Majority of Board Members Realize Cyber Risk but Have No Plan

October, 2013

Property Casualty 360

Three fourths of corporate board of director members view cyber breach as a serious operational threat, said panelists here at Advisen's Cyber Risks Conference.

Until they plug into a cyber risk management framework, however, data breach remains a live wire of exposure.

According to Jody Westby, CEO of Global Cyber Risk, in 2008 Carnegie Mellon University reported around 6 percent of board of director members were looped in to the gravity of cyber risks. By 2012, the number had jumped to 56 percent. Today, three fourths of directors note it as a concern, but "have no real plan to manage privacy and security."

"From a carrier perspective, there isn't much cross communication between cyber and management guidelines," said Kirstin Simonson, underwriting director at Travelers.

The need is there. Chubb has calculated that each lost record costs $188, and breach victims can expect to face hundreds to thousands of leaked records per event.

Furthermore, scrutiny of cyber risk management will "inevitably be pushed into regulation," said Ben Beeson, partner at Lockton Companies. Securities and Exchange Commission (SEC) guidelines, effective February 2014, calls for increased cyber risk information sharing between U.S. companies and the federal government, and seeks to create by February of next year a common cyber security framework for all organizations.

The SEC is interested not only in the amount of personally identifiable information (PII) lost in a breach, but business and service interruption factors and scenarios. It regards senior management as the responsible party for setting mitigating strategies for these scenarios, said the panelists, and it is the board of director's responsibility to supervise senior management in their efforts.

"If anyone argues about the importance of creating a cyber risk plan, the SEC has already sent over 50 letters to board of director members about their unsatisfactory frameworks," said Gerald Ferguson, CEO of Universal Solutions International. "This is the way enforcement initiatives start--with polite letters from the staff."

Cyber risk is not just a regulation issue, but also a reputation issue, says Westby, since at the end of the day, there is "nothing more damaging to a company than reporting to customers that their PII has been leaked."

The panelists said that pushing the importance of cyber risk management onto corporate clients falls on insurers, by developing cost/benefit analysis for buying cyber insurance, and to focus on the market impacts of cyber breaches. This is a challenge, as much of the fallout of data theft, such as loss of business secrets and client trust, is uninsurable.

Insurers can look back to Y2K, said Ty Sagalow, president of Innovation Insurance Group, when the industry pulled together to face a looming, more than multi-million dollar threat. Some underwriters even developed special Y2K policies, and those companies that didn't look into Y2K exposure management strategies ended up with an exclusion for losses caused by the event if the event came to pass.

"It was a combination of underwriting and innovation that paved the way to serving client's needs while ensuring (policy) profitability," said Sagalow.

www.nationalunderwriter.com

Forward this article to a colleague

Address To | Recipient Name

Subject

Message

Send | Reset