Audit Committee Leadership Summit

July 2022

ACLS

SUMMARY of THEMES

Dialogue with FBI Director, China, future of cyber risk, ESG, and blockchain applications

On June 29-30, 2022, the Audit Committee Leadership Summit brought together members of the North American and European Audit Committee Leadership Networks (ACLN and EACLN) in New York for a conversation with the Director of the United States Federal Bureau of Investigation (FBI), as well as for discussions on topics including China; the future of cyber risk; oversight of environmental, social, and governance (ESG); and blockchain applications.

Below is a summary of those conversations.[1] Three forthcoming *ViewPoints* will provide additional details on the dialogue with FBI Director Christopher Wray, the future of cyber risk, and the members-only discussion on ESG.

Dialogue with FBI Director Christopher Wray

Members met with Director Wray for a discussion on the overall threat landscape, ransomware, and cyber incident response. They discussed several important points:

- **Cybersecurity, counterintelligence, and counterterrorism are strategic priorities for the FBI—and all three impact and involve the private sector.** Nation-state actors and criminal gangs are attacking the private sector on multiple fronts including infrastructure, intellectual property, and thefts of personally identifiable information. Counterterrorism is highly relevant for companies, said Director Wray, because actors employ *"more primitive, easy-to-implement, lower-cost attacks on soft targets like companies, malls, and schools."*
- **China poses an unparalleled threat to US and global economic vitality.** *"No other country poses as broad and comprehensive of a threat to our innovation, intellectual property, and economic security,"* said Director Wray. Several members reported that their companies are rethinking strategies related to China. One member said: *"Three years ago, our board thought China was a massive opportunity, but we have completely changed our plans and are no longer pursuing new opportunities there."* Director Wray highlighted that boards have a *"particularly important role"* to play in addressing the China threat. While management may be more focused on shorter-term goals, boards can ensure a *"long term, existential perspective,"* he explained, which is especially important when it comes to the China threat.
- **Cyber threats are growing in complexity—from blended nation-state and criminal gangs, to disinformation, to insiders.** Director Wray discussed blended threats, in which

nation-states, such as Russia and China, turn a blind eye toward cybercriminals or even work with them. He also discussed how counterintelligence threats such as disinformation and insider threats can amplify the risk to companies and often go hand-in-hand with cyber threats.

- **Companies should be proactive in engaging the FBI, even when an attack occurs outside of the United States.** Director Wray encouraged companies to establish relationships with their local FBI office before a crisis occurs and to involve the FBI early during cyberattacks, especially when a ransom is or may be requested. While the Bureau discourages paying ransom, he stressed that it views and treats an attacked company as the victim and that the FBI can provide significant assistance to affected companies. *"By contacting the FBI early, we may know the actor, when they hit other companies, the methods they used, and what their next step has been,"* he noted, which in turn can help companies make more informed decisions. Early engagement with law enforcement can be viewed favorably by the Department of Treasury *"as a significant mitigating factor"* should a payment violate sanctions, he added. He recommended that both US and foreign companies engage the FBI: *"Call us, especially for cyber. Don't worry about trying to figure whose lane it is. The reality is there is very little chance that a significant cyberattack does not involve a US hacker, victim, company, or infrastructure."* Director Wray also noted the FBI's ability to quickly engage with partners around the world.
- **Companies and the FBI are keen to enhance information sharing and partnerships.** Members and Director Wray had an open dialogue about private sector partnerships with the FBI, and the importance of sharing information in both directions that will maximize impacts and outcomes for all. Many members reported positive interactions. Others called for improved information sharing from the FBI to the private sector. Director Wray stressed that enhancing private sector partnerships is a priority and said that the Bureau continues to work toward improvements.

The risks and opportunities of doing business in China

Members discussed the risks and opportunities associated with China with Ambassador Susan Schwab, former US trade representative, strategic advisor to Mayer Brown LLP, and professor emerita at the University of Maryland School of Public Policy, as well as Ryan Hass, senior fellow at the Brookings Institution and nonresident fellow with Yale Law School.

Mr. Hass provided an overview of the macropolitical environment, including several themes:

- **China's growth targets are off track, but it has not lost its way.** *"This is the first time China will not reach its growth targets since 1990,"* he said. *"The International Money Fund has revised its growth target goal to 4.4% (from China's target of 5.5%) and many analysts expect they will not even reach the revised goal."* This puts pressure on Chinese President

Xi Jinping. Mr. Hass expects China will continue to *"muddle through, but it is clearly underperforming."*

- **The United States has bipartisan consensus on China.** Mr. Hass noted that *"public disapproval of China is at a record high in the US—79% have negative views on China's behavior"* and it is one of few issues that Democrats and Republicans typically agree on.
- **Neither the United States nor China is satisfied with current relations, but neither want a conflict.** Mr. Hass suggested that the US-China relationship has reached a *"cruising altitude with high turbulence,"* which he described as being costly for either side to change. He believes that both sides remain motivated to avoid overt conflict.
- **China is learning from Russia's invasion of Ukraine.** Mr. Hass and Ambassador Schwab noted that President Xi Jinping is sympathetic to Vladimir Putin and has observed the Russian invasion of Ukraine through the lens of a potential Chinese move on Taiwan. Both guests noted that, although it might take China some time to build military and strategic readiness for an invasion, Russia's experiences in its attack on Ukraine could accelerate the Chinese timeline.

Ambassador Schwab and Mr. Hass also provided perspectives on issues directors should consider. Both strongly cautioned companies to protect their data, technology, communications, and trade secrets from theft by China. Ambassador Schwab compared a board's roles in overseeing China risk with the balance of efficiency versus resiliency or sustainability required to manage ESG issues. She shared practical recommendations:

- **Insist on regular geopolitical briefings.** Ambassador Schwab recommended boards request regular briefings to understand specific challenges and risks associated with China for their companies. Briefings could be held quarterly, as a regular board exercise, or as a deep dive. *"Brainstorm what ifs, look at your exposure to China, including what your Chinese competition may be doing or be poised to do to your business in third country markets,"* she advised.
- **Strengthen and prioritize cybersecurity and data protection practices.** Both Ambassador Schwab and Mr. Hass told members to assume that information is being compromised and that video meetings can be listened to. Ambassador Schwab acknowledged that Chinese employees of multinational companies can be placed in difficult positions and recommended that companies with Chinese operations hold meetings outside China and think carefully about what information or technology is shared with Chinese employees.
- **Remember the unique—and positive—role companies play**. With dialogue between the US, European, and Chinese governments at a low point, companies can play an important role in "*keeping bridges open,"* said Ambassador Schwab. *"If you can hang in there, do so … I think that it is imperative for US and European companies to contribute to the future of relations with China."*

The future of cyber risk

Members were joined by General (Ret.) Keith Alexander, founder, chairman, and co-CEO of IronNet, Inc. and former director of the National Security Agency; Tim McKnight, executive vice president and chief security officer of SAP; and Lee Foster, senior vice president of Alethea Group. The discussion highlighted emerging cyber and technology risks, quantum computing, and disinformation attacks:

- **Cyberattacks on companies are evolving.** General Alexander reiterated themes that FBI Director Wray, Ambassador Schwab, and Mr. Hass had emphasized earlier in the meeting. Increased tensions between the United States and China, and with Russia, will fuel cyber threats and companies should stay on high alert. *"The target is not just government—it is industry,"* General Alexander said. *"China has said—as indicated in its military doctrine—that they will use cyber as part of their campaign in the event of a war. In addition to intellectual property theft, using cyber as an element of national power would also include destroying data … which is a near-term risk for small and mid-sized companies in your supply chains."*
- **Technology advancements create new types of risks.** Mr. McKnight discussed how technologies like artificial intelligence and machine learning can open opportunities, but also bring new risks. Transparency and integrity are key to risk management. *"You need to retain the ability for humans to override automated processes if an outcome is being driven by bias or inaccurate models,"* he explained.
- **Cybersecurity will be significantly challenged by quantum computing.** While the timeline for quantum computing to be widely available remains unclear, experts agree it will transform information security through its ability to overcome current encryption methods. While cyberattacks are not yet breaking encryption, Mr. McKnight said that his team is focused on building crypto agility to ensure a rapid response to any changes in cryptographic standards. He advised directors to begin thinking about the implications of quantum.
- **Talent management is a top cyber concern.** Mr. McKnight shared that there are close to 3 million unfilled cyber jobs. He suggested boards ask management and chief information security officers about how they develop and retain talent for their cyber and technology programs. Mr. McKnight shared good practices for chief information security officers, including working closely with HR teams and universities to develop talent early. As a hedge, he also advised investing in automation to perform *"lower value-add services"* where possible.
- **Disinformation is an issue boards should be thinking about.** *"Companies should take disinformation seriously as a threat and start preparing for targeted incidents,"* said Mr. Foster. Financial gain, politics and ideology, or a desire to disrupt companies or markets

