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 Commerce, Science & Transportation

Protecting Personal Consumer Information from Cyber Attacks and Data Breaches

March 26, 2014
Washington, DC

Introduction

Good afternoon Chairman Rockefeller, Ranking Member Thune, and members of the Committee. I am Peter Beshar, the Executive Vice President and General Counsel of Marsh & McLennan Companies. I commend you for convening this hearing and am grateful for the opportunity to participate.

Marsh & McLennan Companies operates through four market-leading brands — Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Our 55,000 employees provide advice and solutions to clients across an array of industries in the areas of risk, strategy and human capital. In particular, Marsh and Guy Carpenter assist companies in identifying and then mitigating key risks to their business — including cyber security.

I wanted to offer a couple of initial observations and then focus my remarks on a single topic — cyber insurance.

First, hyperconnectivity has been a boon for enhancing our productivity. We are able to connect the world and execute tasks with a speed that was inconceivable even a decade ago. With that hyperconnectivity, however, comes the risk of a significant disruption through a cyber attack.

Second, the government has led the way in identifying the significance of this risk and then pushing industry and the non-profit sector to bolster their defenses. A case in point was the release last month of the Administration's Cyber Security Framework. This is an important tool to help enterprises assess their preparedness and then enhance their resilience against a cyber attack.

Moreover, this Committee has been at the vanguard of the effort to raise awareness of the threat posed by a cyber security attack. In particular, this Committee's interactions with the SEC have served to help companies, and investors, better understand the potential disruption that can occur from a significant attack.

In the area of cyber security, offense is a lot easier than defense. There is no silver bullet or panacea that will eliminate this risk. Rather, it will take a collaborative effort between government and business and among professionals in different disciplines — IT, HR, Legal and Compliance — to assess vulnerabilities and link arms to confront this risk head-on.

This afternoon, I would like to discuss the role that cyber insurance can play as one component of a comprehensive risk mitigation strategy.

To begin, what is cyber insurance? Who is buying it? What role can it play to mitigate this risk?

As the largest insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

The concept of cyber insurance was first introduced in the 1980s, when insurers began providing coverage for computer failures at banks and other Fortune 500 companies. Marsh launched its first cyber insurance product, NetSecure, in 1999.

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

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

The second form of coverage protects companies if their 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.

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

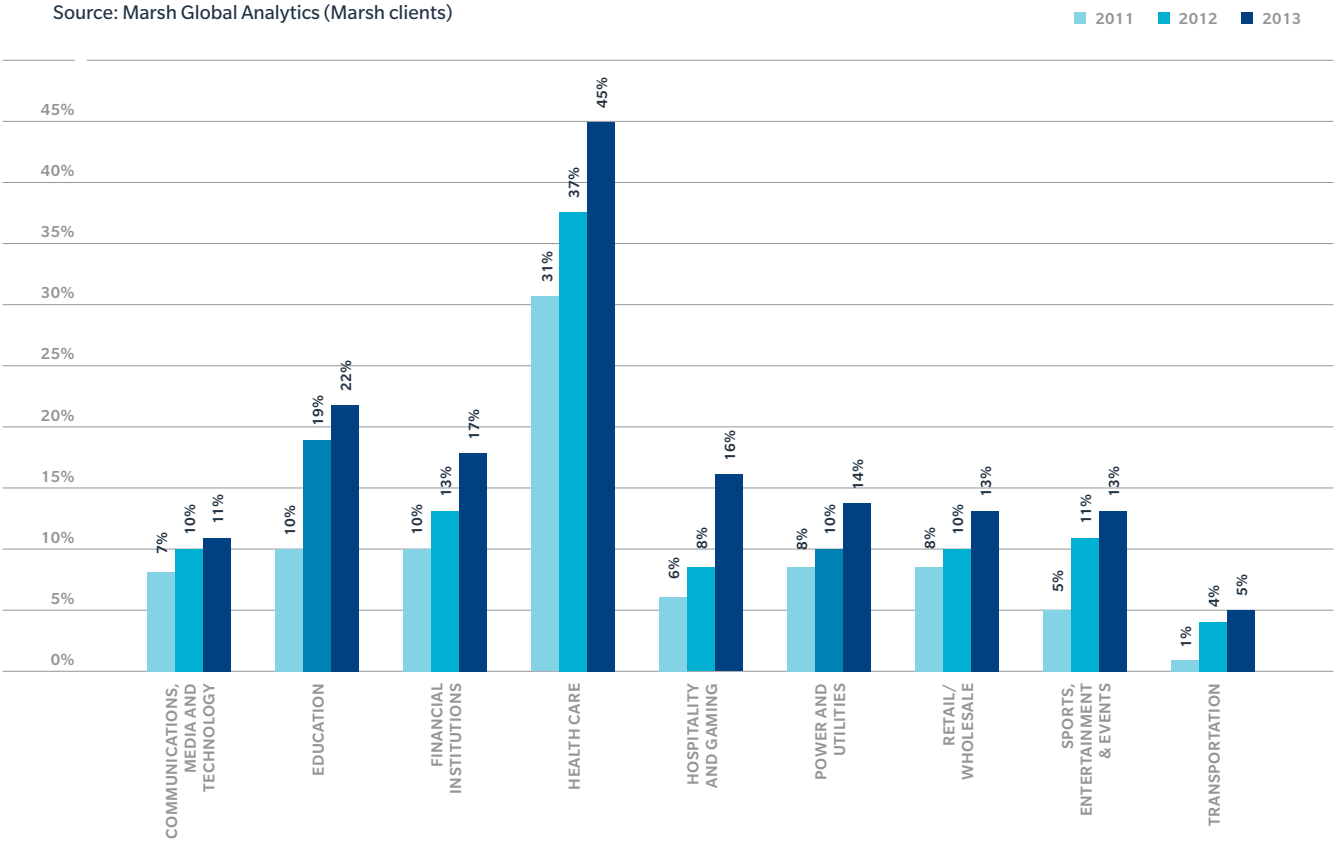
To give the Committee insight into this market, Marsh conducted a comprehensive survey of the type of companies that are currently purchasing cyber coverage — broken down by industry and size of company.

