EY Center for Board Matters

What companies are disclosing about cybersecurity risk and oversight in 2020

Building a better working world

Cybersecurity risk is intensifying, particularly with widespread remote working and increased online interactions amid the pandemic. The rapid adaptation of multiple business processes and protocols to enable this virtual environment has exponentially increased the corporate attack surface and introduced new risks to the confidentiality, integrity and availability of critical company data and supporting systems.

The return of some workers to a physical workplace is also raising new data security risks and privacy questions, with companies collecting data related to employee, contractor and customer health such as COVID-19 testing, temperature checks and contact tracing. At the same time, harnessing new and disruptive technologies — and enabling the trust of stakeholders and the marketplace in doing so — is key to helping organizations lead, innovate and differentiate.

In this environment, remaining cyber-resilient and building stakeholder trust in the company's data security and privacy practices is a strategic imperative. Public disclosures can help build trust by providing transparency and assurance around how boards are fulfilling their cybersecurity risk oversight responsibilities.

For the third consecutive year, EY researchers have 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 76 Fortune 100 companies that filed those documents from 2018 through May 31, 2020. We focused on the areas of cybersecurity board oversight (including board-level committee oversight and director qualifications), 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 as it relates to cybersecurity, as well as perspectives from investors, directors and EY cybersecurity professionals.

What we found

Many companies are enhancing their cybersecurity disclosures, with modest increases across most of the disclosures tracked. The most significant changes this year related to the area of board oversight, including board-level committee oversight and the identification of director skills and expertise. Other notable findings include the continued scarcity of disclosures related to cyber-readiness simulations and the use of independent third-party advisors — practices that are prevalent in the market and vital to enhancing cyber resiliency from the EY perspective (see "Our Market Observations").

Fortune 100 company cybersecurity disclosures

Topic	Disclosure	2020	2019	2018
Board oversight				
Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	89%	88%	79%
Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	87%	82%	74%
	▸ Disclosed that the audit committee oversees cybersecurity matters	67%	62%	59%
	▸ Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	26%	28%	20%
Director skills and expertise	Cybersecurity included among areas of expertise sought on the board or cited in at least one director biography	58%	51%	39%
	▸ Cybersecurity included among the areas of expertise sought on the board	37%	29%	22%
	▸ Cybersecurity cited in at least one director biography	46%	41%	30%
Management reporting structure	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	61%	58%	54%
	▸ Identified at least one "point person" (e.g., the Chief Information Security Officer or Chief Information Officer)	33%	34%	25%
Management reporting frequency	Included language on frequency of management reporting to the board or committee(s), but most of this language was vague	47%	45%	38%
	▸ Disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like "regularly" or "periodically"	17%	17%	14%
Statements on cybersecurity risk				
Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%
	Included data privacy as a risk factor	99%	99%	93%
Risk management				
Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	92%	91%	83%
	Referenced response readiness, such as planning, disaster recovery or business continuity considerations	62%	57%	50%
	Stated that preparedness includes simulations, tabletop exercises or response readiness tests	7%	3%	3%
	Included cybersecurity in executive compensation considerations	5%	1%	1%
Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	29%	26%	18%
Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	12%	12%	7%
Use of external advisor	Disclosed use of an external independent advisor	16%	13%	16%
	Disclosed board engagement with an external independent advisor	5%	4%	3%

*Percentages based on total disclosures for companies. Data based on the 76 companies on the 2020 Fortune 100 list that filed Form 10-K filings and proxy statements in 2018, 2019 and through May 31, 2020. *Some companies designate cybersecurity oversight to more than one board-level committee.*

Board-level committee oversight

More boards are assigning cybersecurity oversight responsibilities to a committee. Eighty-seven percent of companies this year have charged at least one board-level committee with cybersecurity oversight, up from 82% last year and 74% in 2018. Audit committees remain the primary choice for those responsibilities. This year 67% of boards assigned cybersecurity oversight to the audit committee, up from 62% in 2019 and 59% in 2018. Last year we observed a significant increase in boards assigning cybersecurity oversight to non-audit committees, most often risk or technology committees, (28% in 2019 up from 20% in 2018), but that percentage dropped this year (26% in 2020). A minority of boards, 7% overall, assigned cyber responsibilities to both the audit and a non-audit committee.