are some of the possible motivations behind disinformation campaigns. These attacks can diminish consumer trust, damage brands, lead to financial losses, and create physical security risks. Mr. Foster described how a vaccine company, Ocugen, recently experienced bot-like accounts coordinating to manipulate its stock performance. He noted that it is relatively easy to launch a disinformation attack and that a variety of actors get involved, including for-hire contractors, nation-states, ideological individuals, and conspiracy theorists. *"It takes very little technical acumen to push out a false narrative around a company,"* he said.

- **Companies should proactively monitor and prepare for disinformation.** Mr. Foster provided some good practices related to disinformation. Companies should take the threat seriously and continuously monitor for disinformation. They should also identify relevant stakeholders—starting with the internal threat response team if there is one—and assign responsibility for aspects of disinformation that are wrapped into legal, communications, cyber and IT, and physical security functions. Finally, companies should create an incident response plan that includes practice exercises.

Members-only discussion on ESG

Audit chairs discussed ESG governance, evolving regulatory regimes, and the audit committee's role in controlling and reporting on ESG data. The following key themes emerged from the discussion:

- **Getting clear around who owns which aspects of ESG oversight is key.** Members reported that ESG oversight is typically split between the full board, the nominations and governance committee, and the audit committee. A few companies have established ESG or sustainability committees. The challenge for boards in overseeing ESG, said one member, is "*getting very crisp on who owns the decisions on what you disclose, where you disclose it, and who owns the quality assurance around the disclosures."*
- **Audit committees are focused on controls around ESG data collection and reliability of disclosures.** All members agreed that the audit committee is best positioned to ensure proper controls and accurate reporting of ESG data. *"The process of what to disclose and how to disclose it is iterative,"* said one member. Whether something can be disclosed reliably and with good controls impacts when her company discloses certain ESG information.
- **ESG disclosure committees are being used to implement rigor and processes around ESG data and disclosures.** More than half of the audit chairs at the meeting reported that their companies have established ESG disclosure committees. A member explained that many participants on the ESG disclosure committee also serve on the financial disclosure committee. This helps instill discipline in ESG reporting and *"gives the audit committee and board comfort that it improves the rigor."*

- **Evolving regulatory environments create challenges.** Rapidly changing regulatory regimes in both the United States and Europe make ESG oversight challenging. Companies and boards should be clear on the standards they are complying with. One member noted that her company uses a matrix to show which standards and regulatory requirements they are applying to their ESG reporting. "*As regulatory requirements continue to evolve and get more fine-tuned, the matrix will get more complicated*," she explained.
- **Lack of common standards and frameworks makes assuring ESG information difficult.** Members reported that today, engineering firms are most commonly used to assure ESG information. But with the pending proposal on climate-related disclosures from the US Securities and Exchange Commission, several thought that financial auditors might make more sense. "*Having the same firm audit financials and ESG would be my preference,"* underscored one member, adding, *"But what are they going to audit against? There are still too many choices for how you report."*

Applications of blockchain—from cryptocurrency to supply chain management

Paul Brody, global blockchain leader at EY, discussed blockchain applications and risks and opportunities members should be aware of including:

- **Blockchain technology's greatest advantage is also its biggest weakness.** Mr. Brody noted that blockchain's value proposition is that it *"makes it possible to run complex ecosystems without a central authority."* But this decentralization comes at the cost of privacy, and many businesses worry that sensitive information may end up on someone else's digital ledger. Private ledgers can secure information, but they defeat the purpose of a decentralized database. However, new mathematical techniques permit verifying the authenticity of a transaction without disclosing competitive data such as pricing in a supply chain system.
- **Blockchain technology has a wide range of applications.** While many associate blockchain with cryptocurrency, other blockchain applications are transforming finance and supply chain management. Decentralized finance and smart contracts are a particular growth area and allow for more streamlining, transparency, and automation of transactions. Blockchain also has useful supply chain applications, including tracking products and services as they travel through a supply chain, with full transparency for end-to-end participants.
- **In finance, blockchain will not replace existing systems.** Centralized financial systems have become highly scalable and efficient. Mr. Brody said that blockchain technology has *"no value proposition for replacing existing systems that are highly centralized and efficient, especially if regulated."* While he does not think that stock exchanges or systems are good

candidates for blockchain, he does think that the technology can be valuable for Electronic Data Interchange and Enterprise Resource Planning.

- **Blockchain risks are manageable.** Mr. Brody noted that there are short-term risks around blockchain technology and coding. Taking traditional assets and turning them into programmable items can yield *"unintended consequences,"* he said. In addition, every online system creates risks; a blockchain is built out of software, but most people who participate in it are not software developers. He added that companies should be vigilant about brand risk and cultural issues specific to digital communities and be thoughtful and strategic about *"how your brand presents itself online."* Mr. Brody emphasized that *"the most useful risk management tool is to do a little bit to start—manage risk by getting your feet wet incrementally."*
- **The risks of adopting blockchain late are greater than the risks in adopting it early.** Mr. Brody expects that businesses will be widely and deeply impacted by blockchain technology. By 2030, he said, half of all new contracts and agreements will be on blockchain and smart contracts will overtake paper ones. He compared blockchain's rapid adoption to that of other technologies such as the cloud, mobile networks, personal computers, etc.: *"Companies that take the market lead at the time the market accelerates are remarkably hard to dislodge. If you are late, how do you catch up?"*
- **Audit firms have built out blockchain expertise.** Members wondered if accounting firms have the capabilities to audit blockchain. Mr. Brody said that they are already doing this. Auditors have established key control standards such as being able to prove a firm or an individual has control over an asset, matching transactions on a blockchain with those in a company's financial system, and testing digital assets to see if they perform in a reasonably predictable manner.

Appendix: Participants

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

- Joan Amble, Booz Allen Hamilton
- Judy Bruner, Applied Materials and Seagate Technology
- Jeff Campbell, Aon
- Janet Clark, Texas Instruments
- Pam Craig, Merck
- Ted Craver, Wells Fargo
- Dan Dickinson, Caterpillar
- Bill Easter, Delta Air Lines
- Lynn Elsenhans, Saudi Aramco
- Tom Freyman, AbbVie
- Gretchen Haggerty, Johnson Controls
- Bob Herz, Fannie Mae and Morgan Stanley
- Akhil Johri, Boeing and Cardinal Health
- Lori Lee, Emerson Electric
- Arjun Murti, ConocoPhillips
- Louise Parent, FIS
- Ann Marie Petach, Jones Lang LaSalle
- Peter Porrino, AIG
- Kimberly Ross, Cigna
- Tom Schoewe, General Motors
- Leslie Seidman, GE
- Cindy Taylor, AT&T
- Fred Terrell, Bank of New York Mellon
- Tracey Travis, Meta
- Jim Turley, Citigroup

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

- Julie Brown, Roche
- Marion Helmes, Heineken
- Pilar Lopez, Inditex
- Benoît Maes, Bouygues
- John Maltby, Nordea
- Marie-José Nadeau, ENGIE
- Karyn Ovelmen, ArcelorMittal
- Ana de Pro Gonzalo, STMicroelectronics
- Jon Erik Reinhardsen, Telenor Group
- Guylaine Saucier, Wendel
- Maria van der Hoeven, TotalEnergies

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

- Julie Boland, EY US Chair and Managing Partner, and Americas Managing Partner
- John King, EY Americas Vice Chair—Assurance
- Patrick Niemann, EY Americas Leader, EY Audit Committee Forum

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.