EY Center for Board Matters

What cyber disclosures are telling shareholders in 2023

Investors need accurate and timely disclosures on cybersecurity risk governance and management to make informed decisions. Yet there is tension for companies to disclose enough information for investors to understand whether the business is responding to and recovering from a material cyber incident without providing a roadmap to attackers or undermining law enforcement efforts.

Furthermore, the cyber threat landscape has reached a new and dangerous stage in its evolution, with cybercrime expected to cost the world some US$8 trillion in 2023.[1] Our latest EY Global Information Security Survey (GISS) shows that 30% of senior cybersecurity leaders report that hackers are using new strategies that could potentially outsmart their defenses.

In addition to long-standing threats such as IP theft and ransomware, new technologies are dramatically affecting the cybersecurity landscape. ChatGPT reached 1 million users in five days, making it one of the fastest-growing online platforms in history. By comparison, the most popular social media platforms ranged anywhere from several months to years to reach that same milestone. But more importantly, it's a signal of what's to come: Generative artificial intelligence (AI) is poised to reshape our society. Not only are people adopting it in droves, but unlike social platforms, its business applications appear infinite. This technology is maturing fast, and real opportunities and risks for businesses are months, not years, away. But despite these risks, 35% of board directors polled in an EY analysis say they lack an understanding of the AI-related risks their companies face. Organizations need a board-approved strategy on evolving technologies (e.g., generative AI).

[1] "2022 Official Cybercrime Report," Cybersecurity Ventures, available at www.esentire.com.

In brief

- Directors play a critical role in overseeing enhanced disclosures to clarify the rigor of the board's oversight of cybersecurity risks and its competency to provide it.
- In the US, more cybersecurity regulation and additional requirements for cyber disclosures are here or on their way.
- Cybersecurity risk management is about response preparedness and resilience, based on comprehensive crisis response plans that are regularly stress-tested.

Fortune 100 cybersecurity disclosures, 2018–23

Note: References to SEC and ISS denote disclosure areas included in the SEC's rules and ISS's list of 11 cybersecurity-related risk factors. Additionally, some elements of the SEC's rules, notably those relating to material breaches, are not reflected in the chart.

Area of focus	Topic	Disclosure	2023	2022	2021	2020	2019	2018
Category: Board oversight								
	Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the approach proxy statement	96%	95%	88%	89%	85%	75%
SEC ISS	Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	91%	88%	89%	87%	81%	72%
		▸ Disclosed that the audit committee oversees cybersecurity	75%	71%	69%	68%	63%	59%
		▸ Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	31%	29%	29%	25%	27%	19%
ISS	Director skills and expertise	Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	77%	68%	71%	64%	53%	41%
		▸ Cybersecurity disclosed as an area of expertise sought on the board	61%	49%	43%	36%	27%	20%
		▸ Cybersecurity cited in at least one director biography	68%	57%	60%	53%	44%	33%
SEC	Management reporting	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	87%	80%	69%	63%	60%	55%
		Identified at least one "point person" (e.g., the chief information security officer or chief information officer)	57%	48%	40%	35%	32%	23%
SEC ISS	Management reporting frequency	Included language on frequency of management reporting to the board or committee(s)	83%	72%	57%	49%	45%	37%
		Disclosed reporting frequency (e.g., annually, quarterly)	49%	43%	32%	16%	16%	12%
Category: Statements on cybersecurity risk								
	Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%	100%	100%	100%
		Included data privacy as a risk factor	99%	99%	99%	99%	97%	93%
Category: Risk management								
SEC ISS	Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	99%	99%	97%	93%	91%	85%
		Disclosed alignment with external framework or standard	25%	17%	9%	3%	3%	1%
		Referenced response readiness, such as planning, disaster recovery or business continuity considerations	72%	68%	65%	61%	57%	52%
		Stated that preparedness includes simulations or response readiness tests	16%	9%	5%	7%	3%	3%
		Stated that the company maintains a level of cybersecurity insurance	36%	28%	24%	21%	21%	17%
		Included cybersecurity in executive compensation considerations	12%	11%	11%	7%	1%	0%
ISS	Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	55%	45%	36%	29%	25%	17%
	Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	16%	15%	12%	11%	12%	7%
SEC	Use of external advisor	Disclosed use of an external independent advisor	45%	32%	21%	15%	12%	15%
		Disclosed board engagement with an external independent advisor	12%	8%	7%	4%	3%	1%
		Disclosed that the external independent advisor provided attestation	19%	15%	9%	4%	4%	4%

Percentages based on total disclosures by companies. Data based on the 75 companies on the 2022 Fortune 100 list that filed Form 10-Ks and proxy statements in 2018, 2019, 2020, 2021, 2022 and 2023 through May 31, 2023. Areas of focus were referenced in the SEC rules and/or by ISS in its list of Governance QualityScore cyber risk factors released in February 2021.

*Some companies delegate cybersecurity oversight to more than one board-level committee.

Emerging technologies and existing cybersecurity risk management can often present competing challenges for management and the board's attention. In a time of turbulence, boards have a critical role to play in strengthening risk management. Board effectiveness in overseeing cyber risk management starts with its tone at the top, access to the right data and consistently engaging chief risk officers (CROs), chief information security officers (CISOs), business leaders and third parties.

Having robust cyber-related disclosures informs shareholders of how the company is currently addressing the fast-paced challenges of cyber risk, including notifying them of cyber incidents, to help them make more informed investment decisions. Additionally, many organizations will need to comply with new regulations such as the U.S. Securities and Exchange Commission (SEC) recent final rules requiring disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

In our latest analysis of cyber-related disclosures in the proxy statements and Form 10-K filings of Fortune 100 companies, we found more companies providing information about board directors' cyber-related skills and expertise and management's reporting structure and frequency of reporting.

