EY Center for Board Matters

Cybersecurity disclosure benchmarking

Building a better working world

Boards, executives, investors, regulators and other governance stakeholders have expressed growing interest in understanding how companies guard against, plan for and respond to cybersecurity incidents.

As cybersecurity threats evolve and risks become more complex and widespread, focus on corporate disclosures in public filings on the subject likely will intensify.

Cybersecurity crime is an increasing threat with unique challenges resulting from the complexity of an interconnected business ecosystem and the rapid evolution in technology. While the U.S. Securities and Exchange Commission (SEC) has required registrants to disclose information about business risks and material developments in their annual reports for decades, companies face particular challenges in publicly reporting cybersecurity threats. This is due in part to the need to disclose material information while keeping potentially sensitive information out of the hands of attackers.

To help inform stakeholders, we conducted an analysis of cybersecurity-related disclosures of Fortune 100 companies. These companies often are leaders as governance disclosure practices continue to evolve. The review was based on two prominent investor-facing public filings: proxy statements and Form 10-K filings.

Our observations revealed that the depth and nature of cybersecurity-related disclosures vary widely, suggesting there is opportunity for enhancement in how cybersecurity risks, cybersecurity risk management frameworks and board oversight are communicated. This report seeks to provide companies and other stakeholders with insights on this quickly evolving area of disclosure.

Our perspective

Cybersecurity-related risks are complex, which can make it challenging to provide meaningful information to investors and other stakeholders without disclosing facts that could harm company efforts to protect data security.

In the wake of several major cybersecurity incidents, companies, investors and policymakers have been re-examining what and when information is communicated by companies and opportunities for enhanced disclosure.

There are many forces driving the increased focus on corporate disclosures around cybersecurity-related risks and incidents, several of which are outlined in this report. Our aim is to enhance consideration and discussions around cybersecurity-related disclosures by offering insights on current disclosures, along with perspectives on the topic from regulators, investors and boards of directors.

Current regulatory landscape

2018 cybersecurity guidance from the SEC

The SEC issued guidance on 21 February 2018 "... to assist public companies in preparing disclosures about cybersecurity risks and incidents." In framing the matter and the SEC's motivation in issuing it, the guidance states that "Cybersecurity risks pose grave threats to investors, our capital markets, and our country. Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the US economy depend on the security and reliability of information and communications technology, systems, and networks."

The new guidance reinforces and builds on the SEC's 2011 cybersecurity staff guidance, which clarified companies' obligations to disclose cybersecurity risks, material breaches and the potential impact of the breaches on business, finances and operations. This includes two new topics: (i) the importance of public companies having strong disclosure controls and procedures to enable timely and accurate disclosures of cybersecurity risks and incidents, and (ii) insider trading prohibitions as related to cybersecurity incidents.

SEC Chairman Jay Clayton expressed his views on the guidance in a press statement stating it "... will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors." He encouraged "... public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

> There are many forces driving the increased focus on corporate disclosures around cybersecurity-related risks and incidents.

SEC officials have stated that the Division of Corporation Finance will monitor cybersecurity disclosures as part of its selective filing reviews, and encouraged stakeholders to provide feedback on the guidance. It should be noted that the timing of the 2018 SEC guidance – issued shortly before annual reports for 2017 were due to be filed and at the start of the 2018 proxy season — means that companies may not have had full opportunity to consider and implement it.

Investors view cyber as integral to risk oversight

Investors view cybersecurity risk management as a critical component of the board's risk oversight responsibilities. That is what many leading institutional investors have shared with EY during our annual investor outreach program, which most recently included conversations with more than 60 institutional investors representing US$32 trillion in assets under management.

In light of the importance of cybersecurity, some investors seek additional and enhanced disclosure from companies and engagement with boards on cybersecurity planning, risks and incidents. Investors generally want to understand how boards are actively overseeing cybersecurity risks and strategy.

Through engagement, some investors also seek to learn whether the board is receiving regular reports from management and input from third-party independent experts as appropriate.

The Council of Institutional Investors (CII) published a list of questions for investors to pose to boards in an effort to understand how they are prioritizing cybersecurity. The publication recommends that companies proactively communicate how they address cybersecurity matters as a way to enhance investor confidence and suggests that directors need to "understand management's cybersecurity strategy; learn where cybersecurity weaknesses lie; and support informed, reasonable investment in the protection of critical data and assets."

> Recent high-profile hearings on Capitol Hill highlighted broad bipartisan concerns over how companies manage, plan for and disclose cybersecurity attacks.

"Users should expect companies of various sizes, industries and cyber risk profiles to bring different strategies, in varied stages of implementation, in response to this massive and growing challenge," according to the CII. The questions posed by the CII were as follows:

1. How are the company's cyber risks communicated to the board, by whom, and with what frequency?
2. Has the board evaluated and approved the company's cybersecurity strategy?
3. How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?
4. How does the board evaluate the effectiveness of the company's cybersecurity efforts?
5. When did the board last discuss whether the company's disclosure of cyber risk and cyber incidents is consistent with SEC guidance?

Boards of directors

Boards also are increasing engagement on the subject. Consider that the recent SEC guidance states "... we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."

The National Association of Corporate Directors issued a Cybersecurity Handbook in 2017 that outlined five principles for board cybersecurity oversight. "Along with the rapidly expanding 'digitization' of corporate assets, there has been a corresponding digitization of corporate risk. Accordingly, policymakers, regulators, shareholders and the public are more attuned to corporate cyber risk than ever before," states the handbook.

According to the NACD, these are the five principles boards should consider as they seek to enhance their oversight of cybersecurity risks are:

Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Principle 3: 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.

According to the handbook, when needed, directors should look to outside experts to help them evaluate the assertions made by management and security leadership. Boards should schedule "deep-dive briefings" for independent third-party experts to help validate the extent to which the cybersecurity program is meeting objectives.

Principle 4: Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget. The handbook also recommended regular reviews of the effectiveness of the organization's cyber-risk management.

Principle 5: Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

US policy environment

While it is difficult to legislate or dictate prescriptive policy to address cybersecurity risks, the issue is being contemplated by a host of regulators and government agencies in the US and around the world. US regulators across sectors from the Federal Trade Commission to the Department of Commerce are stepping up activity in this area.

Congress is also increasing its oversight and engagement on cybersecurity disclosure and risk management. Recent high-profile hearings on Capitol Hill highlighted broad bipartisan concerns over how companies manage, plan for and disclose cybersecurity attacks. Members also have heard testimony on legislative proposals such as the Cybersecurity Disclosure Act of 2017.

The bill, introduced by Senator Jack Reed (D-RI) and supported by Senator 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.

While political headwinds and institutional challenges make passage of cybersecurity legislation unlikely in the near term, interest from Congress and other policymakers in Washington continues to increase.

> Forty-one percent of companies include cybersecurity experience as among the key director qualifications highlighted or considered by the board.

What we found

We conducted an analysis of cybersecurity-related disclosures in the proxy statements and annual reports on Form 10-K of Fortune 100 companies for which documents were available as of September 1, 2018. The analysis was based on voluntary cybersecurity-related disclosures on the following topics:

- Board oversight including risk oversight approach, board-level committee oversight, director qualifications, management reporting structure and management reporting frequency
- Statements on cybersecurity risk and strategy, including disclosure of related strategy-focused language, shareholder engagement and risk factors
- Risk management, including cybersecurity risk management efforts or program, education and training, engagement with outside security experts and use of an external advisor

The depth and company-specific nature of the disclosures vary widely, including the level of detail.

In considering these findings, note that the analysis represents disclosures at a single point in time (i.e., the date of filing) and may not reflect ongoing changes in company practices. Additionally, companies may not have had full opportunity to consider and implement the recent SEC guidance given the timing of its release.

In light of these considerations, the analysis offers an informative assessment of the current state of cybersecurity-related disclosures, which can help inform emerging best practices and further dialogue on how companies can be more effective in communicating about these issues to investors and other stakeholders.

Board oversight

Most companies disclosed that cybersecurity is among the risks overseen by the board and whether any committees are charged with oversight responsibilities regarding cybersecurity.

How management reports to the board on this topic is an emerging area for disclosure with less than half of companies disclosing this information and a smaller subset offering detail around the frequency of that reporting and what it includes.

