Catherine Mulligan, SVP Zurich
Testimony before the US Senate Commerce Committee
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
Hearing Titled: "Examining the Evolving Cyber Insurance Marketplace."
March 19, 2015

Good morning Chairman Moran, Ranking Member Blumenthal and members of the subcommittee. My name is Catherine Mulligan and I am Senior Vice President of the Management Solutions Group for Zurich (North America). I lead the market facing team of underwriters responsible for working with brokers and customers on the placement of "cyber" insurance. I appreciate the opportunity to speak to the subcommittee on the state of the cyber insurance marketplace and to share thoughts on some of the challenges we are seeing.

As a brief introduction, Zurich Insurance Group (Zurich) is a leading multi-line insurance provider with a global network of subsidiaries and offices. Founded in 1872, Zurich is headquartered in Zurich, Switzerland with approximately 55,000 employees serving customers in more than 200 countries and territories.

While Zurich is named after the Swiss city where it was founded, we are quite proud of our U.S. roots and our global platform for diversifying risk. In 1912,

Zurich entered the U.S. as the first non-domestic insurance company and quickly became a leading commercial property and casualty insurance carrier.

Over the last 103 years, Zurich has grown and its U.S. companies now employ more than 8,500 people in offices throughout the country with major centers of employment in the metropolitan areas of Chicago, New York City, Kansas City, Atlanta, Dallas, and Baltimore. Mr. Chairman, as I am sure you are aware, we employ nearly 400 people throughout the state of Kansas and write coverage in every single state. Zurich's U.S. insurance group accounts for roughly 40% of its total global business.

As a result, Zurich is the fourth largest commercial property and casualty insurer in the United States by gross written premium. It is the fourth largest writer of commercial general liability insurance, which includes coverages that, among a wide array of other risks, protect U.S. manufacturers, importers and retailers against product liability losses. In addition to this capacity, Zurich also protects many U.S. construction projects throughout the country as the third largest fidelity and surety insurer. Zurich protects hundreds of thousands of U.S. employees and their employers as the fifth largest workers compensation insurer.

With this context as to who Zurich serves, it was two years ago when Zurich's senior leadership decided to act to address the risk management questions and concerns raised by many of our cyber customers. This began a global thought leadership initiative with the Atlantic Council and resulted in a white paper report titled: *Beyond Data Breaches: Global Interconnectedness of Cyber Risk.* This report was released in April 2014, and Zurich has shared its findings and recommendations with its stakeholder community to generate dialog and steps forward to address the cyber threats.

As cyber attacks occur in ever changing forms on business and industry that compromise increasing amounts of sensitive information, this hearing is extremely timely to level set what cyber insurance is, what it is not, and most importantly some of the challenges marketplace actors are seeing.

I will dive into specifics later in my testimony, but overall here is how I see the market. Unsurprisingly given recent high profile breaches, so-called cyber insurance is quickly becoming a need for commercial customers. However, as a new market it faces a number of challenges. Some are somewhat more straight-

foward, such as capacity and pricing, which are in flux as the industry grows and learns of new challenges.

Yet, others reflect the complexity of the challenge. The term cyber insurance is a misnomer. A network security and privacy event - the more accurate term of cyber insurance - can also be caused by something simple such as improper disposal of paper records. At the same time, one cyber event can trigger multiple types of claims, for multiple insureds within one company, and even cause physical damage to a manufacturer or utility.

The lesson can be boiled down to the simple fact that the scope of the challenge is too broad to be solved by the private sector alone. Not all losses from a cyber attack will be or even could be covered by an insurance policy. This market is new and evolving daily which will require time to fully mature.

Market overview:

In October 2014, Dowling and Partners called security & privacy (also known as "cyber") insurance "one of the few growth markets in the U.S. Property and

Casualty Industry" with growth potential up to $10B Gross Written Premium.[1] Sources, including Dowling and Guy Carpenter,[2] suggest the current market is $2 billion with five or six carriers offering primary coverage. Guy Carpenter also states that the six largest carriers have 70% of the market share, a statistic that remained relevant throughout 2014. These premium numbers are difficult to verify. The coverage can be offered on a stand-alone basis or blended with other coverages, such as Errors & Omissions.

Coverage overview and history

The product was first introduced about 15 years ago and has its roots in technology errors & omissions coverage. This is a third party liability coverage designed to respond to financial damages resulting from negligent acts, errors, and omissions in the deliverance of a product or service. As our world and economy became more networked, privacy issues came to the fore, which led to the development of privacy regulations. Companies found they incurred first-party costs to respond to privacy events and to comply with these regulations.

[1] "Cyber Security: with CEO Jobs Now on the Line, It's No Longer Just an 'IT' Issue." Dowling & Partners IBNR Weekly #39, October 20, 2014

[2] Guy Carpenter's State of the Tech/Cyber market report (2012) and Management Liability – Market Overview report (Oct. 2013)

Network Security & Privacy Liability policies were developed to respond to this blend of first and third-party costs.

The product in its current iteration has been in the marketplace since around 2009. There is no industry standard policy language, but the core elements of the coverage are as follows:

- The third-party liability costs arising from network breaches and privacy events as well as some media liability events;
- The first-party or direct costs a company incurs in responding to a breach. These include forensics analysis, legal guidance in compliant breach response, credit and identity monitoring costs, and the costs associated with a call center and public relations.

First-party coverages have further expanded to include Business Interruption and Extra Expense. This is a familiar coverage on most commercial property policies, but here, instead of responding in the event of physical loss or damage, this optional coverage can apply to direct damages arising from downtime caused by a network security breach.

