Prepared Testimony and
Statement for the Record of

Ola Sage
Founder and CEO
e-Management

Hearing on

"Examining the Evolving Cyber Insurance Marketplace"

Before the

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

March 19, 2015

253 Russell Senate Office Building

Examining the Evolving Cyber Insurance Marketplace

Opening Remarks

Good morning Chairman Moran, Ranking Member Blumenthal, and distinguished members of the Committee. It is an honor for me to be here today.

My name is Ola Sage and I am the Founder and CEO of e-Management, a small business provider of high-end IT services and cybersecurity solutions to clients in the private and public sectors, including the largest U.S. federal agencies. Founded in 1999 and headquartered in Silver Spring, Maryland, we employ close to 60 IT professionals who deliver services in our core areas of IT Planning, Engineering, Application Development, and Cybersecurity. In 2013 we were honored to receive the Department of Energy's Cybersecurity Innovative Technical Achievement award, highlighting the expertise of our cybersecurity experts in designing and implementing advanced cybersecurity detection and risk management capabilities. Our newest cybersecurity risk intelligence software solution, *CyberRx*, automates the National Institutes of Standards and Technology (NIST) Cybersecurity Framework (CSF) and is designed to help small businesses easily *measure* their cybersecurity capabilities, *manage* their cybersecurity risks, and *communicate* their cybersecurity readiness to internal and external stakeholders.

I am a champion and advocate for Small and Medium-Sized business (SMB) cybersecurity readiness. I currently serve as an elected member on the *Executive Committee of the National IT Sector Coordinating Council (IT SCC)*. The IT SCC, comprised of the nation's top IT companies, professional services firms, and trade associations, works in partnership with the Department of Homeland Security (DHS) to address strategies for mitigating cybersecurity threats and risks to our nation's critical infrastructure, especially for organizations and businesses that are particularly vulnerable such as SMBs. I am also an 8-year member of Vistage, an international organization of 19,000 CEOs that control businesses with annual sales ranging from $1 million to over $1 billion. I regularly meet with and speak to small business CEOs in Vistage, and other small business forums about why cybersecurity should matter to them and how it can affect their ability to keep business, stay in business, or get new business. In the last 3 months alone, I have spoken to more than 100 SMB CEOs that represent a diverse mix of industries.

Thank you for the opportunity to testify today on behalf of e-Management as a small business consumer of cybersecurity insurance products. In my testimony today, I will discuss:

- My company's involvement with cybersecurity insurance including our application and renewal process
- Perspectives that I have as a CEO and from other CEO's relative to cybersecurity insurance
- Opportunities for the cybersecurity risk insurance industry
- Concluding thoughts

Our Driver

My company's foray into the cybersecurity insurance market began in November 2013 as I prepared for a webinar on cybersecurity titled "We've Tipped: 5 Ways to Increase Your Cybersecurity Resiliency." The webinar discussed the wave of cyber-attacks that were occurring across all industries, highlighting the significant increase in attacks on small businesses and the impacts – including financial, legal, and reputational – that they were having on all sizes of business, including the disproportionate and negative impact to small business. According to the Cyber Security Alliance, 60% of small businesses go out of business within 6 months of a significant cybersecurity event.

Among the five key recommendations I made in the webinar was for businesses to make sure they had appropriate business and legal protections (e.g., business policies, insurance, etc.). I thought about my own company and whether we had taken appropriate steps to include business and legal protections in the area of cybersecurity. As a company, we had participated for more than a year with NIST as they worked with thousands of security professionals in government and private industry to develop the CSF. Upon release of the Preliminary Draft of the CSF, NIST encouraged companies and organizations to try it and provide feedback that could inform the final version (v 1.0 which was ultimately published in February 2014). We took the challenge.

Methodology

In our "test drive" of the CSF, we used the Framework as a way of assessing our cybersecurity readiness in the five core cybersecurity functions (Identify, Protect, Detect, Respond, and Recover) and mapped the results to the four Implementation Tiers to help us to understand how our current cybersecurity risk-management capabilities measured up against the characteristics described by the Framework and to assess the degree of risk management rigor we were applying to each of the five core functions. Overall, the CSF provided a common language that I could use with my management and IT teams in organizing our thinking around cybersecurity. We were able to distill where we needed to prioritize our efforts and focus our dollars. We found it to be a very effective and useful tool.

Our Cybersecurity Insurance Experience

In addition to technical and operational changes we made after our initial CSF readiness assessment, we decided to move forward with researching what cybersecurity insurance products were available on the market, specifically available offerings for SMBs. As I'm sure it will come as no surprise to anyone here, we could not find cybersecurity insurance products designed specifically for SMBs. The cybersecurity insurance industry was and is still in a nascent stage.

