EY Center for Board Matters

How cybersecurity risk disclosures and oversight are evolving in 2021

Building a better working world

Public disclosures about cybersecurity governance and risk management help build stakeholder confidence by providing transparency around how boards are fulfilling their cybersecurity risk oversight responsibilities. Securing the trust of investors and other stakeholders through robust cybersecurity governance and disclosures is critical in today's dynamic cyber risk environment.

As the cyber attack surface increases, threats and incidents are also intensifying, creating more extreme pressure than ever for companies. According to the EY Global Information Security Survey 2021, 81% of executives say the COVID-19 pandemic forced organizations to bypass certain cybersecurity processes or controls. Over the same period, many organizations were rolling out new customer-facing technology and cloud-based tools to enable remote working and to keep distribution channels open. Threat actors also hit a new level of maturity, and high-profile cyber attacks continue to demonstrate the criticality of cybersecurity to organizations throughout the world.

To effectively oversee these evolving cybersecurity risks, boards should set the tone at the top, emphasizing the importance of cybersecurity in the context of risk management. Boards can also encourage enhanced disclosures that clarify for investors and other stakeholders the rigor of the board's oversight in this area and the use of vital cyber risk mitigation and response practices.

For the fourth consecutive year, the EY Center for Board Matters team analyzed cybersecurity-related disclosures in the proxy statements and Form 10-K filings of Fortune 100 companies to identify emerging trends and developments and help companies identify opportunities for enhanced communication. We looked at 77 Fortune 100 companies that filed those documents from 2018 through May 31, 2021.

We focused on the areas of cybersecurity board oversight (including board-level committee oversight, director qualifications and management reporting to the board), statements on cybersecurity and data privacy risks, and risk management (including cybersecurity risk mitigation and response efforts and engagement with external security consultants). We also examined the current regulatory and US public policy landscape related to cybersecurity, as well as perspectives from directors and EY cybersecurity professionals.

In brief

- Cybersecurity risks have intensified as the pandemic forced many companies to bypass certain cybersecurity controls and adopt new technology to enable remote working.
- Enhanced cybersecurity-related disclosures can help investors and other stakeholders better understand the effectiveness of how cybersecurity risk is governed.
- Following recent cybersecurity incidents, the federal government's focus on how organizations are preventing and responding to cyber attacks has increased.

Fortune 100 company cybersecurity disclosures, 2018–21

Topic	Disclosure	2021	2020	2019	2018
Category: Board oversight					
Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	90%	90%	88%	79%
Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	90%	87%	82%	75%
	▸ Disclosed that the audit committee oversees cybersecurity matters	68%	66%	61%	58%
	▸ Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	30%	26%	27%	19%
Director skills and expertise	Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	65%	57%	51%	36%
	▸ Cybersecurity disclosed as an area of expertise sought on the board	43%	38%	29%	21%
	▸ Cybersecurity cited in at least one director biography	56%	44%	38%	27%
Management reporting structure	Provided insights into management reporting to the board or committee overseeing cybersecurity matters	69%	64%	62%	58%
	▸ Identified at least one "point person" (e.g., the chief information security officer or chief information officer)	44%	35%	35%	26%
Management reporting frequency	Included language about frequency of management reporting to the board or committee, but most of this language was not specific	56%	49%	47%	39%
	▸ Disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like "regularly" or "periodically"	34%	18%	18%	13%
Category: Statements on cybersecurity risk					
Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%	100%
	Included data privacy as a risk factor	99%	99%	99%	95%
Category: Risk management					
Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	96%	94%	91%	87%
	Disclosed alignment with external framework or standard	10%	3%	3%	1%
	Referenced response readiness, such as planning, disaster recovery or business continuity considerations	64%	61%	57%	55%
	Stated that preparedness includes simulations, tabletop exercises or response readiness tests	5%	6%	3%	3%
	Stated that the company maintains a level of cybersecurity insurance	42%	35%	35%	31%
	Included cybersecurity in executive compensation considerations	12%	8%	3%	1%
Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	34%	29%	25%	18%
Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	10%	9%	10%	6%
Use of external advisor	Disclosed use of an external independent advisor	22%	17%	14%	17%
	Disclosed board engagement with an external independent advisor	6%	5%	4%	3%
	Disclosed that the external advisor provided an attestation opinion	0%	0%	0%	0%

Percentages are based on total disclosures by companies. Data is based on the 77 companies listed on the 2021 Fortune 100 list that filed Form 10-K filings and proxy statements in 2018, 2019, 2020 and 2021 through May 31, 2021.

