Tapestry Networks

April 2022

TN

VIEWPOINTS

Cybersecurity leadership and governance

Cybersecurity oversight is a challenge for the board of every large company. The threat landscape is constantly changing; Russia's invasion of Ukraine is the latest in a string of global events that heightens these concerns. In late February, the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) wrote an open letter to directors advising them to ensure that their organizations have their "shields up" because of the increased possibility of malicious cyber activity.[1] A month later, President Biden said, "I urge our private sector partners to harden your cyber defenses immediately by implementing the best practices we have developed together over the last year. You have the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely."[2]

Corporate directors are not taking these messages lightly. They are tightening their cybersecurity oversight practices and are eager to learn more as good practices continue to emerge. In March 2022, Tapestry Networks convened two in-person and four virtual discussions that brought the following cybersecurity experts together with the audit committee chairs of more than 100 large US public companies:

- Diane Brown, Vice President of IT Risk Management and Chief Information Security Officer, Ulta Beauty
- Marianne Brown, Director, Northrop Grumman, Charles Schwab, Akamai Technologies, VMWare; Former Chief Operating Officer Global Financial Solutions, FIS
- Shirley Edwards, Partner, EY
- Jamil Farshchi, Chief Information Security Officer, Equifax
- Patrick Hynes, Principal, Cyber Threat Management West Region Leader, EY
- Shabnam Jalakian, Vice President and Chief Information Security Officer, First American Financial
- John McKinley, Technology Committee Chair, Equifax
- Michael Palmer, Chief Information Security Officer, Hearst Communications
- Chuck Seets, Partner, EY
- Myrna Soto, Director, TriNet Group, Popular Inc, Spirit Airlines, CMS Energy; Former Global Chief Information Security Officer, Comcast
- Sean Wessman, Principal, Americas Central Region Cyber Leader, EY

For a full list of meetings and participants, please see the appendix that begins on page 11.

This *ViewPoints* synthesizes discussions about three key topics that emerged in the meetings:[3]

- **The CISO is getting a seat at the table**
- **Directors employ a range of tools to understand their companies' cyber capabilities**
- **Boards are assessing how best to provide and structure cyber oversight**

The SEC's proposed rules on enhanced cyber disclosure

On March 9, 2022, the Securities and Exchange Commission (SEC) proposed rules that would require public companies to include new cybersecurity disclosures, with a goal of providing consistent and comparable information on the topic. Under the proposed rules, companies would have to take the following steps:

- File an 8-K within four business days of determining that a cybersecurity incident was material.
- Provide periodic reports with updates about previously reported incidents.
- Describe their policies and procedures for the identification and management of risks from cybersecurity threats.
- Explain the board's oversight of cybersecurity risk and management's role in assessing and managing this risk.
- Disclose whether they have cybersecurity experts on the board of directors and, if so, provide their names and a description of their experience. [4]

Companies are still digging into the implications of the proposal, but some voiced early concern, especially with the incident reporting requirement. One said, *"What I find challenging is incident reporting within four days for a material event. Cyber incidents are ubiquitous, so determining materiality within that time frame during a crisis is a whole new trial."* Another member said, *"If we disclose the vulnerability, it seems like we are providing the bad actors with a road map for how to break in."*

Audit chairs and guests alike urged their peers to take advantage of the SEC's comment period, which is open until at least May 9, 2022. Ms. Soto shared, *"I've received multiple emails from industry associations urging companies to work with them to supply comments that they can submit. If we find the right threshold of materiality for reporting, I think sharing more will only help demystify the shame on reporting and disclosing. We need to remove that stigma because despite our best efforts, none of us are immune."*

The CISO is getting a seat at the table

In the not-so-distant past, the role of a chief information security officer (CISO) did not even exist. Information security was usually a technical function embedded within the information technology organization. As cyberthreats have worked their way up companies' risk registers, CISOs have become high-ranking, critical leaders at most large organizations.[5] With this change, many companies are giving careful thought to where the CISO sits in the organization and how the CISO can gain and maintain clout.

