cos., The Chertoff Group, November 2014.

Fig. 15

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



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



tightening of rates, terms and conditions for certain cyber risks in 2015, especially in the retail and health-care sectors hard-hit by data breaches in the last two years. Insurers are being increasingly selective about the risks they underwrite.

# Obstacles to Writing Cyber Coverage

Cyber risk 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.<sup>47</sup> 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 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.48
- Lack of Historical Data: Although many costly cyber events have occurred, there is a lack of historical data for cyber risk making it difficult for insurers to write and price policies appropriately. Surveys can help identify and track trends, but they do not provide an adequate basis for actuarial analysis. According to ratings agency A.M. Best: "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."<sup>49</sup> This lack of actuarial data is holding back the growth in market capacity, industry players say.<sup>50</sup> Several brokers, including Marsh and Willis, recently introduced new analytical tools to manage cyber risks. These models evaluate a company's potential loss exposure as a result of a data breach. Despite the challenge of capturing historical data, at least one catastrophe modeler is also reported to be developing a model for cyber risks.<sup>51</sup>

**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.52 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. 53 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.<sup>54</sup> 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.<sup>55</sup>



# CONCLUSION

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

This level of awareness has put increased pressure on government leaders, legislators and regulators to address cyber risks.

As information-sharing of cyberattacks 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 a growing acceptance that insurance has an important role to play in mitigating some of the costs that arise from data breaches and attacks. However, cyber insurance is not a fail-safe.

Cyber risks remain challenging for insurers to underwrite for a number of reasons.

- The complex and rapidly shifting nature of cyber risk 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.
- 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 well we are protected from cyber risks in the years to come.



## Appendix 1

# 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.



## Appendix 2

# 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.



## Appendix 3

## Summary of Major Cybersecurity Legislative Proposals

Source: I.I.I. research and National Conference of State Legislatures (NCSL), as of May 2015.

### 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)

**Summary:** Would require 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 2014, at least 19 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 2015, 10th Edition, reports.weforum.org/global-risks-2015.
- 2. ESADEgeo (Center for Global Economy and Geopolitics) and Zurich, *Global cyber governance: preparing for new business risks*, Risk Nexus, April 2015, <u>knowledge.zurich.com/wp-content/uploads/2015/04/risk-nexus-april-2015-global-cyber-governance.pdf</u>.
- 3. Current statistics are found at Identity Theft Resource Center, <u>www.idtheftcenter.org/images/breach/ITRC-BreachStatsReportSummary2015.pdf</u>.
- 4. Randy Maniloff, White and Williams LLP, *There Aren't As Many Cos. With Cyberinsurance As You Think*, Law360.com, February 24, 2014.
- 5. Judy Greenwald, *Target SEC filing details insurance coverage and outlines costs of data breach*, Business Insurance, March 30, 2014.
- 6. Allianz Risk Barometer 2015, January 2015, www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015\_EN.pdf.
- 7. Allianz Global Corporate & Specialty, A Guide to Cyber Risk: Managing the Impact of Increased Interconnectivity, September 2015.
- 8. Andy Greenberg, After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix, Wired, July 24, 2015.
- 9. Elden Nelson, *BYOD* and cloud are top data breaches and malware risks, survey shows, CSOonline.com, April 6, 2015.
- 10. Rick Betterley, editor of the Betterley Report, interviewed on WRIN.tv, February 20, 2015.
- 11. PricewaterhouseCoopers, The Global State of Information Security Survey 2015, September 2014.
- 12. Damian Paletta, *Obama Calls For Tough Legislation to Combat Cyber-Attacks*, The Wall Street Journal, January 20, 2015.
- 13. <u>www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m%20</u>
- 14. International Institute for Counter-Terrorism (ICT), Cyber-Terrorism Activities, Report No. 10, July—September 2014.
- 15. ICS-CERT Monitor, September 2014-February 2015, <a href="https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT\_Monitor\_Sep2014-Feb2015.pdf">https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT\_Monitor\_Sep2014-Feb2015.pdf</a>.
- 16. Siobhan Gorman and Julian E. Barnes, Cyber Combat: Act of War, The Wall Street Journal, May 30, 2011.
- 17. Division of Corporation Finance, Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, October 13, 2011, <a href="www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm">www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm</a>.
- 18. Robert Hartwig, interview by Kenneth Simon, WRIN.tv, April 13, 2015. Dr. Hartwig is president of the Insurance Information Institute.



