In this issue

04 The board’s role in confronting crisis
A corporate crisis can impact an organization’s culture, business operations and reputation — all of which can have significant financial, legal and regulatory ramifications. Find out what a company’s board can do to provide effective oversight before, during and after a crisis.

13 Cybersecurity disclosure benchmarking
As cybersecurity threats evolve and risks become more complex and widespread, there is growing interest in how companies guard against, plan for and respond to cybersecurity incidents. In an effort to identify leading practices and further the dialogue around such disclosures, we reviewed and report on cybersecurity-related disclosures by Fortune 100 companies.

19 Improving board performance through effective evaluation
Many boards are seeking to enhance their effectiveness and address stakeholder interests by enhancing their board evaluation processes and disclosures. Read about the key elements for designing an effective board evaluation process and gain insight into Fortune 100 company board evaluation practices.

26 Today’s independent board leadership landscape
We look back almost two decades to find out how board leadership structures have evolved. In 2000, just 10% of S&P 1500 companies had independent board leadership. Today, 92% do. This change corresponds to a rise in independent directors, as well as the continuing separation of chair and CEO roles. Discover what else we found.
The board’s role in confronting crisis

A corporate crisis in today’s world accelerates more quickly with a larger impact than ever before. The 24-hour news cycle and prevalence of social media contribute to the risk of destabilization.

A crisis can be the result of a number of different types of incidents and developments and takes on many forms. For example:

- Reports or even hints of executive misconduct or a toxic work culture can ignite a media firestorm.
- Negative and misleading videos and comments can go viral and damage reputations.
- The polarization of people, governmental policies and politicians can catch companies unaware and put them in highly public debates.
- Executing business-model initiatives and certain compensation incentive strategies can result in unintended consequences and enterprise-wide risk.
- Natural and man-made disasters throw tightly linked supply chains into imbalance, amplifying how a regional event can have significantly greater and more far-reaching impacts.
- A single cyber breach can have devastating consequences.

These incidents may call into question the effectiveness of a company’s board of directors and its ability to provide effective oversight and governance.

While prevention must always remain a priority, advance crisis preparation is now imperative as avoiding crises entirely is nearly impossible. For example, the current cyber threat environment is such that it is likely only a matter of time before all businesses will suffer a cyber breach. Whether the cause of the crisis is corporate malfeasance, a terrorist attack or a natural disaster, a company’s ability to manage a timely, well-coordinated crisis response and communicating with stakeholders is critical.

To help companies prepare for the challenge, boards should determine that management has a practical and relevant crisis response program and actively oversee and challenge all aspects of that program, including key considerations before, during and after an event. This includes determining that management has the right framework in place and
that it has sustainable capabilities to allow the company to react to and quickly recover from crisis events. In preparing for and especially when confronting a crisis, boards should also understand the roles and potential implications to key stakeholders. Boards should also participate in various simulations and tabletop exercises with management teams to enhance their effectiveness in responding to crises.

**Overseeing management’s crisis response program**

A corporate crisis can impact organizational culture, business operations and reputation—all of which can have significant financial, legal and regulatory ramifications. Therefore, a crisis management program should bring together a variety of stakeholders who can understand the potential implications and help plan for and recover from a crisis. The program should be managed by someone with in-depth legal and compliance experience who is able to manage day-to-day operational and tactical responses. It should also closely align the internal and external communications leaders to make sure the decisions and messaging are clearly and directly articulated to the key audiences.

The crisis management program should be a process within the company’s broader resiliency toolkit and integrated into its enterprise risk management (ERM) program. This integration helps safeguard that crisis response planning is aligned with and informed by the company’s strategic plan and risk tolerances, and that it is dynamic and evolves along with changes to risk assessments and prioritization. Most important, a robust ERM program is foundational for risk management, litigation prevention and loss mitigation.

**Stakeholders involved in crisis response**

As the linchpin of the company’s response, the crisis response program must involve key constituencies and integrate their knowledge and expertise in managing and recovering from the crisis. The crisis response team should work closely with impacted business-unit leaders in executing upon disaster recovery or business continuity plans. The key roles in the company’s response may include:

- **Chief executive officer (CEO)** – The CEO should be involved with leading the crisis management efforts (unless determined otherwise), including activating the management team and appropriate resources to gather information and work swiftly to determine the appropriate steps to mitigate the effects of the crisis.