The role of the CISO is continuing to evolve

The number of devices that store sensitive information and data has exploded, triggering a transformation of the CISO role from a technical resource to a true business leader. Many CISOs are now working across functions and are at the center of conversations about both risks and opportunities. Mr. Palmer shared how he has seen the role change: *"In the past, the technology supported the business. Today, every business is a technology business. It used to be that you could implement a firewall and then you were secured, but now, with remote work, you need leaders who truly understand how data travels throughout the organization."* He noted that understanding the strategy of the business has been a critical success factor in his current role: *"I consider myself to be a connector and influencer throughout the organization, especially in the areas where I don't have direct oversight,"* he said.

Audit chairs confirmed the more comprehensive talent profile desired for the CISO role. One said, *"It needs to be the right person to make a broad impact across the role, link the security strategy tightly with the business strategy—a strong technical leader who can also build relationships across the company. It's a difficult role to fill."* Mr. McKinley shared his perspective as a board member with technology expertise: *"The board needs to ask itself, 'Does our organization have an A athlete in this position?' Not all do. You can't afford a B athlete in this role."*

The CISO's reporting structure sends a signal

According to a recent survey, the traditional arrangement, in which the CISO reported to the chief information officer (CIO), is on the decline among both public and private companies.[6] In speaking with experts and audit chairs, one theme emerged clearly: regardless of the specific reporting line, sufficient stature within the organization is essential to a CISO's success.

One way to clearly elevate the role is to have the CISO report directly to the CEO. Mr. Farshchi said, *"At Equifax, I report to the CEO. In previous companies, I reported to the CIO, and back then, I thought that model worked fine. Here's the difference: By reporting to the CEO, it gives me the right level of authority, visibility, and accountability, to drive change … and it also gives me insight into what's happening across the organization that I didn't have before."* This reporting structure allows CISOs to hear firsthand about product development, acquisition targets, and broader company strategy, which, in turn, allows them to think about how to build in security

features before these pursuits go live. *"I can manage risk far more effectively than I otherwise would have,"* said Mr. Farshchi.

What works best for one company may not be right for another. Mr. McKinley observed, *"There is no binary answer."* Audit chairs and guests shared their views on what works best. *"I've seen the CISO report into the chief risk officer, general counsel, chief operating officer, chief trust officer, and the CEO. It really depends on the industry and the company. There is no right answer, only one wrong one—and that's reporting into the CIO,"* Ms. Soto joked.

In many cases, the title of the person the CISO reports to matters less than what that person does to provide support. Ms. Diane Brown said, *"A true advocate makes such a difference."* Ms. Marianne Brown added, *"It's ultimately the responsibility of the CEO to ensure the CISO is enabled no matter where the CISO sits in the organization."*

The board has a role in empowering the CISO, too

An EY survey of more than 1,000 senior cybersecurity leaders found that CISOs are grappling with insufficient budgets and regulatory fragmentation and are failing to find common ground with the business functions that need them most.[7] So how can board members advocate for and empower the CISOs within their organizations? Ms. Marianne Brown suggests, *"Access and exposure. We need to make sure the CISO is on the audit committee calendar every quarter and in front of the full board annually. They have an urgent voice in the room, and the full board needs to listen to leverage their competency and enable oversight."* Some stressed the importance of developing a board-level relationship with the CISO. One audit chair said, *"Our CISO attends our board dinners, and we don't even think about his reporting structure. Every member knows him personally, and it helps bring us into his world."*

It is critical for CISOs to feel supported enough that they do not feel tempted to paint a rosy picture when reporting to the board or audit committee. Ms. Soto said, *"The weather report always wants to be sunny with no high pressure coming—so let the CISO know they have cover and no one expects us to be bulletproof. What you really want to know when there is a problem is what are we doing about it."* An *"all green"* dashboard should itself be a red flag for directors. Mr. Hynes added, *"The true test of an empowered CISO is whether they feel comfortable delivering the real state of the company to the board. There are always areas to improve upon when it comes to cybersecurity."*

Directors employ a range of tools to understand their companies' cyber capabilities

In a heightened threat environment, ensuring open, honest, two-way communication between management and the board is essential. CISA's "Shields Up" warning to board directors presented five steps for boards to take: (1) empower the CISO; (2) lower reporting thresholds; (3) participate in a test of response plans; (4) focus on continuity; and (5) plan for the worst.[8]

