Audit Committee Leadership Summit

August 2022

ACLS VIEWPOINTS

Dialogue with FBI Director Christopher Wray

Large, global companies increasingly face attacks from both criminals and nation-states whose motives reach beyond financial gain and include economic espionage and disruption of physical security. The US Federal Bureau of Investigation (FBI) is a critical partner for companies as they respond to these attacks. Geopolitical tensions and technological developments present new risks in these areas, and corporate directors are interested in how they can most effectively collaborate with the FBI.

On June 29–30, 2022, members of the North American and European Audit Committee Leadership Networks (ACLN and EACLN) met with FBI Director Christopher Wray for a discussion on the overall threat landscape and its impact on global companies. They particularly focused on the heightened risks posed by cybercriminals and China.

Christopher Wray became the eighth director of the FBI in August 2017. His professional career has spanned both the private sector and federal government service, including serving as a partner with the law firm King & Spalding, where he represented Fortune 100 companies, and leading the Criminal Division at the US Department of Justice (DOJ) while also playing a key role in the DOJ's evolving national security mission.

This *ViewPoints* summarizes three key themes that emerged from the discussion:[1]

- **Cyber threats and economic espionage are top concerns for both companies and the FBI**
- **Boards need to stay educated on China**
- **Effective cybersecurity relies upon partnership and information sharing**

For Mr. Wray's full biography, see Appendix 1 (page 7); for a list of network members and other participants, see Appendix 2 (page 8); and for a list of reflection questions, see Appendix 3 (page 9).

Cyber threats and economic espionage are top concerns for both companies and the FBI

The FBI is the principal investigative arm of the DOJ and a member of the US Intelligence Community. Charged with both intelligence and law enforcement responsibilities, its mission includes investigative responsibility for counterterrorism, counterintelligence, and federal criminal matters, as well as cyber threats perpetrated by criminals and nation-states. The FBI has a significant footprint both domestically and internationally, with more than 38,000

employees, 56 field offices across the United States, special agents assigned in over 80 countries, and a budget of $10.8 billion.

The breadth of the FBI's mission and operations provides it with a unique vantage point on the threats facing global companies. Mr. Wray provided an update on the complex threat landscape that requires engagement between the FBI and business community. He highlighted several key points:

- **Cybersecurity, counterintelligence, and counterterrorism are strategic priorities for the FBI—and all three impact the private sector.** Nation-state actors and organized criminals are attacking the private sector on multiple fronts, including infrastructure, data, intellectual property, and innovation. Motives for attacking companies vary. Criminals tend to be financially driven, whereas nation-states often seek to steal proprietary information or to damage critical infrastructure or data. Intelligence sharing and partnerships between the FBI and private sector are essential to effectively respond to these threats, said Mr. Wray. Companies should stay on high alert for cyber threats and economic espionage, especially from China. Counterterrorism should also be on companies' radars because threat actors, he said, now 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 vitality.** China's targeting of innovation, trade secrets, and intellectual property is unprecedented in scale and deserves special attention, said Mr. Wray. He emphasized the significance of the threat: *"No other country poses as broad and comprehensive of a threat to our innovation, intellectual property, and economic security."* He also stressed that the risk stems from the Chinese government, not Chinese people or Chinese Americans. The threat is particularly challenging for companies because of the range of tactics the Chinese government employs. China exploits *"lawful techniques like joint ventures, acquisitions, and other kinds of business partnerships and uses unlawful techniques like hacking, insider threats, and theft,"* he explained. As an example, Mr. Wray described an instance in which the Chinese government required several foreign companies to use a legally mandated tax software system; the software was later discovered to have embedded malware that provided access to the companies' systems and proprietary information. *"The key is to look at the threat holistically,"* he said, referencing in particular the need to think about how near-term decisions impact security over the long-term.
- **Cyber threats are growing in complexity—from blended threats, to disinformation, to insider threats.** Mr. Wray discussed blended threats, in which nation-states, such as Russia and China, turn a blind eye to independent cybercriminals or even work with them. While some analysts expected cyberattacks to intensify this year following Russia's invasion of Ukraine, members reported mixed experiences. Some said their companies have seen a clear decrease; one member's company *"explicitly said that volume is down."* Regardless,

cybersecurity remains a high priority for boards and audit chairs. *"The level of intrusion is ultra-high every day,"* a member said. Mr. Wray pointed out that the Russian conflict *"is far from over, and as things go badly for Russians on the battlefield, the risk of more aggressive cyber activity goes up,"* discussing how adversaries may use access they previously relied on to spy to launch an attack if their risk calculus changes. He also discussed how threats such as disinformation and insider malfeasance can amplify the risk to companies and often accompany more common cyberattacks.

