NACD Audit Committee Chair and Risk Oversight Advisory Councils

Emerging Trends in Cyber-Risk Oversight

Increasing threats to corporate information systems, critical infrastructure, and intellectual property—as well as compliance risks, liability concerns, and the potential for reputational damage or lost business—continue to make cybersecurity a top priority in the boardroom and the C-suite.

On March 31, 2015, NACD collaborated with KPMG's Audit Committee Institute (ACI), PwC, and Sidley Austin LLP to co-host the first-ever joint meeting between the NACD Audit Committee Chair Advisory Council and the NACD Advisory Council on Risk Oversight. The session brought together committee chairs from Fortune 500 corporations, technology experts, and governance stakeholders for an open dialogue on the key issues and challenges impacting audit committee and risk committee agendas.

Council delegates joined Charles Beard, a principal in PwC's forensics practice; Jim Liddy, vice chair of KPMG's US and head of the firm's Americas audit practice; and Edward McNicholas, a co-leader of Sidley Austin's privacy, data-security, and information-law practice to discuss a question now on the minds of many board members: What does good cybersecurity oversight look like?

The conversation highlighted several considerations for directors—and for risk and audit committee members in particular—to keep in mind as they deepen their engagement in their companies' efforts to manage cybersecurity risk. Takeaways included the following:

- Stay abreast of changing regulatory and risk management developments related to cybersecurity.
- Assess the effectiveness of the IT function's structure and skills with respect to cyber-risk management.
- Recognize that internal vulnerabilities exist at every level of the organization—including the board.
- Assess the company's management of cybersecurity in the context of leading industry practices.

Stay abreast of changing regulatory and risk management developments related to cybersecurity.

Despite an increased focus on cybersecurity, the cyber-risk landscape remains fluid and opaque, even as expectations rise for more-engaged board oversight. *"This is very much a moving target,"* said one delegate. *"The threats and vulnerabilities are changing almost daily, and the standards for how to manage and oversee cyber risk are only beginning to take shape."*[1] Directors can ask

management, in-house and outside counsel, and the external audit firm to brief the board at regular intervals on cyber-related developments relevant to the company (including those related to the firm's industry and operating footprint) and their associated implications for the company's cybersecurity activities.

The lack of a common framework and vocabulary for managing and overseeing cyber risk—particularly in a global context—is clearly a concern, as businesses and boards look for leading practices and guidance on taking a proactive approach to cyber risk. Sidley Austin's Edward McNicholas noted that support is growing for use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[2] a voluntary protocol for reducing cyber threats to critical infrastructure, as a common standard that could be implemented by companies in any industry: "There is good consensus forming around the NIST framework following the presidential Executive Order. It is voluntary, but NIST will no doubt be referenced in insurance ratings after attest standards are formalized by the [American Institute of Certified Public Accountants]. I think you'll see more and more business partners expecting it from each other." Some delegates observed, however, that other protocols are in active use, and that no single framework has yet become the universal standard.

Meeting participants also noted that more clarity is needed regarding the role and responsibilities of the external auditor with respect to cybersecurity matters, and they emphasized the importance of having robust discussions with the auditor to understand the scope of the audit relative to the firm's cyber risk. As KPMG's Jim Liddy remarked, "If there's confusion about the auditor's role on cyber, there may be a more fundamental misunderstanding of what the auditor does and doesn't do."

