ARTICLE

Creating Cyber-Certainty in an Uncertain World

*Team @ Nasdaq Centre for Board Excellence

Understanding how to offset, mitigate and transfer risk is the true work of executive leaders and board directors. This work becomes even more important amid increasing and evolving cyber threats. To respond to these threats effectively, boards need the right level of insights and analytics to "contextualize" them and make informed decisions around risk transfer, acceptance and management. Fortunately, risk and governance experts have provided direction for boards to effectively operate even among uncertainties.

The cyber threat surface has exploded in size and capacity because of our global interconnectedness, our reliance on devices and our increasing number of internet-connected things—from cars and appliances to wearables. According to Dominique Shelton Leipzig, partner and head of Global Data Innovation at Mayer Brown, 127 new and connected devices are created every second. Last year, connected devices around the globe generated 2.5 quintillion bytes of data a day, with the global economic cost of data breaches in that year at $6.1 trillion, the equivalent of the world's third-largest GDP.

"Boards can prepare for a lot of the scenarios that seem to unfold today with greater regularity," said Steve Roycroft, CEO of RANE Network, a provider of risk intelligence to help companies build operational resiliency. "It comes down to the operating rhythm of the company, and whether training and reporting are woven into the DNA of how the company operates. How the company embraces risk as it matures is a critical area for board oversight. It is up to the board to encourage resiliency as part of the DNA of the enterprise."

> "To respond to these threats effectively, boards need the right level of insights and analytics to "contextualize" them and make informed decisions around risk transfer, acceptance and management."

Amid the rise in cyber threats are heightened cybersecurity regulatory activities at the international, federal and state levels. Proposed rules have been announced by the European Union (EU) and the U.S. Securities and Exchange Commission (SEC), in a growing number of states and by various industry-specific regulators.

Ransomware is "an 800-pound gorilla that is consuming a lot of time and money in terms of response and containment," according to Christopher Hetner, former Senior Cybersecurity Advisor to the SEC Chair. Hetner noted that SEC filings show mid-market companies are especially vulnerable because many lack the resources required to defend themselves when compared to larger firms. Moreover, the need for board preparedness is not just reserved for public companies, private companies have increasingly come into risk, particularly ones identified as targets by private equity firms.

On March 9, 2022, the SEC proposed regulations that would require public companies to disclose how their boards oversee cybersecurity and to report cybersecurity breaches within four days of the corporation's determination that a breach is a material event. Thus, public companies and their boards need reliable methods to discern whether an incident exceeds the threshold for materiality requiring disclosure.

In addition to SEC regulations, industry-specific mandates focused on earlier disclosure and awareness like the Computer-Security Incident Notification (CSIN), which requires reporting

of cyber risk incidents by financial services firms, are coming into effect May 1, 2022. And, just as the 2018 General Data Protection Regulation (GDPR), the security and privacy law passed by the EU which ushered in steep fines for non-compliant companies, new and stiffer regulations, such as the EU's Digital Operational Resilience Act (DORA), which targets the financial sector, are now making their way through the EU's regulatory maze.

Resources to aid executive leaders and directors to determine the material impact of cybersecurity risk quickly and accurately are essential, Hetner explained. But the market has struggled to connect the value of cybersecurity to a company's bottom line, rendering investments in cybersecurity difficult to justify. "There's a disconnect between cyber risk and business risk, and the way that's expressed in the boardroom," Hetner asserted.

The solution lies at the intersection of the cybersecurity insurance ecosystem and arming boards with data that is going to be meaningful and actionable, informing what types of oversight they should lean into. Boards need to be provided with insights and analytics to contextualize cyber risk and incidents to business, operational and financial impacts, to make confident decisions about risk.

*The article has been authored by for the **Nasdaq Center for Board Excellence** by their internal team.**

The Nasdaq Center for Board Excellence is a community and collaboration environment in which board engagement is deepened and experiences are shared.

For more details on the '**Nasdaq Center** for Board Excellence' please scan QR Code:

**The views and opinions expressed herein are the views and opinions of the author and do not necessarily reflect those of Nasdaq, Inc.

The Nasdaq Center for Board Excellence is a community and collaboration environment in which board engagement is deepened and experiences are shared.