- **Business operations and impacted business units** – The chief operating officer (or equivalent executive of the impacted business unit) should focus on obtaining an understanding of the enterprise-wide impact the crisis had on operations (including customers, suppliers and any other impacted parties), as well as executing upon disaster recovery and business continuity plans. The business operations team should make sure operations are adequately supported during the crisis and strive to revert back to “business as usual” as quickly and efficiently as possible.

While prevention must always remain a priority, advance crisis preparation is now imperative as avoiding crises entirely is nearly impossible.
The crisis management program should be a process within the company’s broader resiliency toolkit and integrated into its enterprise risk management (ERM) program.

- **In-house and external counsel** – In-house counsel is integral to nearly all response activities and needs to be equipped with as much information as possible in order to determine potential compliance and legal impacts and interface effectively with various parties, including external counsel, which also plays a critical role throughout the entire response. In advance of a crisis, in-house counsel should verify that initial briefings and any statements made to the press via talking points and scripts are developed for crisis events (including considerations regarding potential liabilities, material omissions or misstatements). In addition to the message, companies also need to make sure the lines of approval are clear and determine who the messenger will be. The internal counsel should also verify that agreements or retainers are in place for critical external parties (including direct and easy access to mobile numbers of third parties). In particular, in-house counsel should make certain they are knowledgeable about the specific insurance requirements and related criteria and protocols that must be followed in order to be eligible for insurance recoveries.

- **Chief communications officer (CCO) or equivalent** – The CCO is integral toward establishing trust through sharing credible and transparent messaging that defines what has occurred, the impact and how the organization is seeking to stabilize, learn and improve from the crisis. The CCO will also oversee the monitoring of any feedback or new developments on social media or elsewhere. He or she acts as the conduit for taking the decisions made and turning them into reactive or proactive messaging and actions. Depending on the severity of the issue, an external crisis communications team may also be engaged.

- **Chief risk officer (CRO)** – The CRO should work closely with in-house counsel to proactively identify and manage any risks that may arise as a result of the crisis or the crisis response plan (e.g., compliance, safety).

- **Chief financial officer (CFO)** – Depending on the financial impact, the CFO will work closely with in-house counsel to file any required public disclosures (e.g., Form 8-K) relating to the event and will also play a key role in coordinating with in-house counsel in filing insurance claims and following related required protocols. The CFO is also integral in working with business units to assess the impact of the crisis (e.g., financial and liquidity considerations, operational and functional impacts, implications to the investor community) and quickly working with other members of the executive team on possible responses.

- **The external auditor** – The auditor needs to understand and evaluate any potential adverse financial impacts of the crisis (including regulatory, legal and internal control implications) and make sure that the related financial effects and appropriate disclosures are accurately reflected in financial statements.

- **Technology, information systems and security teams** – Depending on the nature of the crisis event, key systems, supporting technologies and data may not be accessible or compromised. In the event that the crisis has a cyber dimension, the chief information officer, chief security officer and chief technology officer are at the heart of the operational response. These individuals may need to work with other business functions to determine alternatives to key processes to support affected stakeholders (customers, employees, etc.) and possibly implement backup processes (such as manual workarounds) during the crisis.

- **Investor relations, corporate governance and public relations** – These functions will play a pivotal role in assessing the implications of the crisis to the investor community and developing an appropriate communications strategy.

- **External investigators, public relations, marketing and human resources** – These functions may have key roles to play in evidence gathering, identification and discovery, as well as internal and external communications.
## Crisis components and considerations