While the external auditor is responsible for auditing financial statements and internal control over financial reporting—potentially including financial reporting-related IT systems and data—the audit does not currently look at cybersecurity risks across a company's entire IT platform. Participants suggested that while audit firms do not currently provide separate attestation services around cybersecurity, such services may be offered in the near future. In the meantime, *"[while] auditors are not going to opine on the efficacy of the company's IT systems, … they can offer perspective based on all the work they do at the company—and the audit committee or board*

[1] Italicized comments are from delegates and guests who participated either in the Mar. 31, 2015, meeting or in related teleconferences on Apr. 14, 2015, or Apr. 20, 2015. Discussions were conducted under a modified version of the Chatham House Rule, whereby names of meeting attendees are published but comments and ideas are not attributed to individuals or organizations (excepting cohosts of the event).
[2] For additional details, see National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Feb. 12, 2014.

should be asking for that perspective," said one director. In addition, delegates pointed to the Center for Audit Quality's member alert, "Cybersecurity and the External Audit," as a helpful resource in clarifying the external auditor's role as it relates to cybersecurity risk.[3]

Assess the effectiveness of the IT function's structure and skills with respect to cyber-risk management.

Delegates described changes their companies have recently made in their IT function's leadership team in order to better respond to cyber threats. In previous meetings of the Audit Committee Chair Advisory Council, delegates discussed similar trends taking place within the internal audit function at many organizations.[4] In both cases, critical skills include the ability to translate cyber risks into business and strategy risks and to collaborate with business unit leaders and peers across the organization. *"At one company we had a serious breach several years ago,"* said one director. *"After we got out of the denial phase, we made significant changes, including replacing the CIO with an individual who was much more skilled in thinking about people, process, and behavior issues related to cybersecurity, not just the technology issues."* Several directors noted that their companies have hired chief information security officers (CISOs), an increasingly common role: *"They can serve as a check-and-balance on the CIO and work with the businesses to ensure that the firm is operating smoothly and growing, but in a secure way."*

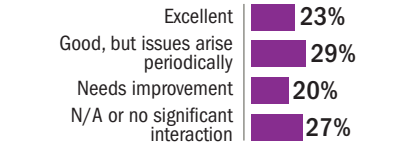
Delegates also suggested that board members need to ask questions about IT leaders' performance measures and incentives, as well as their stature in the organization: "*Does your CIO actually have the proper decision-making authority? CIOs are typically evaluated on things like system uptime and controlling costs—so is the board getting an unbiased view of the company's vulnerabilities?"* One participant described a scenario at a company where the CIO's responsibility extended only to the corporate IT network—decisions related to new product development, including Internet-connected devices that could pose significant risk to customers, were outside this executive's purview. Many audit and risk committees now meet regularly with CIOs or CISOs to discuss such cybersecurity issues, and several delegates suggested that executive-session meetings with these

By the Numbers

Please assess the quality of information provided by management on cybersecurity and information technology risk:

Source: National Association of Corporate Directors (NACD), *2014–2015 NACD Public Company Governance Survey* (Washington, DC: NACD, 2015)

Please rate the quality of the audit committee's interactions with the chief information officer:



Source: KPMG Audit Committee Institute (ACI), *KPMG's 2015 Global Audit Committee Survey* (Washington, DC: KPMG ACI, 2015)

[3] See Center for Audit Quality, "Cybersecurity and the External Audit" (CAQ Alert #2014–03), Mar. 21, 2014.
[4] See NACD Audit Committee Chair Advisory Council, *The Audit Committee's Role in Cybersecurity Oversight* (Washington, DC: NACD, 2014).

executives, analogous to those that take place between the CFO or chief audit executive and the audit committee, might become more common in the future.

Recognize that internal vulnerabilities exist at every level of the organization—including the board.

