Audit Committee Leadership Network

July 2021

ACLN

SUMMARY of THEMES

Ransomware, sustainability reporting, ESG ratings, and new horizons for boards

On June 28–29, members of the Audit Committee Leadership Network (ACLN) met virtually to discuss ransomware and incident response, environmental, social, and governance (ESG) reporting, ESG rating agencies, and the future of boards and board service. This *Summary of Themes* provides a brief overview of the meeting.[1] Two forthcoming *ViewPoints* documents will provide additional detail on the discussions of ransomware and sustainability reporting.

Ransomware and incident response

ACLN members met with Orion Hindawi, CEO of Tanium, a cybersecurity software and services company; Chuck Seets, Americas assurance cybersecurity leader at EY; and Phyllis Sumner, partner and chief privacy officer at the law firm of King & Spalding, to discuss the recent explosion of ransomware attacks and how companies and boards can respond to these and other kinds of cybersecurity incidents. Several major themes emerged from the discussion:

- **Cyber extortion now operates as a well-developed business.** The guests noted that cyber-enabled extortion has grown into a *"multibillion dollar industry."* The drivers of growth include high profitability and low risk for perpetrators, who can launch attacks against an ever-expanding array of targets from jurisdictions that are unlikely to successfully prosecute them. Cryptocurrencies have enhanced attackers' ability to stay anonymous, and ongoing technology deployment can distract companies from shoring up their cybersecurity defenses. At many companies, Mr. Hindawi said, a lack of basic cybersecurity hygiene—measures such as patching systems and two-factor authentication—makes life easier for attackers.
- **Policies on ransom payments need to be flexible.** Members described *"eye-opening experiences"* from which they concluded that *"you have to look at the situation"* rather than adhere to a strict policy against paying. A member pointed to the example of the Colonial Pipeline attack: *"Philosophically, you can say, 'Heck no,' but when you know the East Coast is going to run out of gasoline in three to four days, the pragmatic side takes over."* Ms. Sumner had seen cases of companies not paying and still recovering successfully, but she said that savvy attackers often ask for ransom sums that are low enough to make payment the easier option. Mr. Hindawi noted that *"the stigma of paying is diminishing—it's becoming a cost of doing business."*

- **Preparations for responding are crucial.** Even if a decision on payment cannot be made in advance, companies can take steps that will make that decision and others easier when the time comes. Ms. Sumner said that companies need to *"prepare to act strategically, with great speed."* That means developing *"a playbook with critical decision points,"* including trigger points for escalating the response and communicating with stakeholders. It means lining up third-party support in advance, including experts who can handle the negotiations with attackers. Ms. Sumner stated that *"the engagement process should contemplate that such vendors will be hired under privilege, and some may need to be put on retainer."* Incident response plans should be integrated across the organization, including executives and the board, Ms. Sumner added, and Mr. Hindawi highlighted the importance of a clear chain of command. Guests and members also mentioned the importance of testing response plans, including red-team attacks (i.e., attacks by outside teams of ethical hackers). Mr. Seets said, *"You play like you practice; and companies should incorporate an element of surprise into their simulation exercises."*
- **Boards have an important role in preparations.** A member noted that boards cannot micromanage incident responses, but they can ensure that there is a framework in place to bridge the silos that exist in every organization. Ms. Sumner noted that the incident response plan, which may include a board engagement model, should lay out how the board will be involved. Given the complexity of the issues, both the members and guests stressed the importance of expert advice to the board. A member advised that *"the best time to meet your experts is before something happens,"* and Mr. Hindawi recommended that boards have someone who can facilitate communications with the chief information security officer. However, he also noted that increasing board involvement during an actual incident *"doesn't necessarily correlate with success: seconds count, and you don't want management to spend time on anything but remediation."* Where boards can really make a difference, he argued, is in promoting the cybersecurity hygiene that mitigates the impact of breaches or even prevents them in the first place.

Dialogue on sustainability standards

Janine Guillot, CEO of the Value Reporting Foundation, and Eric Hespenheide, chair of the Global Reporting Initiative (GRI), joined members in a conversation about the state of ESG standards and sustainability reporting.

- **Audit chairs demand swift movement toward simplification.** *"We are doing everything we can to merge and simplify,"* Ms. Guillot told audit chairs. She sees the creation of the Value Reporting Foundation as a step in the right direction. In addition, both guests emphasized the significance of the proposal put forward by the International Financial Reporting Standards (IFRS) Foundation for a global sustainability standards board. *"I am very optimistic,"* Ms. Guillot said. *"I would have said this was 20 or 30 years away."* Mr. Hespenheide pointed to developments taking place at the Securities and Exchange

Commission. *"The fact they are even having conversations about ESG disclosures with such intensity is unheard of."* But members did not seem as hopeful. *"The regulators are not moving quickly enough,"* one director said. *"By their standards, they are moving rapidly,"* Ms. Guillot countered.

