MARSH & McLENNAN COMPANIES

Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
+1 212 345 5000
Fax +1 212 345 4808

Testimony of

PETER J. BESHAR

Executive Vice President and General Counsel

Marsh & McLennan Companies

Before the United States Senate
Committee on Homeland Security & Governmental Affairs

"Protecting America from Cyber-Attacks: The Importance of Information Sharing"

January 28, 2015
Washington, DC

Introduction

Good afternoon Chairman Johnson, Ranking Member Carper, and members of the Committee. I am Peter Beshar, the Executive Vice President and General Counsel of Marsh & McLennan Companies. I am grateful for the opportunity to participate in this important hearing about enhancing cyber resilience.

Marsh & McLennan operates through four market-leading brands — Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Our 56,000 employees provide advice to clients across an array of industries in the areas of risk, strategy, and human capital. As the leading insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

The evolution in the sophistication and intensity of cyber threats has been astonishing. Just a few years ago, the principal form of cyber threat was a denial of service, or DDoS, attack that might disable or deface an organization's website for a brief period.

In 2013 and 2014, hackers turned their focus to the theft, particularly in the retail sector, of credit card and other personal data.

Last month, however, we saw an attack whose ramifications are far reaching. On December 17, Germany's Federal Office for Information Security reported that hackers had caused "massive damage" to an iron plant by disabling the electronic shut off systems on the plant's furnaces. Armed with "detailed knowledge of the industrial control systems," hackers utilized an elaborate spear phishing campaign to damage the entire plant.

This escalation of cyber-attacks to physical assets reflects the growing threat posed to our critical infrastructure.

Senior government officials who previously warned of the threat of a "Cyber Pearl Harbor" appear increasingly prescient. Indeed, the government has been out in front of most of the business community in identifying the significance of the threat posed by cyber-attacks. The adoption of the NIST Cybersecurity Framework in early 2014 has helped organizations — large and small — conduct gap assessments regarding their cyber preparedness. Though under no obligation to do so, the FBI, the Secret Service, and other government agencies have repeatedly alerted companies and non-profit organizations that their systems had been breached. And just last month, this Committee and the entire Congress took an important step

in advancing cyber threat information sharing by formally authorizing the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security.

I would like to focus my remarks today on the importance of incentives, with a particular focus on cyber insurance, to drive behaviors in the marketplace.

What is cyber insurance?

Broadly stated, there are three core types of cyber insurance.

The most basic provides protection for out-of-pocket expenses that a company incurs in the wake of a data breach. These expenses include notifying individuals, setting up call centers and providing credit monitoring.

The second form of coverage protects a company if its computer network is effectively shut down for days or longer. With this broader business interruption coverage, a company can recover the actual harm it suffers in the form of lost profits or extra expenses.

The third type of coverage is for harm caused to an insured's customers or consumers as a result of a significant breach. This is called third-party coverage.

Why does cyber insurance matter?

