tapestry NETWORKS

VIEWPOINTS

Cyberattack simulation: lessons from leading European and US audit committee chairs

February 2024

The integration of technology in virtually all aspects of business operations means that cybersecurity has become a business-wide risk management issue. Boards strive to keep updated on the cybersecurity landscape and to ensure company resilience in the event of an attack.

On July 13 and November 10, 2023, members of the European Audit Committee Leadership Network (EACLN) and Audit Committee Leadership Network (ACLN) met in London and Washington, DC, respectively, to participate in cyberattack simulations.

For a list of participating audit chairs, please see Appendix 1 (pages 14–15). For a list of questions that the board can ask the executive team, see Appendix 2 (page 16).

This *ViewPoints*[1] highlights the lessons learned and key takeaways from the cyberattack simulations:

EY Building a better working world

The cyber simulation

The cyber simulation was run in coordination with EY and Microsoft. Audit chairs participated in a simulated emergency board meeting of "XtraEnergy," a large company specializing in renewable energy solutions—and the target of a cyberattack. Audit chairs played the role of XtraEnergy board members, and leaders from EY and Microsoft played the roles of chief executive officer, chief information security officer, general counsel, and external auditor.

Resilience to a cyberattack is key

The unprecedented pace of technology development makes it increasingly challenging to keep abreast of emerging threats. Technology is now involved in every aspect of a company's business. The consequences of cyberattacks therefore go far beyond financial loss and include other impacts such as operational disruption, information data and intellectual property theft, legal and regulatory implications (such as penalties), and reputational damage.

Resilience against a cyberattack is thus more important than ever. Boards must actively oversee attack resistance as well as resilience after an incident. The simulation demonstrated the essential role for boards in a cyber incident and highlighted the importance of effective communication with the management team. Good practices identified during the simulation include:

- **Continuous education.** It is essential that board members are armed with the right questions to be able to understand and critically assess the decisions being made by leadership—and feel confident doing so. Cybersecurity education, including keeping up to date with emerging cyber risks and evolving regulatory developments, is critical. One member explained, *"You sometimes think you're feeling comfortable, but you shouldn't feel comfortable with today's knowledge for tomorrow. You have to continuously update your knowledge."*
- **Focusing on resilience, not just prevention and detection.** A company's cyber-defense and -detection systems should ward off threat actors and keep IT systems safe. But as one audit chair explained, this is wishful thinking: *"Some organizations think they can completely control the cyber environment they're in, but I think that's naïve. Something's going to happen; what do you do about it when it does?"* One member described how, after creating a strong foundation in cyberattack

"What are the right questions to ask, and when? How do you manage the fear?"

prevention, the company shifted its focus to robust response to an incident: *"We've invested in a lot of detection. Our view is while we can try and build the strongest wall around us—and we'll want to know when they've got through and isolate them—the work we've been doing recently on how to respond to an event rather than prevent it has been a breakthrough."*

- **Participating in tabletop exercises.** Management teams typically participate in cybersecurity tabletop exercises to run through crisis scenarios. Some companies regularly involve the board in these exercises; others involve only specific board members, such as the audit chair; and others do not involve the board. Board involvement can help directors understand the quality and rigor of the tabletop exercises, the critical questions to ask during a crisis, and governance issues that can arise during an attack.

Establish a detailed crisis plan and update it regularly

Comprehensive, multiscenario crisis plans are important but not sufficient on their own. The plans must be regularly drilled, reviewed, and revised. Audit chairs discussed how a well-established crisis plan can enable companies to do the following:

"Having a plan is the starting point. Drilling robust scenarios won't prepare you for everything but gives you some muscle memory."

- **Act swiftly.** A robust crisis plan provides a predefined set of procedures and responsibilities. Ensuring that all team members know their roles and responsibilities during a cyberattack reduces confusion and delays in decision-making, enabling management and the board to respond quickly and efficiently. As 75% of organizations take an average of six months or longer to detect and respond to a cyber incident,[2] boards should encourage management to create and regularly review a strategic crisis plan so it is ready in the event of an attack. One member said, *"It's about how seriously cybersecurity risk is taken by the company, how the organization is set up, and how they can ensure that all necessary measures are taken to prevent cyberattacks. But if something happens, how fast will the response be? How fast can the company react so the attack doesn't go into the operating systems?"*

- **Ensure clear and timely communication.** In the throes of a cyberattack, communication is vital. Having a plan that establishes key contacts, predefined channels for information flow, and specific protocols

helps to ensure that critical information is swiftly and accurately conveyed—and to the right people. This should also include when management informs the board. One audit chair knows exactly when he will be contacted in a cyberattack: *"I've invested for years in cybersecurity, so I know a lot to be dangerous and have dedicated a lot of time to it and will continue. We war-game. As audit chair, I'm phone call number three."*

- **Make decisions that are deliberate, not impulsive.** The best decisions are seldom made in highly stressful, time-sensitive situations. A robust strategic response plan provides management and the board with a structured framework that includes protocols, scenarios, and risks, guiding them away from impulsive reactions and toward calculated, strategic decisions.
- **Rapidly assess going-concern issues.** A top concern for audit chairs is to understand the organization's operational viability, or "going-concern" status, as quickly as possible. By mapping potential impacts and recovery paths, a crisis plan equips management and the board with essential insights to evaluate the organization's ability to continue operations during a cyber crisis.
- **Better support leaders.** Cyberattacks generate significant mental stress. A crisis plan with clear roles and procedures reduces cognitive overload, helping leadership to focus on specific tasks rather than the overwhelming entirety of the crisis. It can also offer a sense of control and direction, providing reassurance that the crisis is manageable.

  Even with a plan, boards should be prepared to support leaders who may "crack under pressure." But crises can also reveal emerging leaders: one member noted that his company's current CEO was selected because of the way she had stepped up during the COVID-19 pandemic.

EY: Response strategies can help in the ambiguous, confusing environment of an attack

Even though most boards expect management to have a plan for responding to an attack, many events occur without a strategic crisis plan in place that extends to the board. When that happens, the executive team often falls back on technical and operational plans, putting strategic goals at risk.

- *It is worthwhile asking to what extent the organization has a response strategy, rather than a tactical series of activities, including how executives will work with the board in a crisis.*

Cyber crises also present tremendous challenges related to ambiguity. At the time of impact, there will be many unknowns, with a timeline for resolving them often expanding to days and weeks. These unknowns can amplify any executive disagreement around consequence management and can lead to apparent disharmony in decision-making.

- *Ambiguity is ever present in cyber-crisis events. Consistent exercising and scenario discussions can help articulate decision-making processes to overcome knee-jerk responses that conflict with corporate values.*
- *Regulators are strongly encouraging businesses to include the board in these exercises and scenario discussions.*

Microsoft: Employ strategies to manage incident-response team stress and fatigue

Poor leadership can quickly escalate a crisis into a catastrophe, and one of the most overlooked leadership strategies is that of managing incident-responder stress and fatigue, especially during an acute crisis. Stress symptoms for individuals can include irritability, anger, hostility, blaming, reduced ability to support teammates, and conflicts with peers. Coupled with fatigue, cognition can change and create an inability to recognize poor judgment. Equally, studies show that the physiological impact of tiredness is very similar to the impact of alcohol, paving the way for cognitive lapses in how the responder perceives and reacts to the world around them.

- *In times of acute crisis, plan for 50% of your staff operating at 50% of mental capacity; rotate response-team members early and often; and call in external reinforcements if internal resources are struggling.*

A communications plan is essential

Communication is a top priority during a cyberattack, and including a detailed internal and external communication plan is a vital component of crisis readiness. There needs to be consistent and timely communication about the cybersecurity breach so that all key stakeholders, within and outside of the company, understand how the incident is being handled. Several important elements of a communication plan were highlighted during the simulation:

- **Determine in advance who owns key stakeholder relationships.** Key stakeholders—such as investors, regulators, governments, law enforcement, staff, and customers—need to be informed during a cyber incident. Doing so quickly can deepen trust. One director highlighted key questions: *"What are we going to say externally? Have we met our internal and external reporting duties on this?"* Preassigning ownership of stakeholder contact channels within the board and management helps to speed up this process.
- **Create a backup plan in case of issues with the communication infrastructure.** Cyberattacks can interfere with crucial communication systems—for example, shutting them down or jeopardizing their security. A crisis plan that identifies emergency protocols (e.g., using satellite phones when voice-over-IP phones are disabled) can preserve continuity.

> *"If you can connect with each other, you can figure it out. And if you can't communicate, you are dead in the water."*

EY: Cyber-crisis communication is a unique challenge; planning is essential

Communications strategies are crucial to not just having a "good response" but also conveying the company's response to the incident to relevant stakeholders to maintain trust. While plans may exist to enable an operational and tactical response, often broader stakeholder engagement is left until the time of need, and it is then developed without sufficient time and forethought.

- *Preplanning a response should include precrisis engagement mapping, nodal or key-person analysis, and clear relationship owners for a cyber-crisis response, including for the communications that are required.*
- *Each organization will have a communications function; ideally, the communications plan for a cyber incident will also be linked to how the board's communications are developed for investor and regulatory purposes.*
- *Executive and board members will likely have been through media training, but crisis communications is different and uniquely challenging. When the issues presented involve cybersecurity, there is often additional pressure to present technical knowledge. Stakeholder engagement and communications will need to include a broader skill set than the usual.*

A strategic and proactive approach to crisis communication can transform a cyberattack response into an opportunity to strengthen key stakeholder trust and engagement. Additionally, collaborating with key partners to resolve cyber incidents can lead to faster and more effective solutions, benefitting entire supply chains and business ecosystems.

Microsoft: Keep the customer as your North Star

Organizations are often operating "in the fog of war" during serious cyber incidents and may not have a clear picture of what has happened or how bad it really is for weeks after an incident is detected. Regardless, the organization is expected to communicate clearly and transparently right from the start with internal and external stakeholders, such as employees, customers, regulators, law enforcement, and the media. It is critical to have the communication plan, the nominated spokesperson, and the roles and responsibilities planned out before an incident.

- *Think about what you are going to say, to whom, and the tone you will adopt, but above all keep your customers (internal and external) as your North Star. This is especially true of critical services that may have life and safety impact.*

Determine priorities in the event of a cyberattack

Time is a critical but scarce resource during a cyber incident. The simulation highlighted the importance of knowing beforehand what areas need to be prioritized in the event of an attack in order to save time. Several priorities emerged:

- **Getting the right information to the right people.** A predefined process for collecting and disseminating information regarding the attack is foundational. Clear reporting lines and a process that sets out who will be responsible for collecting and reporting the necessary information so that decisions can be made without delay will help establish what needs to be dealt with quickly.
- **Bringing in critical external help.** Responding to a cyberattack often relies on bringing in specialized skills. Identifying ahead of time who might be needed during a cyberattack—including external IT specialists, auditors, legal counsel, law enforcement, and regulators—will help with quicker access to these resources, reducing response time and further potential damage. Establishing open lines of communication with them beforehand, or even involving them in the planning, is even more helpful. One member noted, *"No matter what the expertise of one or two members, we will rely heavily on regular outside evaluations of our cybersecurity program."*
- **Understanding the company's legal obligations so that they are complied with early and transparently.** Understanding legal and regulatory obligations in the event of a cybersecurity attack, as well as contracts in place, will help determine required actions and will help reduce further complications later.
- **Engaging with law enforcement.** Government organizations often play a critical role in a company's defense and recovery. Law-enforcement agencies, such as the US Federal Bureau of Investigation (FBI), have significant experience and expertise in dealing with cyber breaches. A member had recently attended an event in which FBI Director Chris Wray laid out numerous reasons for engaging law enforcement early in any cyberattack, pointing to

EY: Engage with the external auditor

Each audit firm has procedures in place to provide support during a cyber event; these are clearly but not exclusively focused on the security and assurance of the financial systems. However, there is value in exploring, before any impact, how that support would play out and the processes needed to ensure effective support from the external auditor.

- *The external auditor can also provide insights and knowledge obtained when performing audit procedures or about potential dysfunction that may impede the leadership in its response.*

the bureau's experience with cyber aggressors and its interest in shutting down their criminal networks.

- **Adapting the recovery plan as needed to quickly get back up and running.** It is essential that the company's operations are resumed as quickly as possible. The cyberattack recovery plan, which should be established before a cyber incident, provides a useful road map for recovering from cyberattacks, but its effectiveness lies in its ability to be adapted based on the specifics of the threat. Each cyberattack is unique, and assessing the recovery plan early and amending it as needed will help to restore business operations as quickly as possible.

