tapestry NETWORKS

ACLN VIEWPOINTS

# Cybersecurity and data privacy: a dialogue with chief information security officers and data privacy leaders

April 2024

**Cybersecurity remains a top priority for large, global companies. The threat landscape grows increasingly complex, with a rise in both the volume and sophistication of threats. Stricter regulation and greater scrutiny from stakeholders overlay this evolving landscape.**

**On March 5, 2024, members of the Audit Committee Leadership Network (ACLN) convened to hear insights from cybersecurity and data privacy executives and to discuss good practices for cyber oversight. Guests included Christine Boucher, deputy general counsel and chief compliance officer at Delta Air Lines; Eric Lataladi, global chief information security officer at MetLife; and Deborah Wheeler, global chief information security officer at Delta Air Lines.**

*For a list of reflection questions for audit committees, see page 10. For the list of participating audit chairs, see Appendix 1 (page 12), and for guest biographies, see Appendix 2 (page 13).*

This *ViewPoints*[1] covers key themes that emerged in the discussion:



EY Building a better working world

# Companies face an increasingly challenging cyber and data privacy risk landscape

The cyber threat landscape continues to rapidly evolve. In 2023, the FBI received a record 880,418 cybercrime complaints from the American public, with potential losses exceeding $12.5 billion.[2] Yet the actual impact is likely much more significant, the FBI explained: "As impressive as these figures appear, we know they are conservative regarding cybercrime in 2023. Consider that when the FBI recently infiltrated [one] ransomware group's infrastructure, we found that only about 20% of [its] victims reported to law enforcement."[3] Threats are clearly intensifying, and as data becomes more valuable, the overlap between cybersecurity and data privacy risks grows.

Guest executives highlighted contemporary risks for global companies:

- **Advancing technologies and tactics.** Cyber adversaries are using advanced technologies, like artificial intelligence (AI), to amplify the sophistication and efficiency of their attacks. Delta, for example, saw a spike in phishing attacks: *"We saw a 900% increase in the number of phishing events coming out of the pandemic versus the years leading into it,"* Ms. Wheeler said. She noted that it is also becoming much harder to see some of the telltale signs of a phishing message: *"With the use of AI in phishing, we're now seeing perfect emails."* More bad actors are also using identity-theft tactics and other intrusion techniques that make it difficult to differentiate between normal activity and a breach—a concerning trend highlighted in CrowdStrike's *2024 Global Threat Report*.[4]
- **Geopolitical tensions.** Active conflicts in Ukraine and Gaza heighten risks on top of existing tensions with China, North Korea, and Iran. One member said, *"The amount of cyber activity emanating from China concerns me most of all. It has always been a big issue and it's just getting bigger."*
- **Cybersecurity regulations.** The regulatory environment, which varies by industry and by country, is increasing in complexity. As examples, guests cited the SEC's new cybersecurity disclosure rules, as well as the European Union's Digital Operational Resilience Act, which aims to strengthen the IT security of the financial services sector in Europe and takes effect in 2025. Chinese regulators have said that "data is more valuable than oil," and the emergence of new cyber and privacy laws and the active regulatory enforcement in China are increasing the exposure and risk to foreign companies operating within China's borders.[5]
- **Supply chain and third-party risks.** Many companies find themselves increasingly reliant on third-party vendors, which bring additional risks. *"The proliferation of third-party vendors is the biggest challenge,"* one member said, especially since the vendors themselves face intensifying cyber threats, but with fewer resources to defend against them compared to their global customers. Ms. Wheeler noted that in the years leading

up to the pandemic, Delta *"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 100 or more vendors/third parties being compromised per year."*

- **Digital transformation, cloud migration, and the Internet of Things (IoT).** Today every aspect of a company's business involves technology. The EY *2023 Global Cybersecurity Leadership Insights Study* found that "too many attack surfaces" was the most cited internal challenge to an organization's cybersecurity approach.[6] Further, 75% of respondents ranked cloud and IoT as the biggest technology risks in the next five years. The study cautioned that attack surfaces for companies "have increased exponentially" as more companies migrate to the cloud and that "these rapid changes have the potential to expose organizations to data loss, breaches, and disruption when organizations onboard cloud and IoT without sufficient design and planning around the cloud interfaces and environment."[7]
- **Data privacy regulations and increased enforcement.** Global companies face heightened data privacy risks due to stricter regulations and a greater focus on enforcement worldwide. When it became effective in 2018, the European Union's General Data Protection Regulation (GDPR) was often cited as a global standard for privacy programs: a company that complied with GDPR was likely to be compliant with other regimes. But the regulatory environment is evolving, in particular in the Asia-Pacific region, where countries are 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—but the landscape has shifted,"* she said. *"In addition, we are also seeing a lot more enforcement by regulators in those regions. In light of this, global companies should be continuously evaluating their privacy program given these emerging regulations and enhanced enforcement posture."*