Our refreshed analysis of the proxy statements and 10-K filings, the sixth in an annual series, was designed to identify emerging trends and opportunities for enhanced communication. We looked at filings from 75 Fortune 100 companies that filed during each fiscal year from 2018 through May 31, 2023. We cited sample language from their disclosures and examined the current US regulatory and public policy cyber landscape.

To be sure, the latest proxy statement and 10-K filings provide a look back. By contrast, the SEC's rules, among others, may shape the future.

The SEC's rules

In July 2023, the SEC adopted rules that will, among other things, require cybersecurity incident reporting and disclosure by public companies about their cybersecurity risk management, strategy and governance. The rules require registrants to disclose the following information:

- The disclosure of a material cybersecurity incident in Form 8-K within four business days of determining that it is material, with a delay only when the U.S. Attorney General concludes that disclosure would pose a substantial risk to national security or public safety (registrants should take into consideration both quantitative and qualitative factors to determine whether an incident is material).
- If any required information is not determined or is unavailable at the time the company prepares the Form 8-K, the company must file an amended Form 8-K containing such information within four business days after it determines such information, or the information becomes available.
- The board's role in overseeing risks from cybersecurity threats. Registrants are required to identify any board committee or subcommittee that oversees cybersecurity risks, if applicable, and describe the processes by which the committee is informed about such risks.
- Their processes, if any, to assess, identify and manage risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. For example, a registrant is required to disclose whether and how any such processes have been integrated into its overall risk management system or processes.
- Whether the registrant uses assessors, consultants, auditors or other third parties in connection with such processes, and whether it has processes in place to oversee and identify risks related to its use of third-party service providers.
- Whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect its business strategy, results of operations or financial condition and if so, how.
- Management's role in assessing and managing material risks from cybersecurity threats, including whether certain management positions or committees are responsible for measuring and managing cybersecurity risk and their relevant expertise.
- Registrants must also disclose the processes by which management is informed about and monitors the prevention, detection, mitigation, and remediation of cybersecurity incidents, including whether management reports information about such risks to the board.

See page 10 for further information on key US regulatory and public policy developments.

What we found

In comparing the proxy statements and Form 10-K filings of Fortune 100 companies over the past six years, we have seen steady and significant increases in the percentage of disclosures in certain categories of cyber management and oversight.

Providing insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters had a disclosure rate of 87% in 2023, up from 55% in 2018. Identifying at least one point person responsible for reporting to the board, such as the CISO or chief information officer (CIO) was 57% this year, up from 23% in 2018.

Other areas of noteworthy increases in disclosure rates in the 2023 filings:

- Frequency of management reporting to the board or committee(s) (83%, up from 37% in 2018)
- Cybersecurity disclosed as an area of expertise sought on the board (61% in 2023, up from 20% in 2018)
- Director cybersecurity skills and expertise in at least one director biography, for example, had a 68% disclosure rate in 2023, up from 33% in 2018
- Use of an external independent advisor (now 45%, up from 15% in 2018)

A detailed analysis of the latest disclosures and in context of six-year trends follows. In certain key areas, we provide a comparison with the SEC rules, underscoring the gaps that some companies will need to address in their practices and disclosures.

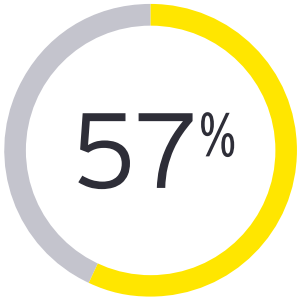
Management reporting to the board

The new SEC rules require disclosing the processes by which the board or committee responsible is informed about cyber risks. Over time, we've seen disclosure enhancements regarding management reporting on such risks to the board. This year, 87% of companies provided insights into management reporting to the board and/or committee overseeing cyber matters, up from 55% in 2018.

While that change is notable, the real change we're seeing is around who is providing that information and how often it is conveyed. In 2023, 57% identified at least one person who is reporting to the board on cybersecurity, most often the CISO or CIO, up from 23% in 2018. Similarly, 49% disclosed this year that management is reporting to the board on cybersecurity at least annually, with a number of companies reporting on a least a quarterly basis, up from 12% in 2018. Many other companies include language on the frequency of management reporting, but typically that language is not specific, alluding to reports to the board that occur "regularly" or "periodically."

As the rules indicate, the Commission directs registrants to disclose management positions or committees responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise. Disclosing details of the frequency of reporting could be included as part of describing the processes by which the board or relevant committee is informed about cybersecurity risks.

Adding specificity to these disclosures may help stakeholders assess whether the board is engaging with the CIO, CISO or equivalent executive with an appropriate cadence to conduct its oversight. While it is common for either the CIO or CISO to routinely brief the board, in our discussions with directors, many indicate that they intentionally raise cyber risks in their interactions with other members of management. In doing so, directors invoke a heightened tone at the top and demonstrate that cyber is viewed as a critical enterprise risk that is ultimately owned by the businesses and touching key activities across the company, from M&A to product development to vendor management to human resources.



of Fortune 100 companies identify at least one point person responsible for reporting to the board (e.g., CISO or CIO), up from 23% in 2018

Board-level committee oversight

Under the final rule, the SEC requires companies to identify and disclose whether any board committee or subcommittee is responsible for cybersecurity oversight. In our research, 91% of companies this year charged at least one board-level committee with cybersecurity oversight, up from 72% in 2018. Since 2018, we've observed an increase in boards assigning oversight to committees other than audit, most often risk or technology committees. This year, 31% of boards chose a committee other than audit, for primary or additional oversight, up from 19% in 2018. Among the boards making that choice, 86% added cyber responsibilities to the committee charter.

For now, at least, audit committees remain the primary choice to oversee cybersecurity risk. This year, 75% of the boards chose audit, up from 59% in 2018. Among the boards that chose the audit committee, 82% formalized that responsibility in the committee charter.

