tapestry NETWORKS

ACLN SUMMARY OF THEMES

Cybersecurity and data privacy, assurance in new domains, and corporate culture

March 2024

On March 4-5, 2024, the Audit Committee Leadership Network (ACLN) met in Austin, Texas to discuss cybersecurity and data privacy, assurance in new domains, and corporate culture. Members also visited Texas Robotics at the University of Texas at Austin for a tour and discussion about robotics and artificial intelligence (AI).

Members were joined by guests Christine Boucher, deputy general counsel and chief compliance officer at Delta Air Lines, Deborah Wheeler, global chief information security officer at Delta Air Lines, and Eric Latalladi, the global chief information security officer at MetLife for the cybersecurity and data privacy discussion. Page Motes, vice president, sustainability and impact of The Hertz Corporation, joined members for the corporate culture discussion, and Anvita Sahai, assurance partner, EY, for a conversation about assurance in new domains.

Forthcoming *ViewPoints* will provide additional details on the cybersecurity and data privacy and corporate culture sessions.

For a list of meeting participants, see Appendix 1 (page 9).

This *Summary of Themes*[1] provides an overview of each discussion:

EY Building a better working world

Cybersecurity and data privacy: a dialogue with CISOs and data privacy leaders

With an ever-changing risk landscape, members were eager to hear perspectives from Ms. Boucher, Ms. Wheeler, and Mr. Latalladi on how threats are evolving and good practices for effective cybersecurity and data privacy risk management at large, global companies. Several themes emerged:

- **The volume and sophistication of cyber threats are rising.** As an example, Ms. Wheeler noted that Delta *"saw a 900% increase in the number of phishing events coming out of the pandemic versus the years leading into it."* Guests also cautioned that attackers are increasingly exploiting identity theft. They highlighted several factors contributing to the growing complexity of cyber risk:
  - **Advancing technologies.** Citing a recent incident where fraudsters used deepfake technology to pose as a company's chief financial officer and direct an employee to pay USD 25 million,[2] a member asked, *"How realistic are these deepfakes?"* The guests emphasized that technology is rapidly advancing. *"It is becoming much harder to see some of the telltale signs of a deepfake. And with the use of AI in phishing, we're now seeing perfect emails,"* Ms. Wheeler said. To combat this, Delta advises employees: *"Do not trust anything sent to you electronically. Pick up the phone and contact the individual or stop by their office. Use a code word. Have an external way of validating the authenticity of what you are being sent."*
  - **Geopolitical tensions and regulatory challenges.** Increased cybersecurity risks from geopolitical tensions are a major concern. The active conflicts between Russia and Ukraine and Israel and Gaza heighten risks on top of the elevated tensions that already exist with China, North Korea, Iran, and Russia. Large companies also face an increasingly complex regulatory environment, which can vary by industry and countries of operations. As examples, guests referenced the SEC's cybersecurity disclosure rules, as well as the European Union's forthcoming Digital Operational Resilience Act, which aims to strengthen the IT security of the financial services sector in Europe and takes effect in 2025.
  - **Increasing use of third parties.** *"Prior to the pandemic, we had four or five suppliers annually that would report they had been the victim of a data compromise or cyber intrusion. Coming out of the pandemic, we have seen a hundred or more vendors/third parties being compromised per year,"* Ms. Wheeler said. *"Proliferation of third-party vendors is the biggest challenge,"* a member said. Both CISOs advised a rigorous approach to using third parties, aiming to minimize the number of vendors while strengthening the security of remaining partnerships. Large companies can also educate vendors: *"Many third parties we work with are smaller companies that cannot afford the cyber presence of Delta. We direct them to the Cybersecurity and Infrastructure Security Agency which makes a lot of tools and capabilities available to them at no cost,"* Ms. Wheeler said.
  - **Digital transformation and cloud migration.** As companies migrate to the cloud, some may want to quickly *"lift and shift"* workloads, but that can result in heightened risks. Delta adopted a *"lift, tinker, and shift"* approach, Ms. Wheeler said, to ensure that anything moved to the cloud was not only transferred but also optimized to meet security standards. Re-engineering software was

not easy once it was operational in the cloud, she warned: *"Be very intentional. You want to make as many decisions as possible in putty, not concrete."* The group discussed the importance of leveraging cloud-native capabilities, noting that the real value of cloud technology lies in utilizing the full range of cloud services.