Director qualification observations

Forty-one percent of companies include cybersecurity experience as among the key director qualifications highlighted or considered by the board. The disclosure does not always indicate which directors (if any) have this expertise, and there are variations in what is considered cybersecurity expertise.

Category	Topic	2018 Fortune 100 (% of companies reviewed)
Board oversight	Risk oversight approach	▸ 84% disclosed in the risk oversight section of the proxy statement a focus on cybersecurity
	Board-level committee oversight	▸ 84% disclosed that at least one board-level committee was charged with oversight of cybersecurity matters ▸ 70% disclosed that the audit committee oversees cybersecurity matters* ▸ 20% disclosed oversight by a non-audit-focused committee (e.g., risk, technology)
	Director qualifications	▸ 41% included cybersecurity experience among the key director qualifications highlighted or considered by the board
	Management reporting structure	▸ 41% provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters ▸ 24% identified at least one "point person(s)" (e.g., the Chief Information Security Officer or Chief Information Officer)
	Management reporting frequency	▸ 34% included language on frequency of management reporting to the board or committee(s), but most of this language was vague ▸ 11% disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like "regularly" or "periodically"
Statement on cybersecurity risk and strategy	Strategy-focused statement	▸ 14% voluntarily highlighted cybersecurity as a strategic focus in the proxy statement
	Shareholder engagement	▸ 6% disclosed that cybersecurity was a topic in shareholder engagement conversations
	Risk factor disclosure	▸ 100% included cybersecurity as a risk factor consideration with 92% prominently highlighting this topic by using a subheading or subtitle
Risk management	Cybersecurity risk management efforts or program	▸ 71% described efforts to mitigate cybersecurity risk, such as investing in personnel, training, monitoring and the establishment of processes, procedures and systems ▸ 30% referenced response planning, disaster recovery or business continuity considerations ▸ 3% stated that preparedness includes simulations, tabletop exercises, response readiness tests or independent assessments
	Education and training	▸ 15% disclosed use of education and training efforts to mitigate cybersecurity risk
	Engagement with outside security community	▸ 5% disclosed collaborating with peers, industry groups or policymakers
	Use of external advisor	▸ 14% disclosed use of an external independent advisor

Note: Percentages based on total disclosures for companies in 2018. Data based on the 79 companies on the 2018 Fortune 100 list that filed Form 10-K filings and proxy statements through 1 September 2018.

** Some companies disclose that cybersecurity is overseen by the full board and not any specific committee. Others may designate oversight to more than one board-level committee.*

Strategy-focused statement

A handful of companies highlighted in their proxy that cybersecurity is a current or emerging strategic focus, or state that data privacy is central to the company's purpose and core values.

Shareholder engagement

Some companies that disclosed engagement with investors also disclose the topics discussed during engagement. For topics beyond executive compensation, that disclosure is often high level (e.g., sustainability, risk oversight, strategy). As a result, the data here may understate the actual amount of engagement discussions involving cybersecurity.

Risk factor disclosure

All companies disclosed cybersecurity as a risk factor and provided general statements, which may or may not be company specific in nature. For example, most companies disclosed that regardless of company efforts, there still may be a breach and that in such an event, company operations may suffer.

Cybersecurity risk mitigation efforts

These disclosures cited company efforts on cybersecurity risk monitoring, training, planning and prevention, but the depth of disclosures varied widely, with few companies providing details on these efforts.

Conclusion

This report aims to enhance consideration and discussions around cybersecurity-related disclosures by offering insights on current disclosures, along with perspectives on the topic from investors, regulators and boards of directors.

Cybersecurity risk management and incidents and related disclosures are a critical issue for investors, companies and other key stakeholders. We expect the interest and focus on enhanced communication will continue to grow as the challenges continue to evolve. Recent SEC guidance on the issue is just the latest indication that regulators and stakeholders want to better understand a company's efforts around cybersecurity planning, incident response and notification procedures. As with many other emerging issues, public disclosures present an opportunity for a company to demonstrate leadership on this vital matter.

By sharing information on the state of current disclosure efforts, stakeholders can gain an understanding of where opportunities for enhancement exist, and how to drive and establish leading practices.

