NACD Risk Oversight Advisory Council

Current and Emerging Practices in Cyber-Risk Oversight

Introduction

As cyberattacks increase in frequency and severity, cybersecurity oversight continues to top the list of boardroom priorities. Data from the *2018–2019 NACD Public Company Governance Survey* finds that directors selected the threat of cyberbreach as the third most likely to have the greatest impact on their companies in the coming 12 months.[1] NACD data also finds that a significant number of directors of both public and private companies are looking to improve cybersecurity oversight across the coming year—97 percent and 94 percent, respectively.[2] Additionally, a majority of corporate directors (57%) cite increased resources or budget dedicated to cybersecurity, according to PwC.[3]

On March 13, 2019, NACD, PwC, and Sidley Austin LLP convened a meeting of the Risk Oversight Advisory Council. The discussion with risk and audit committee chairs from Fortune 500 companies focused on leading practices related to the board's oversight of cybersecurity risks. The following insights emerged from the discussion:

- At its core, cybersecurity is a people issue, and boards should tailor their oversight activities accordingly.
- Cyber-risk reporting to the board should evolve to keep pace with the changing needs of the organization, and of the board itself.
- Boards should ask how their companies are engaging in information-sharing within their own industries and with the public sector.

At its core, cybersecurity is a people issue, and boards should tailor their oversight activities accordingly.

Security Policy Implications

Recognizing its importance, meeting participants highlighted two aspects of the human side of cybersecurity that should be included on the board's

2019 BOARD PRIORITIES

What five trends do you foresee having the greatest effect on your company over the next 12 months? (Percentage of respondents including issues in top five trends. Only the top five trends are shown below.)

n=495

48.9%
Change in the regulatory climate

48.3%
Economic slowdown

41.8%
Cybersecurity threats

39.8%
Business-model disruptions

39.0%
Geopolitical volatility

Source: *2018–2019 NACD Public Company Governance Survey*

[1] NACD, *2018–2019 Public Company Governance Survey* (Arlington, VA: NACD, 2018), p. 11.

[2] NACD, *2018–2019 Public Company Governance Survey* (Arlington, VA: NACD, 2018), p. 46; NACD, *2018–2019 Public Company Governance Survey* (Arlington, VA: NACD, 2018), p. 31.

[3] PwC's 2018 *Annual Corporate Directors Survey*, p. 11.

agenda: security policy implications, and skill requirements and gaps. It's essential for organizations to have programs and policies in place that allow enterprise-wide visibility into potential threats, whether they originate internally or externally. Catherine Bromilow, partner at PwC's Governance Insights Center, notes that while "current employees are the top source of security incidents—whether intentional or not—only half (52%) of executives say their company has an employee security awareness training program."[4] Council participants also shared the following:

- *"Sometimes the exposure is from people who don't realize {that} what they're doing—for example, sending documents to a home computer or using USBs—is creating a security issue."*
- *"At one company we had an issue where an employee's downloading behavior was flagged. It turned out they were acting on behalf of a foreign country and we were able to prosecute."*
- *"[Our chief information security officer (CISO)] breaks things down into malicious and nonmalicious activity. The latter may be due to ignorance, or desire for speed and convenience—these things can be addressed through training and monitoring. The former is more difficult, but things like rigorous annual background checks as part of some job descriptions, so the organization is transparent about the requirements for these roles, can help."*

To mitigate against these risks, delegates noted that boards' discussions with senior leaders of the security team should include the following considerations:

- **How close is the collaboration between key functions?** Information security departments are increasingly partnering with human resources (HR), as well as legal, compliance, and ethics departments, to ensure these functions are collaborating on cybersecurity activities. Collaboration between these functions should include the development of clear procedures around employee entry and exit procedures. As a meeting participant explained, *"At some companies, HR, corporate security, IT, and compliance are all separate entities. Silos can create blind spots."*

[4] Paula Loop, Catherine Bromilow, and Sean Joyce, PricewaterhouseCoopers LLP, *The Harvard Law School Forum on Corporate Governance and Financial Regulation* (blog), "Overseeing Cyber Risk," February 18, 2018.