Among the boards assigning cybersecurity oversight responsibilities to the audit committee, nearly two-thirds (65%) formalize those responsibilities in the audit committee charter. Among the boards assigning such responsibilities to non-audit committees, most (85%) include those responsibilities in the charter.

Identification of director skills and expertise

The percentage of companies discussing cybersecurity in the context of director qualifications has increased significantly in recent years. In 2020, 58% of companies included cybersecurity as an area of expertise sought on the board or cited in a director biography, up from 51% last year and 39% in 2018. However, a few companies explicitly cited cybersecurity experience in certain director biographies one year but not the other. The disclosures indicate that companies are paying more attention to noting director experience or expertise in cyber.

Data privacy

Nearly all (99%) companies we reviewed addressed data privacy in the risk factor disclosures included in their 2020 and 2019 10-K filings, compared with 93% in 2018. The degree of explicit focus on data privacy as a material risk varied widely. Around a quarter (24%) focused on data privacy as a stand-alone risk factor, often noting increasingly complex and changing data privacy regulations that create high financial and legal exposure in addition to the reputational and operational risks involved. Thirty-percent grouped data privacy with cybersecurity as a risk factor, addressing the overlapping risks in tandem. Just under half (45%) of the companies addressed data privacy in the context of broader risk factors, generally those related to information technology or regulatory risks.

Industry trends were not pronounced. Companies from industries where data privacy risks are less prominent (e.g., energy and industrials) were among those that treated data privacy as a unique risk factor, and companies from industries with significant data privacy risks (e.g., health care, financial services, consumer discretionary and consumer staples) were among those that addressed data privacy only in the context of broader risks.

Compensation incentives

Five percent of companies included cybersecurity in executive pay considerations, generally as a qualitative factor considered relative to annual incentive pay. Notably, over the past three years a few companies have received shareholder proposals seeking to integrate cybersecurity metrics into compensation incentives for senior executives. However, none of those companies was among the few that we captured during our review. The proposals that went to a vote averaged 17% support, with the targeted companies generally explaining that there is not necessarily a correlation between a senior executive's actions and the prevention of cybersecurity incidents, or that the consideration already exists as part of an individual executive's overall performance, if applicable.

Response readiness simulations and tabletop exercises

While the percentage of companies disclosing that they performed cyber-incident simulations or tabletop exercises more than doubled from 3% last year to 7% in 2020, the number of companies making this disclosure remains low. 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 these exercises.

Simulations are a critical risk-preparedness practice that EY leaders and others believe companies should prioritize. Even the most robust cybersecurity program can never eliminate all risk. If plans are not practiced and a breach occurs, the reaction is largely improvised. Well-designed incident simulations and tabletop exercises can stress-test the organization and improve readiness by providing clarity of roles, protocols and escalation processes. Management should conduct these exercises to test the company's significant vulnerabilities and where the greatest financial impact is at stake. Boards should consider participating in at least one of these simulations annually.

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 maintaining preparation and responding effectively.

Use of external independent advisor

The number of companies disclosing the use of an external independent consultant to support management held fairly steady, with 12 companies making the disclosure this year vs. 10 in 2019 and 12 in 2018. Among the companies making the disclosure in 2020, only four made clear that the board met directly with the independent third party. The National Association of Corporate Directors (NACD) and the Internet Security Alliance's recently updated *Director's Handbook on Cyber-Risk Oversight* encourages boards to consider having deep-dive briefings from independent third-party experts validating whether the company's cybersecurity program is meeting its objectives. Our research did not identify any discussion of whether an attestation opinion was obtained utilizing the American Institute of Certified Public Accountants' System and Organization Controls for Cybersecurity framework, which provides for an entity-wide independent assessment of the company's cybersecurity risk management program.