## For management, rigorous cybersecurity and data privacy risk management is more important than ever

Cybersecurity and data privacy executives need to remain vigilant to adapt to the rapidly evolving threat environment. *"It requires us to think the way that threat actors think. We have to think creatively and push our vendors to be more creative in how they approach solutioning,"* Ms. Wheeler said. Resiliency is the goal, the guests emphasized, noting that a company cannot be completely *"bulletproof."*

They highlighted key areas of focus for audit chairs:

- **Employee awareness and training.** *"It only takes one employee to have a massive data breach,"* Ms. Boucher said. This can be especially challenging for ACLN companies. A member asked, *"Given the diversity of geography and function at our large companies, how do you explain to employees about these issues, where it isn't just a*

*compliance certification that they read through?"* Ms. Wheeler and Ms. Boucher shared examples of how Delta approaches employee training and awareness, noting the constant need for partnership between the cybersecurity and privacy teams:

- **Customized communication strategies.** *"You have to meet employees where they are. The vast majority of our employees don't sit behind a desk,"* Ms. Wheeler said. Delta addresses this by making training accessible on devices such as smartphones, engaging younger employees through internal social media, and incorporating gamification. Ms. Wheeler also noted, *"One of our broader core principles is 'safety first, always,' so we deliver our cyber messaging through the language of safety."*
- **Heightened awareness around phishing and deepfakes.** Members worried about employee resiliency in the face of increasingly sophisticated phishing and deepfakes. They cited the recent incident in Hong Kong where fraudsters used deepfake technology on a Zoom call to represent a fake CFO, who directed an employee to transmit funds worth $25 million.[8] Ms. Wheeler underscored the importance of external validation*: "We talk about 'out-of-band verification.' Don't trust anything sent to you electronically. Pick up the phone and contact the individual on a known number or stop by their office. Have an external way of validating the authenticity of what you're being sent. Use a code word."*
- **Employee ambassadors.** 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. *"They are our eyes, ears, and mouthpieces in the divisions. We make it a point of pride for them to be privacy champions. They are out there messaging to thousands of employees, and they come back to us with questions, which helps enhance our program. And it is not a heavy lift,"* she said.

- **Rigorous third-party risk management.** The guests advised an intense approach to third-party risk management. They recommended minimizing the number of vendors while helping chosen partners strengthen their own security. 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. The guests described how the approach to third-party risk management has evolved in the past few years, sometimes now incorporating preemptive assessments of potential breaches before vendor approval. Additionally, the growing use of AI—which necessitates vast data inputs and often relies on external AI services—presents a risk all companies must navigate and manage.

*"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."*

—Deborah Wheeler, Global Chief Information Security Officer, Delta Air Lines

- **Care in moving systems to the cloud.** As companies migrate from data centers to cloud servers, some may be tempted to *"lift and shift"* entire applications, including legacy software created decades ago, when cybersecurity was not a concern. This approach can miss opportunities to strengthen cybersecurity or even 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 current security standards. Warning that reengineering software was not easy once it was operational in the cloud, she advised, *"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 cloud technology delivers the most value when companies use the full range of cloud services.
- **Revisiting privacy policies.** Privacy regulation is becoming stricter in key jurisdictions, and global companies may need to reassess their policies and approaches to compliance. A changing regulatory landscape may even drive companies to consider where they are doing business. Ms. Boucher highlighted a case where concerns about new regulations caused Delta to escalate a privacy issue to its executive-level Delta Risk Council. *"We asked all of the decision-makers in the room, 'Do we want to continue to operate in these countries? Do we want to provide sensitive information to these foreign regulators about our information security network?'"* She warned that even business-to-business companies, often perceived as less exposed to data privacy risks, must pay attention to these regulations if they have employees, operations, or data-processing activities in certain regions.

## Boards and audit committees seek to enhance their oversight amid intensifying threats and scrutiny

Cyber-risk oversight is a priority for every board. Some delegate cyber risk to their audit committees while others tackle it using different structures, but all directors are keen to strengthen their governance of this rapidly evolving risk.

Audit chairs were particularly interested in the reporting they receive from management through dashboards and other mechanisms. *"How do we really know whether the dashboards and the assurance being provided are effective?"* a director asked. *"How do we know that the picture being portrayed is accurate? Are we asking the right kinds of questions?"* Another underscored the challenge: *"You can go through all of the cyber reporting, but there is always a real question of how can the audit committee truly get comfortable that the risk has been mitigated."*

Members had varied views on the effectiveness of current reporting. One cautioned that cybersecurity reports can be overly detailed and emphasized the need for a high-level interpretation that shows the importance of events in the reporting stream and highlights the most significant ones. Another felt the need for more structured reporting: *"As an audit committee, we have pretty solid structures in place in terms of what gets reviewed from an*

*accounting and finance perspective, but we don't really have that framework for cybersecurity. I think sometimes the cybersecurity review can be a little random and focus just on what the CISO [chief information security officer] wants to share that quarter."* To address this, the member incorporated a new format for cybersecurity reports: *"Each report will have three primary parts, starting with what's new in the cybersecurity environment; then, a scorecard presentation on the key metrics and project progress; and third, a deep dive into a particular area that the audit committee has requested to hear about."*

Guests shared their perspectives on reporting and highlighted several good practices for audit committees that oversee cyber risk:

- **Talk to the CISO about the audit committee's reporting goals.** The guests emphasized that every board is different and will require different styles of reporting. Ms. Wheeler encouraged audit chairs to have an open dialogue with their CISOs about reporting: *"Have those discussions. This is a topic that CISOs talk about relentlessly. We want to know what questions audit committees and directors have. We are always wondering how to give them the feeling of assurance that we've got everything under control or, in some cases, that we don't."*
- **Ensure that metrics have purpose and answer the audit committee's key questions.** Many companies have thousands of metrics that could potentially be reported. The guests advised being intentional about which metrics are reported to the audit committee or board. The selected metrics should make directors comfortable in their understanding of the cybersecurity status but not overwhelm them. 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 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."*
- **Ask about mitigation time.** Audit chairs should inquire about the organization's ability to promptly address critical vulnerabilities, often by installing patches in software around the world. Ms. Wheeler said, *"If you don't know how quickly your cybersecurity teams can do that, you need to ask. If your CISO says that critical and zero-day patches cannot be made within three days or better, that is a problem."* A member agreed; after another large, global company experienced a ransomware attack, her board asked how long it would take to recover if its company experienced a similar attack. *"The first answer was, 'We don't know.' The second time around, the answer was, 'It would take a matter of months.' It has been interesting how continuing to work on that question has driven quite a different approach to thinking about recovery and bringing everything back up again."*

- **Understand the company's technology footprint and the state of its asset inventory.** A company's technology assets are often spread around the world and can number millions of computers, so a comprehensive grasp on the state of the technology is crucial. Ms. Wheeler advised members to ask, *"What is the technology footprint and state of the asset inventory? How do you know that you are protecting everything you need to protect? What percentage of the technology is end-of-life or can no longer be supported by the vendors you're doing business with? What are the plans to address that?"* An audit chair underscored this point*: "I was comforted when some of the most important metrics from our CISO were not 'how to protect' but a clear view of the company's assets. Our scorecards start with an update on our asset inventory. The reporting is robust and real time."* Despite challenges like shadow IT—where employees use unauthorized applications—Ms. Wheeler said that a competent CISO should know the footprint and the proportion of technology nearing end-of-life.

## 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?

In addition to reporting, the discussion highlighted three areas where boards will need continuing focus:

- **Increased regulatory and public scrutiny of cybersecurity.** The guests explained several considerations for audit committees in the current regulatory landscape:
  - **Evaluate existing cybersecurity processes to ensure alignment with the SEC's recent disclosure rules.**[9] The rules require reporting a material cyber breach within four business days. Large, global companies likely have processes in place for assessing materiality and will not need to *"reinvent the wheel,"* but companies should consider if any updates are needed. Ms. Boucher noted that Delta held a tabletop exercise to help pinpoint potential gaps in compliance that might exist under the new requirements.
  - **Ensure visibility into all cyber incidents across the company.** A key challenge is ensuring cybersecurity and privacy teams have clear visibility into all of the company's incidents. The group discussed how cyber incidents do not always manifest clearly and can occur in different functions and locations around the globe.
  - **Review disclosures relating to the board's oversight role in cyber-risk oversight.** The SEC's new rules mandate disclosures related to the board's oversight of risks from cybersecurity threats. This includes how often and in what

manner the board discusses cyber risks, its involvement in setting cybersecurity policies, and how its oversight fits within the broader risk management strategy. While initial proposals sought extensive disclosures on board members' backgrounds and committee compositions, the final rules made such disclosures optional. Nevertheless, investor expectations often lean toward transparency regarding the board's cybersecurity expertise and capabilities.[10]