Identification of director skills and expertise

Although the final SEC rules do not require disclosing whether directors have expertise in cybersecurity, it represents one of the more significant shifts in disclosure rates that we've observed since initiating this analysis six years ago. In 2023, 61% of companies disclosed cybersecurity as an area of expertise sought on the board, up from 20% in 2018. More than two-thirds of the companies now cite cybersecurity experience in at least one director biography, up from 33% in 2018. Gartner predicts 70% of boards will include at least one member with cybersecurity experience by 2026.[2]

A closer look at these changes over the past few years shows that, in most cases, the increases in director experience are related to most companies adding cyber-related experience to longer-standing board member bios, with some boards adding a new director with cybersecurity experience. The new arrivals have included former CIOs and senior information technology executives, the head of a cybersecurity company, and former leaders in federal intelligence agencies or the Department of Defense.

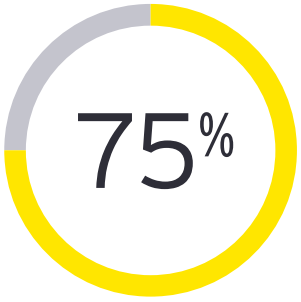
Alignment with an external framework or standard

The number of companies that disclosed the alignment of their cybersecurity program and information security practices with an external security process or control framework increased to 25% this year, up from just 1% in 2018. The framework of the National Institute of Standards and Technology (NIST) was cited by 16 companies, more than any other. Among the others referenced were the International Organization for Standardization (ISO) 27001 and HITRUST. A number of companies also disclosed that certain portions of their controls were covered by the American Institute of Certified Public Accountants (AICPA) System and Organization Controls for Service Organizations: Trust Services Criteria (SOC 2) service audit reports.

Compensation incentives

This year, we observed a modest increase in companies specifically disclosing performance related to cybersecurity or privacy issues as a consideration in determining executive pay. This year, 12% of companies did so, compared with zero in 2018. Nonetheless, companies generally cited cyber considerations (e.g., maintained strong cyber defense with no material business-impacting events amid a heightened cyber-threat environment) among a host of other nonfinancial company or individual performance considerations in executive pay decisions.

[2] "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," Gartner Security & Risk Management Summit, March 2023, Sydney, Australia.



of Fortune 100 companies are delegating oversight of cybersecurity matters to the audit committee, up from 59% in 2018

Response readiness simulations

The percentage of companies disclosing that they performed cyber incident simulations with management and/or the board remains low, increasing to 16% this year, from 3% in 2018. Of the companies that disclosed such exercises, several disclosed that the board participated, and one specified that the board actively participates in discussions and simulations of cybersecurity risks both internally and with law enforcement, government officials, and peer and industry groups. Rigorous simulations are critical risk preparedness practices that Ernst & Young LLP (EY) and others believe companies should prioritize.

If cybersecurity breach simulation plans are not practiced and a breach occurs, the reaction by the board and management is largely improvised. Well-designed incident simulations can stress-test the organization's capabilities and improve readiness by providing clarity of roles, protocols and escalation processes. These simulations often include third parties (e.g., a public relations firm, forensic specialists, outside counsel and/or law enforcement as noted previously). Policies on ransomware should also be established ahead of time, including whether the company and board would approve payment and under what circumstances, as well as a full understanding of insurance contract terms and conditions. Management should conduct these exercises to test the company's significant vulnerabilities and identify where the greatest financial impact could occur. Boards should consider participating in these simulations so that their insights and experiences can be incorporated to elevate the company's ability to respond and recover.

Further, such exercises help companies develop and practice action plans related to data privacy issues. Cyber breaches can — and often do — result in the loss of personal data. These events require compliance with a host of complex state and federal laws (all of which call for prompt notice to states, regulators and affected persons), and may require compliance with the laws of non-US jurisdictions. Regular practice is key to establishing effective preparation and responses.

Use of external independent advisor

Another component in the SEC rules requires registrants to disclose whether it uses assessors, consultants, auditors or other third parties in connection with its processes to assess, identify and manage risks from cybersecurity threats, and whether it has processes in place to oversee and identify risks related to its use of third-party service providers. In our analysis, the percentage of companies disclosing the use of an external independent advisor to support management on cybersecurity matters grew to 45% this year, from 15% in 2018. Among the companies that made the disclosure this time around, nine indicated that the board received reports from the independent third party. One company disclosed that the audit and compliance committee annually engages third parties (as well as the company's internal audit department) to audit the company's information security programs, whose findings are reported to the audit and compliance committee.

The National Association of Corporate Directors (NACD) and the Internet Security Alliance (ISA) Director's Handbook on Cyber-Risk Oversight encourage boards to request deep-dive briefings from independent third-party experts validating whether the company's cyber risk management program is meeting its objectives. In the absence of a cyber expert on the board, retaining an independent expert (or organization) to regularly advise the board on cyber matters may become a growing practice, as boards already avail themselves of similar expertise on matters such as executive compensation and fairness opinions.

The percentage of companies disclosing that they performed cyber incident simulations with management and/or the board remains low, increasing to 16% this year, from 3% in 2018.

2023 Director's Handbook on Cyber-Risk Oversight

The NACD and the ISA *2023 Director's Handbook on Cyber-Risk Oversight* helps directors validate that they have complete information to fulfill their oversight role, while also providing principles to consider and compare when benchmarking their organization's risk management efforts.

Principle 1	Principle 2	Principle 3*	Principle 4	Principle 5	Principle 6**
Directors need to understand and approach cybersecurity as a strategic enterprise risk — not just as an IT issue.	Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.	**Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on board meeting agendas.**	Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.	Board and management discussions about cyber risk should include identification and quantification of the financial exposure to cyber risks and which risks to accept, mitigate or transfer, such as through insurance, as well as specific plans associated with each approach.	Boards should encourage systemic resilience through collaboration with their industry and government peers and encourage the same from their management teams.

* Within Principle 3, the handbook indicates the board should schedule deep-dive briefings or examinations from independent and objective third-party experts to validate that the cybersecurity risk management program is meeting its objectives.