<table>
<thead>
<tr>
<th>Types and causes of a crisis</th>
<th>Potential actions to consider</th>
<th>Key stakeholders to consider and involve</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Corporate scandals or fraud</td>
<td>• Continuously communicate throughout the crisis</td>
<td>• Internal stakeholders</td>
</tr>
<tr>
<td>• Employee and/or executive misconduct</td>
<td>• Investigate to determine:</td>
<td>• The board</td>
</tr>
<tr>
<td>• Corporate governance breakdowns</td>
<td>• How and what occurred?</td>
<td>• In-house counsel</td>
</tr>
<tr>
<td>• Product failures or recalls</td>
<td>• When did the company first know about it?</td>
<td>• Compliance/risk management</td>
</tr>
<tr>
<td>• Cyber-related events and breaches</td>
<td>• Who else knows about it? Who should know about it?</td>
<td>• Internal audit</td>
</tr>
<tr>
<td>• External market events</td>
<td>• Is management implicated?</td>
<td>• Investor relations</td>
</tr>
<tr>
<td>• Geopolitical developments</td>
<td>• Were laws, regulations or corporate policies violated?</td>
<td>• Human resources</td>
</tr>
<tr>
<td>• Environmental events or natural disasters</td>
<td>• What aspects of the company’s operations have been disrupted?</td>
<td>• Finance</td>
</tr>
<tr>
<td>• Negative social media coverage</td>
<td>• Who was responsible?</td>
<td>• Information security</td>
</tr>
<tr>
<td>• Poor corporate culture</td>
<td>• Which properties or technologies were affected?</td>
<td>• Corporate security</td>
</tr>
<tr>
<td>• Workplace violence</td>
<td>• Is there any information the company is waiting for?</td>
<td>• Public relations</td>
</tr>
<tr>
<td>• Unintended consequences of business model execution</td>
<td>• Has the media covered this or a similar issue?</td>
<td>• Impacted business lines</td>
</tr>
<tr>
<td></td>
<td>• How is the situation likely to change?</td>
<td>• Employees</td>
</tr>
<tr>
<td></td>
<td>• Perform forensic activities, as needed</td>
<td>• Company governance affairs</td>
</tr>
<tr>
<td></td>
<td>• Assess damage and severity of the crisis</td>
<td>• External stakeholders</td>
</tr>
<tr>
<td></td>
<td>• Contain, remediate, eradicate, communicate</td>
<td>• Law enforcement agencies</td>
</tr>
<tr>
<td></td>
<td>• Monitor (internal and media outlets, including social media)</td>
<td>• Policymakers and regulators</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key goals of an effective crisis response program

Before an event

Support desired risk-aware culture. A risk-aware culture with robust ethics and compliance programs can help prevent certain types of crises and improve responses to others. The company’s ERM process should encourage escalation of concerns, clearly communicate responsibilities for management of risk across the organization, and align core values and behaviors with pay incentives.

Enhance early-warning systems. Ahead of an actual crisis, companies should decide which key issues must be elevated to business-unit leaders, senior management and the board. Where possible, companies can adopt explicit escalation triggers so as to limit the degree to which upward communications are inadvertently delayed. In particular, the company’s disclosure controls and ERM processes should allow for risk evaluation and mitigation before a crisis erupts, including risks that may be embedded in the company’s strategy or culture. This requires the company to encourage escalation of concerns (including elevation of information to the board as appropriate) and spend more time analyzing the external business context for risks on the horizon. It also requires that companies identify and understand the connectivity and interdependence among different business lines, geographies and across the supply chain. In particular, boards should have a robust understanding as to management’s process and elevation criteria used when reporting to the board.

Define roles, responsibilities and decision-making, and communication protocol in a crisis situation. Management and the board should clearly understand their respective roles and responsibilities before, during and after a disruptive event. Companies need to define the appropriate activities of the board and senior leadership during a crisis, such as who will be making decisions, how those decisions will be informed and made, and who will be brought in to assist. Processes and channels of communication (potentially including alternative platforms of communication) should be agreed to in advance. This includes identifying and training a company spokesperson, which may vary based on the nature of the crisis. When a crisis event occurs, companies should not be wrestling with questions around who should be informed, who will speak to the regulators, how to deal with the media, what kind of message needs to be communicated, and so on. Having defined protocols and responsibilities in place will allow for a continuous, coordinated response. Business operations may be disrupted during a crisis so it is important to determine which members of the management team (including substitutes) will be focused on operations and those who will be focused on remediating the effects of a crisis.
Identify and engage key allies and external advisors. The company should identify points of contact, open lines of communication and, in some cases, have agreements in place with external advisors they may need to secure and activate quickly during a crisis (e.g., legal advisors, public relations firm).