Understand the complexities of ransomware

Ransomware attacks involve malicious software designed to block access to specific data or even an entire computer system until a sum of money is paid. These attacks can cause significant disruptions to business operations. Deciding whether to make the payment can be complex, difficult, and contentious. Several considerations emerged during the simulation:

- **It is essential to understand the difficult trade-offs in paying a ransom.** Deciding whether to pay is complex and often requires highly specialized counsel. Audit chairs identified many difficult issues:
  - **Legal.** The legal implications of paying a ransom vary by jurisdiction, and most large companies are subject to multiple legal regimes. Making payments can contravene laws related to funding criminal or terrorist activities.
  - **Ethical.** Threat actors are often anonymous, and identifying them is a slow process—if they can be identified at all. Paying an unknown entity can mean funding further illegal activities and potentially tying the company to an organized-crime or terrorist group. Some audit chairs also noted that succumbing to ransom

Microsoft: Minimize the financial and operational impact of ransomware attacks by protecting backup and restoration capabilities

Attackers focus on crippling an organization's ability to respond without paying, so they will intentionally target backup and restoration documentation and capabilities.

- *Make sure critical systems are backed up and backups are protected against deliberate attacker erasure or encryption. Run regular recovery exercises to ensure the validity of the backup strategy. Consider the use of cloud capability to restore data quickly to minimize downtime and data loss*.
- *It is essential to protect the identities that have access to backups.*
- *Keep an offline copy of the most critical data and consider the same for recovery and incident response documentation.*

demands could set a harmful precedent, potentially affecting not just the company but others in the industry and beyond.

- **Practical.** The logistics of making a secure, untraceable payment can be complex and may inadvertently expose the company to further vulnerabilities. Even if a payment is safely delivered, there is no guarantee that it will lead to data recovery or prevent further attacks.

- **Companies should clarify and understand ransomware policies, including cybersecurity insurance.** Crisis plans should include ransomware protocols so that management and the board know who has the authority to authorize payment. Regular review of these policies and procedures will lead to greater confidence in the decision-making process in the time of a crisis. Boards should also consider the extent and limitations of the company's cyber-insurance coverage.

"Even if we do pay, is the key that we're going to get going to work? And even if we have the key, is that going to give us a solution quicker and get us back to our backups?"

EY: Monitor the legislative and regulatory landscape in ransomware

Ransomware has been a lucrative activity for threat actors of all sizes for many years. The scale of ransomware and malware activity, the technical competence of threat-actor groups, and the proliferation of affiliate networks is further accelerating the magnitude and impact.

As a result, regulators, investigators, and nation-states have been working on how to counter the threat and reduce or prevent threat groups from financially benefiting from their activities. In various jurisdictions, this is resulting in increased legislative, regulatory, and investigative powers aimed at stifling the income of the ransomware marketplace.

- *Across every jurisdiction, there is an evolving landscape of legal requirements around ransomware that is likely to be changing rapidly in the next few years. High-impact events, such as the ransomware attacks on the Colonial Pipeline in the USA and the Health Service in Ireland, have focused efforts to protect critical infrastructure and directly address the threat groups through their income generation. As a result, we would expect organizations to monitor the legislative and regulatory environment and urgently reflect any impending changes within their own preparedness and response plans.*

Payment by insurers, and cyber insurance coverage more generally, has been a developing issue in recent years. Some insurers have required greater preventative investment before providing coverage or, by proving negligence in prevention, they have refused payout. Identification of a threat actor's affiliation with a nation-state has also been used to negate coverage under act-of-war clauses.

- *It would be advisable to gain clarity about the nature of each organization's cyber-insurance coverage, including how comprehensively it covers the business, and its limitations.*

Dealing with the 2023 SEC cybersecurity rules

On November 10, 2023, audit chairs discussed the US Securities and Exchange Commission (SEC) cybersecurity rules with Elad Roisman, former commissioner and acting chair of the SEC, and Michael Arnold; both are partners at Cravath, Swaine & Moore LLP.

