Testimony of Erica Davis
Senior Vice President and Head of Specialty Products Errors and Omissions
Zurich North America
before the
House Committee on Small Business
"Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option"
July 26, 2017

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee, thank you for the opportunity to speak with you today about the important issue of cybersecurity and the role of the private sector in providing risk management solutions to businesses to protect against cyber risk.

As leader of a team of market-facing underwriters at Zurich North America, I work with brokers and customers on the placement of cyber insurance. While there is increased awareness of the threats across all sizes of organizations, businesses are still struggling to understand cyber risk: the full scope of their exposures and how best to protect themselves and their customers.

Zurich

Zurich is a leading multi-line insurance group with more than 140 years' experience serving businesses worldwide. Zurich employs approximately 54,000 people and serves customers in more than 210 countries and territories.

Zurich entered the United States in 1912, and for more than 100 years has served businesses of all sizes in America, including Fortune 500 companies, small and medium size businesses, as well as farmers and ranchers. We are proud to help them manage risk and give them the confidence to contribute to the U.S. economy. Zurich's North American headquarters is in Schaumburg, Illinois, and supports the jobs of over 9,000 employees across the United States. We are proud to have a market and employment presence in each of your states. We are also pleased to offer risk management solutions to customers in Puerto Rico and will explore the marketplace of American Samoa.

As one of the five insurance providers currently leading the North American cybersecurity insurance market, Zurich is invested in identifying risks and delivering solutions for its customers. Zurich is committed to staying at the forefront of the cybersecurity issue, as both the likelihood of a security breach and costs continue to escalate.

Zurich's Approach to Cyber Risk

Understanding Attitudes to Cyber Risk. As the cyber threat landscape continues to evolve, companies across all industries find themselves increasingly vulnerable to potential harm from a security or privacy event.

Most loss dollars arise from first-party privacy breach costs, such as forensics, breach coaches, consumer notification and credit monitoring. We are also seeing:

- Business interruption loss

- Liability lawsuits
- Regulatory fines
- Reputational damage
- Shareholder suits

Businesses today face difficult decisions about cybersecurity and how best to manage their risks: deciding whether they should retain the residual risk or transfer it through the purchase of a cyber insurance product.

The role of insurance is continuously increasing as customers are now seeking industry feedback and risk insights. It has become more of a partnership, with businesses focusing on not just what happens post-breach and a loss being paid. They value having a stable of pre-vetted vendors available to them if they are impacted by a data or security event. They are also focusing more on pre-breach services to guide them through risk mitigation tools like technology assessments.

In October 2016, Zurich and Advisen (a leading provider of data, media and technology solutions for the commercial property and casualty insurance market) released a sixth annual survey of risk managers, insurance buyers, and other risk professionals on the current state of trends in information security and cyber risk management. Key findings included:

- Eight-seven percent of respondents believe a technology interruption would have a moderate-to-significant impact on their business.
- Over the last six years, the proportion of companies buying security and privacy cyber insurance has increased by 85%, from 35% in 2011 to 65% in 2016.
- For the first time in the six years of this study, general counsel has surpassed information technology as the department most frequently responsible for assuring compliance with all applicable federal, state, or local privacy laws, including state breach notification laws.
- Most companies surveyed (97 percent) clearly recognize the importance of collaboration between their risk management and information technology departments on issues related to cyber security.
- Industries with substantial personally identifiable information, personal health information and/or personal financial information, in general, consider data security and privacy to be a more significant risk. As a result, they also are more likely to purchase security and privacy insurance and engage in risk management activities.
- Costs related to a breach of customer/personal information are the leading reason for purchasing cyber insurance.

Coverage. Zurich provides coverage for cyber risk to businesses of all sizes, and cyber coverage is tailored based on customer need. While the historical reason for purchasing cyber insurance is liability concerns and costs related to breach of customer or personal information, coverages recently have focused on business interruption and supply chain downtime as the result of a cyber event.

Risk culture is also critical to underwriting any line of business. Cyber insurance is no exception. It is critical for businesses to build a culture of awareness at all levels. Events in

recent years have raised awareness of cyber risk across all industry segments. Businesses must adopt a mindset of resilience rather than just protection.

More businesses are beginning to view information security as an organizational challenge rather than just a technology issue. The business community's interconnectivity and reliance on technology has increased, which creates more points of entry and new threat vectors. The exposure has broadened to include potential property damage for something like critical infrastructure, bodily injury caused by autonomous vehicles or cyber espionage.

Therefore, the underwriting of the cyber product is evolving as the risks are morphing. The insurance community is continuously working to understand the full scope of the exposures and what the controls might need to be. Each business needs to be underwritten differently.

Resilience. Organizations of all sizes now realize they are at risk of a security or privacy event. Finding solutions to the most complicated of cyber risks will require collaboration between the insurance industry, governments, academia and other think tanks to establish standards, encourage information sharing, build resilience and create adequate global governance.

In an effort to continuously help customers understand and protect themselves from risk, Zurich began participating as a key industry consultant in a "first of its kind" public-private partnership by the University of Maryland and the National Institute of Standards and Technology (NIST). The partnership embarked on a research project to assist companies ascertain the effectiveness of their information security and cyber supply chain best practices, with an end goal of helping organizations increase their cyber risk assessment and management capability. The project built on an existing Cyber Risk Portal, which collects data by allowing participating businesses to anonymously upload information to compare their cybersecurity capabilities to the existing NIST Framework, as well as to their peers and competitors.

To further assist businesses with their security and privacy risk management, Zurich is also collaborating with Deloitte to help improve a company's cyber resilience. Policyholders can complement Zurich's cyber coverage with pre-breach cyber risk assessment and management services through Deloitte to understand their level of cyber exposure and resilience. These services include standards-based risk assessment of an organization's threat detection and incident response capabilities, as well as risk mitigation recommendations. This is just one area where Zurich is focusing on cyber risk mitigation rather than solely risk transfer.

Insurance Issues

Data Breach Uniformity. Because there is a myriad of state laws governing data breach, we are interested in a national, uniform standard on data security and breach notification. While this is not directly in the jurisdiction of this committee, it is certainly relevant for you as Small Business Committee Members to recognize the complexity of cybersecurity governance from a business perspective. We appreciate the efforts of Congressman Luetkemeyer in this regard.

Cyber Accumulation. A challenging issue for all insurers is cyber accumulation. Given the cyber interconnectedness of potential data loss, business functions, and supply chains, the ability

to quantify exposures, accurately price risks, and manage accumulations and capital requirements will remain a difficult issue for the insurance community for the foreseeable future.

Cyber as a Peril. Zurich is contributing to the public dialogue around interconnectivity and the full range of exposures from cyber as a peril. The extent of exposures presented by a cybersecurity event is beyond the current scope of coverage. For example, physical damage is rarely offered on a cyber insurance policy, but can result from a cyber attack. The full range of the exposure is too broad to be covered by the private sector; not all causes of loss can be transferred to an insurance policy. Cybersecurity breaches can cause losses including property damage, bodily injury and reputational risk, and we are investigating the best way to consider these impacts.

Conclusion

Zurich continues to refine its understanding of cyber exposures so we can help our customers understand the risk, make thoughtful decisions on our current product, and develop additional insurance solutions going forward.

With data breach, ransomware and other attacks on small businesses occurring daily, we appreciate your focus on risk management solutions provided by the private sector.

Thank you again for the opportunity to testify today. I look forward to answering your questions.