Sample 2020 Fortune 100 disclosures

Management reporting structure and frequency

> *As part of its program of regular oversight, the Risk Committee is responsible for overseeing cybersecurity risk, information security, and technology risk, as well as management's actions to identify, assess, mitigate, and remediate material issues. The Risk Committee receives regular quarterly reports from the Chief Information Security Officer and the Chief Cybersecurity Risk Officer on the Company's cybersecurity risk profile and enterprise cybersecurity program and meets with the Chief Information Security Officer at least quarterly. 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.*

Response readiness and tabletop exercises

> *We have a robust Cyber Crisis Response Plan in place which provides a documented framework for handling high severity security incidents and facilitates coordination across multiple parts of the Company. 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. All colleagues receive annual cybersecurity awareness training.*

Use of external independent advisor and board engagement

> *We continued an industry leading practice of engaging an independent cybersecurity advisor for the fourth year in a row and reviewed a cyber crisis simulation exercise that was used by our senior leaders to prepare for a possible cyber crisis. The audit committee regularly receives reports from its independent advisor regarding our cybersecurity program.*

Sample charter language on key cybersecurity oversight responsibilities

> - *Oversee the Corporation's cybersecurity plan, business continuity program, information protection management strategy and related risks to all of these areas.*
> - *Review the Corporation's cyber insurance policies to ensure appropriate coverage.*
> - *Review the Corporation's development and training plan for critical IT staff as well as succession planning.*

Our market observations

Over the past two years, EY leaders have regularly engaged with boards and hosted gatherings of directors and cybersecurity experts to discuss challenges and leading practices for overseeing cybersecurity risk. This includes a series of director dialogues in late 2019 and throughout 2020 involving over 500 directors. Earlier in 2020, we released recommended questions that boards, and particularly audit committees, should consider to be more vigilant with their oversight of cybersecurity risks in today's post-COVID-19 virtual work environment.

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 company sizes, we have identified the following leading board practices:

- **Set the tone.** Demonstrate that cybersecurity and privacy risk are critical business issues by increasing the board and/or committee's time and effort spent discussing the topic.
- **Stay up-to-date.** Increase the frequency of board and/or committee updates on specific actions to address new cybersecurity and privacy issues and threats as a result of the seismic shift to remote work. This includes having regular unfiltered board discussions with the CISO in executive sessions.
- **Determine value at risk.** Understand the company's value at risk in dollars beyond insurance and reconcile against the board's risk tolerance.
- **Embed security from the start.** Embrace a "Trust by Design" philosophy by designing new technology, products and business arrangements with security in mind.
- **Independently assess the Cybersecurity Risk Management Program (CRMP).** Confirm the CRMP is independently and appropriately assessed by a third party with their direct feedback to the board.
- **Understand protocols.** Obtain a thorough understanding of the cybersecurity incident and breach escalation process and protocols, including a defined communication plan for when the board should be notified.
- **Manage third-party risk.** Understand management's processes to identify, assess and manage the risk associated with service providers and the supply chain. Also, consider the need for an assessment to cover third-party risks across the company's supply chain.
- **Test response and recovery.** Enhance enterprise resilience by having the company's ability to respond and recover tested through simulations and arranging protocols with third-party professionals before a crisis.
- **Monitor evolving practices.** Stay attuned to evolving board and committee cybersecurity oversight practices and disclosures, including benchmarking against peer disclosures for the last two to three years.

Disclosure of cyber incidents

Disclosures around material cybersecurity incidents are steadily rising but remain low at 13%, up from 12% in 2019 and 7% in 2018. In 2020, 10 companies disclosed cyber incidents, with each company disclosing a single incident. Only one of those events had occurred in the past year, with the rest as far back as 2006. Around a third of the disclosed data breaches related to cyber attacks of third-party service providers. The depth of the disclosures varied, often based on how recent the event was. Disclosures ranged from stating the occurrence of an incident and related broad implications to providing a more in-depth account, including the number of account holders affected, the nature of the data and remedial steps taken to fix the security vulnerability.

A recent report by Audit Analytics, *Trends in Cybersecurity Breach Disclosures*, examining cybersecurity breaches affecting public companies from 2011 to 2019 found that the number of reported incidents climbed to a high of 140 in 2019, a 400% increase since 2011. The report also found that on average it took firms more than 100 days to discover that a breach had occurred.