Working through our insurance broker, we submitted applications to several large insurance companies. The applications varied in length and substance, with very little consistency in the questions asked. When the quotes arrived, they ranged from a couple thousand dollars from one insurer to twelve thousand plus for another. Comparing the policies against one other was virtually impossible as the language used in one policy was quite different from the next and it was unclear whether or not they covered the same conditions. As expected, all of the policies contained exclusion clauses, however it was not clear from policy to policy whether the exclusions were similar or not.

Regrettably I cannot tell you that our selection of a cybersecurity insurance product was based on a simple and easy analysis of options. We ended up with a policy that combines cybersecurity liability and errors and omissions, but honestly, as I sit here today, I cannot say with confidence we have the right policy for us. All told, the process from start to finish took four months and cost over ten thousand dollars. This was a significant investment for a company our size.

We continue to regularly monitor and manage our cybersecurity risks, and implement preventative measures based on the results of our Framework assessment. We call it "operationalizing" the CSF. We understand it is not possible to achieve 100% cybersecurity, but as a provider of IT and cybersecurity services, we believe it is important to convey to our employees, customers, and vendors that we take cybersecurity seriously and understand the potential damage it could cause to them. In addition to doing it for the right reason, we also see it as a competitive advantage.

We have taken it a step further. Understanding the value the CSF gave us, we wanted to share our experience with other small businesses. Drawing on our entrepreneurial instincts, we created and brought to market a software solution that automates the CSF in a way that is simple and affordable for other small businesses to use. In two hours or less, a small business can conduct a "fitness" review of their cybersecurity readiness in the CSF's five core areas. In addition, the small business CEO receives information unique to their company that provides them insight into their level of technical, operational, and financial exposure. It is actionable risk intelligence. We call it CyberRx. CyberRx makes it easy for a small business to understand how prepared their business is to identify, protect, detect, respond, and recover from cybersecurity attacks and alerts them to areas that need attention. They quickly know what areas to focus on and what their next steps should be. We use CyberRx in our company today to continuously manage our own cybersecurity risks.

Renewing our Cybersecurity Insurance

This brings me back to our cybersecurity insurance experience. We have just passed our one year anniversary and this time around the process started with a letter from the insurance company informing us that our coverage wouldn't automatically renew. We received an abbreviated application (3 pages vs 15) which we completed and sent back. There was only one question around cybersecurity asking whether there had been any changes regarding the security and protection of our facility and network. The instructions indicated that if the response was "Yes", we needed to indicate if we had experienced a security breach? As we thankfully did not experience a breach (that we know of) we were able to answer no. We received our renewed policy in approximately three weeks, which was the good news. The surprising news was that our premium increased by 12%.

Stunned, surprised, frustrated, confused, discouraged, etc. are all words that would accurately describe our reaction. After a year of investing in processes and tools to strengthen our cybersecurity posture, the result was an increase in premiums. Doing the right thing didn't seem to pay, literally. We went back to our broker to better understand how this could have happened and were informed that there were a variety of factors that went into the underwriting process. In our case, ironically, because our revenues grew in 2014 vs 2013, that appeared to be the primary contributor to the increase. When we asked whether or not using the CSF could be a factor, our broker wrote that "although they do not specifically inquire as to whether or not an insured is following the voluntary cyber security framework provided by NIST, they obviously take into consideration any preventative measures an insured implements when underwriting a risk."

SMB CEO Perspectives

My experience is not unique. As I speak to small business CEOs across the country, there is a general lack of awareness about (1) the need for cybersecurity insurance; (2) what cybersecurity insurance products exist on the market; (3) what the various polices cover; and (4) what the costs are.