Mr. Seets told audit chairs that this type of communication directly to board members is unprecedented: *"We encourage directors to talk to their management teams and find out what they're doing today that they don't ordinarily do, to reveal whether or not the organization has elevated to a crisis management level. The cyber-risk emanating from the Ukraine crisis is clearly not a 'business as usual' environment. Keeping the lines of communication open right now is of utmost importance."*

Finding a common language is essential

According to one survey, only 9% of boards are extremely confident that the cybersecurity risks and mitigation measures presented to them can protect the organization from major cyberattacks—a metric down from 20% the previous year.[9] Audit chairs and guests shared what they look for in cybersecurity dashboards, metrics, and reporting:

- **Frameworks are a helpful starting point for board-level dashboards.** There are several cybersecurity frameworks available for organizations to consider. Many practitioners use the framework from the US National Institute of Standards and Technology (NIST), as its broad approach to security risk management makes it a good starting point for companies in any industry.[10] Audit chairs and experts emphasized that a framework is just that, a starting point. Mr. McKinley encouraged using the NIST framework but cautioned, *"It's insufficient in terms of having the right measures in place to cover all aspects of security. Our CISO has layered on a fuller dashboard with key focus areas. So having NIST in place is great in terms of talking externally to regulators and customers, but you should not sleep well at night if that is all you are doing."* Both Ms. Jalakian and Ms. Soto urged ensuring that the cyber risk framework dovetails into the company's ERM framework. Ms. Soto said, *"Be sure to ask your CISOs about residual risks and the controls to contain and segment those to lower overall inherent risk. It's an opportunity to quantify the risk for those board members more comfortable working with numbers."*
- **The right key performance indicators are critical.** Board-level cybersecurity presentations are only successful if management is tracking and sharing the right information. Ms. Marianne Brown shared the information she seeks from her companies' management teams: *"These are the cyber hygiene areas I focus on: (1) firewall—keep out the bad guys, (2) asset management/threat management, (3) access management, (4) vulnerability management, (5) event detection and response, and (6) egress traffic filtering—don't talk to strangers."* Mr. Palmer added that a board should be briefed on *"the company's ability to detect a threat within the system and their maturity level to respond and get the business to recover from an attack."* Audit chairs noted the importance of using external sources of data to verify that the company is doing as well as its managers say it is doing. Ms. Diane Brown suggested that board members review ratings from organizations like SecurityScorecard: *"Our board members have found this helpful to benchmark our organization against our industry competition."*

- **Companies are increasing the frequency of board reporting.** A 2021 survey found that 39% of boards put cybersecurity on their agendas quarterly, up from 29% in 2020.[11] Ms. Diane Brown shared her journey as a CISO: *"I have presented to the board for seven years. It started as once a year, then twice a year, and it's evolved to every audit committee meeting and annually to the full board."* Of course, in the case of a crisis, frequency increases dramatically. An audit chair said, *"When a crisis hits, the board is meeting weekly, at a minimum."*
- **Executive sessions with the CISO are beneficial.** A dialogue with the CISO in executive session, without other managers present, can be extremely valuable. Ms. Soto said, *"Body language alone can tell you so much. Ask the CISO, 'Was there something you expected me to ask you today that I didn't?' and 'Do you have the funds to support what you need?' Simple questions like this can yield very informative responses."*

Governance of ransomware

As cybercriminals become more sophisticated, they wreak more havoc. A Mimecast survey found that 80% of participants "had been targeted with ransomware over the past two years. Of that 80%, 39% paid a ransom, with US victims paying an average of $6,312,190."[12] Audit chairs wanted to hear their peers' thoughts about these attacks. One asked, *"Has the board had conversations around the ramifications that could arise from payment?"* Part of the calculation depends on the often impossible task of determining who the bad actor is and whether the company is even permitted to pay them. One member said, *"We have a process in place to get as comfortable as we can that the attacker is not on the government's list of prohibited entities. It's more than just an internal determination. We would involve third parties, law firms, and government agencies."*

Participants had varied positions on paying a ransom. Some took a firm stance against paying, worried it would only fuel the perpetrators further. Others appreciated that sentiment but wondered if, in the heat of the moment, they would change their minds. Mr. Hynes suggested, *"I think a formal policy is good to have. Preparation is the key to minimize disruption."* An audit chair said, *"We all have a pretty good handle on continuity and cost of lost business opportunities. But creating a policy seems challenging because payment very much depends on the circumstances. It's not a simple yes or no."* Ms. Marianne Brown said, *"If you think there is the slightest chance you would pay, develop a relationship with a crypto broker to ensure you have the currency du jour and to be on speed dial in that situation."*

Should the board participate in cyber simulations?