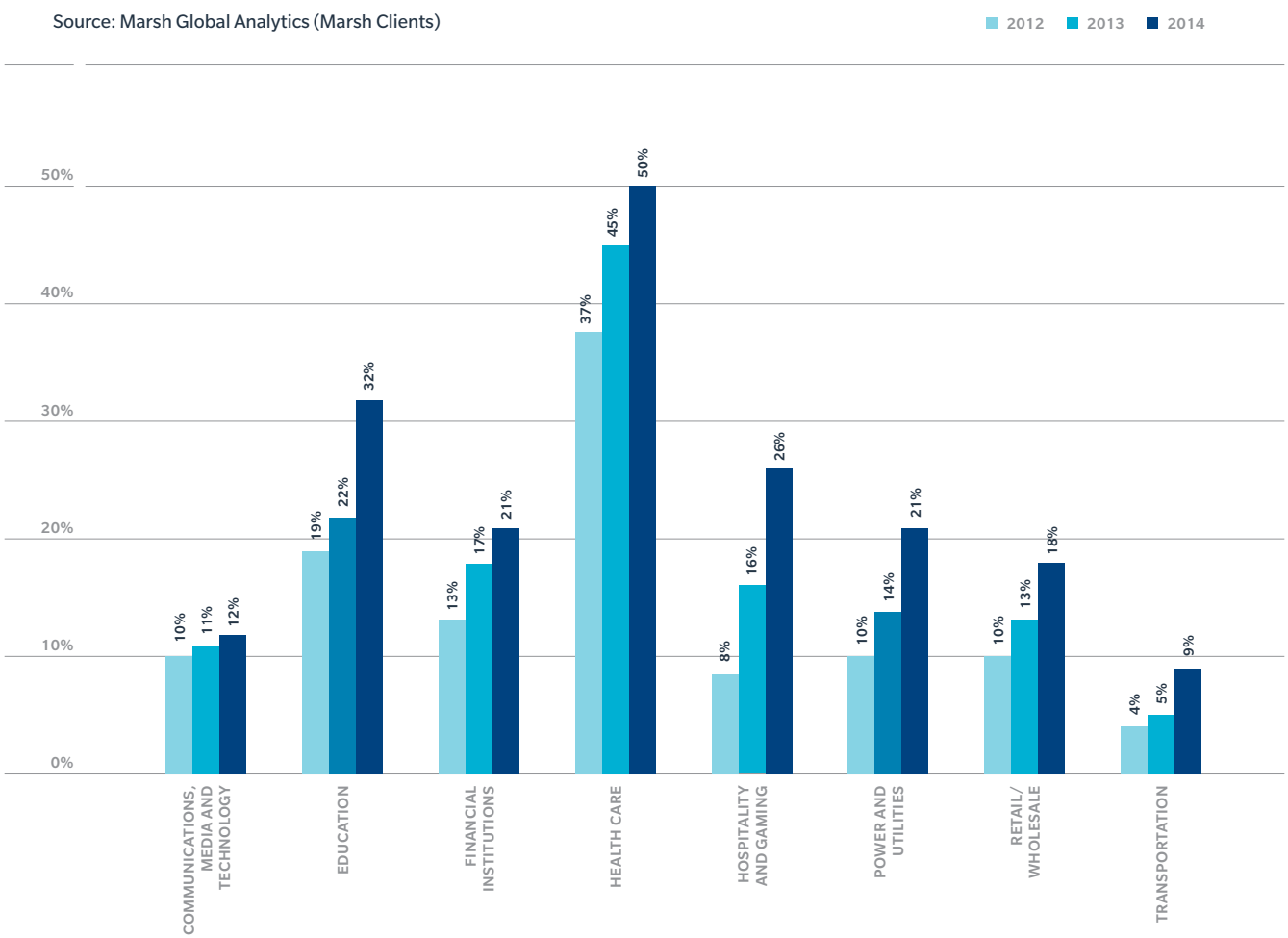
Cyber insurance creates important incentives that drive behavioral change in the marketplace. As a threshold matter, the simple act of applying for insurance forces insureds to assess the strength of their cyber defenses. Whether prodded by a board of directors or by a desire to get coverage as cheaply as possible, companies conduct gap analyses against industry benchmarks, including the NIST Framework and ISO 27001. Underwriters want to know whether the company has an incident response plan, disciplined procedures for patching software and robust protocols for monitoring its vendor network. Thus, this process, in and of itself, is an important risk mitigation tool.

Once a cyber policy is purchased, the insurer then has the incentive to help its policyholders avoid and mitigate cyber-attacks. As a result, many insurers now offer monitoring and rapid response services to policyholders.

Not surprisingly, the market is responding. In 2014, the number of Marsh clients purchasing standalone cyber coverage increased by 32% over 2013. And these numbers do not capture those clients that purchase cyber protection as part of a blended policy covering other lines.