- **Data privacy risks are increasing for global companies due to stricter regulations and increased enforcement worldwide.** The European Union's General Data Protection Regulation (GDPR) previously set the standard for global privacy programs. However, the regulatory environment has evolved, in particular with countries in the Asia-Pacific region enacting more rigorous privacy laws concerning consent management and data localization, Ms. Boucher explained. *"As a global company, when we structured our privacy program, we set it at the GDPR level and thought that should cover us everywhere else. But the landscape has shifted,"* she said. *"On top of that, we're also seeing a lot more enforcement by regulators in those regions."* In light of these developments, global companies may need to reassess their operations and compliance approaches—this applies to consumer-facing companies and business-to-business (B2B) companies that have employees, operations, or data processing activities in certain regions.
- **Employee awareness and training are vital for both cybersecurity and data privacy.** *"It only takes one employee to have a massive data breach,"* Ms. Boucher said. For companies with large, global workforces, customized communication strategies are key. *"The vast majority of our employees don't sit behind a desk,"* Ms. Wheeler said. Delta addresses this by making training accessible on various devices, engaging younger employees through internal social media, and incorporating gamification. For data privacy, Ms. Boucher described Delta's use of *"privacy ambassadors"* who serve as the frontline of communication and feedback and promote a culture of data protection. *"We make it a point of pride for them to be privacy champions, and it is not a heavy lift to do it,"* she said.
- **Audit chairs grapple with what type of cybersecurity dashboards and reporting are most effective.** *"How do we know that the picture being portrayed is the picture? Are we asking the right kinds of questions?"* one member asked. Reports should be customized to the unique requirements of a company and its audit committee. One reporting approach described during the meeting includes key operating metrics, overall strategy development and execution, and an outside, independent perspective on the company's performance and the threat landscape. Ms. Wheeler noted that metrics can be tricky: *"Some boards want to know how many times a month we are being attacked, but what purpose does that number serve? Numbers are only one point in time, and they change the*

Critical questions for audit committees to ask CISOs?

Ms. Wheeler shared three questions that boards and audit committees can ask to better understand critical aspects of their company's cybersecurity. *"These questions have measurable impact and should give you a good understanding of where the security program is,"* she said.

1. How quickly can the organization patch critical or zero-day vulnerabilities?
2. What is the technology footprint and state of the asset inventory? How do you know that you are protecting everything you need to protect?
3. What percentage of the technology is end-of-life and can no longer be supported by the vendors that you're doing business with? What are the plans to address that?

minute you publish them." Instead, her reports to the audit committee focus on *"explaining the story of the security journey: how it has grown, how capabilities have improved, what the threat landscape looks like, and how the company has either risen to the challenge or identified areas for further improvement."*

- **Companies should evaluate their existing processes to ensure alignment with the SEC's recent cybersecurity disclosure rules.** The rules require reporting material cyber breaches within four business days. Delta reviewed its materiality assessment process to ensure there are no gaps in compliance. While large, global companies likely do not need to *"reinvent the wheel,"* it is important to formalize the processes used for determining materiality, ensure visibility into all cyber incidents, and have a crisis management process in place. Ms. Boucher noted that Delta held a tabletop exercise to help pinpoint any potential issues under the new requirements.

A forthcoming ViewPoints will provide additional detail on the key themes discussed during the session.

Assurance in new domains: ESG, AI, and beyond

Assurance builds trust in the reliability of the information that companies disclose to investors and other users. "Assurance" can mean many things—not only a reasonable or limited assurance opinion from an external auditor, but also an impact assessment, a compliance audit, certification, performance testing, or some other way of attesting to the trustworthiness of the disclosure. Ms. Sahai joined members to share her views and discuss developments around providing reliable information in the emerging areas of sustainability/ESG disclosures and AI-generated information.