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

What we found

Many companies are enhancing their cybersecurity disclosures related to the identification of director skills and expertise and insights into management's reporting to the board. Over time, there have also been notable increases in disclosures related to the assignment of board-level committee oversight and discussing workforce education and training efforts and cybersecurity insurance.

We also see modest increases in companies disclosing the alignment of their cybersecurity program and information security practices with an external framework and including cybersecurity in executive compensation considerations. We continue to see opportunities for companies to disclose practices that are prevalent in the market and vital to enhancing cyber resiliency. Such practices include collaboration with peers, industry groups or policymakers, as well as the use of cyber readiness simulations and using external expertise.

Identification of director skills and expertise

The most significant disclosure shift we've observed in four years is the change in cybersecurity expertise on the board. In 2021, 65% of boards disclosed cybersecurity as an area of expertise sought on the board or cited in a director biography, up from 36% in 2018. Notably, a majority (56%) now cite cybersecurity in at least one director biography, up from 44% last year and 27% in 2018.

A closer look at these changes over the past year shows that for most of the companies adding cyber experience in a director biography, the change is related to a new director joining the board. These new directors include former chief information officers and information technology (IT) executives, the head of a cybersecurity company and a former leader in the US Government. For a few companies, the change reflected a change in disclosure, with the companies explicitly citing cybersecurity experience in certain director biographies one year, but not the other. In one instance, this related to a director completing a cybersecurity oversight certification. The disclosures indicate that companies are paying more attention to noting director experience or expertise in cyber.

Management reporting to the board

The next area in which we're seeing disclosure enhancements over time regards management reporting to the board. This year, just over two-thirds (69%) of companies provided insights into management's reporting to the board or committee overseeing cybersecurity matters, up from 58% in 2018.

While that change is notable, the real change we're seeing is around the specific information companies are providing in this area. In 2021, 44% of companies identified at least one person who is reporting to the board about cybersecurity, most often the chief information security officer (CISO) or chief information officer (CIO). That's up from 26% in 2018. Similarly, this year 34% of companies disclosed that management is reporting to the board about cybersecurity at least annually or quarterly, up from 13% in 2018. Many other companies include language about the frequency of management reporting, but it usually is not specific, saying that the board receives reports regularly or periodically.

Adding specificity in this area of disclosure may help stakeholders recognize the board is engaging with the CIO or CISO on an appropriate cadence to conduct its oversight. While it is common for either the CIO or CISO to routinely brief the board, many directors indicate they intentionally raise cyber risks in their interactions with other members of management. In doing so, directors invoke a heightened tone at the top, as well as demonstrating that cyber is viewed as an enterprise risk, not just an IT risk.

Board-level committee oversight

Ninety percent of companies this year charged at least one board-level committee with cybersecurity oversight, up from 87% last year and 75% in 2018. Audit committees remain the primary choice for those responsibilities. This year, 68% of boards assigned cybersecurity oversight to the audit committee, up from 58% in 2018. Among the boards assigning cybersecurity oversight responsibilities to the audit committee, only about two-thirds (65%) formalize those responsibilities in the audit committee charter.

Since 2018, we've observed a significant increase in boards assigning cybersecurity oversight to non-audit committees, most often risk or technology committees. Specifically, this year 30% of boards assigned cyber to a non-audit committee, up from 19% in 2018. Among the boards assigning such responsibilities to non-audit committees, all include those responsibilities in the charter.