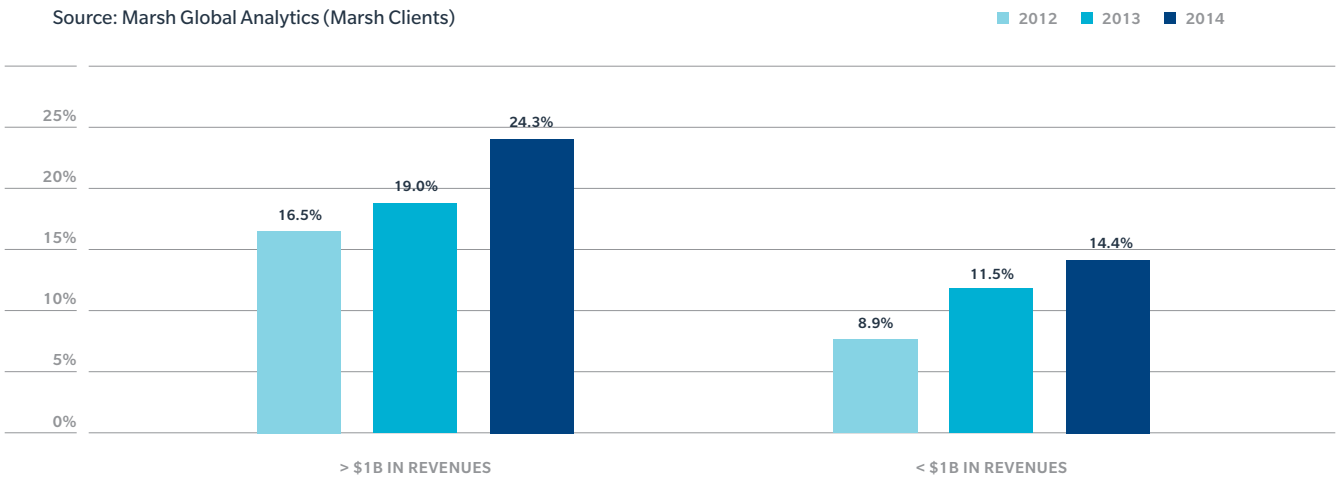
Marsh also tracked cyber insurance take-up rates by industry sector. As reflected in the chart below, the highest take-up rates for cyber insurance in 2014 were in: (1) health care; (2) education; and (3) hospitality and gaming. These industries handle a large volume of sensitive personal information, including health care data, Social Security numbers, and credit card information. In fact, as a result of statutes like HIPAA, the take-up rates in health care are higher than any other sector of the economy. There were also marked increases in the power and utilities sector.

Cyber Insurance Take-up Rates by Industry



A key takeaway from the cyber-attacks of 2014 has been the importance of securing a company's vendor network. Hackers gained access to Fortune 500 companies by stealing passwords and log-in credentials of smaller vendors, including air conditioning and food delivery companies. Thus, a large company's defense is only as good as the weakest link amongst its vendors. Accordingly, Marsh analyzed segment data to assess how the size of a company's business impacts its decision whether to purchase cyber insurance. While take-up rates increased noticeably in both large and small companies, there is a substantial, and indeed growing, gap between the two segments.