Boards should ensure that policies and procedures are designed with the new rules in mind and *"get the disclosures right,"* Mr. Roisman advised. This includes boards of European companies classified as foreign private issuers (FPIs). An EY newsletter notes, "The rules apply to nearly all registrants that are required to file periodic reports with the SEC, including smaller reporting companies (SRCs) and [FPIs], except for Canadian FPIs under the multijurisdictional disclosure system."[3]

Aligning policies and procedures with the new rules will aid companies in the event of cyber incidents and help if there is a future SEC enforcement investigation. Mr. Roisman encouraged boards to participate in cybersecurity tabletops or practice exercises to help detect any gaps in their companies' processes. Some members said that their boards have undertaken such simulations, while others have not. One described takeaways from a recent simulation: *"It is important to have a business-impact assessment at a detailed level to help with materiality determination. The messaging needs to be controlled because it is always leaked by vendors or employees anyway. And regardless of the four-day rule, it's important to have solid policies and procedures in place that can be followed to help navigate through the incident."*

Mr. Arnold identified challenges around the cyber rules:

- **Requesting notification delay in the event of public-safety or national-security risks.** The current rule provides a 30-day extension if disclosure would create a substantial risk to national security or public safety, but this requires the approval of the US attorney general.[4] SEC Commissioner Hester Pierce, in a dissent from the final rule, noted that "obtaining approval within four days will be quite a feat."[5] Mr. Roisman noted that additional guidance for companies would be helpful: *"We're hoping the SEC will provide more clarity on how to obtain the 30-day extension."* One month later, on December 12, the FBI and Department of Justice issued guidelines that provided additional detail on the process for public companies to request such a delay, emphasizing the need for immediate contact with the FBI upon discovery.[6]
- **Making the materiality determination.** *"It is important to clarify who makes the materiality determination, how they obtain any relevant information about the cyber incident, and how and when they come together,"* Mr. Arnold advised. He also emphasized the importance of understanding in advance the factors that will be used to guide the materiality determination, noting that the facts and circumstances of the incident will drive those factors that are used.

- **Assessing incidents at third-party service providers.** Mr. Arnold emphasized the importance of understanding when a cyber event at a third-party service provider could be material and require disclosure. He encouraged consideration of current agreements with the third party and relevant clauses that would help the company obtain the information needed from the third party to make the required disclosures.
- **Issuing a Form 8-K to minimize risks.** Members questioned whether, out of an abundance of caution, it is prudent to issue a Form 8-K even while a company is still determining whether a cyber incident is material or not. Members voiced concerns that this could set a precedent they would later regret. Mr. Roisman acknowledged the concerns, but predicted that many companies may err on the side of caution and opt to file 8-Ks concerning cyber incidents. He highlighted the high-level nature of the information required for the disclosures, explaining that the information required to be disclosed would often be publicly accessible elsewhere. But he cautioned members that *"over time, the content and accuracy of the disclosure would become more important to help investors understand the impact in light of many Form 8-K disclosures."*

EY: Implementation and integration of a whole-chain response is key

New legislative and regulatory requirements need to be integrated into existing business processes. It is important to assess how well-prepared your business is.

A key outcome of these regulatory changes is the formalized notification timeline for the company's response, replacing the previous approach based on best efforts or guidelines set by insurers and data regulators. Organizations need to understand this timeline, including the potential for a "substantial risk" extension, if they are to plan effectively.

To meet the new timelines, companies need detailed plans, so that everyone in the response chain can be aligned on data, awareness, and decision-making. This is even more crucial in highly regulated sectors that already have strict reporting requirements and timelines.

How EY can help

EY Cyber Resilience, Crisis, & Incident Response Services support business leaders by helping them to identify and monitor potential threats, developing and testing crisis plans and teams, and responding with speed and integrity when an incident occurs. Preparedness is the key to cyber resilience, but we help clients at all points in their cyber security lifecycle.

To find out more contact Dr. Paul Robertson (paul.robertson@uk.ey.com), Dave Burg for USA (dave.burg@ey.com), and Richard Watson for APAC (richard.watson@au.ey.com).

How Microsoft can help

Microsoft has a comprehensive portfolio of security products and services that can help organizations protect, detect, and respond to cyberthreats across multi-cloud and hybrid environments.

To find out more, please contact your local chief security advisor. Regional contacts are: Lesley Kipling (leskip@microsoft.com) for EMEA, Jim Eckart (james.eckhart@microsoft.com) for USA, and Abbas Kudrati (abbas.kudrati@microsoft.com) for Asia.