Develop reference materials for communications in advance. Companies can prepare for the 15 to 20 most common disruptions they may face, with messages suitable for different constituents, circumstances and media channels. Draft press release templates and scripts that can be delivered through print and television news at the local and national level, and through key social media channels, should be crafted in advance. Additionally, companies can develop a library of customer communications that covers likely experiences and alternatives, and craft specific messages for high-value customers for each major product or service. Draft crisis communications should also cover counterparties, vendors and employees.

Rehearse a response. Companies need to exercise the muscle that is responsible for responding to a crisis. Leading companies test their crisis readiness plans through tabletop exercises that challenge key senior leaders and those involved in the crisis response (e.g., lawyers, public relations) using realistic scenarios. These simulation exercises build efficiency and confidence, and allow companies to act with more precision when an actual crisis occurs. Crisis preparation and rehearsal of such responses will help organizations identify any possible gaps and enable them to navigate the crisis better. Boards should oversee these readiness exercises and take part in them when appropriate.

During an event

Deploy a communication and briefing plan among all internal stakeholders. A centralized response program should provide guidance to all lines of business involved in the response and set a level of understanding about what information is critical for senior leaders to know – as well as when and how to express it. Companies should work to carefully investigate and swiftly gather as much information on the crisis as possible (including proactively monitoring social media and other blogs to gain an understanding of stakeholder and media perceptions). During the information-gathering process, companies should verify accuracy of facts to prevent acting on any misinformed assumptions or bad information. While the visibility of the CEO should depend on the nature of the crisis, it is critical that she or he be prepared to go public as needed to protect the company and trust in the brand, demonstrate strong leadership and communicate credibility to key stakeholders.

Centrally manage all inquiries received from external and internal groups. Communications to both internal and external audiences should be carefully and thoughtfully planned, performed by management and executed with
oversight by the board. Such communications should link to the company’s ethics and values and be timely, accurate and consistent, as lack of clear messaging can pose or introduce litigation risk. There is less room for conflicting or inaccurate messaging when all crisis-related communications are centrally managed by the response team.

**Navigate the complexities of working with external groups.** Crisis management will involve a variety of external parties, such as outside counsel, regulators, third-party advisors or investigators (particularly if management is implicated in the crisis), and law enforcement agencies. A centralized response program helps to safeguard a timely and coordinated flow of information to these groups that integrates the knowledge of key internal stakeholders.

**Collaborate with business units to support ongoing operations and execute upon disaster recovery and business continuity plans.** It is imperative that the company has management that can focus on running the business (while managing and maintaining customer experience) during a crisis as others focus on managing the crisis and restoring operations. During a crisis, companies may need access to additional financial resources and working capital, and those resources may have to last during a prolonged crisis. Accordingly, it is critical that companies have shored up, in advance, robust, tested financial contingency plans that are linked directly to their crisis management processes; this way, when crises hit, the crisis and operational teams can work effectively with treasury resources to manage liquidity and working capital needs. Companies should also recognize that those financial contingency plans may have to withstand industry-wide market failures, during which time liquidity and capital may not be readily available. Additionally, establishing contingency arrangements with major business partners (especially critical vendors) in advance of a crisis event may also be helpful in transitioning back to business as usual.

**After an event**

**Define recovery effort by critical business needs.** Disconnected initiatives by different business units could have conflicting priorities and hinder timely recovery. A central point of authority is required to oversee the prioritization of critical business processes across the organization to align with the company’s strategic objectives and to base that prioritization on the greatest risks to the company.

**Prioritize communications with key stakeholders.** The recovery effort should prioritize fact-based, timely and open communications with employees, customers, shareholders, joint ventures, business alliances and other key stakeholders to help create transparency, foster a culture of integrity and restore confidence.

**Identify and remedy any underlying or systemic causes of the crisis.** Companies should have procedures in place to continually learn from incident response and improve, including an analysis to identify causes that may be rooted in the company’s culture and practices. Management teams should perform postmortems on any near misses post-crisis to assess the effectiveness of response plans and discern lessons learned.