Audit chairs pondered how involved the board should get in cybersecurity simulations and tabletop exercises. Some felt it best to leave the simulations to management but to ensure the board received a readout. Ms. Soto said, *"None of us as board members want or need to be in the weeds dissecting tactical results of a simulation, but we do want to understand how effective the company was in detection, protection, and response."* Ms. Diane Brown worried that the board could misinterpret management's capabilities if they were to sit through an entire simulation: *"Seeing an IT team work through an incident can look like utter chaos. I prefer to brief the audit chair to explain what's happening after we get our ducks in a row, and I think it's appreciated."* One audit chair added, *"The door swings both ways. For the audit chair to get invited to the tabletop exercise comes with some responsibility. You have to commit you won't run around like your hair is on fire. I think for board members, getting a readout of what management is doing to expose vulnerabilities is the right level of detail."*

Others, however, suggested that the board should be involved in these exercises. One audit chair shared an example of a company that has tabletops with board members in the room: *"The board is asked to stay quiet until it's over. We then participate in a postmortem with management because we want to see how the team operates together and provide feedback. It teaches you so much about cyber, culture, and the executive team, and we are always searching for an answer to that."* Another said, *"We also do a narrative of lessons learned, which provides us some comfort."* One member's company is considering an exercise in which board members are assigned roles during a simulation: *"The idea is to give the board a sense of what it's actually like and to ask the tough questions and get the answers."* Mr. Hynes introduced the concept of a "three-pack" for cyber simulations: *"I've seen one realistic scenario delivered three times to three different audiences, tailoring each version for each group: the technical staff, senior management, and finally the board. That model works well."*

Third parties help the board verify cyber maturity

The SEC's proposed cybersecurity rules would require companies to disclose whether they engage assessors, consultants, auditors, or other third parties in connection with their cybersecurity risk assessment programs.[13] Participants shared their experiences having outsiders assess their cyber capabilities.

Audit chairs, CISOs, and other experts all found value in having a third party come in every so often to do testing and benchmarking. Mr. Farshchi said, *"I want the board to trust me, but not so much that they don't verify what I am saying. We bring in independent parties to assess us against NIST and our peers, and it's a powerful way to convey the progress of your program."* Mr. Hynes recommended *"inviting a third party to one of your board meetings to have an open dialogue and observe your interactions with the CISO. Afterwards, they can talk to you about what they observed so you can highlight those areas to the CISO."*

In some cases, an outside perspective can come from within the company. One audit chair shared, *"We use internal audit to certify our controls against NIST on a pass-fail basis. It's been incredible. Seeing the areas of the fails has helped both the CISO and management team understand where the vulnerabilities are."* Some audit chairs worried, however, about the limitations of this approach because it can be difficult to retain the requisite knowledge and talent on the internal audit team.

Boards are assessing how best to provide and structure cyber oversight

Whether by adding cybersecurity expertise to their boards or by creating separate technology committees that carve out cybersecurity responsibilities, boards are adopting creative measures to address the daunting task of cyber oversight.

Pros and cons of recruiting cyber expertise to the board

The SEC's proposed enhanced disclosures include explicit disclosures about board cyber expertise. Relatedly, Gartner predicts that "By 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% today."[14] Several audit chairs expressed concerns about rushing to add cyber experts to boards. One said, *"I think financial expertise is well defined, but cyber expertise? Not so much. And if it's technical skills we are looking for, is the board the right place? Shouldn't we hire those folks into management?"* Another suggested, *"I could see this evolving to a situation where the board brings in independent experts, like the role of compensation consultants. That to me seems more realistic."*