Boards need to stay educated on China

Mr. Wray and members discussed important considerations for audit chairs as they seek to better understand the vulnerabilities and full scope of risks associated with China. Three main concerns emerged:

- **The strategic and operational risks of doing business with China are escalating.** Members reported concerns related to China, including operational and strategic risks from ongoing COVID-19 lockdowns, supply chain challenges, raw material sourcing, and theft of intellectual property, technology, and data. They voiced concerns about geopolitical tensions and the potential for a Chinese move on Taiwan, which could trigger widespread consequences for businesses and the global economy. In a pre-meeting conversation, one member remarked that *"every company should have a living will for China right now … We should be learning from the situation in Russia."* During the meeting, another pointed out that Hong Kong poses new risks. Some companies previously located sensitive functions and data there, due to stronger property rights and legal protection of businesses. However, China's new national security laws are causing foreign businesses to feel less comfortable operating in Hong Kong.[2] *"We used to think of it more like two Chinas, with Hong Kong being separate, but it is more like one China now when it comes to cyber and intellectual property,"* the member said.
- **Companies are reassessing their strategies but may still be underestimating the risk.** Corporate leaders have taken note of the intensifying risk landscape in China, and some are beginning to rethink fundamental strategies. *"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,"* said one member. Another added: *"We continue to invest in our Chinese operations, but very cautiously … and we are moving things like cyber and IT out of China to places like Singapore."* Even so, global business leaders still may not fully appreciate the level of risk. *"Are we too naive?"* a member asked. Mr. Wray replied saying that companies should remain cautious. He added that *"CEOs understand the risk of intellectual property theft and other concerns, but China's tactics are more sophisticated than many CEOs anticipate … Even really sophisticated companies should dig deeper and be more skeptical."*

- **Boards have a particularly important role to play on China risk.** While management may need to focus on shorter-term goals such as quarterly earnings, boards can ensure a *"long term, existential perspective"* vis-à-vis China, Mr. Wray said. Boards should be educated on the risks arising from China and ask for regular geopolitical briefings to understand the challenges specific to their companies and operations.

Effective cybersecurity relies upon partnership and information sharing

Collaboration between the FBI and the private sector is improving, but challenges persist. Continuing to strengthen its partnership with companies is a key priority for the Bureau, and one Mr. Wray hopes will represent a paradigm shift in the way the Bureau and companies think about security over the next ten years.

Mr. Wray offered several recommendations for boards related to cyber risk oversight:

- **Form relationships with the FBI before a crisis occurs.** *"The best time to patch the roof is when the sun is shining—that analogy applies here. It is very hard to get to know each other in the middle of a crisis,"* Mr. Wray said. As part of the Bureau's cybersecurity and counterintelligence strategy, each FBI field office has a private sector coordinator tasked with proactively reaching out to companies in their region and understanding their security issues. Boards should encourage their companies to establish and maintain relationships with the local FBI field office before incidents occur.
- **Engage the FBI as soon as possible during ransomware attacks.** Ransomware has surged in the past year and Mr. Wray emphasized that companies need to engage the FBI early during an attack. Since total prevention is no longer a practical goal, companies should prioritize acting quickly and contacting the Bureau right away. For all cyberattacks, time from discovery is one of the most meaningful metrics in determining how effectively an attack can be mitigated, he noted. If a breach occurs, boards should ask their cybersecurity leaders how long hackers were in the system before being detected. While the Bureau discourages paying ransom, the FBI views and treats an attacked company as the victim and can provide significant assistance to help boards make informed decisions. This may include identifying the attacker, their methods, next steps, and other companies that have been hit. *"We want to be engaged the minute you think there has been a breach,"* Mr. Wray said, emphasizing that quick contact is often a determinative factor in how effective the Bureau and companies can be in mitigating potential damage.
- **Involve the FBI because ransomware attacks may not always be what they seem.** *"There are times when what looks to you like a ransomware attack is in fact a nation-state attack, in which case there may not be a decryption key."* He added that early engagement with the FBI can be viewed favorably by the Department of Treasury *"as a significant mitigating factor"* should a ransom payment violate sanctions. Members also asked Mr. Wray about

the US Securities and Exchange Commission's proposed cybersecurity disclosure rules,[3] which could significantly impact how quickly public companies disclose cyber incidents and potentially create conflicts with intelligence and law enforcement investigations. Mr. Wray stated that the FBI, DOJ, and Securities and Exchange Commission are in dialogue and working to address law enforcement and national security provisions for those proposed rules.

- **Reach out, even if attacks occur outside the United States.** As audit chairs of multinational US and European companies, members were keen to better understand how the FBI should be engaged if attacks occur outside of the United States. As one member noted, *"I'm unclear on when and how to engage the FBI if you are a US-listed company and an attack is outside the FBI's jurisdiction."* Mr. Wray recommended that both US and foreign companies contact the FBI: *"Call us, especially for cyber. Don't worry about trying to figure out 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."* He also emphasized the FBI's ability to quickly engage with partners around the world to help encourage their assistance and added that non-US companies can form relationships with the FBI through agents based in their country, or via US subsidiaries.