- **Readiness for quick, decisive incident response.** Boards must be prepared to act quickly during a cyber or privacy incident. *"It's not a matter of if these things happen; it is when they happen and how we respond to them that is key,"* one audit chair said. Members and guests identified several good practices:
  - **Ensure that a strong crisis-management team is in place.** As the threat landscape becomes more and more complex, boards should ensure their company can swiftly mobilize the appropriate leadership and expertise to respond effectively to crises. Today, that often means cybersecurity, privacy, legal, communications, and other leaders are working closely together, the guests said.
  - **Document processes.** One member noted, *"We've documented the escalation paths and criteria for different issues—for example, when the CISO needs to call the audit chair versus when the full audit committee or full board needs to be involved."* Such documentation is more important than ever under the new SEC rules.
  - **Regularly conduct tabletop exercises that include the board.** Tabletop exercises can be hugely revealing in terms of how *"complicated and sensitive"* cybersecurity crises can be, a member said. Yet while many companies run simulations for management, board members are not always included despite the clear benefits: they help directors understand critical questions to ask during a cyber incident, which may include considerations related to materiality determination(s) and whether to pay a ransom.

## Safe and effective communication channels

One member questioned whether non-executive directors should use dedicated corporate tablets and phones for communication. The experiences of members varied: some receive corporate tablets and exclusively use corporate emails; others use corporate emails on personal devices; a few use personal emails for nonsensitive matters. One reported a strict approach: *"We go to the extreme of using a company iPad that the company controls, so if anything happens to it, they shut it down. When we have physical meetings, they are in a faraday cage."* Whether using corporate-issued or personal devices, secure communication is achievable, but the setup details matter and user experience must be factored in. Directors may want to consider investigating further with their own boards. A recent *Wall Street Journal* article highlighted research that indicated board members themselves may "become the weak link in an organization's cyber defenses." The authors found that directors have unique vulnerabilities and may not be adequately prepared for potential attacks targeting them directly.

- **Learn from cyber incidents at other organizations.** Audit committees can get valuable information about their companies' own cybersecurity measures by asking, *"Could this happen to us?"* when learning of cyberattacks experienced by others. A member explained, *"One of the most interesting things we do as a committee is to take outside, external incidents and look at how our controls would stand up if a similar attack happened to us."* This promotes a proactive approach to cybersecurity and fosters innovative thinking about what a company's potential vulnerabilities may be.

*"One of the most interesting things we do as a committee is to take outside, external incidents and look at how our controls would stand up if a similar attack happened to us."*

—Audit chair

- **Established relationships with the FBI.** The FBI plays many roles in cybersecurity: finding and arresting bad actors, proactively identifying threats, and helping companies respond in the face of an attack, particularly where other law enforcement and regulatory agencies are involved. Several members underscored the necessity of proactively establishing relationships with the FBI—before a crisis occurs—as a crucial component of cyber readiness. In June 2022, ACLN members met with FBI Director Christopher Wray, who emphasized the FBI's commitment to assisting companies with cybersecurity and outlined how the FBI can help during cyber incidents. A detailed summary of that discussion can be found here: *ViewPoints: Dialogue with FBI Director Christopher Wray*.

Reflecting on the discussions, the intensifying threat landscape, and the growing need for robust defenses, one member noted how crucial it is for audit chairs to support cybersecurity and data privacy leaders. He encouraged his peers, *"We have to be cheerleaders. Sometimes there are internal battles about the resources that cybersecurity and privacy teams need. We need to be very in tune to that and lend a hand if needed."*

## Reflection questions for audit committees

- What are your company's top cybersecurity priorities for the next one to two years? How has this changed from previous years?
- What privacy issues have been the most challenging for your company? How are you addressing new data privacy concerns from technologies like generative AI?
- How are the cybersecurity and data privacy functions structured at your company? How do they interact and collaborate? How can the board and audit committee better support cybersecurity and data privacy executives within the company?
- As a board member, what type of cybersecurity and data privacy dashboards and reports have you found most helpful? Has the board and/or audit committee shared its feedback with management on ways that board reporting on cybersecurity-related matters can be enhanced?
- Have you asked your company's cybersecurity leaders critical questions about the company's technology footprint, such as:
  - How quickly can the organization patch critical or zero-day vulnerabilities?
  - What is the technology footprint and state of the asset inventory? How do you know that you are protecting everything you need to protect?
  - 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?
- How comfortable are you that your company has the proper processes in place to comply with the SEC's new cybersecurity disclosure rules, including how to determine the materiality of a cyber incident? Are you comfortable with the roles the audit committee and board play in those processes?

