CYBER RISK GOVERNANCE A KEY RESPONSIBILITY FOR BOARDS OF DIRECTORS, LEADING EXECUTIVES SAY

Former SEC Commissioner and former Chief Risk Officer lead an international group of board directors, chief risk officers, and other C-level executives in providing guidance to boards and standards by which external parties can measure board performance on cyber risk governance.

June 26, 2018 – Amid growing demand for accountability and assurance that data, trade secrets, and infrastructure are secure from cyber-attacks, boards of directors often find themselves without clear guidance on their responsibilities as governors. This week, the Directors and Chief Risk Officers group ("the DCRO") published Guiding Principles for Cyber Risk Governance to help boards and those who depend on them assess the practices their organizations use.

"It's no longer a question of whether a company will be attacked but more a question of when, and what the company is going to do about it," said David X Martin, former Chief Risk Officer of asset manager Alliance Bernstein and co-Chair of the DCRO Cyber Risk Governance Council. Along with former SEC Commissioner, Roel Campos, Martin co-chaired the initiative that brought together experts from around the world to assemble these principles.

Kevin R. Brock, former Assistant Director for Intelligence at the U.S. Federal Bureau of Investigation, who was a member of the governance council, noted the domestic importance of the initiative. "Corporate America, like it or not, is both the prime target of and frontline defender against malicious cyber-attacks," he said. "Government cannot be relied upon for adequate deterrence, the problem is simply too large." While many of the headline cyber breaches have happened in the United States to U.S. companies, the issue is global and may be vastly underreported. Estimates of loss almost always rely on companies' self-reported tabulation of the costs of cyber incursions. In some cases, companies might have an incentive to underestimate losses to appear more secure than they really are. Or sometimes, organizations may simply be unaware of the attacks that are underway, with future costs yet to be determined.

Back in 2016, the FBI estimated that cyber risk losses from just ransomware attacks surged to over $1 billion from $24 million the year before. More recent estimates have increased 2016's costs more than five-fold, suggestive of the appearance of exponential growth in losses. And while it is difficult to establish authoritative figures, it is estimated by some that, collectively, cyber risk events worldwide will cost companies over $3 trillion this year.

"Cyber risk represents an existential threat that goes beyond traditional risk management frameworks and practices," said Lloyd Komori, who is a member of multiple boards of directors, a former Chief Risk Officer, and is an instructor at McMaster University's Directors College. Calling on boards to enhance their understanding of the governance of cyber risk, Komori continued, "we wrote the DCRO Guiding Principles for Cyber Risk Governance to provide a robust foundation that will help board directors execute their fiduciary duties relating to the effective oversight

of their organizations' specific actions relating to information security, data protection, and privacy related risks."

Brock echoed the call for better understanding and actions by organizations, saying, "Corporate leaders must take the helm on this issue and do their part. These guiding principles can help with desperately needed strategic cyber risk management in the private sector."

It is becoming more apparent that boards do not have a sufficient grasp on the placement of cyber risk governance in their wide range of legal duties. Mark Trembacki teaches Enterprise Risk Management at the University of Illinois and was the chair of the 2017 Cybersecurity Conference for the Private Directors Association, an association of board directors at privately held companies. "Cyber risk is unavoidable given the integral role of technology in innovation, growth, and performance," he noted. "We must support the board's critical oversight responsibility by elevating cyber security to a strategic imperative with corresponding treatment as an enterprise risk."

Braden Perry, a litigation, regulatory and government investigations attorney with Kennyhertz Perry, LLC., shared his experience in working with boards seeking to better understand their role. "One area that I consistently counsel a board is being proactive versus reactive. Having a sophisticated board, not only in business strategy, but in today's cyber and IT security, is a must to understand the issues and protect the company from these types of harms," Perry pointed out.

The five key guiding principles focus on:

1. The identification of key assets that are vulnerable to attack.

2. Recognition that cybersecurity is a strategic issue, not just a technological one.

3. Establishment of three lines of defense and response/adaptation to changing threats.

4. The role of third-party vendors in attenuation or exacerbation of cyber risks.

5. Corporate culture around cyber threats.

Avinash Persaud, Emeritus Professor at Gresham College and Chairman of Elara Capital PLC in the U.K., provided guidance to the governance council co-chairs during the development of the guiding principles. "The stakes are as high as they get," he said. "Whether the digital economy proves to be a source of empowerment and plenty or division and scarcity hinges on governments, firms, and individuals managing cyber risks well." Persaud also sits on multiple corporate boards and is a member of the Council on the International Monetary System for the World Economic Forum.

"The guiding principles give board members specific direction on how to oversee a very complex and high-risk issue that will continue to escalate as technology evolves," said Carol Gray, a member of the board at IFM Investors Pty in Australia and chair of the board risk committee at Amex Bank of Canada. "The board can support management's efforts within the well-established three lines of defense and set the expectation to stay appraised of the changing risk environment," she added. Like Persaud, Gray provided advice to the co-chairs of the governance council.

Emphasizing the important role that boards play in ensuring that all individuals at organizations understand the cyber risk culture and risks, Florence Anglès, Chief Risk Officer, REYL & Cie Ltd. and founder of GIROS, a Risk Manager Association in Switzerland, said that "individuals are often the weakest link in cybersecurity. They need to be aware and trained individually in order to make it a part of the DNA of the organization. Collective effort is the secret sauce of a successful cybersecurity culture." Perry believes that the guiding principles, when adopted, will echo proactivity from a board perspective, "translating an understanding of the importance of a proactive IT security policy, and feeling like the company is 'on board' with IT security efforts, will communicate the right culture to individuals."

Komori, Anglès, Trembacki, and Perry were among more than twenty other experts from five continents who lent their knowledge and support to the development of the DCRO Guiding Principles for Cyber Risk Governance.

"The DCRO is a non-commercial, practitioner-led, collaborative initiative to advance risk governance practices at boards around the world," said David R. Koenig, founder of the Directors and Chief Risk Officers group. "The work done by this group will help ensure the stability of institutions that we trust - as long as boards take action and incorporate these principles into their governance practices."

Governance Council Co-Chair Roel Campos, who leads the Securities Enforcement practice at Hughes Hubbard & Reed law firm in Washington, DC, noted the intent of these guiding principles to be practical and helpful for boards. "Directors are drowning in their many responsibilities and duties to investors," he said. "These cybersecurity principles for directors provide welcome relief and will help ease the burden of properly overseeing cybersecurity in their companies." Governance council co-Chair Martin added that "Cybersecurity is not a problem to be solved. It's an ongoing risk to be managed. "These guiding principles are an important step in that direction," concluded Persaud.

The DCRO Guiding Principles for Cyber Risk Governance are freely available for download**.**

About the Directors and Chief Risk Officers group - The DCRO was formed in 2008 to focus on the top-level governance of risk in practice. Bringing together leading board members, chief risk officers, and other c-level officers whose jobs include a fiduciary responsibility for governance and risk management, the DCRO counts more than 2,000 members from large and mid-size for-profit and nonprofit organizations, coming from over 115 countries. DCRO members participate in facilitated meetings, conference calls, benchmarking research, and governance councils that allow them to compare current practices with those adopted by fellow members, those being required by regulatory bodies, or those expected by investors. Membership in the DCRO is strictly limited to active or recently active, board members, chief risk officers, or c-level executives with risk governance responsibilities.