"

Since 2018, we've observed a significant increase in boards assigning cybersecurity oversight to non-audit committees, most often risk or technology committees.

Institutional Shareholder Services Inc. adds cyber risk factors to its Governance QualityScore methodology

In February 2021, Institutional Shareholder Services Inc. (ISS) announced methodology changes to its Governance QualityScore rating solution, including the addition of 11 new factors concerning information security risk oversight and management. The factors relate to:

- How many directors with information security experience are on the board
- How often senior leadership briefs the board about information security matters
- The company's approach to identifying and mitigating information security risks
- Whether the company is externally audited or certified by top information security standards
- Whether the company maintains a cyber risk insurance policy
- The existence and related impacts of recent security breaches, and more[1]

A number of the new factors ISS announced that it is considering correspond to disclosure enhancements we're seeing in this year's proxy statements and Form 10-K filings, including disclosures related to director qualifications and experience, management's reporting to the board, and the use of external security standards or frameworks. We expect that the ISS change will be among many factors shaping the continuing changes in company cyber disclosures, including the impact of more companies enhancing their disclosures, and thereby raising the standards across peers.

Alignment with an external framework or standard

This year, the number of companies that disclosed the alignment of their cybersecurity program and information security practices to external security process or control frameworks increased to 10%, up from 1% in 2018. The most common framework cited was the National Institute of Standards and Technology's (NIST) cybersecurity framework, which was cited by 6% of companies. Other information security frameworks or reporting standards cited include the International Organization for Standardization (ISO) 27001 (3%), NIST 800-53 (3%) and more. In addition, a number of companies disclosed that certain portions of their cybersecurity 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 (1%).

Compensation incentives

While still modest, this year we also observed an increase in companies including cybersecurity or privacy in executive pay considerations. Twelve percent of companies did so, up from 8% last year, 3% in 2019 and 1% in 2018. These companies generally cited cyber considerations (e.g., enhancing the company's cybersecurity and privacy posture, leading cybersecurity teams in navigating the shift to working from home) among a host of other nonfinancial company or individual executive officer performance considerations in their executive pay decisions.

> "This year, the number of companies that disclosed the alignment of their cybersecurity program and information security practices to external security process or control frameworks increased to 10%, up from 1% in 2018.

[1] "ISS ESG Unveils 2021 Methodology Enhancements for Governance QualityScore," *Institutional Shareholder Services website*.

Response readiness simulations and tabletop exercises

This year, the percentage of companies disclosing that they performed cyber incident simulations or tabletop exercises remained largely the same. Of the handful of companies communicating that simulations, drills or tabletop exercises were conducted at the management level, none disclosed whether the board was involved in those exercises.

Simulations are a critical risk preparedness practice that EY professionals and others believe companies should prioritize. Even the most robust cybersecurity program can never eliminate all of the risk of a material cyber incident requiring board involvement. If plans are not practiced and a breach occurs, the reaction by the board and management is largely improvised. Well-designed incident simulations and tabletop exercises can stress-test the organization and improve its readiness by providing clarity of roles, protocols and escalation processes. Policies on ransomware also should be established, including whether the company and board would approve payment, and under which circumstances. Management should conduct these exercises to test the company's significant vulnerabilities and determine where the greatest financial impact is at stake. Boards should consider participating in these simulations so 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. Practice is key to ensuring preparation and responding effectively.

Use of an external independent advisor

The percentage of companies disclosing the use of an external independent advisor to support management grew from 17% to 22% this year. Among the 17 companies that made the disclosure in 2021, only five indicated that the board received reports from the independent third party. The National Association of Corporate Directors (NACD) and the Internet Security Alliance's *Cyber-Risk Oversight: Key Principles and Practical Guidance for Corporate Boards* encourages boards to consider having deep-dive briefings from independent third-party experts validating whether the company's cybersecurity risk management program is meeting its objectives.

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

> "Simulations are a critical risk preparedness practice that EY professionals and others believe companies should prioritize.