No one is enthusiastic about electing a single-issue director; business acumen is paramount for success as a director. Ms. Jalakian said, *"You need a business executive who happens to be steeped in cyber expertise. There is a major gap in some CISOs' that may have the right technical chops but not the right business acumen."* An audit chair added, *"There are definitely merits of a cyber expert on the board, but it seems that any time there is an issue du jour, there is another expert you should bring in. To think there is enough talent to get a cyber expert on all Fortune 500 boards seems unreasonable."*

Some audit chairs suggested that the lack of board-ready talent in the CISO community should be a wake-up call. If companies seek to place CISOs at the leadership table, board members and senior leaders should offer them coaching and development opportunities. An audit chair said, *"I plead guilty: we are not working to broaden our CISO to become a more credible board candidate. That would be a substantial investment, and it would take him away from his day job of keeping us from being robbed!"*

Boards that are lucky enough to find the elusive director with both business and cybersecurity expertise enjoy a variety of benefits. The word that came up most often to describe such a director was *"translator."* Ms. Marianne Brown said, *"As a translator, I drive three things: (1) cyber*

literacy at the board level, (2) an effective cyber hygiene dashboard as a communication tool, and (3) engagement with the CISO to further enable oversight and outcomes." Ms. Soto also shared her experience: *"You don't have to be technical to provide oversight, but given my background, I am trained to listen and pick up on red flags, and I know the right questions to ask of management to really dig in."*

Audit chairs stressed that the vague definition of cyber expertise contributes to the perception that an expert might not make a good director. But people bring cyber expertise from a variety of professional backgrounds. One said, *"I've seen a board with a global CIO and another with the CEO of a security company. Different backgrounds, both experts. It's important to remember that expertise can come in various packages and not all cyber experts are created equal."*

Benefits of dedicated technology committees

In 2021, 68% of Fortune 100 companies assigned primary responsibility for cybersecurity oversight to the audit committee.[15] Some members mentioned risk committees housing this responsibility as well. In addition, more boards have a stand-alone technology committee than a decade ago, but it is still an uncommon practice: 13% of boards have these committees, compared with 6% in 2011.[16] Few member companies had technology committees in place, but Mr. McKinley, chair of Equifax's board technology committee, shared his experience: *"Our charter includes basic monitoring of how the organization is performing on technology day-to-day. Things like service quality, outages, quality of software development and implementation—we want to make sure we keep the trains running. We also have discrete responsibility from the board on ensuring the right security measures are in place. Part of that responsibility includes an annual formal external assessment of the organization's security posture, similar to the way an audit committee uses its external auditor. We also review business continuity plans, technology and security budgets, security of acquisitions and their subsequent integrations, etc. It is a pretty broad mandate."* He added that all board members are invited to attend technology committee meetings, and they frequently do. *"Seeing their level of engagement in these sessions underscores how valuable it is for them to participate and listen in,"* said Mr. Farshchi, Equifax's CISO.

Conclusion

Board members continue to grapple with the challenge of cybersecurity oversight. The heightened tensions in the geopolitical and regulatory environments only enhance the focus. Audit chairs gain confidence in their companies' cyber capabilities when their CISOs are empowered, their managers brief them in a comprehensive but not hypertechnical way, and their boards provide proactive governance. While boards have taken measures to improve oversight practices in recent years, the demands continue to grow as their adversaries develop new capabilities.

Appendix A: Questions for audit chairs to consider

- ? What is the scope of the CISO's role at your company? To whom does your CISO report?
- ? How does the board interact with the CISO? How often does the CISO report to the audit committee? To the full board?
- ? What kinds of information does the CISO report? What types of quantitative data? What types of qualitative information? In what format is the information presented to the board?
- ? How has the relationship between the CISO and the board changed in the last few years? How do you envision it changing in the future?
- ? Does your board meet with the CISO in executive session?
- ? Do third parties regularly assess your company's cybersecurity capabilities? How are these assessments presented to the board?
- ? Does your board have a director with a strong cybersecurity background? If yes, how has this helped the board with overall cyber governance?
- ? Does your board have a technology or cybersecurity committee? How is the work divided between that committee and the audit committee?