- **How clear are our policies related to data access, and how are they reinforced?** One meeting attendee noted, *"For some of our employees, we don't even grant Internet access to connect to our network, [thereby eliminating] any potential threat from [the employees]. [In addition], database administrators hold the keys to the castle; [so] we do a background check every year; there is a higher threshold [for these individuals] and that has helped to lower the threat."*

Skill Requirements and Gaps

Meeting participants reported that their CISOs are dealing with acute talent shortages and skills gaps—making human capital an increasingly important area of board oversight. As boards engage members of the executive team around this issue, directors will need adequate visibility into critical areas of their companies' workforce in order to proactively address relevant risk and strategy implications. In discussing cybersecurity skill shortages, meeting participants shared the following:

- Company size may be an important indicator of how acute a pain point this is. One director explained, *"My companies are finding it difficult to recruit technology talent, including in the CISO's team. Smaller organizations must have an even bigger challenge."* To deal with talent shortages, several meeting participants reported their companies are exploring partnerships with colleges and universities, to strengthen their technology and cybersecurity skills pipelines.
- According to attendees, a leading approach requires investing in training and maintaining high employee engagement and satisfaction in individuals who hold critical roles. A participant noted *"[Our CISO] treats his team like top sales [people]—competitive pay scale, and proactive conversations each year about [overall] benefits. We want them to know they matter. The risk department strives to have the highest employee satisfaction scores in the company."*
- Emerging technologies (including artificial intelligence, robotic process automation, machine learning, etc.) may have the potential to benefit information security organizations, but they alone won't solve the talent shortage problem. As a meeting participant commented, *"Advanced technology tools still require skilled people to run them and interpret the results."* Another attendee added, *"The rate of technology change is unreal, and*

As boards engage members of the executive team around this issue, directors will need adequate visibility into critical areas of their companies' workforce in order to proactively address relevant risk and strategy implications.

cybersecurity organizations [are likely to] benefit. Directors should continue to ask questions about the [return on investment] on [cyber assets], including new tools. [However,] they should not lose sight of the importance of holding business leaders accountable for a healthy cybersecurity culture."

Cyber-risk reporting to the board should evolve to keep pace with the changing needs of the organization, and of the board itself.

Reporting to the board on cybersecurity has come a long way in recent years. According to NACD research, roughly 83 percent of public company directors and 68 percent of private company directors reported that the quality of cyber-risk information provided by management has improved in the past two years.[5] A survey from PwC also finds that roughly two-thirds (67%) of directors say cybersecurity reporting has increased, and more than half are using external advisors to enhance reporting.[6] While these findings point to growing comfort among directors on current reporting practices, the speed of change in cyberattacks requires boards and their companies to adopt proactive approaches to cybersecurity governance. Meeting attendees agreed that the CISO's communication to the board should be flexible enough to reflect the changing threat environment, as well as evolving company circumstances and board needs. Participants reported a number of factors that motivated changes in the way their information security organizations are engaging with the board:

- **Maturity of the information security program.** A meeting participant commented that *"the board [currently] meets with the CISO twice a year. Ten years ago, [it was closer to] four times a year; back then, we were building up our program and in an earlier stage of maturity."*
- **"Steady state" vs. after an incident.** One director noted, *"At one company, we had an established schedule for the CISO's reports to the board. After we experienced a significant cyber incident, the frequency and content of the reports to the board changed for a period of time during the investigation and remediation."*