Investor perspectives

Cybersecurity remains an investor engagement priority. As part of our annual EY Center for Board Matters investor outreach, in the fall of 2019 we asked more than 60 institutional investors representing more than US$35 trillion in assets under management what they view as the biggest threats to portfolio companies' strategic success in the next three to five years. Cybersecurity and data privacy ranked third among the key risks they cited, and these conversations took place well in advance of COVID-19 and the resulting acceleration of remote work.

Investors generally commented that every company in every industry has exposure to these risks, and that as consumer preferences and business-efficiency demands lead to an ever more digitized and electronically connected world, the risks continue to multiply. In the wake of COVID-19, those risks have indeed multiplied even since those investor outreach discussions took place.

Because the threat of a breach cannot be eliminated, some investors stressed that they are particularly interested in resiliency, including how (and how quickly) companies are detecting and mitigating cybersecurity incidents. Some are asking their portfolio companies about specific cybersecurity practices, such as whether the company has had an independent assessment of its cybersecurity program, and some are increasingly focusing on data privacy and whether companies are adequately identifying and addressing related consumer concerns and expanding regulatory requirements.

SEC guidance

The SEC continues its broad spotlight on cybersecurity.[1] In a January 2020 report, the SEC's Office of Compliance and Inspections noted that "[t]he seriousness of threats and the potential consequences to investors, issuers, and other securities market participants, and the financial markets and economy more generally, are significant and increasing."[2] With the COVID-19-driven accelerated shift to digital business and massive, potentially permanent shifts to remote working, including virtual board and executive management meetings, cybersecurity risks are exponentially greater.

The SEC's Division of Corporation Finance also issued guidance in December 2019 relating to disclosure of intellectual property and technology risks associated with international operations in view of increased reliance on digital technology to conduct and manage business.[3] The Division's guidance states, in part, that:

> *We encourage companies to assess the risks related to the potential theft or compromise of their technology, data or intellectual property in connection with their international operations, as well as how the realization of these risks may impact their business, including their financial condition and results of operations, and any effects on their reputation, stock price and long-term value. Where these risks are material to investment and voting decisions, they should be disclosed, and we encourage companies to provide disclosure that allows investors to evaluate these risks through the eyes of management. Importantly, disclosure about these risks should be specifically tailored to a company's unique facts and circumstances. In this same vein, where a company's technology, data or intellectual property is being or previously was materially compromised, stolen or otherwise illicitly accessed, hypothetical disclosure of potential risks is not sufficient to satisfy a company's reporting obligations. We believe that companies should continue to consider this evolving area of risk and evaluate its materiality on an ongoing basis.*

The Division's guidance also reiterates the SEC's 2018 guidance, which clarified companies' obligations to disclose cybersecurity risks, material breaches and the potential impact of the breaches on business, finances and operations — the goal being to enable investors to make more risk-informed investment decisions.[4] Both the Division's and the Commission's guidance remind companies that a number of existing SEC disclosure requirements could require disclosure of cybersecurity matters, including in the business section, legal proceedings, MD&A, financial section, disclosure controls and procedures, board role in risk management, and risk factors.

> "From an issuer disclosure perspective, it is important that investors are sufficiently informed about the material cybersecurity risks and incidents affecting the companies in which they invest.
>
> **Jay Clayton, SEC Chairman**

The SEC has also emphasized the importance of strong disclosure controls and procedures to enable timely and accurate disclosures of cybersecurity risks and incidents, and clear insider trading prohibitions related to cybersecurity incidents.[5]

The SEC staff looks at and comments on cybersecurity-related disclosures as part of its regular reviews of public company filings. The staff also monitors news reports of cyber breaches to assist in this process.[6] The SEC staff has said it does "not second-guess good faith exercises of judgment about cyber-incident disclosures. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action could be warranted."[7] One such case has already been brought.[8] Additionally, the SEC has brought a case against a company for misleading investors about the risks it faced from misuse of user data.[9]

---

1 See Spotlight on Cybersecurity, the SEC and You, U.S. Securities and Exchange Commission.

2 Cybersecurity and Resiliency Observations, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, January 2020.

3 Intellectual Property and Technology Risks Associated with International Business Operations, Division of Corporation Finance, U.S. Securities and Exchange Commission, December 2019.