Questions for the board to consider

- Has the board formally assigned responsibility on cybersecurity matters — at the board and management levels?
- Does the board have access to the needed expertise on cybersecurity? And is the board getting regular updates and reports concerning cybersecurity risk strategy and event preparedness?
- Does the board have regular briefings on the evolving cybersecurity threat environment and how the cybersecurity risk management program is adapting? How is the board actively overseeing the company's investments in new cybersecurity technologies and solutions?
- Does the board know how management has performed in recent tabletop exercises simulating cybersecurity incidents – and has the board participated in any such exercises?
- Is the board hearing directly from and having a dialogue with third-party experts whose views are independent of management?
- How will the SEC guidance and investor interest impact 2019 disclosures?

Contacts

Les Brorsen
+1 202 327 5968
les.brorsen@ey.com

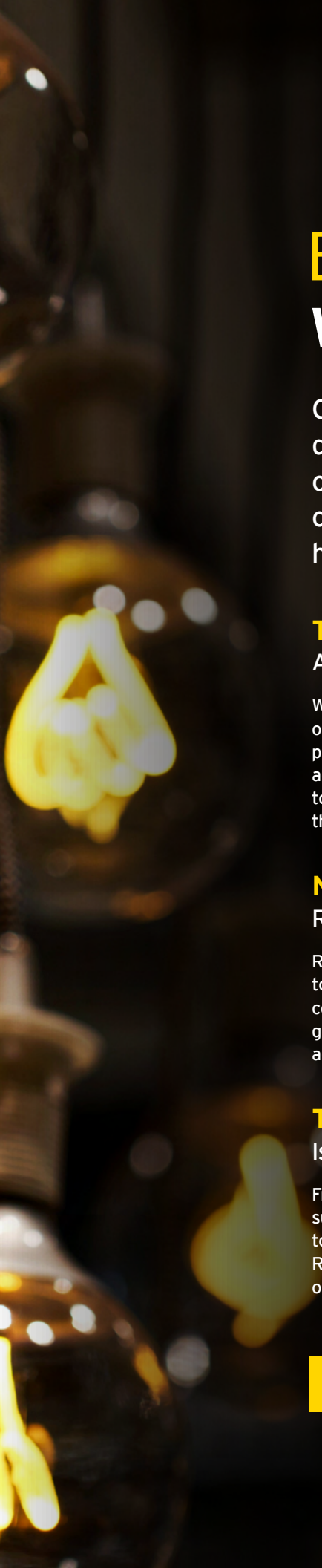
Dave Burg
+1 571 633 3628
dave.burg@ey.com

Chris Holmes
+1 202 327 8890
chris.holmes@ey.com

Steve Klemash
+1 412 644 7461
stephen.klemash@ey.com

Chuck Seets
+1 404 817 5522
charles.seets@ey.com

Phil Nemmers
+1 515 362 7012
phillip.nemmers@ey.com



Better Questions for Boards
Webcast series

Our series is designed to provide directors with insights and questions to consider as they engage with management on a variety of complex boardroom issues. You can access on-demand replays to hear insightful discussion about how boards are approaching a variety of issues.

The board's role in navigating geopolitics
Are you gaining a competitive edge with your geostrategy?

With political outcomes and the economic environment becoming harder to predict, many organizations see policy uncertainty, rising geopolitical tensions, and changes in trade policy and protectionism as key risks. These developments underscore the need for companies to proactively address strategic opportunities and risks stemming from geopolitical and regulatory changes. Listen to a discussion on how leading companies are navigating geopolitics and the board's role in addressing this challenge.