- 19. Matthew Sturdevant, *When Terrorists Attack Online, Is Cyber-Insurance Enough?*, Hartford Courant, January 26, 2015.
- 20. McAfee and the Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, Economic Impact of Cybercrime II, June 2014.
- 21. Ponemon Institute, 2015 Cost of Cyber Crime Study: United States, October 2015.
- 22. 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.
- 23. PricewaterhouseCoopers, 2014 Global Economic Crime Survey, February 2014.
- 24. Ponemon Institute (research sponsored by IBM), 2014 Cost of a Data Breach Study: Global Analysis, May 2014.
- 25. Verizon, 2015 Data Breach Investigations Report, April 2015.
- 26. As of July 22, 2015.
- 27. PricewaterhouseCoopers, *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*, September 2015.
- 28. Stuart Poole-Robb, *Here's why the cyber insurance industry is worth £55.6 billion*, ITProPortal.com, February 7, 2015.
- 29. New ISO Cyber Endorsements for Small, Medium Businesses Now Available, Insurance Journal, March 4, 2015.
- 30. Cybersecurity Brief, National Association of Insurance Commissioners, updated February 13, 2015.
- 31. Historical Development of Cyber (Re)Insurance, GCCapitalideas.com, October 23, 2014.
- 32. Swiss Re, Liability claims trends: emerging risks and rebounding economic drivers, sigma No. 4/2014.
- 33. Court Upholds FTC's Power to Sue Hacked Companies, National Journal Online, April 7, 2014.
- 34. Trends in Data Breach Cybersecurity Regulation, Legislation and Litigation, Mayer Brown, April 17, 2014.
- 35. 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.
- 36. Hiroko Tabuchi, \$10 Million Settlement in Target Data Breach Gets Preliminary Approval, The New York Times, March 19, 2015.
- 37. Young Ha, N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation, Insurance Journal, March 17, 2014.
- 38. Young Ha, Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York, Insurance Journal, May 1, 2015.
- 39. Ben DiPietro, *The Morning Risk Report: Lawsuit Could Define Scope of Cyber Liability Coverage*, Risk and Compliance (blog), The Wall Street Journal, October 21, 2014.



- 40. HM Government and Marsh, *UK Cyber Security: the role of insurance in managing and mitigating the risk*, March 2015. Actual penetration of stand-alone cyber insurance among U.K. large firms is only 2 percent, and this drops to nearly zero for smaller companies, according to the report.
- 41. Advisen (sponsored by Zurich), 2014 Information Security and Cyber Liability Risk Management, October 2014. Of those companies that do purchase coverage, some 47 percent have done so for between three and five years, and 22 percent for more than five years. Some 507 risk managers, insurance buyers and other risk professionals participated in the survey, which was conducted in August 2014.
- 42. Ponemon Institute (sponsored by Experian), *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, August 2013. As well as reducing the potential financial liability of a breach or security exploit, companies' security posture becomes stronger with the purchase of cyber insurance, the survey found. Some 62 percent of respondents said their companies' ability to deal with security threats improved after the purchase of the policy. The findings are based on 638 surveys completed by experienced individuals involved in their companies' cybersecurity risk mitigation and risk management activities in various-sized organizations in the United States.
- 43. Willis Fortune 1,000 Cyber Disclosure Report, August 2013; and Willis Fortune 500 Cyber Disclosure Report, 2012. The earlier Willis Fortune 500 Cyber Disclosure Report reviewed the 10-Ks or annual reports filed by the Fortune 500 in 2012, tracking organizations' response to SEC Guidance issued in October 2011 that asked U.S. listed companies to provide extensive disclosure on their cyber exposures. The Willis Fortune 1,000 Cyber Disclosure Report asked the same questions of the wider pool of companies and highlighted industry groups.
- 44. 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.
- 45. Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise, Marsh Risk Management Research Briefing, April 2015.
- 46. A Cybersecurity Call to Action, Marsh & McLennan Cos., The Chertoff Group, November 2014. Assumptions for Retail Exposure: hypothetical retailer with annual revenues of \$12 billion, holding a maximum 75 million credit and debit card records.
- 47. Liability claims trends: emerging risks and rebounding economic drivers, Swiss Re sigma No. 4/2014.
- 48. Mark Hollmer, *Cyber Attacks Increasing on Public-Sector and Non-Profit Targets*, Carrier Management, March 12, 2015.
- 49. A.M. Best, *Cyber Security Presents Challenging Landscape for Insurers and Insureds*, Best's Special Report, Issue Review, December 5, 2014.
- 50. 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.
- 51. Bill Kenealy, Catastrophe modelers developing cyber risk technologies to assess exposures, Business Insurance, January 4, 2015.



- 52. Liability claims trends: emerging risks and rebounding economic drivers, Swiss Re sigma No. 4/2014.
- 53. The Betterley Report, "Maybe Next Year" Turns Into "I Need It Now", Cyber Privacy/Insurance Market Survey—2014, June 2014.
- 54. 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.
- 55. Alistair Gray, Cyber risks too big to cover, says Lloyd's insurer, Financial Times, February 5, 2015.