4 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, U.S. Securities and Exchange Commission Statement, 2018. See also "SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks," speech by SEC Chairman Jay Clayton, 6 December 2018; EY publication *2018 AICPA Conference on Current SEC and PCAOB Developments*.

5 See also EY's *How the SEC views cybersecurity disclosures and board's oversight role*.

6 "SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks," speech by SEC Chairman Jay Clayton, 6 December 2018; EY publication *2018 AICPA Conference on Current SEC and PCAOB Developments*.

7 Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, SEC press release, 24 April 2018.

8 Ibid.

9 Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, SEC press release July 24, 2019.

US public policy environment

Policymakers in Washington continue to grapple with how to address rising and evolving cyber threats. While a legislative solution is unlikely in 2020, it remains a key concern and focus for Congress and the administration.

In March 2020, the Cyberspace Solarium Commission, established in the 2019 National Defense Authorization Act to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences," issued its congressionally directed report urging the US to adopt a "layered cyber deterrence" plan to reduce the occurrence and impact of cyber attacks through (1) shaping responsible cyberspace behavior, (2) denying benefits to those who engage in inappropriate actions, and (3) imposing costs on actors who target America in cyberspace. The report makes 80 recommendations across six pillars of reform, including amending the Sarbanes-Oxley Act (SOX) to include cybersecurity reporting requirements. Noting that the cybersecurity position of a public sector company is a critical component of its financial condition, the report recommends amending SOX to specify the corporate responsibility requirements for the security of information systems; the performance and recording 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." Congress has not yet made progress toward adopting these recommendations into law.

The Cybersecurity Disclosure Act of 2019 is another proposal that is pending before Congress. The bipartisan bill introduced by Sen. Jack Reed (D-RI) and supported by Sen. Susan Collins (R-ME), 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. Differing from bills introduced in previous congressional sessions, this version permits a company to disclose why having cyber expertise on the board is not necessary because of other cybersecurity protocols put in place by the company. The House Financial Services Committee approved the legislation, which was introduced by Rep. Jim Himes (D-CT), in December 2019, but no further action has been taken in Congress.

Finally, on the administrative front, the Federal Trade Commission announced that its data security orders would include provisions that "improve data security practices and provide greater deterrence." Among these provisions, the FTC will mandate that "every year companies must now present their Board or similar governing body with their written information security program — and, notably, senior officers must now provide annual certifications of compliance to the FTC." These requirements will only be applicable to companies that are subject to FTC consent orders, but the announcement demonstrates how companies' managing of cybersecurity risks will remain a key focus of Congress and other policymakers in Washington.

The lack of congressional action has pushed states to deploy a patchwork of cybersecurity laws. State legislative action surrounding cybersecurity increased during the last session, with over 230 bills introduced related to the creation of cybersecurity task forces, mandatory training of state employees, data breach penalty and notification requirements on private businesses and more. Expect to see states continue to evolve in this space to combat the growing concerns of cybersecurity given the current, and in some cases, permanent increase of remote work.

Conclusion

Digital strategy and technology infrastructure have become critical elements of competitive differentiation, even survival, in today's business environment. At the same time, the rapid acceleration of remote working and learning, online interactions and new disruptive technologies are introducing new vulnerabilities and reshaping the cybersecurity threat landscape. Securing an organization's virtual ecosystem and building trust around that security is more important than ever to future resiliency and value creation.

When data confidentiality, integrity or availability is compromised, or products and services cease to perform as expected, trust built over years can be lost in a day — and stakeholder expectations around, and scrutiny of, security and privacy protections continue to increase. Companies should 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

- Is the board allocating sufficient time on its agenda, and is the committee structure appropriate, to provide effective oversight of cybersecurity?
- Do the company's disclosures effectively communicate the rigor of its cybersecurity risk management program and related board oversight?
- 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?
- Have appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis and given a dollar value?
- How does management evaluate and categorize identified cyber and data privacy incidents and determine which to escalate to the board?
- Has the board leveraged a third-party assessment, as described in the NACD's *Cyber-Risk Oversight 2020* handbook, to validate the cybersecurity 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 participated with management in one of its cyber breach simulations in the last year?
- 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 | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

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. 09999-201US
CS no. 2007-3544129

ED None

ey.com/us/boardmatters