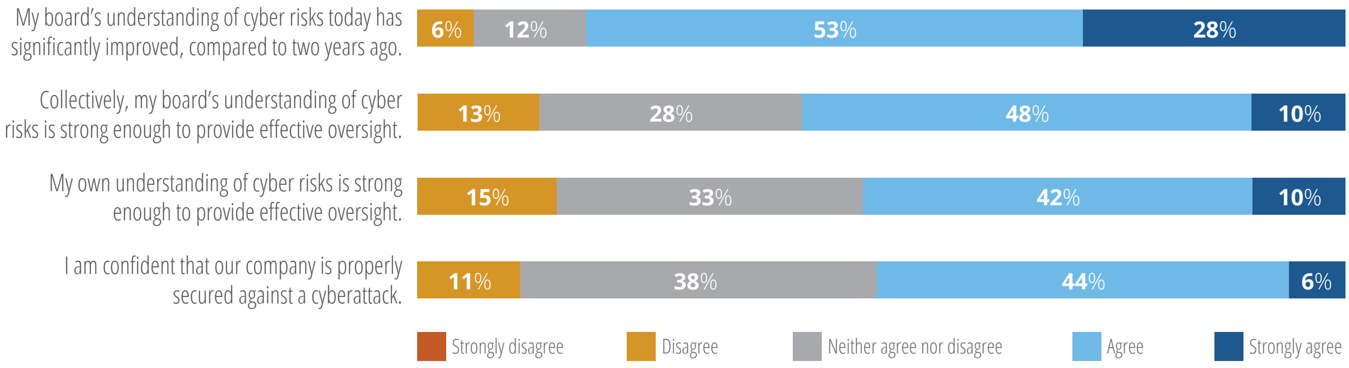
[5] NACD, *2018–2019 Public Company Governance Survey* (Arlington, VA: NACD, 2018), p. 67; and NACD, *2018–2019 Private Company Governance Survey* (Arlington, VA: NACD, 2019), p. 15.

[6] PwC's 2018 *Annual Corporate Directors Survey*, p. 11.

- **Regulatory compliance.** As one attendee said *"We are in a highly regulated industry, and the information the board sees is sometimes influenced by what the regulators require us to report on."*
- **Director tenure.** According to a meeting participant, *"One [factor] that affects our board reporting schedule is the tenure of board members. When [directors] have been there for a long time, they are familiar with our program; but with the introduction of new members, [CISO reporting] may shift." A delegate added, "As the risk committee chair, I sat with the CISO to map out the year's agenda for the cybersecurity portion of our committee meetings. This year we included some additional items because we have some directors that have just joined the committee."*

According to the *2018–2019 NACD Public Company Governance Survey*, a whopping 81 percent of directors now believe their boards' understanding of cyber risks has improved over the last two years.[7] Additionally, more than half of directors, 52 percent, are now confident that they personally have the understanding to provide effective cyber-risk oversight.[8] As directors' cybersecurity fluency has evolved, so has the type of information they are seeking from their management teams.

To what extent do you agree or disagree with the following statements?



Source: *2018–2019 NACD Public Company Governance Survey*

[7] NACD, *2018–2019 Public Company Governance Survey* (Arlington, VA: NACD, 2018), p. 67.

[8] Ibid.

Council members suggested that key committee leaders periodically review the format and content of cyber-risk reporting to ensure that it remains fit for purpose. Attendees also shared several examples of the type of content their boards are receiving from management:

- **Emerging cyber threats, and how they relate to the company.** A participant commented, *"[Our CISO] tracks headlines about cyberbreaches and trends, and reports to the board on what's applicable and the implications for our company."* Another attendee said, *"Directors are asking for more of an 'outside-in' perspective—they are familiar with our infrastructure, so they want to hear the current picture about how the environment is changing."*
- **Relative performance information.** One participant observed, *"The board wants information to answer the question, 'how do we compare?' [The company gets] results from annual penetration testing done by a third party, who also provides a comparative perspective."* A second attendee shared, *"Our CISO does a stack ranking of business units' performance on different cybersecurity metrics. That [practice has] really moved the needle in terms of getting management's attention, because nobody wants to be last on that list."*
- **Summary data.** A meeting attendee remarked, *"Our board gets a one-slide overview that shows risks, trends, and attacks from the last quarter."* A second participant added, *"The CISO at our company shares a monthly 'hot topics' document that summarizes important developments in the cybersecurity environment, including external news items, with the risk committee and audit committee."*

Boards should ask how their companies are engaging in information sharing within their own industries and with the public sector.