** Principle 6 is new in the 2023 handbook.

There is wide variability in what goes into a third-party assessment, from something as simple as an inquiry-only assessment of certain business segments to a more rigorous company-wide assessment that includes a significant amount of verification and testing. Our research noted a few companies leveraging audits (i.e., those performed by internal audit and/or a third party) to validate certain aspects of their information security and/or certain aspects of cybersecurity. But we did not identify any explicit discussion of whether an attestation opinion was obtained utilizing the AICPA System and Organization Controls for Cybersecurity framework, which provides for an entity-wide independent attestation report on the company's cyber risk management program.

“

There is wide variability in what goes into a third-party assessment, from something as simple as an inquiry-only assessment of certain business segments to a more rigorous company-wide assessment that includes a significant amount of verification and testing.

Disclosure of cyber incidents

There appears to be a gap between disclosures related to material cybersecurity incidents, including the depth of the disclosures, as compared with the number and scale of cyber incidents reported in the news media and third-party reports. The 2023 Verizon Data Breach Investigations Report stated there were 5,199 confirmed data breaches between November 1, 2021 and October 31, 2022, from small to large organizations, but the report did not address the materiality of these breaches. Per research provided to EY researchers from Audit Analytics for the same time period, there were 57 cyber incidents reported to the SEC in a public filing.

Another study found that on average, in 2022 breaches were not detected until 207 days after the breach had occurred, and it typically took 70 days to contain a breach.[3]

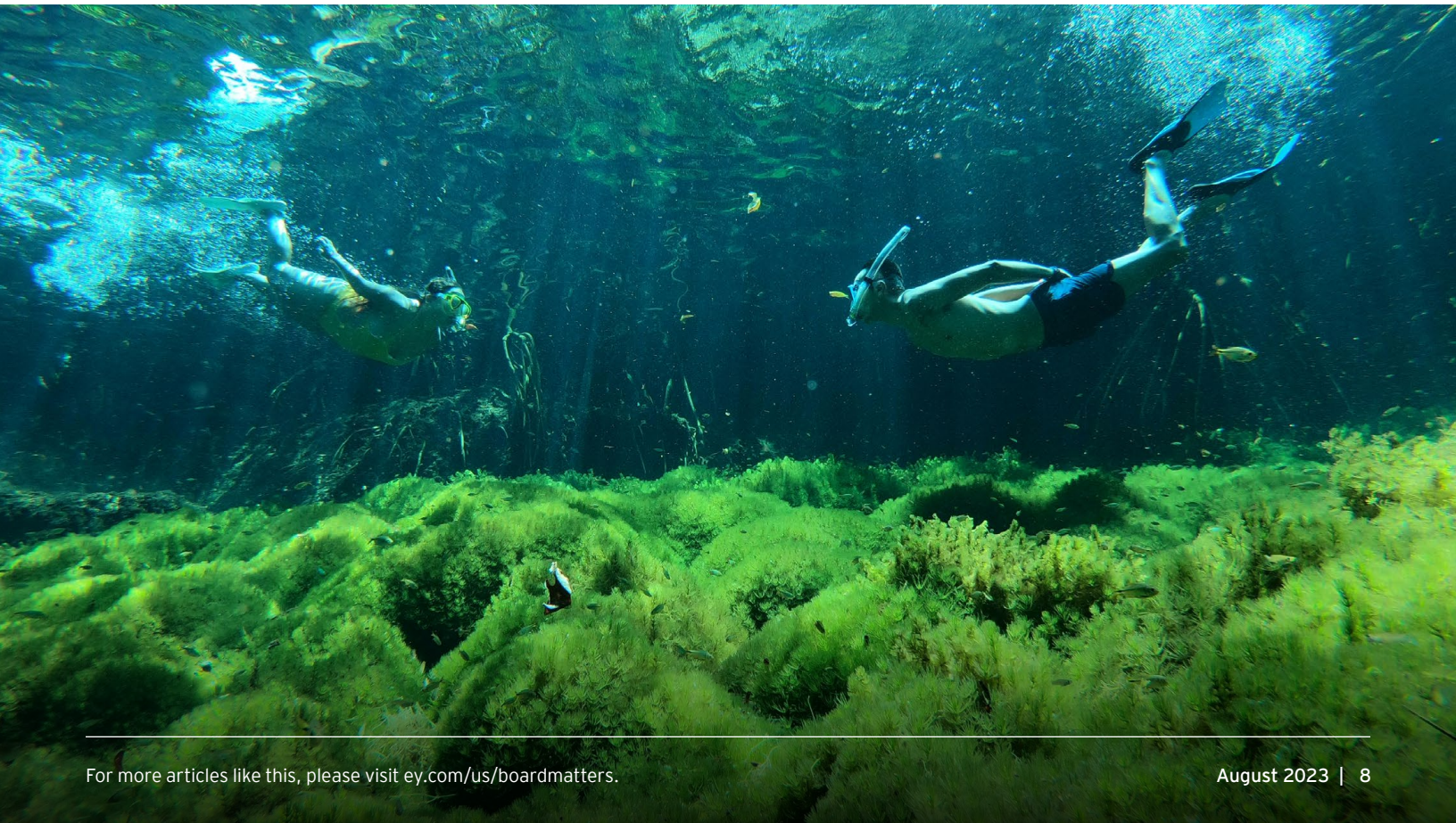
The SEC's rules require disclosure of a material cybersecurity incident in Form 8-K within four business days of determining that it is material. The SEC states the information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to determine whether the incident is material. If any required information is not determined or is unavailable at the time the company prepares the initial Form 8-K, the company must file an amended Form 8-K containing such information within four business days after it determines such information, or the information becomes available.

Disclosures to date range from stating the occurrence of an incident to providing a more in-depth account, including the number of account holders affected; the nature of the data; costs and insurance offsets; and remedial steps taken to fix the security vulnerability.