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: Participants

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

Fernando Aguirre, Audit Committee Chair, CVS Health
Joan Amble, Booz Allen Hamilton
Jeff Campbell, Audit Committee Chair, Aon
Ted Craver, Audit Committee Chair, Wells Fargo
Bill Easter, Audit Committee Chair, Delta Air Lines
Lynn Elsenhans, Audit Committee Chair, Saudi Aramco
Tom Freyman, Audit Committee Chair, AbbVie
Bella Goren, Audit Committee Chair, General Electric and Marriott International
Gretchen Haggerty, Audit Committee Chair, Johnson Controls
David Herzog, Audit Committee Chair, MetLife
Suzanne Nora Johnson, Audit Committee Chair, Pfizer
Akhil Johri, Audit Committee Chair, Boeing and Cardinal Health
Paula Price, Audit Committee Chair, Accenture and Warner Bros. Discovery
Tom Schoewe, Audit Committee Chair, General Motors and Northrop Grumman
Leslie Seidman, Audit Committee Member, Moody's, Audit Committee Chair, Janus Henderson
Cindy Taylor, Audit Committee Chair, AT&T
John Veihmeyer, Audit Committee Chair, Ford

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

Jeremy Anderson, Audit Committee Chair, UBS
Werner Brandt, Audit Committee Chair, Siemens
Ana de Pro Gonzalo, Audit Committee Chair, STMicroelectronics
Liz Doherty, Audit Committee Chair, Novartis and Phillips
Renato Fassbind, Audit Committee Chair, Nestlé
Byron Grote, Audit Committee Chair, AkzoNobel and Tesco
Margarete Haase, Audit Committee Chair, ING
Liz Hewitt, Audit Committee Chair, Glencore
Dagmar Kollmann, Audit Committee Chair, Deutsche Telekom
Pilar López, Audit Committee Chair, Inditex
Benoît Maes, Audit Committee Chair, Bouygues
Maria van der Hoeven, Audit Committee Chair, TotalEnergies

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

Julie Boland, US Chair and Managing Partner and Americas Area Managing Partner, EY
Dante D'Egidio, Americas Vice Chair – Assurance, EY
Marie-Laure Delarue, Global Vice Chair, Assurance, EY
John King, Americas Vice Chair – Assurance, EY
Pat Niemann, Partner, Americas Center for Board Matters, EY

Paul Robertson, UK Cyber Resilience, Preparedness and Response Partner, EY
Julie Linn Teigland, EMEIA Area Managing Partner, EY
Brenton Steenkamp, Partner, Forensic & Integrity Services, EY Advisory Netherlands; Western Europe and Magreb Forensic & Integrity Services Leader, EY

Microsoft was represented by the following in all or part of the simulation:

Terence Jackson, Chief Security Advisor, Microsoft
Lesley Kipling, Chief Cybersecurity Advisor, Microsoft EMEA

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

Jonathan Day, Chief Executive
Beverley Bahlmann, Principal
Todd Schwartz, Principal
Kelly Gillen, Associate
Hannah Skilton, Associate

Appendix 2: Questions the board can ask the executive team

- **?** How is the threat environment to our business changing? Is our ability to prevent and respond keeping pace with that change? Where are there known gaps in our investment to prevent or mitigate risk?
- **?** How would the organization currently respond to a strategically threatening cyberattack? What is the expectation of the roles that the executive and board play in response? What delegation or limitations of authority exist between the board and the executive?
- **?** How effectively is the organization learning from current and recent events? How well is it monitoring changes in the regulatory landscape? Where in the organization are these activities taking place and what assurance exists that known gaps or vulnerabilities are being addressed?
- **?** How are risk and investment choices made between prevention, preparation, response, and recovery? To what extent is there a preparatory function and where does it sit within the organization?
- **?** How capable and confident is the whole chain of response within the organization? Has each team been trained, tested, and exercised within the last 12 months? Was the last exercise strategically significant or merely operationally impacting?

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

[3] EY, "*SEC in Focus: Quarterly Summary of Current SEC Activities*" (EY, October 5, 2023), 1.

[4] Cravath, Swaine & Moore LLP, *SEC Adopts Cybersecurity Disclosure Rules for Public Companies* (Cravath, Swaine & Moore, August 1, 2023).

[5] Hester M. Pierce, "Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (statement, Washington, DC, July 26, 2023).

[6] "FBI Offers Pathway to Request Delay of SEC Cybersecurity Incident Disclosures," Crowell & Moring LLP, December 19, 2023.