the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

Advisen Cyber Risk Panel at RSA 2016

March 2, 2016 San Francisco, California

Quantifying Risk—Closing the Chasm between InfoSec and Cyber Insurance

San Francisco, CA (March 2, 2016) — A panel of experts from the insurance and cyber security industries met to discuss the challenges involved in transferring cyber risk.

The session was convened by PivotPoint Risk Analytics CEO Julian Waits. John Pescatore, Director of Emerging Security Trends at the SANS Institute served as moderator, and the panelists were Devon Bryan *(former CISO, ADP, now CISO of the Federal Reserve System)*, Ben Beeson *(Cyber Risk Practice Leader, Lockton Companies)*, Tom Fuhrman *(Managing Director, Marsh Risk Consulting)*, and David Bradford *(Cofounder & Chief Strategy Officer, Advisen)*.

There's a gap in knowledge and standards between the information security and insurance communities. As PivotPoint's Julian Waits put it in his welcoming remarks, "Both parties define risk very differently." This gap is a barrier to the creation of effective and sustainable cyber insurance product and practices.

Beeson noted, alluding to the Target breach, that "the approach of insurance companies pre-Target was a static approach." They tended to think that they could have a customer complete a survey, engage in some dialogue with them, and that would be that. But the reality is far more complex, and far more dynamic.

Currently, insurance premiums are set by the market as opposed to being established against credible models of risk. There has long been a big idea circulating among consultancies with cyber risk practices: do assessments for clients and use the results of those assessments to drive down the cost of insurance for those clients. But there's a problem here. "Nobody," said Tom Fuhrman, "has sufficient data to do good risk models in cyber."

One of the major concerns companies have about cyber security is, of course, its role in securing their intellectual property. Theft of intellectual property was, to be sure, a big problem in pre-cyber days, but it's grown in importance in recent decades. "Intellectual property is uninsurable," Beeson said, and Bradford added, "Part of the problem lies in quantifying loss."

Part of the complexity to the market is the difficulty of accounting not only for a shifting regulatory environment—an environment that itself imposes risk—but also the difficulty of risk accumulation and aggregation. Cyber risk underlies the entire portfolio; it's not easy, perhaps it's not possible, to confine it to cyber policies narrowly conceived. This too is characteristic of an immature market. "Carriers have to worry about aggregation risk," Fuhrman said, and they must also deal with an equally immature re-insurance market.

Since this is an evolving market, and not a mature one like fire or automobile insurance, the sector continues to need heavy involvement with legal counsel. When asked who should be involved in discussions of cyber insurance purchases, Bryan thought that, in his experience, these decisions are made with about half the contribution coming from chief general counsels. The other major players, he said, were cyber security experts, then privacy officers.

As cyber insurance moves from market pricing to pricing based on risk, it will then become possible to write policies based upon how well the clients reduce cyber risk through their practices. This in turn will drive better enterprise security. We need, the panel thought, more carrot and less stick. Cyber insurance isn't there yet, but one hopes it's moving in that direction.

Pesacatore took the final words, recalling his experience serving with US Secret Service protective details. They always had, he said, short lists they'd check with respect to fire safety—not letting the protectee, for example, stay on the floor of a hotel higher than the ladders of the city's fire department could reach. We need similar kinds of short lists in cyber security. Basic hygiene might stop perhaps seventy to eighty percent of attacks. And that's not bad. Building still burn, but we understand—and the insurance industry helps enforce—the basics of protecting them from fire. That's what we should aspire to in cyber security.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 3.23.16