Marketplace shifts

In January of this year, the Insurance Information Institute reported that market capacity for cyber insurance is on the rise.[3] While this optimism is understandable given the visibility of the issues and the attention significant breaches have garnered from Boards of Directors and C-Suite executives[4], the reality is that the shape of the insurance marketplace continues to shift:

- *Capacity is in flux.*

  Dowling & Partners stated more than 60 carriers wrote the coverage as of October 2014. Subsequently, our broker partners tell us a number of excess markets pulled out of the product line or limited their appetite. Business Insurance has reported on major insurers restricting their appetites for challenging industry segments. The London market was tapped out for retailers by December; although capacity refreshed in 2015, the pressure was on to find strong support for growing programs. Reinsurers are also paying careful attention to their aggregations, and some have amended their appetites for supporting the coverage.

- *Pricing is in flux.*

[3] "Insurance Industry Leaders Believe Market Capacity For Cyber Insurance On The Rise, U.S. Economic Growth On the Upswing, I.I.I. Survey Finds." Insurance Information Institute, January 14, 2015
[4] "Cyber Security: with CEO Jobs Now on the Line, It's No Longer Just an 'IT' Issue." Dowling & Partners IBNR Weekly #39, October 20, 2014

The insurance industry lacks robust actuarial data around the loss experience for a product that is still in its nascency. Unlike general liability policies, which all commercial enterprises carry, the buyers of this coverage are largely in a few key industry sectors (such as health care, financial institutions, technology, and retail) and in the larger company space (ie. companies with annual revenues over $1 billion). As loss experience emerges, and underwriters identify new attack vectors, pricing becomes more refined. Some segments, notably retail[5], are experiencing significant increases in premiums as high profile breaches in the past 12 months have generated substantial first party loss dollars, which continue to rise.

- *Loss experience is developing*

  One major retailer, who suffered a highly publicized breach in late 2013, is reported to have incurred over $250 million in first-party costs in responding to the attack. Those costs reportedly continue to rise, and the liability costs associated with the breach - including liability to consumers and financial institutions - has yet to be determined. This example demonstrates the severity potential as well as the element of the unknown as the liability issues play out in court. Moreover, we see attack vectors shifting, for example,

[5] "Data breaches prompt insurers to boost cost of retailers' cyber coverage," Business Insurance, Sept. 28, 2014

approximately 30% of breaches originate with a business partner or vendor, presenting challenges to underwriting the exposures and controls and to responding to breaches.

- *Coverage and aggregation challenges remain*

  It is important to understand the history of this product. The total scope of exposures presented by a cyber security event is beyond the current scope of coverage. Richard Clarke's acronym[6] for causes of cyber security events remains applicable. He described them as C.H.E.W.: Crime, Hactivism, Espionage, and War.

  While most security & privacy policies do not focus on attribution, the trigger of coverage must still be a network security breach or privacy event. We eschew the term "cyber" for three reasons:

  1. It is not a defined term in most policies;
  2. Privacy events may be triggered by an analog event such as improper disposal of paper records containing personally identifiable information;
  3. A broad term such as "cyber" erroneously may suggest that the coverage could respond to every type of damage caused by an attack on a network.

[6] Richard Clarke, "Cyber War: The Next Threat to National Security & What to Do About it", published 2012

We understand that customers have a range of exposures that exist beyond the financial loss coverage that is provided under a Security & Privacy policy.

- Top areas of concern include Bodily Injury and Property Damage:

  A cyber attack may cause physical damage to a manufacturer or utility. For example, a December 2014 malware attack to a German iron plant caused fire damage when a furnace's controls were compromised.[7] In 2014, Insurance Service Offices (ISO) issued exclusions on their general liability forms to clarify that cyber events are not meant to be covered on the general liability policy. While some limited coverage is available in the marketplace, current security and privacy forms generally exclude bodily injury/property damage.

The scope of the exposures is too broad to be solved by the private sector. Not all causes of loss can be transferred to an insurance policy.

<u>Emerging issues</u>

- *Aggregation tracking and emerging exposures*

[7] "Cyberattack on German Iron Plan Causes 'Widespread Damage': Report," The Wall Street Journal, December 18, 2014

Multiple lines of business may be impacted as the result of a cyber security event. For example, a significant breach to a public company might result in a stock drop, which leads to a derivative suit that comes in as a claim under a Directors & Officers Liability Coverage.

Also, one event might impact multiple insureds. For example, a recent breach at a large health insurer has resulted in claims under policies for a variety of companies who have business relationships with that insurer.

The current coverage structure and pricing will continue to evolve as carriers gain a more comprehensive understanding of the full scope of the potential. The insurance industry is working with the public sector to shape policies around these issues.

- *Public sector*

The 2015 World Economic Forum report states that "global risks transcend borders and spheres of influence and require stakeholders to work together."[8] The focus of the report on "risk interconnections and the potentially cascading effects they create" echoes the theme of the Atlantic Council's 2014 study on

[8] "Global Risks 2015 – 10th Edition", World Economic Forum, January 2015

cyber risk.[9] The WEF report echoes Chairman Thune's comments from the February 4th hearing on the NIST framework: "Real progress can be made by continuing to enhance public-private cooperation and improving cyber-threat information sharing."

Work in this arena includes working groups at the Department of Homeland Security and the Department of Treasury on the issue of data repositories. Data sharing may need to take a few different forms: sharing of cyber event data, such as attack vectors and scope, and cyber insurance data, such as claim and underwriting information by sector. While it is too early to assert any definitive conclusions, the potential upside of these discussions is that more comprehensive information will assist insurers in developing both coverage and risk management solutions and best practices for our customers.

[9] "Risk Nexus. Beyond data breaches: global interconnections of cyber risk", Atlantic Council, April 2014