RSA Conference 2018

Peer2Peer

Partnering in Governance: Cybersecurity Tools for Board/Manager Interaction

P2P1-T10: Partnering in Governance: Cybersecurity Tools for Board/Manager Interaction

Daniel Dobrygowski, Head of Governance and Policy, World Economic Forum

If cybersecurity was a solely a technical problem, it would be mostly solved by now. But true resilience to cybersecurity threats requires a cultural shift – and that requires leadership. This is why ultimate responsibility for cybersecurity strategy sits with the CEO and the Board of Directors.

At RSA Conference this year, we hosted an intimate Peer2Peer discussion on how IT security managers can best to work with boards of directors and CEOs to ensure that companies appropriately consider cybersecurity in their overall strategy and provide for their own cyber resilience. These sessions, one on Tuesday and then again on Friday, brought together CISOs, risk and compliance managers, as well as IT and other managers who work with their boards on understanding the implications of cyber risk to their business.

The conversation began with the proposition that business leaders need to appreciate that their organization's cyber resilience is a responsibility they own— it is not something that can be neatly and completely delegated to executives down the org chart with cyber security, information, or even technology risk in their titles. As more of our businesses and institutions function mainly through digital networks, cyber risks are often structural risks to a business. And for that reason, the risk/reward trade-off requires decision to be made at the strategy layer. As a starting point, responsibility at this level is described in the World Economic Forum's 2017 report *Advancing Cyber Resilience: Principles and Tools for Boards.*

In terms of board attention to this issue, participants noted that both awareness and consideration vary widely. Many of the participants noted that cybersecurity makes it to their boards' agenda at least quarterly. However, more than half of participants (and our own research comports with this) report that boards take up cybersecurity issues annually or only when an emergency arises. In order to get boards (and CEOs) to take up cyber strategy more often, or to make better decisions when they do, the participants shared some practices and mind-sets that they found helpful:

- Trust is vital. In working with the board, it is helpful to take the time to build a trusted relationship with board members. That means meeting with the risk or audit committee (or whoever has the cyber portfolio) and educating the board members on the topic. It also means ensuring that a manager is as transparent as possible with the board, sharing both good news and bad as well as differentiating among solutions

- Speak the language of boards. Managers must put things into terms that the board is familiar with and take the mystery out of cybersecurity. To the extent possible a CISO or IT manager should use risk indicators and frameworks or scorecards that give board members the ability to make informed decisions about where to allocate company resources.

- Activate other executives. Many participants reported that the CFO can be their biggest champion when it comes to advocating for greater resilience. By contextualizing cybersecurity in terms of how it supports the mission of the organization and providing clear solutions, technical managers can help to build a culture of security in their organization and develop a shared narrative about why cybersecurity is important for the board.

- Partner to share good practices. Managers need to encourage their boards and CEOs to take up good practices like scenario-testing and other preparations. It's important to have a game plan developed in advance for how to deal with ransomware or other cyber threats and to ensure that the board knows their part. Partnering—with other CISOs and/or with other boards—is a good way to share and develop these practices.

These discussions brought out a number of good practices for working with boards of directors and a lot of food for thought in cybersecurity governance. Ultimately, it'll be up to companies to ensure that their boards are educated on these issues, just as they are on financial and other risks. In the meantime, CISOs and IT and risk managers have a very important role to play in helping their boards see that company strategy needs to include cyber strategy.

Link: *Advancing Cyber Resilience: Principles and Tools for Boards:*
https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

A first-of-its-kind resource – developed by the World Economic Forum, a neutral platform for public-private cooperation – to support boards of directors and CEOs to take action on cybersecurity and cyber resilience strategy.