Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
Hearing entitled "Examining the Evolving Cyber Insurance Marketplace."
Thursday, March 19, 2015

Written Testimony of Michael Menapace

Sen. Jerry Moran, Sen. Blumenthal, and other members of the Subcommittee -

I am pleased to provide testimony today concerning this Committee's interest in the growing cybersecurity insurance market, the evolution of the insurance coverage, opportunities to strengthen the insurance industry, and the insurance market's impact on cybersecurity.

I would be pleased to respond to specific questions posed by the Committee and I would like to cover in my testimony several specific issues concerning the evolving cyber insurance marketplace. Specifically, I would like to discuss the cost-drivers for cyber insurance, the role that the insurance industry and the government can play in helping in the development and evolution of standards for breach notification, the sharing of data breach information, and flexible, industry-specific standards for protecting consumer data.

The testimony I provide is my own and not necessarily that of any of my firm's clients.

Background and Introduction

I practice law at the law firm of Wiggin and Dana after having previously practiced at a large international law firm. In addition, for the past 6 years, I have taught Insurance Law at the Quinnipiac University School of Law and have published articles and books on a variety of property and casualty insurance issues. In my law practice, I, along with my colleagues, represent companies in a broad spectrum of industries by helping them develop data security and privacy protocols and procedures, and I represent insurance companies in several areas, including cybersecurity. In both my academic role and in private practice, I have the opportunity to work closely with businesses in many market segments, insurance companies, and regulators.

Examining the intersection of insurance and cybersecurity is an important and timely topic for this Committee. Insurance often evolves slowly, but we are in the midst of a period in which technological advancements and the development of a relatively new product are occurring simultaneously. No doubt, we are living through a dynamic period in the insurance industry and we should not underestimate the importance of the insurance industry in terms of risk transfer and the information insurers provide to insureds on loss mitigation strategies and loss trends.

The insurance industry is in a unique position to help regulators, businesses, and consumers assess and respond to the ever-growing threat of data breaches. Insurers can help businesses

and consumers respond quickly and efficiently when breaches unfortunately, but inevitably, occur. Insurers have first-hand experience with large amounts of consumer data. Moreover, insurers are in the business of examining and responding to risks, tracking emerging trends, and finding ways to mitigate their impact. Indeed, insurers often provide information and best practices to their insureds to help avoid losses.

By definition, insurers deal with events that are uncertain from the viewpoint of the insured. There is an element of fortuity at the heart of insurance that insureds cannot predict. While this element of uncertainty is present to insureds, insurers can pool large amount of data and experience to see trends as they evolve – this helps them price insurance policies appropriately and remain in a financial position to pay claims.

In addition to the traditional goal of providing risk transfer, insurers can help insureds avoid loss in the first instance. For example, insurers have traditionally helped in the development of safety programs to help employers and employees avoid workplace injuries. Obviously, such programs help workers, but they also assist the purchasers of insurance by bringing down premiums. In all, the goal of the insurer is for their insureds to avoid losses and to make those losses that inevitably occur smaller and easier to rectify.

The insurance market can play a similar role in cybersecurity with risk transfer products and sharing information and experience with their insureds.

Evolution of Cyber Coverage

There are some insurers, particularly the large insurers, who have been writing some form of cyber coverage for well over a decade. They have become quite sophisticated and efficient in providing excellent risk transfer products to a variety of markets. However, there are approximately 40 insurers in the U.S. that are currently providing cyber coverage, and among those insurers are some that are relatively small by comparison to the market leaders and who are less experienced and sophisticated in providing cyber insurance. While the insurance market as a whole could benefit from the topics we are discussing today, it is the smaller companies and those with a less mature book of business that would likely benefit the most – and, by extension, their insureds would see benefits in the form of lower premiums and thriving insurance marketplace.

I will discuss breach notification standards, the sharing of data, and the development of data protection standards in a few moments, but I would first like to discuss how the cyber insurance market has evolved to where we find it today.

During the “dot com” boom of the early 2000s, some insurers started offering insurance products for technology companies. Originally, those insurers provided first party property loss coverage along with some third party liability coverage. The first party property loss coverage was designed to cover, for example, losses the policyholder experienced for damage to its own

technology equipment and infrastructure. The third party liability coverage was designed for exposure to third party lawsuits against the insureds.

The early coverage was written that way because, in those nascent years, the insurance market believed that the liability losses would be driven by the cost of defending lawsuits and paying settlements or judgments as a result of those lawsuits. But the predictions on the cost-drivers were not entirely accurate and today's products have developed to reflect this reality.

While third party lawsuits are still one factor insurers consider how they draft policy wordings and price the coverage they offer, we have seen that data breach response costs have come to the forefront in the minds of insurers and insureds alike.