Disclosure of cyber incidents

Disclosures around material cybersecurity incidents decreased from 12% last year to 9% this year. This year, only seven companies disclosed cyber incidents, with each company disclosing a single incident. The most recent disclosed incident occurred in 2019, with the rest having occurred as far back as 2006. The depth of the disclosures varied. Disclosures ranged from stating that an incident occurred 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.

A recent report by Audit Analytics, *Trends in Cybersecurity Breaches*, examining cybersecurity breaches affecting public companies from 2011 to 2020 found that the number of reported incidents climbed to a high of 144 in 2019, up from just 28 in 2011, and dropped down to 117 in 2020. The report noted that 2020 still had the third most cyber breach disclosures on record.

Sample language from 2021 Fortune 100 proxy statements

Management reporting structure and frequency

> *"As part of its program of regular oversight, the Risk Committee is responsible for overseeing cyber risk, information security, and technology risk, including management's actions to identify, assess, mitigate, and remediate material cyber issues and risks. The Risk Committee receives quarterly reports from the Chief Information Security Officer and the Chief Technology Risk Officer on the Company's technology and cyber risk profile, enterprise cyber program, and key enterprise cyber initiatives. The Risk Committee annually reviews and recommends the Company's information security policy and information security program to the Board for approval. At least annually, the Board reviews and discusses the Company's technology strategy with the Chief Information Officer and approves the Company's technology strategic plan. In addition, the Risk Committee participates in quarterly cyber education sessions."*

Response readiness and tabletop exercises

> *"We have a robust Cyber Crisis Response Plan in place that provides a documented framework for handling high severity security incidents and facilitates coordination across multiple parts of the Company. We deploy a defense-in-depth strategy with multiple layers of controls including embedding security into our technology investments. We invest in threat intelligence and are active participants in industry and government forums to improve sector cybersecurity defense. We collaborate with our peers in the areas of threat intelligence, vulnerability management and response and drills. We routinely perform simulations and drills at both a technical and management level. We incorporate external expertise and reviews in all aspects of our program."*

Use of external independent advisor and board engagement

> *"Best practices include: utilizes a cybersecurity advisor to provide objective assessments of Company's capabilities and to conduct advanced attack simulations. We are continually enhancing information security capabilities in order to protect against emerging threats, while increasing the ability to detect system compromise and recovery should a cyber attack or unauthorized access occur. The cybersecurity program is regularly reviewed and tested by the Company's internal audit function with quarterly status reports provided to the Audit Committee and the full Board. The Audit Committee receives semiannual reports from its independent cybersecurity advisor."*

Alignment to external framework or standard

> *"We structured our formal cybersecurity program around the National Institute of Standards and Technology, or NIST, Cybersecurity Framework, contractual requirements and other global standards. We leverage industry and government associations, third-party benchmarking, audits and threat intelligence feeds to ensure the effectiveness of our functions and proactive allocation of our resources."*

Our market observations

EY professionals regularly engage with boards and host gatherings of directors and cybersecurity experts to discuss challenges and leading practices for overseeing cybersecurity risk. This includes a series of director dialogues involving over 500 directors. Based on insights shared through these engagements with directors, as well as what EY cybersecurity professionals are doing around the globe and across industries and companies of varying sizes, we have identified the following leading board practices:

- **Set the tone.** Establish cybersecurity as a key consideration in all board matters.
- **Stay diligent.** Address new issues and threats stemming from remote work and the expansion of digital transformation.
- **Determine value at risk.** Reconcile value at risk in dollar terms against the board's risk tolerance, including the efficacy of cyber insurance coverage.
- **Embed security from the start.** Embrace a "trust by design" philosophy when designing new technology, products and business arrangements.
- **Independently assess the cybersecurity risk management program.** Obtain a recent and rigorous third-party assessment of the cybersecurity risk management program with their direct feedback presented to the board.
- **Understand escalation protocols.** Include a defined communication plan detailing when the board should be notified, including ransomware incidents.
- **Manage third-party risk.** Understand management's processes to identify, assess and manage the risk associated with service providers and the supply chain.
- **Test response and recovery.** Enhance enterprise resiliency by conducting rigorous simulations, including restoring off-site backups and testing recovery time and arranging protocols with third-party specialists before a crisis.
- **Monitor evolving practices and the regulatory and public policy landscape.** Stay attuned to evolving oversight practices, disclosures, reporting structures, metrics, and regulatory and public policy developments.