The SEC is not the only corporate governance stakeholder seeking more disclosures about cyber incidents. In its Governance QualityScore rating solution, Institutional Shareholder Services (ISS)[4] includes 11 factors that address information security risk management and oversight. These factors include board members' information security expertise; frequency of briefing the board on information security matters; whether the company maintains a cyber risk insurance policy; and the existence of, and financial impact from, recent security breaches.

[3] "Cost of a Data Breach: A Million-Dollar Race to Detect and Respond," IBM, 2022.

[4] "ISS ESG Unveils 2021 Methodology Enhancements for Governance QualityScore," ISS, February 8, 2021.



Our market observations

Based on insights gained through engagement with directors, as well as what EY cybersecurity leaders have learned from assignments around the globe and across industries and company sizes, we have identified these 10 leading practices to help boards oversee cyber risk:

1. **Elevate the tone**. Establish cybersecurity as a key consideration in all board matters. If technology is a cornerstone of most business decisions, then cyber risk considerations should be part of board and management discussions about strategy, product and service growth plans, digital transformation and so on.
2. **Stay diligent**. Address new issues and threats stemming from remote work and the expansion of digital transformation. And remember that every employee needs to be diligent, too — 74% of breaches involve a human element, according to Verizon's 2023 Data Breach Investigations Report, issued in June 2023.
3. **Determine value at risk**. Reconcile value at risk expressed in dollar terms against the board's risk tolerance, including the efficacy of cyber insurance coverage. The NACD recently formed an alliance with X Analytics to help boards with easy-to-understand business metrics to support effective cyber-risk board oversight, including assigning dollar amounts to cyber risk.
4. **Leverage new analytical tools**. Such tools inform the board of cyber risks ranging from high-likelihood, low-impact events to low-likelihood, high-impact events (i.e., a "black swan" event).
5. **Embed security from the start**. Embrace a "secure by design" philosophy when designing new technology, products and business arrangements. In April 2023, The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and international partners published secure-by-design and -default principles and approaches.
6. **Independently assess the company's cybersecurity risk management program**. Obtain a rigorous third-party assessment of the company's cyber risk management.
7. **Evaluate third-party risk**. Understand management's processes to identify, assess and oversee the risk associated with service providers and third parties involved in your supply chain.
8. **Test response and recovery**. Enhance enterprise resilience by conducting rigorous simulations and arranging protocols with third-party specialists before a crisis.
9. **Understand escalation protocols**. Have a defined communication plan for when the board should be notified, including incidents involving ransomware.
10. **Monitor evolving practices and the regulatory and public policy landscape**. Stay attuned to evolving oversight practices, disclosures, reporting structures, and metrics and understand implications for how the company is staying in compliance with requirements.

If technology is a cornerstone of most business decisions, then cyber risk considerations should be part of board and management discussions about strategy, product and service growth plans, digital transformation and so on.

Public policy landscape

Cybersecurity continues to be a key priority for the SEC. In addition to the above-mentioned finalized rules, the Commission has issued multiple other rule proposals relating to cybersecurity that would impact a wide range of capital market participants. These include:

- The SEC proposed rules that would enhance registered investment advisor and fund disclosures related to cyber risks and incidents and require funds to adopt and implement cybersecurity-related written policies and procedures, among other changes. The SEC has announced plans to finalize the proposal in October 2023.
- Another proposal would require certain market entities, including broker-dealers, clearing agencies and national securities exchanges, to have written policies and procedures designed to address their cybersecurity risks. Other requirements would include providing immediate notice to the Commission of significant cybersecurity incidents and publicly disclosing summary descriptions of cybersecurity risks and significant cybersecurity incidents on a new Form SCIR.
- Another proposal would expand Regulation Systems Compliance and Integrity (SCI) — a set of rules adopted in 2014 to address technological vulnerabilities in US securities markets and improve Commission oversight of the core technology of key US securities markets entities.
- A further proposal would amend Regulation S-P to enhance the protection of customer information by requiring applicable parties to provide notice to individuals affected by data breaches that may put them at risk of identity theft or other harm.

SEC Chair Gary Gensler continues to be vocal about the need for enforcement around cybersecurity. During a March 2023 SEC Open Meeting, he stated, "The nature, scale and impact of cybersecurity risks have grown significantly in recent decades. Market entities across our capital markets increasingly rely on complex and ever-evolving information systems. Those who seek to harm these systems have become more sophisticated as well, in their tactics, techniques, and procedures. Investors, issuers, and market participants alike would benefit from knowing that these entities have in place protections fit for a digital age."

In its report on FY22 Enforcement Results, the SEC cited cybersecurity enforcement matters as a priority. The Commission has pursued enforcement actions involving insufficient policies and procedures to protect investors from identity theft as well as failures to protect personal identifying information, among other issues.

Federal and other national regulatory efforts

Cybersecurity continues to be a focus of Congress and the Biden Administration in 2023.

While the passage of sweeping cybersecurity legislation is unlikely, agencies and regulators have engaged on several fronts in recent months.

One notable development was the March 2023 release of the Biden Administration's National Cybersecurity Strategy (the Strategy) to "secure the full benefits of a safe and secure digital ecosystem for all Americans." The Strategy centers around five key pillars:

- Defending critical infrastructure
- Disrupting and dismantling threat actors
- Shaping market forces to drive security and resilience
- Investing in a resilient future
- Forging international partnerships with like-minded nations

The Strategy also would increase the responsibilities of software developers, noting: "Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance." In order to increase software cybersecurity, the administration plans to work with the private sector on legislation establishing liability for software products and services, saying that any such legislation "should prevent manufacturers and software publishers with market power from fully disclaiming liability by contract, and establish higher standards of care for software in specific high-risk scenarios."