1. ***The need for cybersecurity insurance***
   Many SMB CEOs just don't believe they have anything cyber hackers would want. "We're too small," some will say, believing that hackers are only interested in the large companies where they can get more "bang for their buck." Interestingly, another subset of SMB CEOs believe that cybersecurity insurance is already included in their professional liability coverage, and therefore do not see the need for additional or separate coverage.
2. ***Availability of cybersecurity insurance products***
   Of the 100 or so SMB CEOs I have spoken to over the past three months, easily 70% were not aware of what cybersecurity insurance products are available on the market. Once informed they were curious to learn more. This aligns with a recent 2015 survey by Gartner company, Software Advice, who reported that after defining cyber insurance to the SMB decision-makers in their survey, they found that a combined 52% were either "very" or "moderately" intrigued, with another 32% "minimally" intrigued, giving an overall 84% who expressed some level of curiosity. [1]
3. ***Policy Coverage***
   Understanding what the different cybersecurity insurance policies cover can be a challenge, not just for SMBs, but also for many brokers. There does not appear to be any common terminology or contract organization amongst carriers, thus making it difficult and costly to truly understand what an individual policy covers and to compare competing insurance products.
4. ***Cost of Coverage***
   The cost of cybersecurity insurance varies widely. Our own experience with a range of quotes from $2,000 - $13,000 is not uncommon. This large variance can discourage SMB CEOs from making needed investments in cybersecurity insurance. In addition, for many SMBs, such rates are cost prohibitive for what they might consider "elective" insurance. Given the challenges with understanding and comparing the scope and coverage of various insurance products on the market, SMBs may incur additional costs in connection with the placement or renewal of insurance in addition to the cost of the insurance itself.

Opportunities for the Cybersecurity Risk Insurance Industry to Assist SMBs

There is no 100% level of cybersecurity. At e-Management, we strongly believe cybersecurity readiness is about risk management. We offer the following straightforward recommendations that we believe would encourage SMBs to take greater advantage of cybersecurity insurance products.

1. ***Increase awareness of cybersecurity insurance as a risk transfer option for small businesses.***
   Cybersecurity insurance can be an effective tool to help small businesses manage their financial risk and should be a key part of a company's cyber and information security practice. Several years ago, Symantec reported that the average annual cost of cyberattacks to small businesses was $188,242 with median cost of downtime for an SMB reported at $12,500 per day. These costs can be devastating, in many cases leading small businesses to shut their doors. However, a majority of small businesses are not aware of cybersecurity insurance. According to the 2015 survey by

[1] http://www.softwareadvice.com/security/industryview/cyber-insurance-report-2015/

Software Advice, only a third of small and midsize businesses are even aware that cybersecurity insurance exists and of that number only 2% actually hold cybersecurity insurance. I understand that in the last year there have been extensive discussions among government, private companies, insurance groups, and other relevant stakeholders about expanding the role of cybersecurity insurance in public and private industry business agreements. While I think this is a necessary and important conversation to have, I encourage these discussions to continue to be as thorough and transparent as possible including a full review of potential impacts or consequences that particular policy decisions could have, particularly to SMBs.

2. ***Make cybersecurity insurance affordable for SMBs***
   Cybersecurity insurance needs to provide meaningful coverage that SMBs can actually afford. Various industry reports indicate that SMBs continue to be the fastest growing segment of cyberattack victims, creating a huge vulnerability, not just for the SMBs, but for their customers, vendors, and suppliers. We believe offering competitive cybersecurity insurance products designed for the SMB market can lead to better deals for SMBS. We recommend that insurance companies consider a rating system based on the CSF that underwriters could consider as a factor in the underwriting process. SMBs that demonstrate use of the CSF could receive a higher rating as they have mitigations in place which line up with industry standards and best practices.
3. ***Reward SMBs who are actively managing their cybersecurity risks and implementing reasonable security measures.*** In 2014, the Online Trust Alliance indicated in a report that 90% of the year's breaches could have been prevented if organizations implemented basic cybersecurity best practices[2]. The CSF is a model cybersecurity best practice and offers a defensible way to assess and manage cybersecurity risks. Based on our own experience, we strongly believe that any small business that uses the CSF can significantly reduce their cybersecurity risk exposure. Small businesses that are actively managing their cybersecurity risks should be preferred candidates for lower premiums and tax incentives.

Conclusion

At e-Management, we continue to find the CSF to be a useful tool in helping us and other SMBs organize the way we think about cybersecurity risks and the best practices we need to implement to reduce our overall cybersecurity risk exposure. We appreciate the emphasis that Congress, NIST and the DHS have placed on educating SMBs about the increasing cybersecurity threat and raising awareness of the CSF. We welcome continued efforts in this area and encourage the addition of cybersecurity insurance in the discussion as another tool that SMBs can consider along with other risk management solutions.

While simply obtaining cybersecurity insurance cannot be viewed as a silver bullet, I believe cybersecurity insurance can be an important tool in helping SMBs manage significant financial exposure associated with a successful cyber attack. As the cybersecurity threat and challenge to small business continues to persist, we at e-Management are committed to working with government and industry to identify and develop simple and affordable solutions that enable small businesses to strengthen their cybersecurity readiness and posture.

Thank you again for the opportunity to testify, and I am ready to answer any questions you may have.

[2] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented