Senate Committee on Commerce, Science, and Transportation
March 19, 2015, Hearing
"Examining the Evolving Cyber Insurance Marketplace"

Testimony of Ben Beeson
Vice President, Cyber Security and Privacy
Lockton Companies®

Chairman Moran, Ranking Member Blumenthal, distinguished members of the Committee, thank you for the opportunity to testify today on behalf of Lockton Companies.

My name is Ben Beeson and I am Vice President for Cyber Security and Privacy at Lockton Companies. Lockton is the world's largest privately held, independent insurance broker. I am based in the Washington, DC, office, where I advise clients on a cyber risk management strategy that addresses people, processes, and technology.

Our clients face a substantial set of cyber threats today that include criminal gangs, disgruntled employees, politically motivated actors, and now nation states. Well-publicized attacks have sought to target and monetize personally identifiable data and protected health information. However, it is also now well understood that the theft of corporate intellectual property is a significant problem, with nontrivial impacts on innovation for companies and countries, and companies also face incidents that can disrupt or destroy information technology and other vital assets.

We believe that cyber insurance is an important market force that can drive improved cyber security for companies—and thus improve protection to consumers and the nation as a whole. It should not just be seen as another insurance transaction. As the cyber insurance market develops, it will provide incentives for companies to understand and mitigate their risks.

For example, forward-thinking companies invest in workplace safety to reduce their workers' compensation costs. In the same way, sophisticated companies are investing in stronger cyber security, and those companies ultimately will experience fewer losses, insurers will see fewer claims, and their premiums will be lower.

However, we're not there today. The cyber insurance market is still nascent and developing.

CYBER INSURANCE MARKET TODAY

It is estimated that more than 50 insurers domiciled mainly in the US and the Lloyd's of London marketplace provide dedicated cyber products and solutions today. Buyers are overwhelmingly concentrated in the US with little take-up to date internationally. Annual premium spend at the end of 2014 was estimated to be in excess of $2 billion[1] with the potential to grow to $5 billion.[2] Total capacity (the maximum amount of insurance available to any single buyer) is currently at about $300,000,000. Cyber insurance first emerged at the end of the 1990s, primarily seeking to address loss of revenue and data-restoration costs from attacks to corporate networks. However, the underwriting process was seen as too intrusive and the cost prohibitively expensive, and it was not until 2003, and the passage of the world's first data breach notification law in California[3], that demand started to grow.

WHAT DOES CYBER INSURANCE COVER?

It is important to understand that insurers do not address all enterprise assets at risk. The vast majority of premium spent by buyers has sought to address increasing liability from handling personally identifiable information (PII) or protected health information (PHI), and the costs from either unauthorized disclosure (a data breach), or a violation of the data subject's privacy. Insurable costs range from data breach response expenses such as notification,

[1] The Betterley Report - www.betterley.com

[2] The Cyber Liability Insurance Market 2015 - Jim Blinn, Advisen. www.cyberrisknetwork.com

[3] California S.B.1386

Rev. 03_17_15

LOCKTON

forensics, and credit monitoring to defense costs, civil fines, and damages from a privacy regulatory action or civil litigation.

Insurers also continue to address certain first-party risks including the impact on revenue from attacks on corporate networks, extortion demands, and the costs to restore compromised data.

WHAT DOES CYBER INSURANCE NOT COVER?

Theft of corporate intellectual property (IP) still remains uninsurable today as insurers struggle to understand its intrinsic loss value once compromised. The increasing difficulty in simply detecting an attack and, unlike a breach of PII or PHI, the frequent lack of a legal obligation to disclose, suggests that a solution is not in the immediate future.

Much attention in the industry is now being paid to risks to physical assets from a cyber attack. Much of the credit here must go to the federal government for directly engaging the industry initially in 2013 as part of the creation of the NIST Framework and raising awareness about the risks to critical infrastructure industries. In the absence of actuarial risk modeling data, certain innovative insurers and brokers have started to produce solutions that specially address property damage, resultant business interruption loss, and bodily injury from a cyber attack. However, it is early days, and major challenges lie ahead in establishing significant market capacity as well as addressing the current ambiguity embedded in legacy property and casualty insurance policies.

HOW DO INSURERS UNDERWRITE CYBER RISKS?

Historically, underwriters have sought to understand the controls that enterprises leverage around their people, processes, and technology. However, the majority of assessments are "static," meaning a snapshot at a certain point in time through the completion of a written questionnaire, a phone call interview, or a presentation. In the wake of significant insurable losses in 2014 and early 2015 to the retail and healthcare sectors in particular, a consensus is growing that this approach is increasingly redundant. It is Lockton's opinion that insurers will increasingly seek to partner with the security industry to adopt a more threat-intelligence-led capability as part of the underwriting

LOCKTON

process in the face of threats that continue to evolve. The industry (as discussed later) will also increasingly seek to partner with government to access industry loss data and analytics capabilities.

WHAT IS THE ROLE OF CYBER INSURANCE?

In the context of building enterprise resilience to counter evolving cyber threats, insurance should not just be seen as a financial instrument for transferring risk from one balance sheet to another. Importantly, the actual process of seeking cyber insurance coverage should also be viewed as the catalyst for driving an enterprise-wide risk management approach, and ultimately an improved security posture.

It can bring all relevant stakeholders together in IT, Legal, Risk Management, R&D, Finance, Human Resources, Communications, and the Board of Directors for example. Do not view cyber insurance as just a commodity that you may or may not seek at the end of this process.

NIST FRAMEWORK

In the same vein, Lockton also sees the NIST Framework aligning hand in glove with this strategy. Working closely with the Department of Homeland Security to support its implementation, Lockton sees the framework providing the tool that is needed to help boards of directors understand in layman's terms their current security posture, areas for improvement, and desired future status. As insurance brokers who also advise directors and officers on management liability, we can acknowledge that cyber risk has now entered a governance dialogue, and the NIST Framework has proved immensely helpful in facilitating the discussion.

LOCKTON

CONCLUSION—A PUBLIC/PRIVATE PARTNERSHIP

Lockton, and we believe the industry as a whole, would welcome the introduction of legislation that would reduce barriers and incentivize organizations to share threat indicators with government, and each other, while also protecting individual privacy. Actuarial data is extremely thin on the ground and is holding back the growth in market capacity, particularly to address the previously highlighted risks to critical infrastructure industries.

As part of the insurance industry's engagement with the Department of Homeland Security, discussions are ongoing about the possible formation of a data repository to house anonymized enterprise loss information. The ability to access anonymized loss data, shared between industry and government with appropriate privacy protections would also accelerate the growth of the marketplace, but crucially the ability of cyber insurance to act as a market incentive for industry to invest in cybersecurity.

Thank you again for the opportunity to testify, and I will be happy to answer any questions that you may have.

LOCKTON