The National Institute of Standards and Technology (NIST) continues to play an important role in the development of cybersecurity standards for the private sector. NIST recently released a draft of the Cybersecurity Framework (CSF) 2.0 Core. The changes to the CSF 1.1 Core relate to: outcomes being applicable to all entities, not just critical infrastructure; an increased focus on the "Govern, Identify, and Protect" and the "Detect, Respond, and Recover" functions; organizational structure, risk management, policies, and responsibilities; supply chain risk management; continuous improvement; better securing assets; technology resilience infrastructure; and incident response. NIST is seeking feedback on the draft by November 5, 2023. NIST has also devoted attention to artificial intelligence, releasing version 1.0 of its AI Risk Management Framework in January 2023.

NIST likewise plays a central role in the cybersecurity requirements applicable to private companies that work with the federal government. In May 2023, NIST released a draft of Special Publication 800-171 Rev. 3 for public comment. The publication contains security requirements for protecting the confidentiality of controlled unclassified information (CUI) in nonfederal systems "when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency." Notably, the Department of Defense uses this NIST publication as the assessment baseline for its Cybersecurity Maturity Model Certification (CMMC).

Software used by the federal government also has been a special area of concern. The Cybersecurity and Infrastructure Security Agency (CISA) issued a Request for Comment (RFC) on Secure Software Development Attestation Common Form (CISA-2023-0001) in April 2023. The RFC implements OMB Memo M-22-18 on Enhancing the Security of Software Supply Chain through Secure Software Development Practices. The memo requires US government agencies to obtain a self-attestation from a software vendor before the agency uses the software, and it applies both to new software and existing software to which a vendor makes major changes. The RFC includes questions regarding the practical utility, burden and ways to improve the information collection. The comment period ends 26 June 2023.

Other legislative and administrative actions have been more targeted at specific sectors.

- For example, as part of the omnibus appropriations bill passed late in 2022, the Food and Drug Administration (FDA) was authorized to establish cybersecurity requirements for internet connected medical devices.
- The CHIPS and Science Act (CHIPS), signed into law by President Biden last summer, also included cyber provisions. In addition to providing funds to develop the US semiconductor industry, the CHIPS legislation included a directive for the Department of State to create an International Technology and Security Innovation Fund, which appropriated US$500 million — US$100 million per year over five years, starting in Fiscal Year 2023 — "to promote the development and adoption of secure and trustworthy telecommunications networks and ensure semiconductor supply chain security and diversification." The cyber-specific part of the workstream will expand on existing digital connectivity and cybersecurity partnership activities, such as providing cybersecurity, tools and services to allies and partner countries.
- Concerns about the breadth and strength of the US cyber workforce persist with the National Initiative for Cybersecurity Education (NICE) collecting stakeholder feedback on updates to the Workforce Framework for Cybersecurity (NICE Framework) — a reference for sharing information about cybersecurity employment and training opportunities. The guide is intended to serve workforce stakeholders, primarily those in education, training and workforce development.

Another area to watch in the months ahead is the rapid spread and adoption of AI by an array of businesses and organizations. Policymakers are grappling with how to manage risks associated with the powerful technology, including accountability, ethics and bias. It also has the potential to introduce new fraud and cybersecurity risks. While it is not yet clear what approach US policymakers will take in addressing AI risks and accountability, it is clear the issue will continue to garner attention from Congress, the administration and others in the months to come. And the EU is moving quickly in pursuing new AI policies and regulation.