When it comes to information sharing, a meeting participant emphasized that, *"There is no competitive advantage to not sharing [cyber-threat information]."* While discussing the benefits of information sharing with government entities, a delegate cautioned, *"The first time a company reaches out to the FBI [Federal Bureau of Investigations] or DHS [Department of Homeland Security] should not be in the middle of a cyberattack."*

Council members discussed the following areas where directors can ask about the company's information-sharing activities:

- **Industry-level initiatives.** Meeting attendees discussed Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) as two starting points for companies. (See Sidebar, Examples of US Cybersecurity Information-Sharing Initiatives.)
- **Public-private sector initiatives.** Council members also brought up the following avenues that companies can leverage to collaborate more closely with law enforcement: field office CISO summits, the National Cyber-Forensics and Training Alliance (NCFTA), and the FBI CISO Academy.
- **Law enforcement as a source of information for management and the board.** According to a delegate, *"A local FBI representative partners closely with our CISO and CIO; [the board] asked if the representative would be willing to provide [us] with a briefing. [The representative] met with my committee for about two hours. . . . [We] found this session to be invaluable—not only from an information sharing [perspective], but the level of confidence that he has in our team. It was very validating for us."*

Directors also talked about the potential for legal liability or regulatory action in the wake of outreach to, or information sharing with, law enforcement agencies. Colleen Brown, partner at Sidley Austin, responded to these concerns, noting that, "There has been some easing of those concerns in past years, or at least since the Cybersecurity Information Sharing Act of 2015 was passed. [This provided companies some level of] comfort that when you share, even if regulators are not technically prohibited from receiving that information, [the act] did provide some measure of a liability shield for sharing information, particularly in terms of privacy violations when you follow the sharing protocols."

Examples of US Cybersecurity Information-Sharing Initiatives

- Information Sharing and Analysis Center
- Information Sharing and Analysis Organizations
- National Cyber-Forensics and Training Alliance
- The FBI CISO Academy

Conclusion

Breaches and cyberattacks are expected to continue to escalate, especially as a growing number of companies rely on customer data to transform business models and create value. As malicious actors develop increasingly sophisticated tactics to exploit vulnerabilities in companies' security infrastructures, companies need to be vigilant in guarding their most valuable assets. A completely secure system is unattainable; however, boards and management teams should attempt to achieve the highest level of security possible for the systems they oversee. As one director remarked, *"You'll likely never have enough people or money; so the most important thing is to reduce [your company's] risk exposure. You can look at all external-facing [access points]. You [should also understand] what data your company has, what must be protected, how it's being protected, and how it's being shared with third parties. As a board member you need to be asking, 'are we doing everything we can to reduce our risk exposure?'"*

Questions directors can ask their management teams about cybersecurity:

1. What are our company's crown jewels? Who has access to these and what is our company's framework for protecting them?
2. What processes and policies do we have in place to review our company's cyber incident response plan? How frequently are these revisited? How are we mitigating against potential security gaps?
3. What items or initiatives fell below the cut line on the last budget cycle, and why?
4. What is our talent strategy for critical roles in our company's information security? Are there succession plans in place for those in leadership positions? What is our company proactively doing to attract, retain, and, when applicable, outsource this type of talent?
5. Are there specific areas of the organization (e.g., geographical, business, functional, or levels of seniority) that are allowed exceptions to compliance with cybersecurity policies? Which ones and why? How do we assess the risks of these exceptions?
6. What is the nature of our company's relationship with local, state, and/or federal law enforcement agencies?
7. How is our information security team partnering with our HR, legal, compliance and ethics, and internal audit functions?