There are a number of important headlines. Most importantly, interest in cyber insurance is expanding rapidly. Indeed, the number of Marsh clients purchasing stand-alone cyber insurance increased more than 20% in just the past year.

As reflected below, the highest take up rates for cyber insurance are in the following three industries: (1) health care; (2) education; and (3) financial services. These industries handle a large volume of sensitive personal information, including health care data, social security numbers and credit card information. As a result of statutes like HIPAA, the take up rates in health care are markedly higher — approaching 50% — than any other industry.

Figure 1: Take Up Rates by Industry

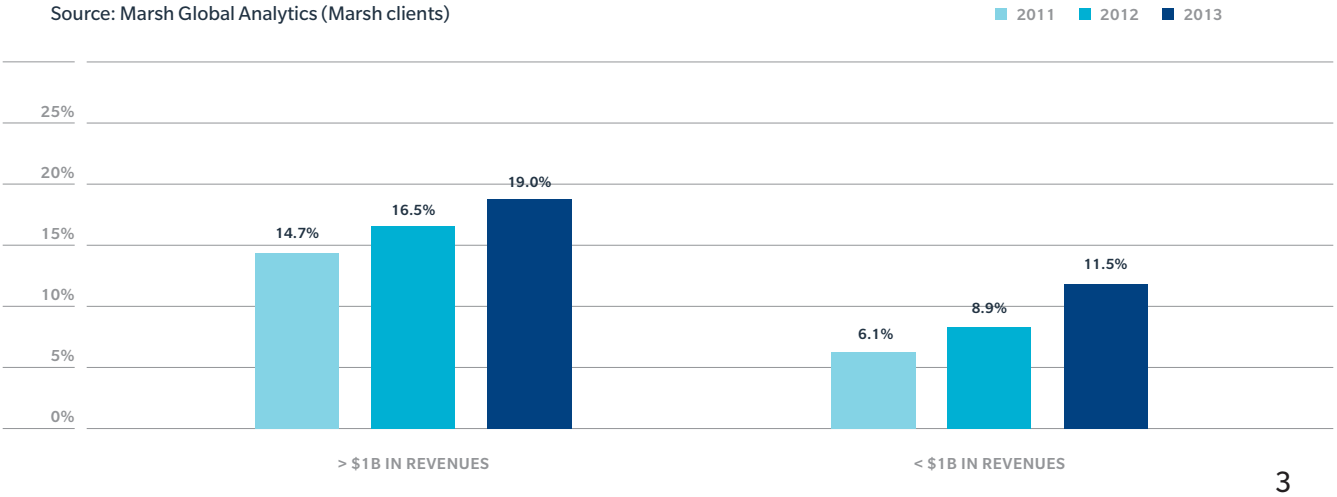
Source: Marsh Global Analytics (Marsh clients)



Marsh also analyzed how the size of a business impacts its decision whether to purchase cyber insurance. As a general matter, larger companies perceive a greater threat to their operations than smaller companies. As a result, the take up rates for companies with revenues over $1 billion are almost twice as high as the rate for companies with revenues below $1 billion.