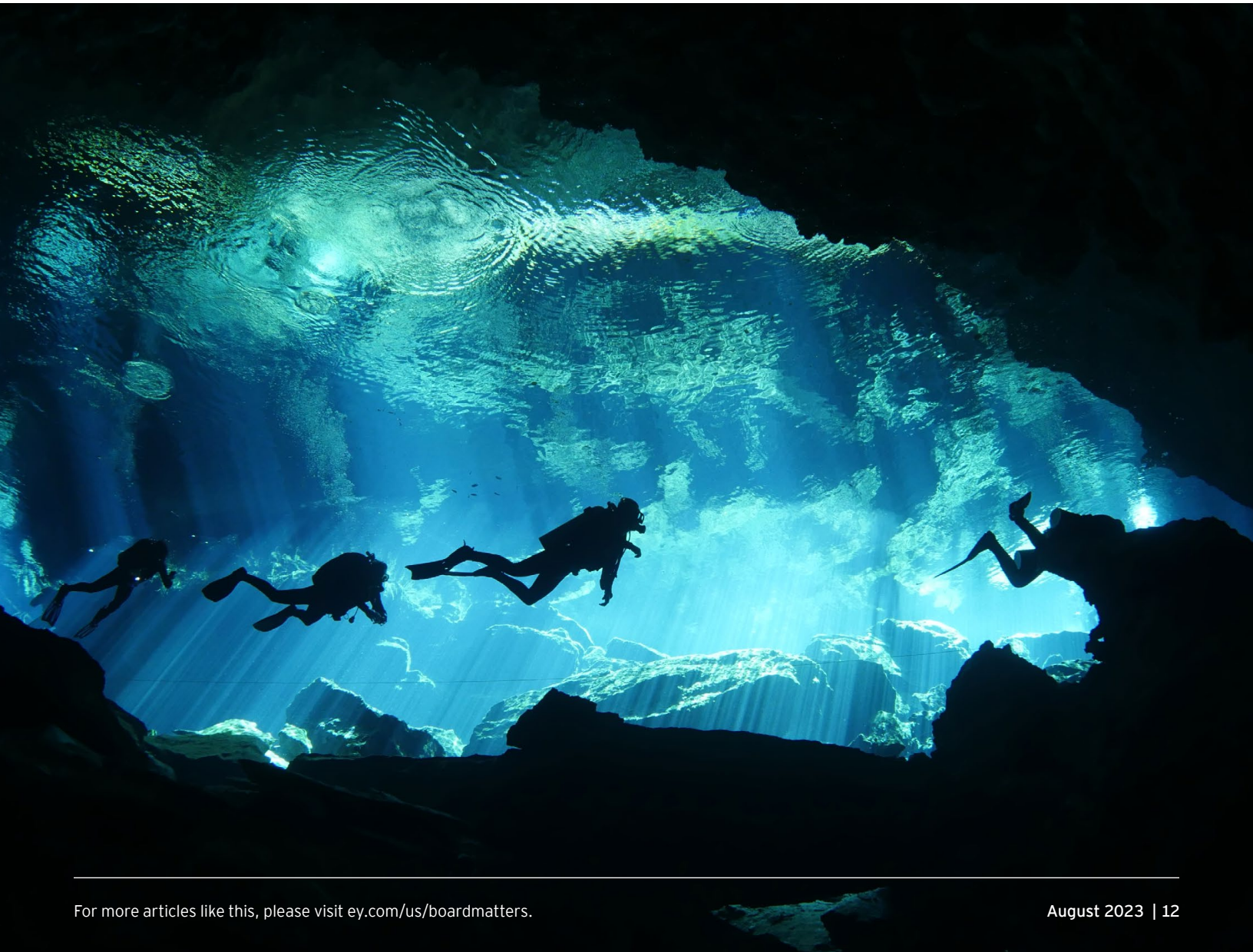
Activity in the states

So far this year, state legislatures have introduced more than 250 bills related to cybersecurity. While many states passed bills directing the establishment of cybersecurity task forces and agencies, others focused on banning certain technologies from state-owned devices.

In all, 30 bills have seen enactment in the states, with eight more awaiting approval from their state's governor. Bills have been enacted in Arkansas, Florida, Iowa, Idaho, Indiana, Kansas, Maryland, Mississippi, Montana, North Dakota, New Jersey, New Mexico, Oklahoma, Utah, Virginia and Washington.

Takeaways for board oversight

To provide effective oversight, boards must be familiar with the risks that cybersecurity can bring. With the appropriate level of familiarity, boards can effectively monitor the extent of the risks and influence investment decisions in order to mitigate the risk presented by cybersecurity threats and to be prepared when cyber incidents do occur. Leading boards are focused on prioritizing cybersecurity oversight, asking probing questions, staying current on regulations and increasingly transparent and timely disclosures to inform shareholders how the company is addressing cybersecurity risk.



Appendix: Sample language from public disclosures

Security reports

Equifax released its 2022 Security Annual Report on March 21, 2023. The report emphasizes collaboration and transparency, according to a company news release, "We believe that more communication, more collaboration, and more transparency, equals stronger security and are committed to helping customers, partners and consumers strengthen their own cybersecurity postures for the benefit of the industry at large." On May 9, 2023, the company also announced via press release that it was "making its security and privacy controls framework public for the benefit of security and privacy teams at organizations of all sizes."

Charters

Charters for board committees should accurately reflect the committee's responsibilities and be updated as needed. The Citigroup Inc. Technology Committee charter and the Progressive Technology Committee charter are two good examples outlining a committee's cyber risk governance responsibilities.

Pointing out the board's cyber expertise

A leading practice for companies to disclose board director expertise is the use of a matrix and director bios in the annual proxy statement. The Lockheed Martin 2023 proxy statement, on pages 8–16, includes a matrix noting the directors' general experience, qualifications and skills and highlighting which members have a cybersecurity background. The qualifications are listed in each of the directors' bios.

Cyber breach notification example

> *We determined that our company was the subject of a targeted cyber-attack. Upon discovering the incident, we shut down most of our operating systems globally to manage the safety of our overall global systems environment. The situation is evolving, and we are working with global cybersecurity experts to manage the situation. While our systems are shut down, we will have limited ability to conduct operations, including but not limited to arranging for shipments of freight or managing customs and distribution activities for our customers' shipments.*
>
> *The security of our systems, minimizing the impacts on our customers, and providing our customers with timely and accurate information are our highest priorities. We are conducting a thorough investigation to ensure that our systems are restored both promptly and securely, and on a parallel track, evaluating ways with our carriers and service providers to mitigate the impact of this event on our customers. Since it is extremely early in the process, we cannot provide any specific projections on when we might be operational, but we will provide regular updates when we are able to do so confidently.*
>
> *We are incurring expenses relating to the cyber-attack to investigate and remediate this matter and expect to continue to incur expenses of this nature in the future. Depending on the length of the shutdown of our operations, the impact of this cyber-attack could have a material adverse impact on our business, revenues, results of operations and reputation.*
>
> *Further communications will be shared as we manage through this significant event.*

Information about the board's oversight of cyber risks, including how it is kept informed and how it or a relevant board committee considers the risks as part of its oversight of business strategy, risk management and financial matter

> **Example A**
>
> *To more effectively prevent, detect and respond to information security threats, the Company maintains a cyber risk management program, which is supervised by a dedicated Chief Information Security Officer whose team is responsible for leading enterprise-wide cybersecurity strategy, policy, standards, architecture and processes. The Audit Committee receives regular reports from the Chief Information Security Officer and the Chief Information Officer on, among other things, the Company's cyber risks and threats, the status of projects to strengthen the Company's information security systems, assessments of the Company's security program and the emerging threat landscape. Additionally, the Chief Information Security Officer chairs the Cybersecurity Risk Oversight Council, which drives awareness, ownership and alignment across broad governance and risk stakeholder groups for effective cybersecurity risk management and reporting.*

Example B

The Board of Directors oversees the Company's information security program that institutes and maintains controls for the systems, applications, and databases of the Company and of its third-party providers. The CISO manages the program, in collaboration with the Company's businesses and functions. The CISO and the head of Global Technology & Operations present updates to the Audit Committee quarterly and, as necessary, to the full Board. These regular reports include detailed updates on the Company's performance preparing for, preventing, detecting, responding to and recovering from cyber incidents. The CISO also promptly informs and updates the Board about any information security incidents that may pose significant risk to the Company. The Company's program is periodically evaluated by external experts, and the results of those reviews are reported to the Board.