## About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is 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: Participants

The following ACLN 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 ACLN 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

## Appendix 2: Guest biographies

**Christine Boucher is Deputy General Counsel and Chief Compliance Officer at Delta Air Lines, Inc.** In this role, Ms. Boucher oversees Delta's ethics and compliance, environmental, privacy, international compliance, commercial transactions, intellectual property, and enterprise records and information management programs. Ms. Boucher focuses on ensuring Delta operates in compliance with the Federal Sentencing Guidelines for Organizations and applicable international regulations while promoting Delta's strong ethical culture. During the height of the pandemic when the federal government granted relief to US airlines, she led a cross-divisional group responsible for implementing a program to comply with the CARES Act restrictions and reporting requirements. She and her team also implemented strong privacy controls to address the increased volume of protected health information required to be handled by airlines during the pandemic.

**Eric Latalladi is the Global Chief Information Security Officer for MetLife.** He leads the teams responsible for evolving and executing MetLife's strategy to protect the company and its employees and customers. In this role, he oversees and implements MetLife's cybersecurity program and policies, information security strategy and governance, security technology, threat management, identity and access control, incident response, and security awareness. He also leads physical security services and manages the MetLife Security Operations Center.

Mr. Latalladi is an accomplished executive with more than 20 years of professional IT experience in financial services. Prior to assuming his current position, he served as MetLife's Global Chief Technology Officer. Mr. Latalladi joined MetLife in 2012 from Royal Bank of Canada (RBC) where he was Global Head of Telecommunications Engineering. He also served as Chief Technology Officer, Chief Information Security Officer, and Chief Information Officer with J.B. Hanauer & Co. He currently serves on Advisory Boards for several large technology companies, including AT&T, Cisco, Dell, Tanium, and zScaler.

**Deborah Wheeler is the Global Chief Information Security Officer at Delta Air Lines, Inc.** Ms. Wheeler is a passionate information technology executive whose career focus has been on the protection and privacy of information and information assets, as well as on technology innovation, education, and awareness. In her current role, she brings more than 25 years of cybersecurity expertise, information technology risk management, and data privacy experiences to the aviation sector. She is a Board Director for the Aviation Information Sharing and Analysis Center and the Vice-Chair of A4A's Cyber Security Council.

Ms. Wheeler has built security programs for PNC Bank, Fifth Third Bank, JPMorgan-Chase, Ally Financial, and Freddie Mac in addition to her work at Delta. She serves on the Customer Advisory Boards for Proofpoint, Sailpoint, Crowdstrike, and ForcePoint Software companies. She was inducted into the 2022 CISO Hall of Fame, and she has been recognized on the 2021 and 2022 Top 100 CISOs list by CISOs Connect, the 2020 Cyber Defense CISO 100 list, and was also recognized as the 2007 ISE CISO People's Choice Award winner for CISO of the year.

# 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. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] Internet Crime Complaint Center, *Internet Crime Report 2023* (Washington, DC: Federal Bureau of Investigation, 2023), 3.

[3] Internet Crime Complaint Center, *Internet Crime Report 2023*, 3.

[4] CrowdStrike, *2024 Global Threat Report* (Austin, TX: CrowdStrike, Inc., 2024), 10–14.

[5] For more information, see "*Cybersecurity Laws and Regulations China 2024,"* International Comparative Legal Guides, November 14, 2023, and US National Counterintelligence and Security Center, *Safeguarding Our Future* (National Counterintelligence and Security Center, June 20, 2023).

[6] Richard Bergman, "Is Your Greatest Risk the Complexity of Your Cyber Strategy?" EY, October 1, 2023.

[7] Bergman, "Is Your Greatest Risk the Complexity of Your Cyber Strategy?"

[8] Heather Chen and Kathleen Magramo, "Finance Worker Pays Out $25 Million after Video Call with Deepfake 'Chief Financial Officer'," *CNN*, February 4, 2024.

[9] US Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* 17 C.F.R. 229, 232, 239, 240, and 249 (2023).

[10] "SEC Adopts Comprehensive Cybersecurity Disclosure Requirements," Cooley LLP, August 2, 2023.