US public policy environment

In the wake of the SolarWinds and Colonial Pipeline cybersecurity incidents, the Biden Administration and Congress have increased the federal government's focus on how to prevent and respond to cyber attacks. While there have been numerous congressional hearings and related legislation introduced, it is unclear whether new laws will be enacted. However, the administration has taken some significant executive actions in the first year of the Biden presidency. The Securities and Exchange Commission (SEC) also is taking action on cybersecurity, including an expected rule proposal on cybersecurity risk disclosures, and states are deploying a patchwork of cybersecurity laws.

Biden Administration

President Biden signed an executive order (EO) on May 12 that seeks to remove barriers to information sharing between the government and private sector to allow information and operation technology service providers to report breaches without fear of legal consequences. The EO encourages new standardized contract language requiring that certain government contractors providing information and communications technology services to the government collect and share information regarding cybersecurity incidents. When issuing the EO, the White House highlighted that recent cyber incidents "share commonalities, including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents."

The May EO was just the first administration step intended to fortify US cyber defenses. In July, the Senate confirmed Jen Easterly to lead the Cybersecurity and Infrastructure Security Agency (CISA) and Chris Inglis to serve as the country's first National Cyber Director. With key personnel in place, the administration is expected to continue to emphasize development of a national cyber strategy and take additional actions to improve coordination between the government and private sector on cyber attack mitigation and cyber readiness.

For example, at a summit on August 25, the administration announced that the National Institute of Standards and Technology (NIST) will work with industry to develop a new framework for public and private entities on how to build secure technology and assess the security of technology in addition to a number of commitments from private sector leaders to invest in the cybersecurity workforce, technologies and practices. With legislation difficult to pass, we expect the Biden Administration to continue to push action through its executive powers and voluntary commitments from industry.

Congressional action

Related legislation in Congress would extend the requirement to report cyber incidents beyond the government contractor community. In July 2021, Sens. Mark Warner, D-Va., Marco Rubio, R-Fla., and Susan Collins, R-Maine, introduced the Cyber Incident Notification Act of 2021, which, if enacted, would represent the first federal mandate for certain entities to report cybersecurity breaches. As introduced, the legislation would require federal agencies, federal contractors, critical infrastructure owners and others to report cyber incidents to the CISA at the U.S. Department of Homeland Security within 24 hours.

Passage of a national cybersecurity reporting law was also recommended by the Cyberspace Solarium Commission (established by the 2019 National Defense Authorization Act to develop a strategic approach to protecting the US against cyber attacks). The Solarium Commission further suggested amending the Sarbanes-Oxley Act (SOX) to include public company cybersecurity requirements to be overseen by the SEC. Noting that the "cybersecurity of a public traded company is a critical component of its financial condition," the report recommends amending SOX to mandate public company responsibility for the security of information systems, the performance of cybersecurity risk assessments, the maintenance of internal records regarding those assessments, and "management assessments and attestation of plans to manage risk from information systems and data." While 25 of the Solarium Commission's recommendations have been enacted, Congress has not yet made progress on the Commission's disclosure recommendations.

The Cybersecurity Disclosure Act of 2021 is another proposal that is pending before Congress. The bipartisan bill introduced by Sen. Jack Reed, D-R.I., and supported by Sen. Susan Collins, R-Maine, would direct the SEC to issue final rules requiring a registered public company to disclose in its annual report or annual proxy statement whether any member of its board has expertise or experience in cybersecurity. If no member of the board has cybersecurity expertise, the company would report which other aspects of the company's cybersecurity were considered by those nominating and evaluating board members. Although the bill has been introduced in the last several sessions of Congress, it has yet to be considered by the Senate.