Cyber Insurance Take-up Rates by Revenue

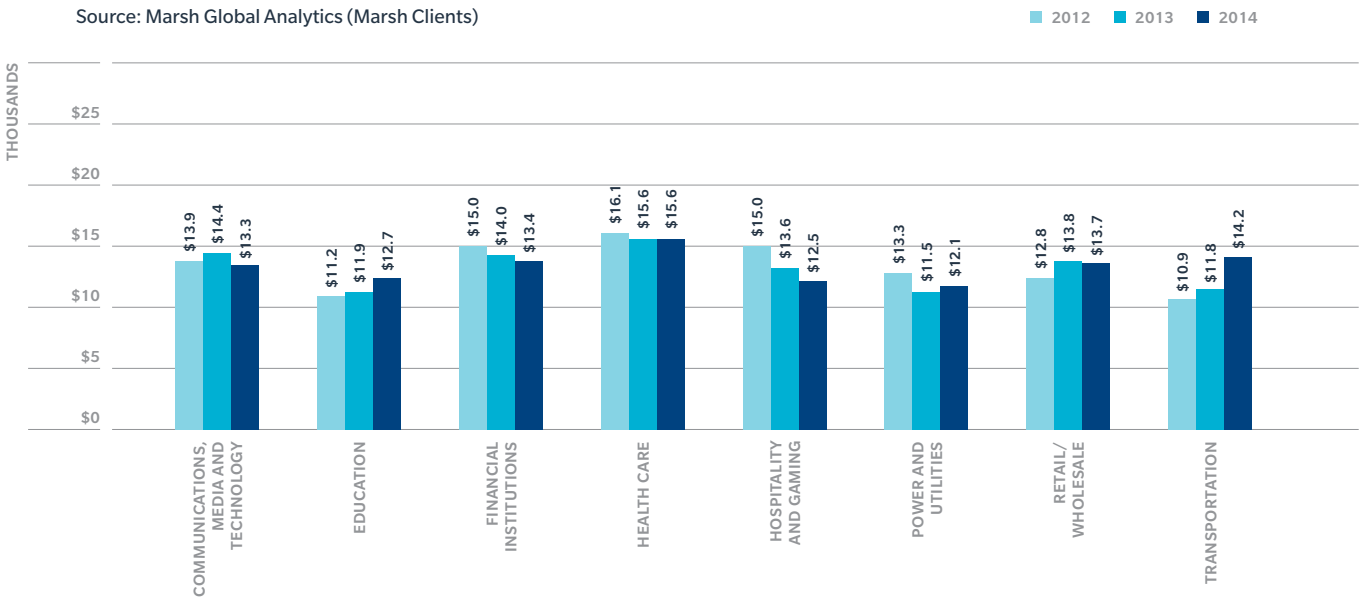


Finally, Marsh tracked cyber insurance pricing trends. Contrary to expectations, pricing trends year-over-year were relatively stable. While certain sectors including transportation and education saw increases, many other sectors saw price decreases.

A deeper analysis of the retail sector is informative. In the fourth quarter of 2014, two trends became evident. First, renewal rates increased by 5% on average and as much as 10% for certain clients. Underwriters have begun differentiating sharply between those retailers that have implemented robust point of sale controls, such as end-to-end encryption, and those that have yet to do so.

Thus, insurance market forces, particularly in the retail sector, are creating important incentives for companies to invest in more robust cyber defenses. In numerous industries, insurers have played a crucial role in developing sound risk mitigation practices. For example, in the area of workers' compensation, insurers identified a set of best practices and provided incentives for employers to reduce injuries and deaths in the workplace. Over the past twenty years, the number of workplace fatalities has fallen by over 35%. This same dynamic can occur in the cyber arena with insurers providing incentives for those companies that implement risk mitigation strategies like two-factor authentication and detonation software.

Cyber Insurance Coverage Price Per $1Million Across Industry Sectors



Overall, the cyber insurance market remains modest in scale. Marsh estimates that the total written premiums for cyber insurance in 2014 were approximately $2 billion. While up significantly, these numbers are a small fraction of total written premiums in the US insurance market of more than $1 trillion.

As Deputy Treasury Secretary Raskin recently stated in a speech to the Texas Bankers Association, cyber insurance is one element, among many, of a comprehensive risk mitigation strategy. [i]

i Deputy Secretary Raskin: "Cyber insurance cannot protect your institutions from a cyber incident any more than flood insurance can save your house from a storm surge or D&O insurance can prevent a lawsuit. But what cyber risk insurance can do is provide some measure of financial support in case of a data breach or cyber incident. And, significantly, cyber risk insurance and the associated underwriting processes can also help bolster your other cybersecurity controls. Qualifying for cyber risk insurance can provide useful information for assessing your bank's risk level and identifying cybersecurity tools and best practices that you may be lacking." http://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx

Information Sharing

As this Committee has recognized, enhanced information sharing between industry and government is another important component of a comprehensive risk mitigation strategy.

Working in isolation, neither the private sector nor the public sector has the tools to protect our nation's critical assets. This is particularly so given that 85% of our country's critical infrastructure is owned and operated by the private sector. To accelerate the identification and detection of emerging threats, there needs to be greater trust and real-time threat information sharing between the private and public sectors. And it should be reciprocal to the greatest extent possible.

Accordingly, we support the sharing of cyber threat indicators, including malware threat signatures and known malicious IP addresses, with the NCCIC provided that reasonable liability protections and privacy considerations are addressed. We believe that the dual considerations of national security and individual privacy can be fairly and appropriately balanced.

I commend you for convening this hearing and look forward to addressing any questions that you might have.