Audit Committee Leadership Summit

July 2019

ACLS

VIEWPOINTS

Cybersecurity governance

Cybercrime is estimated to cost the world trillions of dollars annually,[1] and even companies with the best preventative measures in place are vulnerable to cybersecurity breaches. *"This is a fundamental, existential risk to enterprises. The entire organization can go down,"* a member of the Audit Committee Leadership Network (ACLN) said.[2] Policymakers, too, are keenly aware of the threat. Europe's General Data Protection Regulation requires rapid breach notification and threatens massive financial penalties. In the United States, Securities and Exchange Commission guidance calls out the board's role in cybersecurity oversight: "We believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."[3]

Given the importance of this risk, audit committee chairs are eager to learn and implement techniques for improving board-level cybersecurity oversight. On June 7, 2019, members of the ACLN and the European Audit Committee Leadership Network (EACLN) met in New York to discuss cybersecurity governance with two guests: Marianne Brown, a member of Northrop Grumman's board of directors and co-chief operating officer of FIS, and Diana McKenzie, audit committee member at MetLife and former chief information officer at Workday and Amgen. *For guest biographies, see Appendix 1, on page 9. For a list of meeting participants, see Appendix 2, on page 10.*

Executive summary

The audit chairs and guests addressed two primary topics during their discussions before and during the meeting:

- **Board expertise, structure, and techniques** *(page 2)*

  Cybersecurity presents unique governance challenges. Some boards have added nonexecutive directors with cybersecurity expertise to help translate complex technical issues for the rest of the board. However, it is important for all board members to have some cybersecurity expertise and general information technology (IT) familiarity. Cybersecurity is ultimately a full-board issue, but it is typically delegated to the audit committee or another committee for deeper review. Oversight techniques like off-cycle interactions with cybersecurity managers and deep dives keep the board familiar with a company's cybersecurity practices.

tapestry NETWORKS

EY Building a better working world

- **Coordination between the board and management** *(page 5)*

  Boards rely on management to present cybersecurity issues from a strategy and risk perspective. Managers use cybersecurity frameworks in conjunction with dashboards to relate and benchmark these risks. Third parties can give nonexecutive directors comfort that their management teams have implemented effective practices. But it ultimately falls on boards to ensure that their companies have implemented effective programs.

For a list of discussion questions, see Appendix 3, on page 12.

Board expertise, structure, and techniques

The speed with which cybersecurity has raced to the top of corporate risk matrices presents a unique governance challenge. The still-emerging and ever-changing nature of the risk means that there is no established oversight model or evolved regulatory framework to guide practices at the board level. Effective governance requires a mix of board expertise, strong oversight processes, and new techniques.

Board-level cybersecurity expertise and engagement are critical

Members and guests debated the merits of appointing someone with cybersecurity expertise to the board. As a starting point, members emphasized that the expert cannot be a single-issue director. One said, *"If you have a good cyber person who is a bright, expanded businessperson, great. But having narrow and deep cyber experience is not a recipe for success at the board level."* Ms. Brown noted, however, that there is an expanding pool of candidates with both business experience and cyber expertise: *"When I joined the Northrop Grumman board, they valued my technical and operations expertise and the fact that I had run large businesses. Those daytime roles helped me be successful at becoming cyber-literate."*

A nonexecutive director with deep cybersecurity expertise can bridge the language barrier between management and the board. One member said that nonexecutive directors with a background in IT or security *"can coach chief information security officers [CISOs] to not talk in technical speak; they help translate. We get better at what questions to ask. Helping someone bridge that focus with cybersecurity operations is essential."* Ms. Brown said that she sees the role as more than just a translator. She noted that a director with a technical background can be a valuable mentor to the CISO or other security professionals: *"I engage regularly with our CISO and connect him with others that I know in the field. We all improve by having broader conversations. When I do check-ins, it's a two-way conversation. We often discuss breaches at other companies that have made the news since the last time we spoke."* But she added that cybersecurity expertise is not necessary in all cases: *"The need for cyber expertise on boards depends."*