- **ESG reporting faces looming expectation gaps**. *"Management keeps telling me this is all about as clear as mud, so I have a hard time holding them to account on all this,"* one audit chair said. Directors believe that simplification is desperately needed and that a unified standard would be ideal. Ms. Guillot was clear, however: *"This will never be simple. It can be simpler; it can be more coherent; it can be better understood—but it will never be simple."* Mr. Hespenheide agreed: *"I think we can clarify what you use for what purpose, but that is clarification, not simplification."* Others expressed frustration over the lack of consistency. *"Even in the same industry, we cannot compare*," one director said. Mr. Hespenheide pushed back: *"Comparability is an issue, I agree, but it's not an issue with the standards; it's with the application of the standards."* Members pointed to forward-looking metrics as one area of particular concern: *"There is serious potential for creating an even larger expectation gap, and we already have one."* Ms. Guillot agreed: "*Expectations are all over the map. I'm hearing people talk about assurance on whether or not a company is going to achieve its net zero targets."*

- **Directors emphasize the importance of assurance of ESG reports.** Many companies represented at the meeting currently use third parties to supply some level of limited assurance. *"Both of my boards use a third party to verify gas emissions,"* one member said. *"My understanding is that you get a better score from the CDP [formerly known as the Climate Disclosure Project] if you use some form of assurance."* Audit chairs were unanimous that some level of assurance is needed: *"We certainly don't want to be setting land mines for the company,"* one member said. Another added, *"This is an area where the amount of time and thinking needs to really ramp up."* Mr. Hespenheide insisted that the standards offered by GRI and the Sustainability Accounting Standards Board are auditable as they exist today: *"The AICPA [American Institute of Certified Public Accountants] has published guidelines on the assurance of sustainability reports, but there hasn't been a whole lot of uptake because frankly, companies have not asked for it. The constructs are there, however."* Around forward-looking statements, Mr. Hespenheide said that he expects safe harbors for those parts of sustainability disclosures.

- **Boards have a role to play in advancing standards.** Ms. Guillot told audit chairs*, "At the end of the day, this will take some serious corporate leadership.*" Mr. Hespenheide agreed: *"Corporates are absent many times in this conversation."* Ms. Guillot pointed out that if companies do not engage, regulators will move forward regardless: *"I think that would be suboptimal."* Mr. Hespenheide urged members to continue to *"develop the vocabulary to challenge management on how your companies are addressing these issues."* He concluded, *"If you don't participate in this conversation, others will decide for you."*

ESG rating agencies

Members met with executives from three of the largest ESG rating agencies to discuss the ratings business and the direction of sustainability disclosures: Linda-Eling Lee, global head of research at MSCI ESG; Anthony Campagna, managing director at ISS ESG; and Simon MacMahon, executive vice president and head of ESG and corporate governance research at Sustainalytics. Four themes emerged from the discussion:

- **The ESG ratings business is growing rapidly as standards evolve.** *"This is a very dynamic space at the moment,"* Mr. MacMahon told audit chairs. *"The marketplace is growing somewhere between 25 and 40% every year."* Ms. Lee emphasized the increasing activity on the policy and regulatory side: *"In the last year, I have spent more time consulting with regulators around the world, including in Asia. They have been studying disclosures and if they should be mandated."* Guests expressed their support for global efforts to converge standards, endorsing efforts by the IFRS Foundation and the Task Force on Climate-related Financial Disclosures in this direction.
- **Lack of conformity across ratings reveals divergent methodologies.** Several members expressed concern over divergent ratings given to the same company by different agencies. While the guests acknowledged this irregularity, Mr. MacMahon said, *"You need to compare apples to apples. Different raters measure different aspects of ESG risk and impact."* Ms. Lee explained that MSCI takes a rule-driven, quantitative approach to its ESG ratings, while Mr. Campagna said that ISS's approach allows analysts to tailor each rating to the nuances of a given company. Different rating agencies weight metrics differently and draw from third-party sources to augment issuers' own disclosures. MSCI uses public patent data to evaluate companies' potential profits in a carbon-constrained economy, Ms. Lee said. Sustainalytics, Mr. MacMahon told members, takes "controversies" into account: *"Many clients in Europe take our controversy research and build it into their investment policies. A category five controversy might actually trigger an automatic divestment or removal from their investable universe."* The guests also said that their clients, who include some of the largest asset managers and pension consultants, appreciate the range of perspectives that divergent rating methodologies provide.
- **ESG disclosures are not of uniform quality.** Guests and members noted that ESG disclosures have not matured at the same pace. Certain sectors, like healthcare and energy, are not as well developed as the automotive industry, Mr. MacMahon said. This is true with certain ESG topics as well: bribery and corruption are well disclosed, as are diversity and equity, whereas reporting on newer issues like climate change is less satisfactory. Still, *"ESG disclosures have improved a lot over the last decade,"* Mr. MacMahon said. *"In our universe, about 80% of companies produce a sustainability report. But only about 12% of companies in the US have achieved the kind of reporting that we expect."*