A crisis may be inevitable; however, an effective crisis management plan and ERM program, coupled with strong tone at the top and risk mitigation, can help to detect and prevent a crisis before it hits. While companies cannot predict when a crisis or a black swan event may occur, boards should prepare their organizations to have the ability to react to and recover from a crisis with resiliency and strength. Organizations, and in particular leaders, are defined by a crisis. How a company and its executives weather through a crisis can have enormous brand and economic impact for a company: it can either propel a CEO through stakeholder confidence to take on bigger change, or it may result in negative repercussions because a company or its CEO mismanaged a situation. The criticality of being ready and knowing that this will indeed happen, with a great management team that’s driven to get this right, is one of the most important things CEOs and boards need to prepare for.
Board oversight considerations

Before an event

- The board should set the tone at the top for the importance of crisis management. A robust crisis response program may be considered a low priority, and time and money may not be appropriately allocated to crisis planning, response rehearsal and remediation efforts. The board can help address this challenge and elevate the importance of preparedness and crisis readiness.

- Depending on the nature of the crisis, boards may need to have a spokesperson to speak on behalf of the board and the company. The board should identify a spokesperson for the board (ideally an independent board leader) who will be prepared to represent the company and the board, as needed, and will serve as the key point of contact for management during the event.

- The board should feel comfortable with the crisis response plan, including how the board will be getting information throughout the crisis, and should actively oversee its development and testing.

- The board should have a deep understanding of the company’s strategy, culture, disclosure protocols, ERM process and external business developments. This knowledge enables the board to challenge management’s biases, help identify warning signs that could portend a crisis and provide that the company’s strategic objectives and values drive crisis planning and response. Leading boards may also consider engaging a third party or having an external assessment performed on the effectiveness of the crisis response plan and highlight any significant gaps.

- The board should have a good understanding of the insurance policies held by the company, including criteria for reimbursement of claims, criteria that would trigger insurance coverage to be void, what would be covered and to what extent.

During an event

- The board must understand the scope of the crisis and its existing and potential impact in order to determine the scope of the board’s involvement (including whether a special ad-hoc committee or a designated counsel for the board is warranted) and to oversee and help guide the response strategy. This strategy should include communicating with various stakeholders, including employees, customers, the public, shareholders, external third parties and, potentially, regulators and law enforcement.

- The board should receive regular briefings from management with the latest findings, regulator and law enforcement inquiries, vendor and supplier impacts, customer sentiment, employee reactions, litigation filings, insurance considerations, media coverage (traditional and social media) and reactions of major shareholders. In the case that management is implicated and an external provider or investigator is retained to conduct an investigation, the board (or appropriate committee) should closely oversee that process. The board should also receive any related briefings directly from the third party.

- The board (or appropriate committee) should be supportive while providing effective independent oversight as they interact with the executive management team and other key stakeholders.

- The board can help provide that the company’s crisis response is consistent with its core values and purpose. New risks and unintended consequences may arise from the crisis, and boards should work with management to proactively oversee the dynamic situation. The way an organization responds to a crisis can speak to, and is a test of, the organization’s culture and processes. Once a response
The way an organization responds to a crisis can speak to, and is a test of, the organization’s culture and processes.

After an event

• The board should assess the adequacy of management’s response to the crisis and its post-crisis evaluation, recovery and corrective actions. The most effective crisis response systems are those that institute a continuous feedback loop that allows the organization to better identify risks before crisis arises to lower the probability of a crisis occurring and improve its response should one arise.

• The board should evaluate its own role in responding to the crisis, including whether the board had the adequate skills, structure and information needed to enable quick, decisive and informed action. A crisis is likely to draw investor scrutiny of the company’s compliance and governance, including board and committee leadership and director qualifications. Among other things, this scrutiny could lead to requests for engagement, shareholder proposal submissions, public campaigns opposing specific directors and interest from activist hedge funds. Proactive self-assessment by the board, direct engagement with key shareholders and transparent communications around remediation efforts and board-level changes may help address investor concerns.

Questions for the board to consider

• Has the company developed a crisis management “playbook” with decision process flows and escalation protocols? Do all the participants know their roles and the critical approval processes that are in place to be certain of quick and straightforward approvals?