Members emphasized that having one director with cybersecurity expertise cannot release the rest of the board from its oversight obligations. Ms. McKenzie said, *"Every member should have an appreciation and understanding allowing them to talk about it, so if it were to happen,*

they can understand." Members agreed, with one saying, *"Every business is a digital business. There is a level of board awareness and where the risk is and asking management about it, and it's broader than just cyber experience in a board member."* Full board engagement also informs management that the board prioritizes cybersecurity. *"Truly understanding vulnerabilities at the board level is important. It's good discipline for management to see the board be on top of this,"* said one member. Ms. Brown said that the board's collective ownership of the issue is critical: *"We are a community that's best enabled to fulfill our mission to create shareholder value as a community. Everyone cares about this. We aren't comfortable walking away from this topic."*

Some members were concerned that not all nonexecutive directors share their urgency. *"One problem I'm facing is getting through to boards on cybersecurity and risk,"* said one member. Another suggested that no company can ever have this risk fully covered: *"There's a tendency to feel overly comfortable with the level of preparation that's required to be constantly at the vanguard. We spent hundreds of millions of dollars per year, got periodic reports, and thought we were prepared—but then got punched in the face by a major attack. There's no end to this."*

Boards utilize different structures to oversee cybersecurity

Members and guests said that cybersecurity is ultimately the responsibility of the full board. One member said, *"I fully agree that on the supervisory board it's something that should be addressed—not a committee that takes care of it. For us, it's more important to have the right approach: individuals who assume responsibility for cyber. How is it embedded? Are there businesses that vary and is that a factor?"* Ms. Brown said, *"The conversation most assuredly belongs at the full-board level; it's too critical for the full board not to address. And then it can be enabled by committees on an execution basis."*

While members agreed that the full board is ultimately responsible for cybersecurity, most members said that at least part of the oversight is delegated to the audit committee. One said, *"We have it on every agenda for the audit committee. We cycle through various topics. We look at the overall structure, then identify the areas we'll home in on for the rest of the year. At another company, it's similar. There, it's not on every audit committee agenda, but it's frequent,"* said a member. In some cases, a risk committee is responsible for the topic. Ms. McKenzie noted that it can be challenging to decide how to divide up cybersecurity oversight: *"On my board, I think about the journey we're on. What's covered by the audit committee, by finance and risk, and what do we take to the full board?"*

Some members were concerned that adding cybersecurity oversight to already crowded audit committee agendas may not always be effective. One said, *"In the current-year plan, we have two sessions on cyber. At the audit committee, things get squeezed by other items. We are feeling that we are not spending enough time, but it can be hard to find another 20 to 25 minutes."* A partial solution to overburdened committees is to delegate portions of

cybersecurity oversight to multiple committees. Ms. McKenzie said that some redundancy can be a good thing: *"It's hard to contain it to just one committee; there tends to be overlap. As a board, decide which is the primary committee to which cyber will report. It will bleed into others. Make sure the message is delivered. Internal audit has the final say on controls and how they're applied."*

A cybersecurity committee or an IT committee?

Cybersecurity committees are uncommon, but they can make sense for companies with strategic interests in IT or those that would benefit from a transitory governance focus on cybersecurity and cyber risk. In pre-meeting conversations, two committee chairs shared their perspectives on this issue.[4]

John Inglis, currently chair of **FedEx's Information Technology Oversight Committee**, said, *"In the last 10 years, it was apparent that as much as the strength of the business depended on good people and risk quality, it also depended on the quality of IT. More importantly, we believe that if you're talking about IT, which is a meld of technology and people and roles and responsibilities, you're really talking about an operational activity, not just an enabling one. IT is the lifeblood of FedEx, as it is for banks and other enterprises which stand on substantial and widespread digital infrastructure, so you need oversight at the board. Cybersecurity is a subset of that oversight. We didn't want to give less time to the topic."*

General Motors' Cybersecurity Committee has a narrower purpose. Linda Gooden, the committee's chair, said that the board looked at its products and realized, *"Our number-one goal is safety for everyone who uses GM products and services by ensuring we are building products that are as cyber and tamper proof as possible. To understand the challenges associated with achieving the objective, the board established a committee to look at cyber across GM. The committee spent the first year understanding and assessing the cyber environment; defining the approach and tools to be used to measure progress and identify areas for improvement; and developing the best techniques to inform the board in English. Our second year was devoted to institutionalizing best practices and testing to gain a better understanding of where the cyber programs could be strengthened. This year the cyber committee is being moved under the risk committee as part of the broader risk portfolio."*