Neither insurers nor insureds anticipated that these breach response costs, sometimes called crisis service costs, would be the significant cost drivers that they have become. These breach response expenses have become costs drivers for several reasons, including the fact that many data breach lawsuits are dismissed in the early phases of litigation. These lawsuits are often dismissed because the plaintiffs cannot show or even plead concrete damages – in response to breaches, businesses or their insurers often provide credit monitoring at no cost to consumers and until actual damage to the consumer can be alleged as a result of the data breach, the damages are speculative. Obviously for those cases that are dismissed, there are no settlement or judgment costs borne by insurers and the defense costs are extinguished, whereas every breach will have breach responses expenses.

According to a recent insurance industry survey, the initial crisis service costs account for about half of all data breach costs. Those breach response services include technical forensic investigations, attorney oversight, breach notification to and credit monitoring for affected consumers, call centers, and public relations services. The other half of the costs go towards legal defense and settlement, regulatory response and defense, regulatory fines, and fines imposed by credit and debit card issuers.

<u>A Federal Breach Notification Standard – Reducing the costs of breach responses and treating consumers equally</u>

As of today, the are 47 states, plus Puerto Rico, Washington D.C., and the Virgin Islands, that have requirements for notifying customers after the unauthorized access of personally identifiable information or protected health information. Many of these state requirements also require notification of the state attorney general when a certain number of residents have been impacted.

But, these state requirements are not uniform in terms of when they are triggered and what information must be contained in the consumer notices. Therefore, when responding to a nationwide incident, lawyers like me must assess the impacted data and consumers under 47 different sets of requirements. Among the questions we must ask for each state are:

Has the breach notification standard been triggered?

Must the consumer(s) be notified under the facts of the incident?
What information must be contained in the notification?
Must we notify state regulators or attorneys general?
Must notice be given in a specific timeframe?
Are we required to provide specific consumer protection services such as identify theft insurance and/or credit monitoring?

This 47-state exercise can be a costly endeavor and, frankly, can result in a situation where some consumers and state officials are notified in one state while consumers and officials in other states are not notified about the very same incident. As both industry members and regulatory authorities have noted, this current patchwork quilt of state breach notification requirements creates gaps in consumer protection as well as additional burdens for businesses that experience cyber-attacks

A nationwide standard for breach notification that preempts state law requirements would eliminate the time, expense, and inconsistencies involved in the 47-state analysis for each breach and would provide for uniform treatment of consumers. I note, however, that any such federal standard must carefully consider the timeframe within which business must notify consumers whose data may have been affected. The timeframe must balance the needs of timely notice to consumers with the concern of providing consumers with accurate information. Increasingly, large breaches involve complex attacks that require equally complex forensic investigations to determine the actual scope of data losses.

<u>Nationwide Data Clearinghouse – Assisting underwriting and spotting trends</u>
There are many lines of insurance that have fairly standardized coverage terms and conditions regardless of which insurer is issuing the coverage. For example, the vast majority of general liability policies purchased by businesses are based on standardized policy language. The Insurance Services Offices, Inc. (ISO), publishes standard liability policy language for many lines of property and casualty insurance. Insurers can choose to adopt the ISO forms and, in the case of general liability policies, most insurers do adopt the ISO policy or use policy wording that is very similar.

However, there is no standard insurance policy language for cyber insurance. ISO did recently publish cyber coverage terms, but I know of no insurer that has adopted the ISO policy terms or has plans to do so in the near future.

Among the approximately 40 insurers that offer cyber insurance, there are some with significant experience and who have policy language that they have developed over the course of more than a decade of experience. Those insurers are comfortable with their policies even though they will undoubtedly continue to evolve. Other insurers, some who are newer entrants into the cyber insurance market and others who are looking to differentiate themselves from their competitors, have their own policy language that has not been tested to the same extent as the policy terms used by the insurers with more mature books of business.

Understanding these differences in policy language from one insurer to another can be a challenge to insurance purchasers and brokers, but the diversity in the market also gives purchases more choice to purchase insurance tailored to their specific needs.

In and of itself, this diversity of policy terms and conditions is not problematic for individual insurers. What can be challenging for some insurers is making sure they have enough data to make prudent underwriting decisions when they sell policies.

For insurers to have good underwriting in terms of deciding what risks to insure and how to price the coverage, it is important for them to have a good data set of past experience and loss information. There are some insurers who have been active in the cyber insurance space for a long time, they have developed their own data base of loss experience, have a mature book of business, and have refined their criteria for underwriting decision. But, for the smaller insurers and for new entrants into the market, they do not necessary have the same foundation from which to make underwriting decisions.

A nationwide database or clearinghouse for data breach information, specifically recording how each breach occurred and who was responsible for the breach, could be helpful to the insurance market generally and for businesses that are implementing their own data protection practices, processes, and protocols. Insurers could use the information to supplement their existing underwriting criteria. In addition, businesses in many industries could use the data to learn about the causes of other breaches and apply that information to improve their own efforts to keep consumer information safe. All market participants would be able to use the data, for example, to spot trends in cyber-attacks and hopefully respond before those attacks are repeated.