Acknowledging that changes are forthcoming once the SEC rules for climate disclosures were finalized (the rules were finalized two days after this discussion), members discussed the need for providing trustworthy information on climate and other sustainability practices in the financial report. The following themes emerged:

- **Changes in investor views on ESG/sustainability.** Some members expressed skepticism on the value of ESG/sustainability information to investors. One explained that there is a *"backwards push by some investors on ESG/sustainability"* that impacts the need for voluntarily disclosing this information in the financial report. Others noted the polarization of investors; one said some investors are *"rabid for information while others do not care."* A member noted that *"eighteen months to two years ago, we heard from CFOs and CEOs that investors were asking about sustainability matters all the time. Now they say they are not being asked those questions."*
- **Understanding how Europe has fared thus far.** Europe imposed regulations on sustainability disclosure and assurance well before the US. Members showed interest in how European companies are complying—for example, how their sustainability disclosures align with their financial statements, and how the information will be assured to meet the assurance requirements. A European board member described how ESG disclosures have evolved from very broad, potentially ambiguous statements to much more specific risks: *"What are the key contributions you can make in the sustainability arena that matter to your company and society? There is a focus on what's relevant to your company rather than broader disclosures which are less meaningful as they are less relevant to the company."*

- **Weighing the cost/benefit of providing disclosures and assurance thereon.** Members expressed skepticism about the value of compiling the information and having it assured. *"If you're going to spend all this money and put limited assurance on something that has nothing but estimates in it, I want to know the cost has a benefit,"* one said. Another expressed concerns over what would be assured: the data (which can be overseen by internal audit), or the associated risks and impact on the company. The latter, it was noted, would be harder to assure because of the judgments that would be needed.

Members discussed the use of AI within their companies, which varied significantly. They highlighted the need to differentiate between true AI technologies and advanced technologies or analytics, the latter having been in use for many years in some industries. One explained, *"There's a huge difference between very large-scale data analytics, which is becoming larger because of computing technology, and generative AI. If you talk to experts, the word 'AI' is used when the technology is generating new content and new data. That is what is challenging to audit. But data analytics, machine learning, and robotics have been around for a long time. It's helpful to differentiate them so you understand where the risks are."*

The AI use cases noted by members tended to be on the operational side of the business, using internal data, with less direct impact on financial reporting. While audit chairs expressed caution around the uncontrolled use of AI, they recognized its potential benefits; they also noted increasing use of AI in finance functions—for example, in the analysis of contracts, in MD&A, expense reporting, calculating estimates, and investor relations. Few of these cases struck them as material to the financial statements. Members acknowledged that this would evolve with time.

The concerns they identified included:

- **Whether financial information being produced reflects operating realities in the company.** Determining the validity of the information generated is difficult because the algorithms are not transparent. A member suggested *"a parallel process to validate some of the output."*
- **Inherent biases in the data.** Members questioned what can be done about bias that may be present in the data being used by AI technologies. These could lead to skewed algorithmic decisions, unfair or unintended outcomes, and ethical problems.
- **Evidence needed for regulatory inspections.** Members expressed uncertainty about what they will need to demonstrate to regulators regarding information produced by AI. One noted that *"PCAOB inspections are focused on sources of information, so it would be interesting to understand how they are thinking about information generated by AI."* Ms. Sahai explained that all stakeholders were on the journey and that AI experts from EY and other organizations were continuously educating regulators and other key stakeholders about what works and what does not work. A member added that *"collectively, as a profession, we need to educate so when rules and regulations come out, they are well informed rules and not just reactionary."*
- **An evolving global regulatory environment.** Regulators in Europe and the US are rushing to regulate AI, but the field is moving so quickly that they are always behind its leading edge. Members noted challenges in keeping up with regulations around the globe, and in different US states.

Ms. Sahai delved into good governance practices around the use of AI: *"What we see today are tools or apps that are generally static unless there is manual intervention to change a setting. AI tools by nature, if there is not a framework to limit what they can do, can change at a much faster pace. It brings a different element of risk that needs to be addressed by controls."* She explained the benefit of a risk-based framework around the use of AI in order to identify appropriate controls and recommended creating cross functional teams and revisiting company policies. A member described the establishment of *"an executive committee and steering committee for use of AI within the company. They then solicited input from across the company's different functions and business units about AI projects that employees felt would be useful and wanted to engage in. They got a lot of input. The company selected a number of the projects, primarily ones that impact products and services and process efficiency projects in IT, finance, and HR. The steering and executive committees are monitoring these projects to see what we learn, what issues we encounter, and what benefits we get before they allow more deployment of AI across the company."*

Assessing and communicating culture in a post-pandemic world

The COVID-19 pandemic accelerated a shift in corporate culture by driving employees to reevaluate their purpose and priorities and employers to cope with a sudden scarcity of talent. ACLN members discussed the role of boards and audit committees in overseeing these trends with Ms. Motes, whose career has spanned leadership roles in sustainability, compliance, and ethics.

"One of the good things that came out of the pandemic was we recognized each other's humanity. We gave each other grace and time," Ms. Motes said. The issue now, she suggested, is not how to get things back to *"the way they used to be,"* but how to drive productivity, engagement, and innovation in this *"new normal"* work environment. Companies that can clearly articulate their purpose and mission are ahead of the game, she advised, because employees have reevaluated their priorities. *"How does the company articulate and drive action so employees are not just making a product or selling a service but reaching 'beyond'? Even more so than before pandemic, that is really important now. We are all in it together."*

The discussion surfaced several themes:

- **Corporate culture is shaped by forces that go well beyond pandemic effects.** Working from home has been a focus for many companies when it comes to culture, and the group questioned, *"Is it a symptom or is it the issue?"* Ms. Motes replied that there are other factors contributing to the shift in culture. *"Gen Z has a completely different mentality—they look at leadership, engagement, and even what they wear to work differently. They are not driven as much by money—they are driven by purpose and common values,"* she said. Members pointed to the impact of trends like globalization, cloud computing, and outsourcing. *"The net result is the notion of having to work seamlessly with people around the world inside and outside the walls of the organization, so people want flexibility to figure out what makes the most sense,"* one said. Another emphasized that *"one size does not fit all."*
- **Audit chairs have different opinions about the board's responsibility in developing culture.** There was some debate about the role of the board and its relative importance vis-à-vis the CEO and management in developing a company's culture, but all members said that culture regularly appeared on the board agenda. There was general agreement that even if it is not a direct mandate of audit committees, consideration of culture is vital. As one member explained, *"The right culture substantially*

reduces risk in an organization, and a negative culture substantially increases risk, so it is very much in the audit committee mandate to understand culture." Audit committees should ask *"what the company's strategy is for building and sustaining culture in a hybrid world with Gen Z because that's the world we're heading into. We need to understand what the CEO's strategy is in that context,"* he said.

- **Decisions to bring people back to the office can be a minefield**. While members generally recognized that the world has moved on from full-time in-office work, companies need to find a balance that works for everyone. *"How do you develop and protect culture with today's workforce? What will the result be in five to 10 years?"* one member said. Another underscored the difficulty of driving people back to hybrid or full-time in-office work unless the business purpose is clearly articulated, and many times it is not. *"Decisions that are communicated have to make sense,"* he added.
- **Boards employ a range of tools to assess culture and get a sense of *"what's actually happening on the ground."*** Several members pointed to rigorous employee engagement surveys as a tool to assess and track culture. One member said his company regularly sees response rates approaching 85 percent and attracting tens of thousands of comments. Ms. Motes responded, *"Boards can support this process by encouraging management to ensure surveys are asking the right questions for a post-pandemic world, and by using such tools not just to assess but also to recognize and praise good behaviors and to drive coaching by middle managers—often the front line of company culture."* Other members emphasized the importance of site visits. At one company, board members are *"expected to do four to five site visits a year—go to the site with a sense of purpose and talk to people about culture. All board members do it and we feed it back into a template and discuss what we've seen."* Another described a process called "Sector Day" where a subset of the board visits a business unit, including a dinner with the CEO of that particular

Culture is crucial to the success of mergers and acquisitions

Aligning different business cultures during mergers and acquisitions can be challenging, and members highlighted both positive and not-so-positive stories. One notable example involved a *"merger of equals"* where the board was dominated by one side and management by the other. *"It was a complete mess,"* the member said and resulted in the company's sale. Conversely, successful integrations prioritized culture. One member described a merger where *"we got the best of both worlds through very decisive action by leadership. They chose the best systems to use, guided by the people and the culture that we wanted to have."* Ms. Motes recounted an acquisition where senior leadership took months to bring teams together to intentionally develop a new purpose and strategy, and then disseminate it in a cascading manner from senior management to their direct reports, and from those leaders down to front line employees: *"That became an anchor by which we could operate in a collective culture."* Reaching cultural cohesion and alignment takes time, as one member reflected, *"We did a lot of what the book says: set up a committee for integration, set up the best performing executive on every level. This was over five years ago and we still will require a few more changes before there is one company culture—I think we have a few more years to go before we get there."*

business unit, and then interacts with the rest of the team *"to learn about their operations and culture on the shop floor."* Employees also can ask questions of board members, *"which demystifies the board role."* The *"magic"* of Sector Day is that *"no one from corporate is allowed to be there, which lets us see what is really happening on the ground without being influenced by the understandable strength of the CEO," a* colleague on the same board said.

- **The board's own culture sets the tone.** Members discussed the culture of the board and the audit committee itself. One pointed out that this is a vital element of doing due diligence when joining a board: *"We're all independent and bring that thinking and independence but it is also important to be respectful and listen and learn."* Another pointed to the utility of individual director evaluations and *"direct feedback to each board member on how he or she is perceived by peers—not that we all need to agree, but we need to disagree respectfully."*

A forthcoming ViewPoints will provide additional detail on the key themes discussed during the session.

Field Trip: Texas Robotics

ACLN members visited Texas Robotics at the University of Texas at Austin. As board members of public companies, many audit chairs closely monitor the rapid advancements happening in technology, such as with artificial intelligence (AI), and they recognize the profound impact such advancements have on business. Members met with Professor Peter Stone, director of Texas Robotics, to discuss technology innovation and the future direction of robotics and AI. They were curious to hear his views on the risks associated with AI, projections for the field in the next five years, and the interdisciplinary collaboration that drives innovation. They also asked questions around university-industry partnerships, student education around AI, and strategies for board members to educate themselves about AI.

Professor Stone shared a free online lecture series about AI that he recommended as a potential educational resource for boards: ***The Essentials of AI for Life and Society*.**



Appendix 1: Participants

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

Fernando Aguirre, CVS Health
Joan Amble, Booz Allen Hamilton
Judy Bruner, Applied Materials
Janet Clark, Texas Instruments
Anne Drinkwater, Equinor
Bill Easter, Delta Air Lines
Bella Goren, General Electric and Marriott International
Gretchen Haggerty, Johnson Controls
David Herzog, MetLife
Lori Lee, Emerson Electric
Larry Quinlan, Jones Lang LaSalle
Tom Schoewe, General Motors and Northrop Grumman
Cindy Taylor, AT&T

The following members participated virtually in part of the meeting:

Dave Dillon, 3M and Union Pacific
Tom Freyman, AbbVie
Jim Turley, Citigroup
John Veihmeyer, Ford

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

Julie Boland, US Chair and Managing Partner and Americas Area Managing Partner, EY
Jennifer Lee, Managing Director, Americas Center for Board Matters, EY
Pat Niemann, Partner, Americas Center for Board Matters, EY

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

Beverley Bahlmann, Executive Director
Jonathan Day, Chief Executive
Kelly Gillen, Senior Associate
Todd Schwartz, Executive Director
Abigail Ververis, Project and Event Manager

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 members and guests in connection with the meeting but may be edited for clarity.

[2] Heather Chen and Kathleen Magramo, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'," *CNN*, February 4, 2024.