Directors use various techniques to enhance their oversight

Members and guests shared examples of the practices they have implemented at the board level to improve cybersecurity governance:

- **Deep dives.** Several members said that deep dives generate understanding and confidence in the company's cybersecurity measures. Some members reported participating in full-board sessions at cyber centers. These sessions provided board members with a closer look at the issue. *"The board wants to be more hands on,"* said one member.
- **Off-cycle engagement with management.** Often a board cybersecurity expert or self-appointed leader will engage with the CISO or other members of management and report back to the committee or full board.
- **Tabletop exercises.** Cyber-breach scenarios help board members understand who would handle the response, and how. They also help expose weaknesses in response planning. *"We have the audit committee involved in tabletop exercises. It's very important—nobody knew who was in charge. Directors need to know what the plan is during a cyber breach and when they will be informed,"* said one member.
- **Individual training.** Board members also participate in outside programs to enhance their own cybersecurity expertise. One member endorsed India's legally required cybersecurity training for board members. *"A regulator has required every board member to go to a two-day course, ending with a test. It's amazing. It brings people dealing with cyber—police, bankers, cyber agencies—so you get a good perspective on what's going on. It makes the conversation and the questions being asked more relevant."* Ms. McKenzie said, *"For those who have been on the dark side of an actual cybersecurity breach, there's no better training. Every company is having an issue."* One indicator of board preparedness, Ms. McKenzie said, lies in the answer to a simple question: *"Are we confident in the management and board to react to something happening?"*

Coordination between the board and management

The board's interactions with management are critical to cybersecurity oversight. Managers must be able to clearly explain complex issues to the board, and the board must incorporate that information into its risk oversight and strategic discussions.

Directors and managers seek to communicate on common ground

Since cybersecurity, and IT issues more generally, are often highly technical, it is important for directors and managers to communicate effectively. Many members were concerned about CISOs and other executives who speak to the board in obscure, technical language. They agreed that managers who instead speak from a business and risk perspective—the board's language—are most effective. Ms. McKenzie recommended conversations that focus on the

big picture: *"The discussion at the board needs to be less fraught with technical jargon and confusion. Start with risk. If it's a business conversation about risk, and the executive team takes ownership, then it'll flow from there."*

Frameworks and dashboards can help translate risk

Audit chairs said that it is important to develop metrics for benchmarking and tracking a company's cybersecurity practices. One said, *"You need standards. We're tracking our performance and we feel good where the company is."* Many members said their companies use cybersecurity frameworks, which CISOs can use to populate risk matrices. The National Institute of Standards and Technology (NIST) Cybersecurity Framework includes five core functions—identify, protect, detect, respond, and recover—which represent the "primary pillars for a successful and holistic cybersecurity program [and] aid organizations in expressing their management of cybersecurity risk at a high level."[5] The International Organization for Standardization (ISO) similarly has promulgated standards.[6] Standards tailored to certain industries are also available.[7]

Members and experts generally said that frameworks are important tools, especially for management. Ms. Brown said, *"The NIST framework is most assuredly a tool for management; it's not a board tool. It's a playbook, and it's only good as the connective tissue between the framework and the risk."* Ms. McKenzie recommended working with management to create a customized dashboard that can help turn a technical topic like cybersecurity into a relatable one: *"Make it a business conversation and not a technology one. If we stop talking about cybersecurity and instead talk about information risk and operational resiliency, everyone can participate."* Ms. Brown added that frameworks and dashboards often are most useful for tracking a company's progress and identifying the biggest risks along the way: *"Frameworks can enable a focused board discussion about risk appetite and where cybersecurity fits in."*

Third parties provide useful assistance

There are a many third-party experts that managers and directors can rely on to test and improve cybersecurity practices. Outside views can help board members understand management's approach and provide an extra level of confidence. Ms. McKenzie said, *"Just like we bring in outside people to help us comply with Sarbanes-Oxley, we can bring cyber folks to be the objective third party to make sure the assessments are being done. Work with the management team to have an outside perspective."* Ms. Brown said, *"You leverage third-party engagement to assess the environment, risk, and how management is addressing it. There is nothing like a good, objective team to make an assessment. Third parties may be enabling for boards."*

Directors look for indicators of managerial effectiveness

Members and guests shared some things they hope to see in management with regard to cybersecurity coordination:

- **Tone at the top.** Some members said they hope to see managers demonstrate a greater sense of urgency about cybersecurity. One member said, *"There needs to be a 'get-it' factor at the top."* Ms. McKenzie agreed: *"Management needs to have frequent conversations about cybersecurity and an elevator speech. If something happens, they need to understand their roles and the consequences."*
- **A culture of technological cleanliness.** A member said, *"You need to look at your digital hygiene so it's in your DNA; you need a degree of comfort that your house is clean. And be as prepared as possible and be as resilient as possible. Very few organizations think about it that way."* Ms. McKenzie agreed that policies such as prohibiting employees from using personal devices like thumb drives for business purposes can reduce risk. This push for prevention extends to software patch management. Ms. Brown suggested that asking for data about how quickly software patches are rolled out: *"Understand how patches are distributed. Look for the percentage of users who have installed the patch within 72 hours."*
- **Collaboration across management.** Information security cannot be a siloed function. Companies benefit from a well-informed and wide-reaching effort that touches every part of the organization. As one member suggested, if a software engineer creates a solution in-house and the CISO is unaware, there could be risk exposure. Managers who monitor the company for such exposure need to work closely with colleagues in other departments.
- **Scenario planning and simulation exercises.** Many members said that it is important to regularly test managers' ability to respond in a crisis. A member reported, *"The issue has evolved from IT to operational resilience. A CEO was on the golf course and was called with a scenario. We need to have escalation plans."*
- **Sufficient incident reporting.** The full board will normally hear of large cyberattacks and breaches. Failed attempts do not typically reach board agendas, however, despite being potential indicators of systemic problems. Members said they get some comfort when management regularly reports cyberattacks, however minor, to the board. Ms. Brown said, *"it can be important to have incident reporting and make that part of risk management on a regular basis."* Though audit committees often benefit from regular incident reporting, for the full board, she said, *"too much detail is possible."*
- **Examination of breaches at other companies.** Leading management teams learn from incidents at other companies, even if those companies are in different industries. Ms. Brown said, *"When there is a major incident somewhere else, that is the right moment for a director to ask the CISO, What happened? How vulnerable are we to that?"*
- **Scrutiny of vendors for third-party risk and appropriate internal controls.** One member said, *"We have platforms in which IT vendors have to pass tests."* Ms. McKenzie added, *"One of the challenges is procurement compliance; it can be a slow process. It's an area*

that creates tension. Without the right tone from the top, this balance of ensuring the right amount of risk is difficult, but it's super important."

Conclusion

Nonexecutive directors recognize that they must remain vigilant if they want to prevent cybersecurity threats from becoming realities. This vigilance includes enhancing the board's capabilities through adding directors with cybersecurity expertise or implementing techniques to better assess a company's capabilities. Better oversight also means better conversations with management, utilizing risk-based dashboards and other tools to ensure the board sees the full picture of the risk. While one member acknowledged there is *"no endgame"* to these efforts, most agreed that board oversight is improving.

About this document

The European Audit Committee Leadership Network (EACLN) and Audit Committee Leadership Network (ACLN) are groups of audit committee chairs drawn from leading European and North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The networks are organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Guest biographies

Marianne Brown is the chief operating officer of FIS's Global Financial Solutions organization. In this role, Marianne is responsible for developing and delivering FIS's banking, payments, and institutional wholesale offerings for large financial institutions and capital markets globally. She has a strong reputation as a leader who focuses on crisp execution and delivering stellar results.

Before joining FIS, Marianne served as the chief operating officer of SunGard Financial Systems. She joined SunGard in 2014 and has more than three decades of experience in the financial services and technology industries. Her other previous roles include CEO and president of Omgeo, a global financial services technology company; CEO of the Securities Industry Automation Corporation; and leader of ADP's Brokerage Processing Services business, now Broadridge Financial Solutions.

Marianne holds a variety of community and philanthropic leadership roles and has received numerous awards for her business and volunteer work. She holds a bachelor's degree in business administration, magna cum lade, from Concordia College.

Diana McKenzie is a technology executive, MetLife board member, and a former chief information officer for Workday and Amgen. Diana possesses a unique blend of digital, risk management, and cybersecurity leadership experience across the life sciences, healthcare, and software industries.