Example C

The Audit and Compliance Committee is responsible for reviewing the Company's information security programs, including cybersecurity. The Company annually engages third parties (as well as our own internal audit department) to audit the Company's information security programs, whose findings are reported to the Audit and Compliance Committee. We also actively engage with key vendors, industry participants, the U.S. Department of Homeland Security, and intelligence and law enforcement communities as part of our efforts, which are reported to the Audit and Compliance Committee. Our Chief Security Officer, who manages our information security training and awareness program, also updates the Audit and Compliance Committee on a quarterly basis regarding information security matters. Our Board also receives periodic updates relating to information security and cyber security risks.

Example D

Cybersecurity risk is overseen by management-level committees, which report to the Firm Risk Committee and subsequently to the Operations and Technology Committee as well as the Board. The Operations and Technology Committee has primary responsibility for oversight of operations, technology and operational risk, including information security, fraud, vendor, data protection and privacy, business continuity and resilience, and cybersecurity risks (including review of cybersecurity risks against established risk management methodologies). In accordance with its charter, the Operations and Technology Committee receives regular reporting at each quarterly meeting from senior officers in the Technology Department (Technology), Operations Department (Operations) and Non-Financial Risk on operational risk and the steps management has taken to monitor and control such exposures. Such reporting includes updates on the Company's cybersecurity program, the external threat environment, and the Company's programs to address and mitigate the risks associated with the evolving cybersecurity threat environment.

The Operations and Technology Committee also receives an annual independent assessment of key aspects of the Company's cybersecurity program from an external party and holds joint meetings with the Audit Committee and Risk Committee, as necessary and appropriate. The Board or the Operations and Technology Committee reviews and approves the Global Cybersecurity Program Policy, the Global Information Security Program Policy and the Global Technology Policy at least annually. The Chair of the Operations and Technology Committee regularly reports to the Board on cybersecurity risks and other matters reviewed by the Operations and Technology Committee. In addition, the Board receives separate presentations on cybersecurity risk and in accordance with the Corporate Governance Policies all Board members are invited to attend Operations and Technology Committee meetings and have access to meeting materials.

Senior management, including the senior officers mentioned above, discuss cybersecurity developments with the Chair of the Operations and Technology Committee between Board and committee meetings, as necessary. The Operations and Technology Committee meets regularly in executive session with management, including the Head of Non-Financial Risk, and senior officers from Technology and Operations.

Response readiness

Each year, the Company engages a third-party expert to oversee a cybersecurity incident response exercise to test pre-planned response actions from the Company's Information Security Incident Response Plan and to facilitate group discussions regarding the effectiveness of the Company's cybersecurity incident response strategies and tactics.

Use of external independent advisor and board engagement

Example A

An independent third party also regularly reports to the Audit Committee/Board on cybersecurity and outside counsel advises the Board about best practices for cybersecurity oversight by the Board, and the evolution of that oversight over time.

Example B

The audit committee receives semiannual reports from its independent cybersecurity advisor. The company utilizes an independent cybersecurity advisor reporting to the audit committee to provide objective assessments of the company's capabilities and to conduct advanced attack simulations.

Alignment with external framework or standard

On an annual basis, we conduct risk assessments and compliance audits, both internally and by independent third parties, against standards including the National Institute of Standards and Technology security framework (NIST) and Payment Card Industry Data Security Standards (PCI DSS), and regularly benchmark and evaluate program maturity with industry leaders.

Training

The Firm's Security Awareness Program includes training that reinforces the Firm's Information Technology Risk and Security Management policies, standards and practices, as well as the expectation that employees comply with these policies. The Security Awareness Program engages personnel through training on how to identify potential cybersecurity risks and protect the Firm's resources and information. This training is mandatory for all employees globally on a periodic basis, and it is supplemented by firmwide testing initiatives, including periodic phishing tests. The Firm provides specialized security training for certain employee roles such as application developers. Finally, the Firm's Global Privacy Program requires all employees to take periodic awareness training on data privacy. This privacy-focused training includes information about confidentiality and security, as well as responding to unauthorized access to or use of information.

Questions for the board to consider

- Is the board allocating sufficient time on its agenda, and is the committee structure appropriate, to provide effective oversight of cybersecurity disclosure requirements?
- Does the company have a generative AI strategy?
- How will the company use generative AI to challenge its existing business model? Does the company have a plan in place to mitigate AI risks?
- Do the company's disclosures effectively communicate the rigor of its cyber-risk management program and related board oversight?
- Has the board participated with management in one of its cyber breach simulations in the last year? How rigorous was the testing?
- Have appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis and given a dollar value?
- What kind of threats is the company most concerned about? How does the company monitor the evolving threat landscape? Has the company been the target of a major cyber attack?
- What information has management provided to help the board assess which critical business assets and partners, including third parties and suppliers, are most vulnerable to cyber attacks?
- How does management evaluate and categorize identified cyber and data privacy incidents and determine which ones to escalate to the board?
- What kind of policies has the company established on ransomware? How have the company and board approached the issue of payment?
- Will new or pending privacy regulations and frameworks impact the organization's strategy, competitive position, and business models and practices?
- Has the board leveraged a third-party assessment, as described in the NACD's cyber-risk oversight handbook, to validate that the company's cyber risk management program is meeting its objectives? If so, is the board having direct dialogue with the third party related to the scope of work and findings? Has the board considered the value of obtaining a cybersecurity attestation opinion to build confidence among key stakeholders?

Looking for more?

Access additional information and thought leadership from the EY Center for Board Matters at ey.com/us/boardmatters.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

About the EY Center for Board Matters

Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters supports boards, committees and directors in their oversight role by providing content, insights and education to help them address complex boardroom issues. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content, and practical tools and analysis for directors, institutional investors and other governance stakeholders.

US SCORE no. 20711-231US
CS no. 2307-4287888

ED None

ey.com/us/boardmatters