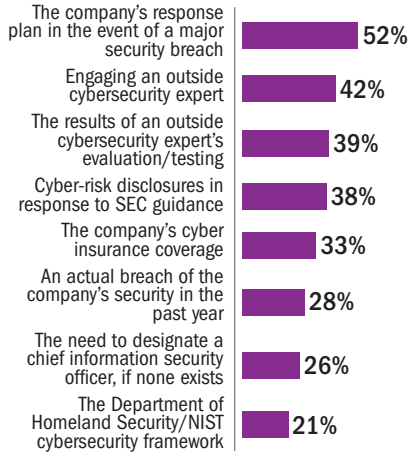
Meeting participants generally agreed with one director who remarked, *"One of the biggest sources of cyber risks comes from people—whether their actions are intentional or unintentional, they can cause great damage."* Accordingly, boards should ask management questions about the extent to which the company's training and operating policies are designed to cultivate a "neighborhood-watch" mentality about cybersecurity at all levels of the organization. Management's reports should include information on how security protocols, data and e-mail retention policies, access permissions, and the like are clearly communicated, regularly updated, and rigorously enforced at all levels of the organization—including at the director level. Charles Beard of PwC reminded the group, "Senior officers are prime targets for cyberattacks such as spearphishing [fake e-mails with embedded malware] via LinkedIn or other social media. And board members are an especially target-rich environment—they have access to the company's most valuable, most confidential, market-moving information." At a previous meeting of the Advisory Council on Risk Oversight, delegates noted that directors and management should also understand the parameters of privileged communications regarding cyber breaches. For example, emails and telephone calls between a CFO and a risk or audit committee chair "are not privileged and must be handled with great care."[5]

Assess the company's management of cybersecurity in the context of leading industry practices.

When a cyber-breach occurs—an event that is becoming inevitable for most companies—directors and management must be able *"to assert a 'good corporate citizen' framework of defense,"* in the words of one participant. In the absence of clearly-established standards for cyber-risk management or board-level oversight, delegates suggested *"starting with what's happening in the industry. What does average versus leading practice look*

By the Numbers, cont.

The following cybersecurity issues have been discussed by the board or its committees:



Source: PwC, *PwC's 2014 Annual Corporate Directors Survey* (Washington, DC: PwC Center for Board Governance, 2014)

[5] NACD Advisory Council on Risk Oversight, *Cybersecurity Oversight and Breach Response* (Washington, DC: NACD, 2014).

like? Where do we fall on the spectrum? Either of those could change in six months, so this has to be an ongoing conversation." Benchmarking sources include information-sharing groups focused on cyber threats—including initiatives that are industry-specific, cross-sector, and multi-country—which continue to gain momentum in the US and internationally, as well as independent advisors and third-party experts. Directors can ask management to report on key takeaways from these data sources, including performance relative to peers or other benchmarks, and on resulting action items that can further strengthen the company's cybersecurity program.

FOR FURTHER READING

- National Association of Corporate Directors (NACD), *Cyber-Risk Oversight*, Director's Handbook series (Washington, DC: NACD, 2014)
- NACD, "Assessing the Board's Cybersecurity Culture" and "Building a Relationship with the CISO: A Road Map for Directors" (Washington, DC: NACD, 2015)
- Craig Bell and Tony Buffomonte, *Connecting the Dots: A proactive approach to cybersecurity in the boardroom* (Washington, DC: KPMG LLP, 2015)
- Don Keller, Barbara Berlin, and Elizabeth Strott, *Directors and IT What Works Best: A user-friendly board guide for effective information technology oversight* (Washington, DC: PwC Center for Board Governance, 2012–2015)
- Center for Audit Quality, "Cybersecurity and the External Audit" (CAQ Alert #2014–03), Mar. 21, 2014
- Holly J. Gregory, "Board Oversight of Cybersecurity Risks," Practical Law (March 2014): 24–28

Advisory Council Meeting Participants*

Charles E. Adair
Tech Data Corp.

James Bachmann
Nationwide Mutual Insurance

Charles Beard
PwC

Dennis R. Beresford
The National Association of Corporate Directors

Jenne K. Britell
Crown Holdings Inc.

Raymond J. Bromark
CA Technologies Inc.

Jeffrey R. Brown
TIAA-CREF

Leslie Brun
Merck & Co.

Mary Ann Cloyd
PwC Center for Board Governance

Irwin Cohen
SUPERVALU

Kathleen B. Cooper
The Williams Companies Inc.

Mary Cranston
Visa Inc.