For Further Reading:

- *NACD Director's Handbook on Cyber-Risk Oversight*
- *Director FAQ: The Board's Role in Data Privacy Oversight*
- *Emerging Trends in Cyber-Risk Oversight*
- *How Your Board Can Better Oversee Cyber Risk*
- "Board Oversight of Cybersecurity Risks"

Advisory Council Meeting Participants*

Tracy A. Atkinson
Raytheon Co.

Maureen A. Breakiron-Evans
Cognizant Technology Solutions Corp.

Catherine Bromilow
PwC

Colleen T. Brown
Sidley Austin

Jeffrey C. Brown
Raytheon Co.

Herman E. Bulls
USAA

Larry Clinton
Internet Security Alliance

Kathleen B. Cooper
Williams Companies Inc.

Steven G. Elliott
PPL Corp.

Juan R. Figuereo
PVH Corp.

Cynthia M. Fornelli
Center for Audit Quality

Martha C. Goss
American Water Works Co. Inc.

Patrick W. Gross
Waste Management Inc.

Christopher Hetner
Marsh & McLennan Companies

Michael W. Hewatt
DR Horton Inc.

Renée J. Hornbaker
Eastman Chemical Co.

Catherine Ide
Center for Audit Quality

Donna A. James
L Brands Inc., Marathon Petroleum Corp.

Letitia A. Long
Raytheon Co.

Mary Pat McCarthy
Palo Alto Networks Inc.

Gregory Montana
FIS

Thomas M. Murnane
Pacific Sunwear of California Inc.

Patricia A. Oelrich
Federal Home Loan Bank Office of Finance

Hon. Lynn Schenk
Biogen Inc., Sempra Energy Corp.

Sherry Smith
Deere & Co.

Gregory C. Smith
Lear Corp.

Robert W. Stein
Assurant Inc.

Stacey L. Stevens
Federal Bureau of Investigation

Thomas M. Tefft
American Family Mutual Insurance Holding Co.

Joel Whitaker
Frontier Strategy Group

Bradford Willke
Department of Homeland Security

Stephen R. Wilson
Huntington Ingalls Industries Inc.

National Association of Corporate Directors

Robyn Bew
Peter Gleason
Stessy Mezeu
Leah Rozin

* This list includes delegates, partners, stakeholders, and guests who participated in all or part of the meeting on March 13, 2019, and/or in a related teleconference on March 20, 2019.

About the Advisory Council on Risk Oversight

The National Association of Corporate Directors (NACD) created the Advisory Council on Risk Oversight with a focus on the common goal of a sustainable and profitable corporate America. Since 2012, this council has brought experienced risk and audit committee chairs from Fortune 500 companies together with key shareholder representatives, regulators, and other stakeholders to discuss ways to strengthen corporate governance in general—and risk oversight in particular. PwC and Sidley Austin LLP collaborate with NACD in convening and leading the council.

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

- Improve communications and build trust between corporate America and its key stakeholders.
- Give voice to directors engaged in risk oversight and related matters and improve the quality of the national dialogue on the board's role in risk governance.
- Identify ways to take risk-oversight practices to the next level.

NACD believes that the dialogue facilitated by this advisory council is vital to advancing the shared, overarching goal of all boards, investors, and regulators: a sustainable, profitable, and thriving corporate America.

National Association of Corporate Directors
1515 N. Courthouse Road, Suite 1200
Arlington, VA 22201
571-367-3700
NACDonline.org

This publication is designed to provide authoritative commentary in regard to the subject matter covered. It is provided with the understanding that neither the authors nor the publisher, the National Association of Corporate Directors, is engaged in rendering legal, accounting, or other professional services through this publication. If legal advice or expert assistance is required, the services of a qualified and competent professional should be sought.