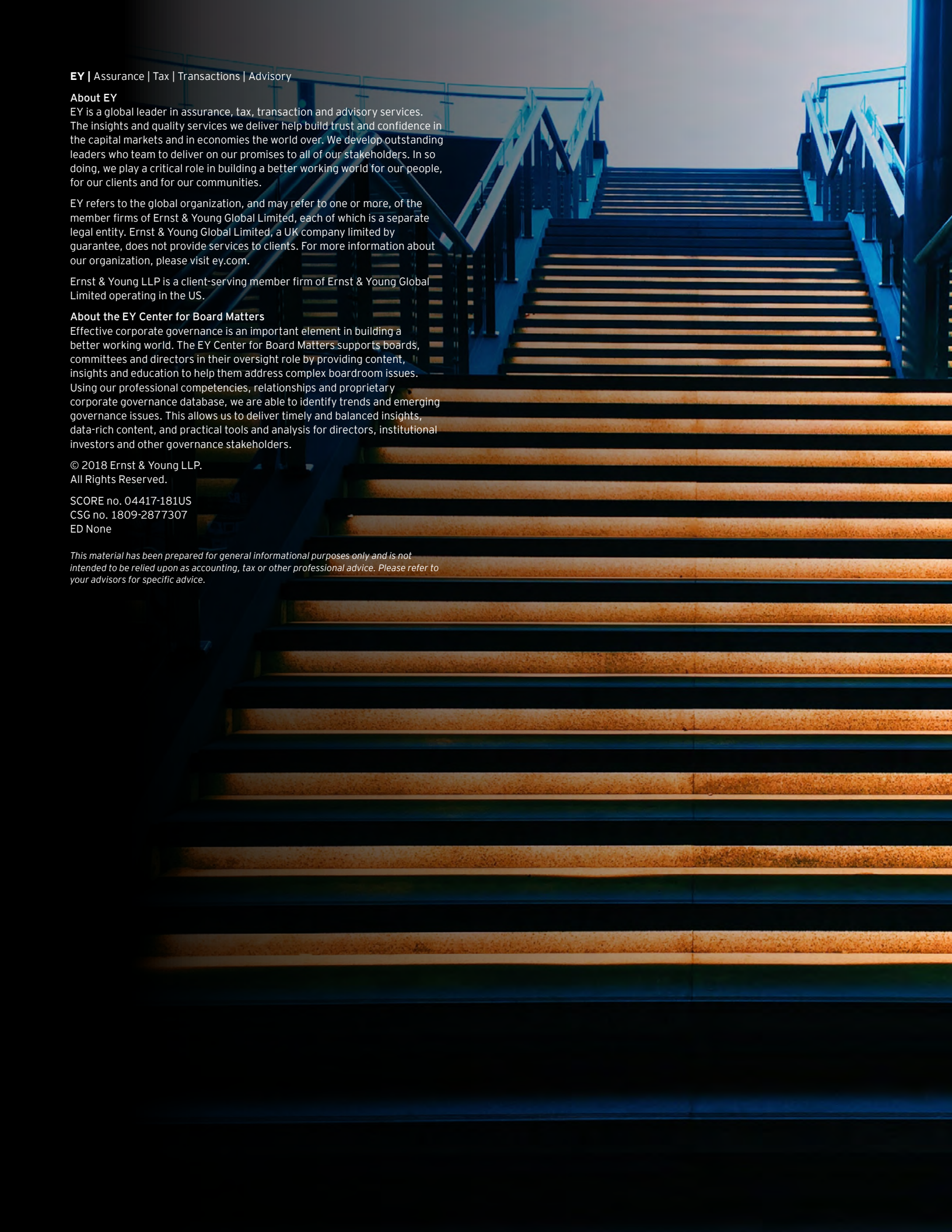
Next-generation enterprise risk management
Risk won't wait, will you?

Risk hasn't just reached the boardroom door — it's pounding to get in! And that's exactly what needs to happen. Boards have to unlock the door and face risk head on. Risks will only continue to grow in complexity, overlapping and impacting business in unprecedented ways. Our panel discussed next-generation enterprise risk management (ERM) and shared their perspectives on how companies are addressing it at the board level.

Talent agenda
Is talent a secret weapon or the biggest challenge for boards?

From building a culture of innovation, to defining purpose and maximizing growth opportunities, a successful people strategy is fundamental for long-term value. That's why talent is quickly moving to the top of board priorities. We talked to Peter Fasolo, Executive Vice President and Chief Human Resources Officer at Johnson & Johnson, and others about talent trends and heard their perspectives on how companies are addressing the talent agenda at the board level.

Access any of our on-demand webcasts at **ey.com/boardmatters.**



EY | Assurance | Tax | Transactions | Advisory

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. 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.

SCORE no. 04417-181US
CSG no. 1809-2877307
ED None