Brian Croteau
U.S. Securities and Exchange Commission

Gerald M. Czarnecki
State Farm Bank

Steven G. Elliott
PPL Corp.

Cynthia M. Fornelli
Center for Audit Quality

Jeannette M. Franzel
Public Company Accounting Oversight Board

Patrick Gross
Waste Management Inc.

Robert L. Guido
Commercial Metals Co.

Mary J. Steele Guilfoile
Interpublic Group

Jay D. Hanson
Public Company Accounting Oversight Board

Leslie Heisz
Ingram Micro

Robert K. Herdman
Cummins Inc.

Robert H. Herz
Morgan Stanley

Irvine Hockaday
Estee Lauder Cos. Inc.

Renée Hornbaker
Eastman Chemical Co.

Barry W. Huff
Legg Mason Inc.

Balakrishnan S. Iyer
HIS Inc.

Thomas J. Kim
Sidley Austin

James A. Lash
Baker Hughes Inc.

Catherine P. Lego
SanDisk Corp.

James P. Liddy
KPMG

William Loomis
Phillips 66

Paula Loop
PwC

Sara Mathew
Campbell Soup Co.

*This list includes delegates, partners, stakeholders, and guests who participated either in the Mar. 31, 2015, meeting or in related teleconferences on Apr. 14, 2015, or Apr. 20, 2015.

Edward R. McNicholas
Sidley Austin

Patrick S. Mullin
The Andersons Inc.

Leslie A. Murphy
Kelly Services Inc.

Bruce P. Nolop
Marsh & McLennan Cos.

Charles H. Noski
Microsoft Corp.

Joseph M. O'Donnell
DTx Inc.

F. Gardner Parker
Carrizo Oil & Gas Inc.

Richard W. Roedel
Lorillard Inc.

Francesca Ruiz de Luzuriaga
Office Depot

James V. Schnurr
U.S. Securities and Exchange Commission

Leslie F. Seidman
Moody's Corp.

Gregory Smith
Lear Corp.

Lawrence W. Smith
Financial Accounting Standards Board

Robert Stein
Assurant Inc.

Richard Swift
CVS Caremark Corp.

Laura S. Unger
CA Technologies Inc.

Dennis T. Whalen
KPMG's Audit Committee Institute

Billie I. Williamson
Energy Future Holdings

David A. Wilson
Barnes & Noble Inc.

Alison A. Winter
Nordstrom

Wilhelm Zeller
Towers Watson & Co.

Robyn Bew
National Association of Corporate Directors

Kenneth Daly
National Association of Corporate Directors

Peter R. Gleason
National Association of Corporate Directors

Kate Iannelli
National Association of Corporate Directors

About the Audit Committee Chair and Risk Oversight Advisory Councils

With a focus on the common goal of a sustainable and profitable corporate America, the National Association of Corporate Directors (NACD) created the Audit Committee Chair Advisory Council in partnership with KPMG's Audit Committee Institute (ACI) and Sidley Austin LLP; and the Advisory Council on Risk Oversight in collaboration with PwC and Sidley Austin LLP. Since 2009 and 2012, respectively, these councils have brought together experienced committee chairs from Fortune 500 companies with key shareholder representatives, regulators, and other stakeholders to discuss ways to strengthen corporate governance generally and the work of the audit and risk committees in particular.

Delegates of the councils have the opportunity to engage in frank, informal discussions regarding their expectations for committee practices, processes, and communications and to share observations and insights on the changing business and regulatory environment. The goal of the councils is threefold:

- to improve communications and build trust between corporate America and its key stakeholders;
- to give voice to directors engaged in audit and risk committee activities and improve the quality of the national dialogue on related matters; and
- to identify ways to take board and committee practices to the "next level."

NACD believes that the open dialogue facilitated by these advisory councils is vital to advancing the overarching goal of all boards, investors, and regulators: building a strong, vibrant capital market and business environment that will continue to earn the trust and confidence of all stakeholders.