Appendix B: Meeting participants

Central Audit Committee Network— March 9, 2022

The following network members participated in the meeting:

- Kapila Anand, Elanco Animal Health
- Anne Arvia, GATX
- Bruce Besanko, Diebold Nixdorf
- Pat Condon, Entergy
- Denise Dickins, Watsco *(SEACN member)*
- Cheryl Francis, Morningstar
- Marla Gottschalk, Big Lots and Reynolds Consumer Products
- Cara Heiden, Casey's General Stores
- Ginger Jones, Tronox Holdings
- Wendy Needham, Genuine Parts *(SEACN member)*
- Neil Novich, Hillenbrand
- Sherry Smith, Deere & Co.
- Karin Teglia, Wintrust Financial Corporation *(SEACN member)*
- Phoebe Wood, Invesco and Leggett & Platt
- Ray Young, International Paper

EY was represented by the following:

- Allison Dixon, Relationship Programs Strategist, Brand, Marketing & Communications
- Cigdem Oktem, Central Region Leader, Center for Board Matters
- Norm Prestage, Global Client Service Partner
- Jud Snyder, Chicago Office Managing Partner
- Bryan Yokley, Audit Partner, Georgia, Alabama, Tennessee Market Leader

West Audit Committee Network-North—March 15, 2022

The following network members participated in the meeting:

- Kimberly Alexy, Mandiant and Western Digital
- Prat Bhatt, Seagate Technology
- Teresa Briggs, DocuSign, ServiceNow, and Warby Parker
- Joe Bronson, PDF Solutions
- Susan Cain, Lithia Motors
- Raman Chitkara, Xilinx
- Earl Fry, Hawaiian Holdings
- Ken Goldman, GoPro
- Linda Harty, Parker Hannifin and Wabtec *(WACN South member)*
- Bala Iyer, Power Integrations
- Lou Lavigne, Zynga
- Jack Lazar, Resideo Technologies
- Sara Lewis, Weyerhaeuser *(WACN South member)*
- Mary Pat McCarthy, Palo Alto Networks
- Jeannine Sargent, Fortive
- Christine Tsingos, Envista Holdings
- Malia Wasson, Columbia Sportswear
- Janet Woodruff, Altus Group *(WACN South member)*

EY was represented by the following:

- Chris Anger, US-West Audit Leader
- Robyn Bew, West Region Leader, Center for Board Matters
- Scott Hefner, Global Client Service Partner
- Frank Mahoney, US-West Region Managing Partner

West Audit Committee Network-South— March 17, 2022

The following network members participated in the meeting:

- Phyllis Campbell, Air Transport Services Group
- Rich Dozer, Viad Corp
- Burl East, Comunidad Realty Partners
- Leslie Heisz, Edwards Lifesciences
- Ginnie Henkels, LCI Industries
- Leon Janks, PriceSmart
- Diana Laing, Spirit Realty Capital
- Michael Montelongo, Conduent
- Kristy Pipes, PS Business Parks and Public Storage
- Dick Poladian, Occidental Petroleum
- Daren Shaw, Ensign Group
- Les Sussman, East West Bancorp

EY was represented by the following:

- Chris Anger, US-West Audit Leader
- Robyn Bew, West Region Leader, Center for Board Matters
- Scott Hefner, Global Client Service Partner
- Kristin Valente, US-West Region Accounts Managing Partner

East Audit Committee Network—March 22, 2022

The following network members participated in the meeting:

- Virginia Addicott, CDW
- Bert Alfonso, Eastman Chemical
- Carl Berquist, Beacon Roofing Supply
- Bill Cary, Ally Financial
- Marie Gallagher, Glatfelter
- Lou Grabowsky, Griffon Corporation
- Mary Guilfoile, Interpublic Group
- Lew Kramer, L3Harris Technologies and Las Vegas Sands
- JoAnn Reed, American Tower
- Wendy Schoppert, The Hershey Company
- David Walker, Chico's FAS Inc. *(SEACN member)*
- Sandra Wijnberg, Cognizant and ADP
- Tim Yates, CommScope

EY was represented by the following:

- Molly Tucker McCue, US-East Audit Leader
- Bud McDonald,
- Dawn Quinn, Director, East Region Strategic Operations
- Carline Thompson, East Region Leader, Center for Board Matters
- Kevin Virostek,

Southwest Audit Committee Network— March 24, 2022

The following network members participated in the meeting:

- Curt Anastasio, Par Pacific Holdings
- Nick Chirekos, Peabody Energy
- Dan Doheny, Univar *(WACN South member)*
- Paulett Eberhart, LPL Financial Holdings
- Bruce Hanks, Lumen Technologies
- Mercedes Johnson, Synopsys
- Don Kendall, Talos Energy
- Debbie Kissire, Celanase
- Holli Ladhani, Marathon Oil
- Cathy Lego, Guidewire Software
- Teresa Madden, Enbridge
- Gil Marmol, Foot Locker
- Ellen Masterson, Insperity
- Royce Mitchell, Pioneer Natural Resources
- Don Robillard, Cheniere Energy and Helmerich & Payne
- Dunia Shive, Kimberly-Clark and Trinity Industries
- Valerie Williams, Devon Energy and DTE Energy

EY was represented by the following:

- Chris Anger, US-West Audit Leader
- Robyn Bew, West Region Leader, Center for Board Matters
- Scott Hefner, Global Client Service Partner
- Frank Mahoney, US-West Region Managing Partner

Southeast Audit Committee Network—March 30, 2022

The following network members participated in the meeting:

- Eddie Adair, Rayonier Advanced Materials
- Curt Anastasio, Par Pacific Holdings *(SWACN member)*
- Art Beattie, PPL Corporation
- Rick Cardenas, Tractor Supply Company
- Bill Creekmuir, Party City *(EACN member)*
- Juan Figuereo, Deckers Outdoor Corporation
- Tom Hough, Equifax
- Jim Hunt, Brown & Brown
- Rich Macchia, FLEETCOR Technologies
- Judy Schmeling, Constellation Brands *(EACN member)*

EY was represented by the following:

- Allison Dixon, Relationship Programs Strategist, Brand, Marketing & Communications
- Cigdem Oktem, Central Region Leader, Center for Board Matters
- Norm Prestage, Global Client Service Partner
- Bryan Yokley, Audit Partner, Georgia, Alabama, Tennessee Market Leader

Endnotes

[1] Department of Homeland Security Cybersecurity & Infrastructure Security Agency, Urgent Letter from the Director of CISA Addressing NACD Members, February 25, 2022.

[2] The White House, "Statement by President Biden on Our Nation's Cybersecurity," news release, March 21, 2022.

[3] *ViewPoints* reflects the use of a modified version of the Chatham House Rule whereby names of participants 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 these meetings.

[4] EY, *SEC Proposes Requiring More Cybersecurity Disclosures,* To the Point (Ernst & Young LLP, 2022).

[5] Stephen Pritchard, "The Changing Profile of the CISO: New Roles, New Demands, New Skills," *Tripwire* (blog), December 22, 2021.

[6] "2022 CISO Compensation & Organizational Structure Survey," Hitch Partners, 2022.

[7] Kris Lovejoy et al., *Cybersecurity: How Do You Rise Above the Waves of a Perfect Storm?* EY Global Information Security Survey 2021 (London: EYGM, 2021), 4.

[8] "Shields Up," Cybersecurity & Infrastructure Security Agency, accessed April 15, 2022.

[9] Lovejoy et al., *Cybersecurity: How Do You Rise Above the Waves of a Perfect Storm?* 10.

[10] Marho Atumu, "Top 5 Cybersecurity Frameworks in 2022," *Liquid Web* (blog), December 22, 2021.

[11] Lovejoy et al., *Cybersecurity: How Do You Rise Above the Waves of a Perfect Storm?* 10.

[12] Jonathan Greig, "Average Ransomware Payment for US Victims more than $6 Million, Survey Says," ZDNet, November 9, 2021.

[13] Jonathan Wolfman et al., "SEC Proposes New Public Company Cybersecurity Disclosure Rules," *Insights and News* (blog), March 10, 2022.

[14] Gartner, "Gartner Identifies Top Security and Risk Management Trends for 2021," news release, March 23, 2022.

[15] Jamie Smith, "How Cybersecurity Risk Disclosures and Oversight are Evolving in 2021," EY Center for Board Matters, October 5, 2021.

[16] Spencer Stuart, *2021 U.S. Spencer Stuart Board Index* (Chicago: Spencer Stuart, 2021), 28.