Figure 2: Take Up Rates by Company Size

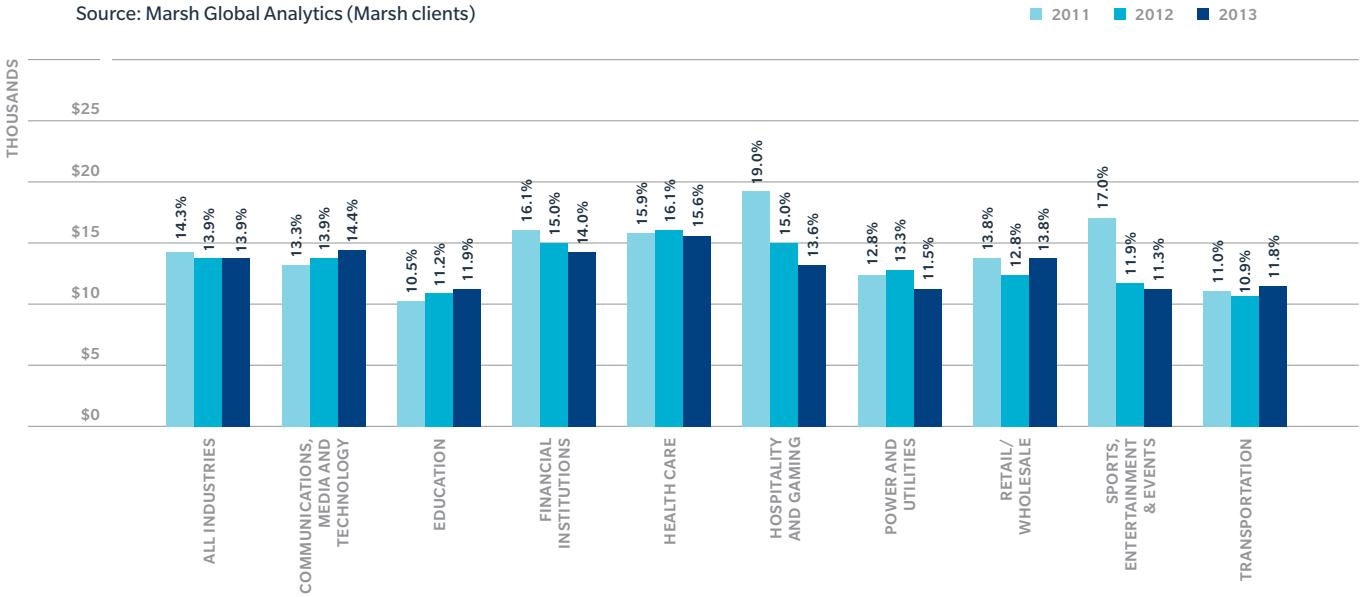
Source: Marsh Global Analytics (Marsh clients)



Third, Marsh analyzed trends in the cost of cyber insurance. Here, the news is quite positive. Throughout 2013, cyber insurance rates remained stable — even as the perception and potential severity of the risk increased. This is partly because a number of new underwriters are interested in providing cyber coverage.

As reflected in the analysis below, the average price per million dollars of coverage for a cyber policy actually dropped in 2013 in a number of sectors, including financial institutions, utilities, and sports and entertainment, while increasing for other sectors, including communications and transportation.

Figure 3: Insurance Coverage Price Per $1Million Across Industry Sectors



Furthermore, the process of applying for cyber insurance — analogous to the process of conducting a gap analysis under the Administration's Cyber Security Framework — is itself a constructive exercise for raising awareness and identifying potential vulnerabilities. At Marsh, we utilize a proprietary Information Security and Privacy Self-Assessment, which is based on international information security management standards known as ISO 27001.

Using the assessment, Marsh brokers perform a high-level review of information security management protocols with respect to access control, physical security, incident response and business continuity planning. The assessment focuses on the strength of a company's governance procedures regarding cyber practices to understand how insurance carriers will view the company's risk profile.

Importantly, a number of cyber coverages also provide access to experts who are available to monitor the client's information security and assist the client to restore operations in the event of a network attack. These services include technical advice from on-call consultants, vulnerability detection to examine network devices and servers, and assistance developing incident response plans.

Conclusion

As the SEC indicated in its cyber security guidance, cyber insurance is one element, among many, of a comprehensive risk mitigation strategy.

This is a race without a finish line. As we strengthen our defenses, adversaries will adjust and develop new methods of attack. Our success in combatting this dynamic and evolving threat will depend on continued collaboration between government, industry and the non-profit sector.

I look forward to answering any questions you might have.