Members also shared their views on private sector partnerships with the FBI:

- **Companies have seen improvements in their FBI partnerships and value the Bureau's cyber threat support.** Several members reported that the FBI provided crucial assistance to their companies during cyberattacks and underscored Mr. Wray's guidance that existing relationships were key. One member, remarking on the Russian invasion of Ukraine, said his chief information security officer had *"contact with FBI agents during that time, which was especially helpful."* He added that during a recent cyber incident, *"the FBI was on the phone and on the case within 30 minutes of us contacting them,"* and within twenty-four hours had their full confidence. Several members also shared that their companies have noticed improved collaboration among federal agencies, such as the FBI, National Security Agency, and Cybersecurity and Infrastructure Security Agency; this has led to helpful and proactive guidance for companies.
- **Companies seek more frequent, two-way information sharing.** Several members said that their companies continue to experience information sharing as one-way—flowing mostly to the FBI. A member recounted a recent experience where engagement with the FBI began strong but then dropped off with minimal communication. Mr. Wray acknowledged that this type of engagement is *"unacceptable."* He said the Bureau is committed to improving how it shares information with companies, whether that's disseminating information more broadly or sharing intelligence in different ways, and to ensuring support is provided throughout an incident. One member pointed out that classified information can be particularly challenging. Mr. Wray noted that the Bureau is working on ways to make certain

information available when companies need to be alerted of vulnerabilities, such as providing one-time read-ins for specific individuals.

- **Boards can engage the FBI during crisis response planning.** *"We asked the FBI to participate in our cyber tabletop exercise to ensure that we have the right muscle memory in place. We ran an extensive drill on ransomware and had our local FBI contacts involved in the exercise with us. We found it to be extremely helpful,"* one member shared with the group. Mr. Wray agreed that this is a good practice. By engaging the FBI in practice drills, boards, management, and FBI agents can better understand how to work together and the types of technical information the FBI will need during a crisis, as well as the types of support the Bureau can provide to impacted companies.

About this document

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

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

Appendix 1: Guest biography

Christopher A. Wray became the eighth director of the FBI on August 2, 2017.

Mr. Wray began his law enforcement career in 1997, serving in the Department of Justice as an assistant US attorney for the Northern District of Georgia. In that role, Mr. Wray prosecuted a wide variety of federal criminal cases, including public corruption, gun trafficking, drug offenses, and financial fraud. In 2001, Mr. Wray was named associate deputy attorney general, and then principal associate deputy attorney general, in the Office of the Deputy Attorney General in Washington, DC. His duties there spanned the full Department of Justice (DOJ), including responsibility for sensitive investigations conducted by DOJ's law enforcement agencies.

Mr. Wray was nominated by President George W. Bush in 2003 to be the assistant attorney general for DOJ's Criminal Division, supervising major national and international criminal investigations and prosecutions. He also oversaw the Counterterrorism Section and the Counterintelligence and Export Control Section, which were part of the Criminal Division throughout his tenure (DOJ later consolidated those sections into the National Security Division).

Mr. Wray was a member of the President's Corporate Fraud Task Force, supervised the Enron Task Force, and served as a leader in DOJ's post-9/11 efforts to combat terrorism, espionage, and cybercrime with domestic and foreign government partners. At the conclusion of his tenure, Mr. Wray was awarded the Edmund J. Randolph Award, DOJ's highest award for leadership and public service.

Mr. Wray was born in New York City. He graduated with a bachelor's degree from Yale University in 1989 and earned his law degree from Yale Law School in 1992. He clerked for Judge J. Michael Luttig of the US Court of Appeals for the Fourth Circuit. In 1993, Mr. Wray joined the international law firm of King & Spalding LLP, where he spent a total of almost 17 years practicing law in the area of government investigations and white-collar crime. At the time of his nomination to be FBI director, Mr. Wray was chair of the firm's Special Matters and Government Investigations Practice Group.

Appendix 2: 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

Appendix 3: Reflection questions for audit committees

- ? How comfortable are you that threats like cybersecurity and China are being adequately addressed at your company?
- ? What specific risks related to doing business with China is your board currently discussing? How is your audit committee addressing risk oversight for those areas?
- ? Do you receive regular geopolitical briefings to understand the challenges specific to your company?
- ? What is your company's engagement with the FBI related to cybersecurity?
    - Does your chief information security officer have an established relationship with the FBI field office in your region?
    - Does your company participate in intelligence exchange programs and receive intelligence bulletins from the FBI?
    - How effective are the relationships? What challenges exist, if any?
- ? Has your company engaged the FBI during a cyberattack, such as a ransomware attack? How quickly was the FBI contacted? How beneficial was the FBI's support during the attack?
- ? Has your board engaged the FBI during its cyber crisis response planning, such as during tabletop exercises; or is this something your board would consider for the future?

Endnotes

[1] *ViewPoints* 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] Jen Kirby, "Will China's National Security Law Break Hong Kong as a Business Hub?," *Vox*, August 5, 2021.

[3] US Securities and Exchange Commission, *Fact Sheet: Public Company Cybersecurity; Proposed Rules*, March 9, 2022.