I do not intend to imply that insurers are making underwriting decisions in a cavalier or uninformed manner. But there is no doubt that not all breach incidents receive national attention in the press and a nationwide database to which business could report information and from which they could learn from others could be a positive force in combating the evolving threat of cyber intrusion and data misappropriation. The federal government could play a role in encouraging the creation of and participation in such a clearinghouse.

I can envision several ways the database or clearinghouse could be established and administered, either by private market participants, the federal government, or a public-private partnership. I do not have a view on the best method to accomplish this, and I concede there is debate on whether this kind of sharing is prudent, but there is a valid argument that more information can be a net positive for the market in general.

<u>Flexible and Industry-Specific Data Protection Guidelines – Assisting Businesses and Underwriters</u>

As this Committee and the other witnesses here today know, there are data protection standards that have been imposed on, or adopted by, certain business segments. For example,

HIPAA provides, among other things, a set of national standards to protect personal health information and applies to "covered entities" and "business associates." This is an example of government imposed standards. On the other hand, the NIST Cybersecurity Framework that was published about a year ago provides a different model from HIPAA. As this Committee is aware, the NIST Cybersecurity Framework was a collaborative effort between industry and government and consists of processes, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. The Framework is not a fixed, uniform standard, but instead is a generalized framework for managing cyber-risk based on a continuous cycle of threat assessment and risk mitigation measures which can be customer by industry sector and by each organization. While still evolving, the Framework may over time become a baseline or benchmark of cybersecurity preparedness in some sectors.

There are other markets and industries that have neither legally-mandated nor widely-adopted voluntary security standards and guidance. For example, the mobile apps industry, education institutions and retailers do not yet have industry-specific guidance on what protections they should employ to protect the data they collect, use, and store. As a result of recent 'mega' data breaches, such as Target and Home Depot, we may see more coordinated industry efforts in this regard.

Industry guidance, even if voluntary, can serve several purposes. One, it could provide a standard that businesses can use to gauge their own policies, protocols, and procedures. Two, the insurance market can look to that industry-specific guidance during the underwriting process to assess whether to underwrite a specific business and what price is appropriate for coverage. The NIST Framework contains subjective criteria – it is not a list of quantifiable metrics. Nevertheless, businesses can look to such frameworks as they examine their own business practices and as they consider what to expect when applying for cyber insurance. Insurance company actuaries may find the Framework less helpful, but guidance like the NIST Framework can provide some common expectations that insurers and insureds alike can use. Three, when government sponsored guidelines are industry-led, market participants can have some confidence in the standard that will be applied by a regulatory body in a post-breach inquiry. And, four, the standards could be a useful tool as private litigants and courts look to the appropriate standard of care that a business should be held to.

It seems that the intent of any guidance or standards is to provide businesses with data protection expectations or best practices. But as a secondary benefit, insurers could choose to use the guidance as part of the criteria considered during the underwriting process.

Any data protection guidance or framework, however, consistent with the approach of the NIST Framework, must be industry specific. For example, the data protections guidelines applicable to retailers are different than those applicable to entertainment companies, banks, education institutions, or health care providers to name just a few industries with uniquely specific needs.

In addition, the industry standards must remain flexible to accommodate the size of the company, the data at issue, and technology as it emerges. Software will change, existing technology will continue to evolve, and we will see the use of wearable technology, drones, and the Internet of Things expand in use. Therefore, any government-sponsored or encouraged security guidance must be able to adapt in real time and should be technology-neutral and risk-based.

Insurers understand already that business should not be required to use specific software or hardware. Instead, when deciding whether to cover a particular business or how much the coverage should cost, insurers sometimes are more interested generally in the business's culture towards data protection. If a company is committed to securing the data it holds, that company will likely update its software, its procedures, and its processes, making insurers more likely to underwrite coverage for that business. In examining the data protection culture of a business, cybersecurity frameworks, like the NIST Framework, can be useful tools even though, as stated earlier, they will not provide the actuaries with objective metrics on a particular insured or industry.

If the government decides not to move forward with security guidelines for particular industries, such industry-specific standards and expectations will nevertheless likely develop over time in the marketplace. But, a partnership between the government and private industry could accelerate the development and adoption of flexible guidelines that will, ultimately, benefit consumers without restricting innovation.

Getting businesses to examine their own practices in the course of purchasing insurance does have a recent precedent. Several years ago, when insurers started asking their business customers how they viewed their susceptibility to climate change impacts and what they were doing to address those risks, some business began looking at those issues for the first time and responded accordingly. There was no government mandate for insurers to ask these questions, but insurers did so because they saw that climate change risks could impact their customers and, by extension, themselves. The insurance market could spur the type of self-examination by businesses with cybersecurity measures and there does seem to be a role that the government can play to encourage this outcome. In the end, if insurers are confident that their concerns have been incorporated into any cyberssecurity guidance that is developed and they adopt that guidance as part of their underwriting processes, businesses will be encouraged and incentivized to address those issues even if security standards are not mandated by the government.

I thank you for the opportunity to provide this testimony and am available to try to address any specific questions the Committee has for me on these or related topics.