As the first CIO at Workday, a leading global cloud-based enterprise resource planning software company, Diana built and led the IT and security organization on a best-in-class journey to fuel the company's growth while preserving its award-winning values and culture. She played an instrumental role in scaling operations, influencing product road maps, strengthening the company's CIO customer community, and advancing its digital strategy.

As CIO at Amgen, Diana spent 12 years applying leading-edge analytics and technologies to further the company's innovation and market position. She led multiple cross-functional and enterprise-wide work streams as part of the company's strategic transformation.

Prior to joining Amgen, Diana served for 17 years at Eli Lilly. She helped to position the company as a trusted technology thought leader with regulators through active engagement in various trade, technology, and governmental organizations focused on improving healthcare.

In addition to serving on MetLife's audit and finance & risk committees, she has served as co-chair of the Ventura County Long Term Services board of directors and is co-chair of the Clinical Research Information Exchange.

Diana is a thought leader and frequent speaker on digital transformation and diversity. She was recognized by the National Diversity Council in 2015 as one of the nation's Most Powerful Women in Technology.

Appendix 2: Participants

The following EACLN and ACLN members, who sit on the boards of over 40 public companies, participated in all or part of the meeting:

- Ron Allen, Coca-Cola
- Jeremy Anderson, UBS
- Werner Brandt, Siemens
- Les Brun, ACLN Alumnus
- Aldo Cardoso, Bureau Veritas
- Pam Craig, Merck
- Pam Daley, BlackRock
- Dan Dickinson, Caterpillar
- Dave Dillon, 3M and Union Pacific
- Sam Di Piazza, AT&T
- Bill Easter, Delta Air Lines
- David Herzog, MetLife and DXC Technology
- Liz Hewitt, Novo Nordisk
- Charles Holley, Amgen
- Mike Losh, Aon
- Nasser Munjee, Tata Motors
- Marie-José Nadeau, ENGIE
- Tom Schoewe, General Motors
- Leslie Seidman, General Electric
- Gerald Smith, Eaton
- Charlotte Strömberg, Skanska
- Isabel Torremocha, Repsol
- Jim Turley, Citigroup
- John Veihmeyer, Ford

Appendix 2: Participants, continued

EY was represented in all or part of the meeting by the following:

- Andy Baldwin, EMEIA Area Managing Partner
- Jean-Yves Jégourel, EMEIA Assurance Leader
- Frank Mahoney, Americas Vice Chair of Assurance Services
- John King, Americas Vice Chair of Assurance Services-Elect

Appendix 3: Discussion questions for audit committees

- ? Do any directors at your company have cybersecurity expertise? What are the benefits of having that expertise on the board? Are there drawbacks?
- ? What, if any, committee is responsible for cybersecurity oversight at your company? Is this an issue that can be delegated to a committee at all? In whole or in part?
- ? How can the committee responsible for cybersecurity oversight keep other board members well informed of the company's progress?
- ? Would your company benefit from a cybersecurity committee or shared committee oversight model?
- ? Who from management has primary responsibility for reporting cybersecurity issues to the board? Under what circumstances do other members of management present on these issues?
- ? What effective communication techniques have you and your company's managers taken? How do you overcome the technical language barrier with the CISO and other cybersecurity experts in management?
- ? How do managers most effectively structure dashboards and other reporting tools?
- ? What kinds of conversations do you have with management? Are they focused on risk and strategy, on the technical aspects of cybersecurity and IT, or on both?
- ? What do you hope to see management doing to stay on top of cyber risk? How do you check management's work?

Endnotes

[1] Cybersecurity Ventures, "Cybercrime Damages $6 Trillion by 2021," news release, December 7, 2018.

[2] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with network members, guests, and other experts in connection with the meeting.

[3] Securities and Exchange Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 C.F.R. 229 and 249 (February 26, 2018), 16.

[4] John Inglis and Linda Gooden contributed to pre-meeting discussions but did not attend the meeting.

[5] "The Five Functions," National Institute of Standards and Technology, accessed July 8, 2019.

[6] ISO/IEC 27000 Family—Information Security Management Systems," International Organization for Standardization, accessed July 8, 2019.

[7] Melanie Watson, "Top 4 Cybersecurity Frameworks," *IT Governance*, January 17, 2019.