was unveiled at the WCD Americas Institute in Miami on March 7, which convened directors from around the world and explored topics ranging from "Next Gen Crises ...

Mar. 19, 2018

The jump in cyber attacks is challenging how boards approach risk management and their readiness to handle emerging threats, says WomenCorporateDirectors (WCD) and Marsh & McLennan Companies' Global Risk Center new joint report, *Cyber Risk Management Response and Recovery*.

"With increasing threats of attack on their data and systems, boards are demanding much more information about their organizations' risk and how well they are covered against loss and breaches," says Susan C. Keating, CEO of WCD.

As the annual global economic cost of cyber-crime skyrockets, WCD has teamed up with Marsh & McLennan's Global Risk Center to explore hot-button issues for directors in the area of cybersecurity, including expanding regulatory requirements and boards' heightened responsibility to oversee new risks.

Marsh & McLennan's Global Risk Center interviewed WCD corporate directors to identify how companies are addressing cyber threats and the use of cyber insurance. "As the global regulatory landscape becomes more complex, cyber security is gaining increased board level attention," said Elisabeth Case, U.S. Cyber Advisory Leader, Marsh, a subsidiary of Marsh & McLennan Companies. "Boards are definitely stepping up their oversight."

Despite this, the report found that directors are still challenged by factors that they believe put their companies at greater risk:

- **Director-level experts are thin on the ground** – Most boards have only one

inadequate transparency from management – Management often paints a rosier picture than reality, leaving directors in the dark about risks, and rendering them unable to sufficiently support risk mitigation efforts.

To increase board awareness of company risk, the report provides "10 Questions to Ask Management about Your Organization's Cyber Readiness." Some questions include:

- Where do we rank in cyber preparedness compared to relevant peers, and how frequently does management perform cyber scenario testing/war games? How do we benchmark our performance?
- Which managers across the organization have accountabilities for cyber risks within IT, business lines, and other operational areas?
- What are the limits of liability of cyber insurance that we have available, and how can we determine if coverage is sufficient?

The report, the first in a joint series of Global Governance Insights on Emerging Risks, was unveiled at the **WCD Americas Institute** in Miami on March 7, which convened directors from around the world and explored topics ranging from "Next Gen Crises that Keep Directors Up at Night" to "How to Deal with a Difficult CEO."

"Cyber risk is just one of the areas in which boards have to 'see around corners' to anticipate what is coming next as far as threats and opportunities for their companies," said Keating. "With the increasingly complex nature of the risks ahead, sharing our best practices and hard-won experiences and insights is the best way to improve governance around these incredibly challenging areas."

Accounting • Advisory • Technology

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us