- **Rating agencies look for sustainability committees with qualified members.** One member asked, *"Where do rating agencies believe sustainability belongs at the board level?"* Mr. Campagna told audit chairs, *"It's too early to tell what would be best practice. Instead, we analyze who sits on that sustainability committee. We assess the skills of that board member and what background or certifications they have in sustainability."*

New horizons for boards and directors

ACLN members met with Dr. Dambisa Moyo, an economist, board director, and best-selling author who has recently published a book entitled *How Boards Work: And How They Can Work Better in a Chaotic World.* The discussion began with reflections on why directors choose to serve on boards. Dr. Moyo highlighted the pleasure of grappling with a variety of important, complex problems lacking clear solutions. Members agreed and mentioned the satisfaction of staying engaged and continuing to contribute to society. The discussion then turned to how boards can improve their performance in key areas:

- **Broaden the criteria for selecting CEOs and board members.** Pointing to a rash of CEO dismissals due to ethical lapses, Dr. Moyo said that boards need to think more about how to include ethics and culture in evaluating candidates. For internal candidates, members noted that they do this by observing candidates in action, preferably over time. *"The best way is to see someone in different roles,"* a member explained. For external candidates, a member suggested spending more time with candidates and avoiding *"shortfalls in due diligence."* Dr. Moyo also said that there is *"scope to add more nonconventional board members."* Headhunters, she said, *"need to widen the aperture because of the challenges society is dealing with now."* A member agreed but added that boards themselves have been part of the problem: *"Headhunters will do what we ask them to do."*

- **Enhance the board's input into strategy.** Dr. Moyo said that boards could take a more active role in crafting company strategy: *"We should take more of a lead in thinking about strategy instead of just approving it."* Boards could bring in outside talent to challenge the strategy, she noted, and members suggested measures such as devoting a day before the formal discussion to agree on key assumptions or brainstorming the five worst things that could happen to the company. One member said that their board conducted an excellent strategy discussion during the pandemic, precisely because so much remained uncertain: *"Everything wasn't fully baked, which led to a really rich discussion … My mantra is, show us the options."*

- **Continue to drive the integration of ESG into the business.** Dr. Moyo and the members noted that companies are making progress on integrating ESG issues into the core of their business operations. Reflecting on their company's efforts to help employees during the pandemic, a member said, *"Taking care of employees is just good business … You can't compartmentalize ESG."* The separate ESG report will eventually go away, Dr. Moyo said, but she added that the pace of change and the complexity of understanding and

incorporating ESG issues will require ongoing effort by companies and boards: *"The world is moving so fast that we shouldn't expect that we're going to land somewhere and be done."*

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of network members or participants, their affiliated organizations, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Tapestry Networks and EY are independently owned and controlled organizations. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

Appendix: Participants

The following members of the ACLN participated in part or all of the meeting:

- Barbara Byrne, ViacomCBS
- Pam Daley, BlackRock
- Dan Dickinson, Caterpillar
- Dave Dillon, 3M and Union Pacific
- Sam Di Piazza, AT&T
- Bill Easter, Delta Air Lines
- Tim Flynn, JPMorgan Chase and Walmart
- Alan Graf, Nike
- Gretchen Haggerty, Johnson Controls
- Fritz Henderson, Marriott
- Bob Herz, Morgan Stanley
- David Herzog, MetLife and DXC Technology
- Charles Holley, Amgen and Carrier Global
- Michele Hooper, United Airlines
- Hugh Johnston, Microsoft
- Nick LePan, CIBC
- Mike Losh, Aon
- John Lowe, Phillips 66
- Edward Ludwig, CVS
- Louise Parent, FIS
- Ann-Marie Petach, Jones Lang LaSalle
- Peter Porrino, AIG
- Paula Price, Accenture
- Tom Schoewe, General Motors
- Leslie Seidman, GE
- Gerald Smith, Eaton
- John Stephens, Freeport-McMoran
- Tracey Travis, Facebook
- Jim Turley, Citigroup and Emerson Electric
- John Veihmeyer, Ford
- Robin Washington, Salesforce.com
- Maggie Wilderotter, Hewlett Packard Enterprise

The following members of the European Audit Committee Leadership Network (EACLN) participated in part or all of the meeting:

- Jeremy Anderson, UBS
- Carolyn Dittmeier, Assicurazioni Generali
- Margarete Haase, ING
- Liz Hewitt, National Grid
- Dagmar Kollmann, Deutsche Telekom
- Pilar Lopez, Inditex
- Kalidas Madhavpeddi, Glencore
- Stephen Pearce, BAE Systems
- Bernard Ramanantsoa, Orange
- Guylaine Saucier, Wendel

Audit Committee Leadership Network

July 2021

ACLN

SUMMARY of THEMES

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

- Kelly Grier, EY US Chair and Americas Managing Partner
- John King, EY Americas Vice Chair of Assurance Services
- Steve Klemash, EY Americas Leader, Center for Board Matters
- Pat Nieman, EY Greater Los Angeles Managing Partner, Center for Board Matters

Endnotes

[1] *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from conversations with guests and network members in connection with the meeting.