The SEC

The SEC also is taking action on cybersecurity, placing a rule proposal to require cybersecurity risk governance disclosures on its regulatory agenda for later this year. This followed a May 2021 appropriations hearing at which SEC Chair Gary Gensler stated that there is an investor appetite for such disclosures. The Commission last provided guidance to publicly traded companies about cyber-related disclosures in 2018. This guidance provides the Commission's views about the application of the federal securities laws to cybersecurity issues. In particular, the guidance highlights the importance of cybersecurity policies and procedures, including disclosure controls, as well as the application of insider trading rules in the cybersecurity context.

Since taking his seat as SEC Chair in April, Gensler has emphasized the Commission's role as a "cop on the beat." Thus, it is expected that the Division of Enforcement will continue to vigorously pursue investigations relating to cybersecurity issues — also a priority under former SEC Chairman Jay Clayton. In June and August, the Commission settled cases and fined companies with deficient cybersecurity disclosures.

"

While 25 of the Solarium Commission's recommendations have been enacted, Congress has not yet made progress on the Commission's disclosure recommendations.

In the states

The COVID-19 pandemic caused disruption and major shifts in the way governments and businesses operated in the past year, and a lack of congressional action has prompted states to deploy a patchwork of cybersecurity laws.

The SolarWinds incident, in addition to impacting the federal government and the systems of many companies, also resulted in breaches of state and local government systems, making cybersecurity a priority for many state lawmakers.

During the 2020–21 state legislative sessions, 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that significantly deal with cybersecurity. The primary issues legislators attempted to tackle include:

- Requiring notification of governments and consumers about cybersecurity incidents
  - Reporting timelines and responsible parties vary across states, but this remains a growing trend being addressed legislatively
- Requiring government agencies to implement cybersecurity training; set up and follow formal security policies, standards and practices; and plan for and test how to respond to a security incident
- Regulating cybersecurity within the insurance industry or addressing cybersecurity insurance
- Creating task forces, councils or commissions to study or advise on cybersecurity issues
- Supporting programs or incentives for cybersecurity training and education

“

During the 2020-21 state legislative sessions, 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that significantly deal with cybersecurity.

Conclusion

The rapid transformation of today’s business environment continues to bring new risks and opportunities. During the pandemic, new cybersecurity vulnerabilities emerged that continue to threaten businesses today. At the same time, cybersecurity has become essential to enabling growth and building stakeholder trust.

Our analysis of 2021 cybersecurity-related disclosures found that companies are enhancing their cybersecurity disclosures and providing clarity around topics like director expertise, management reporting to the board and committee oversight. We also see emerging trends related to the use of external frameworks or standards and including cybersecurity in executive compensation considerations. Still, opportunities remain for companies to strengthen their cybersecurity disclosures to demonstrate accountability and engagement on this issue, and build stakeholder trust around how cybersecurity is prioritized, managed and overseen as a critical enterprise risk and strategic opportunity.

Questions for the board to consider

- What kinds of threats is the company most concerned about? How does the company monitor the evolving landscape of threats? 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 critical 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 to escalate to the board?
- What kinds of policies has the company established on ransomware? How has the company and board approached the issue of payment?
- Has the board participated with management in one of its cyber breach simulations in the last year? How rigorous was the testing?
- Is the board allocating sufficient time on its agenda, and is the committee structure appropriate, to provide effective oversight of cybersecurity?
- Have appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis and given a dollar value?
- 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 cybersecurity risk management program is meeting its objectives? If so, is the board having a direct dialogue with the third party about the scope of work and the findings?
- Do the company's disclosures effectively communicate the rigor of its cybersecurity risk management program and the related board oversight?
- 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. 13878-211US
CS no. 2108-3866937

ED None

ey.com/us/boardmatters