• Has the company considered and challenged itself as to the types of crises it may face, where and how likely such events might be?

• Has the company identified the individuals who will lead communications during a crisis?

• Has the company identified the external advisors in the various scenarios that the company plans on seeking counsel from? If so, are agreements in place with the external advisors such that they are able to be mobilized quickly? Does the company have a place or virtual room secured to gather in the event of a crisis?

• How often do senior leaders take part in tabletop exercises using realistic crisis scenarios? And what is the board’s role in these?

• Does the company’s response planning prioritize communications with key stakeholders, including employees, customers, shareholders and business partners?

• If a crisis were to unfold today, how prepared is the company to react with precision, speed and confidence?
Cybersecurity disclosure benchmarking

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, the 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 reexamining 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.”

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.”

“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:

**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.

Investors generally want to understand how boards are actively overseeing cybersecurity risks and strategy.
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.

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 1 September 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.

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

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

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?

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.
Improving board performance through effective evaluation

Investors, regulators and other stakeholders are seeking greater board effectiveness and accountability and are increasingly interested in board evaluation processes and results. Boards are also seeking to enhance their own effectiveness and to more clearly address stakeholder interest by enhancing their board evaluation processes and disclosures.

The focus on board effectiveness and evaluation reflects factors that have shaped public company governance in recent years, including:

- Recent high-profile examples of board oversight failures
- Increased complexity, uncertainty, opportunity and risk in business environments globally
- Pressure from stakeholders for companies to better explain and achieve current and long-term corporate performance
- Board evaluation requirements outside the US; the UK, in particular
- Increased focus on board composition by institutional investors
- Activist investors

In view of these developments, we reviewed the most recent proxy statements filed by companies in the 2018 Fortune 100 to identify notable board evaluation practices, trends and disclosures. Our first observation is that 93% of proxy filers in the Fortune 100 provided at least some disclosures about their board evaluation process. This publication outlines elements that can be considered in designing an effective evaluation process and notes related observations from our proxy statement review.

Planning and designing an effective evaluation process

Prior to designing and implementing an evaluation process, boards should determine the substantive and specific goals and objectives they want to achieve through evaluation. The evaluation process should not be used simply as a way to assess whether the board, its committees and its members have satisfactorily performed their required duties and responsibilities. Instead, the evaluation process should be designed to rigorously test whether the board’s composition,
dynamics, operations and structure are effective for the company and its business environment, both in the short- and long-term, by:

- Focusing director introspection on actual board, committee and director performance compared to agreed-upon board, committee and director performance goals, objectives and requirements
- Eliciting valuable and candid feedback from each board member, without attribution if appropriate, about board dynamics, operations, structure, performance and composition
- Reaching board agreement on action items and corresponding timelines to address issues observed in the evaluation process
- Holding the board accountable for regularly reviewing the implementation of evaluation-related action items, measuring results against agreed-upon goals and expectations, and adjusting actions in real-time to meet evaluation goals and objectives

In determining the most effective approach to evaluation, boards should determine who should lead the evaluation process, who and what should be evaluated, and how and when the evaluation process should be conducted and communicated.

### Leading the evaluation process

Leadership is key in designing and implementing an effective evaluation process that will objectively elicit valuable and candid director feedback about board dynamics, operations, structure, performance and composition.

A majority (69%) of Fortune 100 proxy filers disclosed that their corporate governance and nominating committee performed the evaluation process either alone or together with the lead independent director or chair. These companies also disclosed that evaluation leaders did or could involve others in the evaluation process, including third parties, internal advisors and external legal counsel. Twenty-two percent of Fortune 100 proxy filers disclosed using or considering the use of an independent third party to facilitate the evaluation at least periodically.

### Determining who to evaluate

Board and committee evaluations have long been required of all public companies listed on the New York Stock Exchange. Today, board and committee evaluations are best practice for all public companies.

Approximately one-quarter (24%) of Fortune 100 proxy filers disclosed that they included individual director self-evaluation along with board and committee evaluation. Ten percent of Fortune 100 proxy filers disclosed that they conducted peer evaluations. Individual director self- and peer evaluations are discussed below.

### Prioritizing evaluation topics

Board, committee and individual director evaluation topics should be customized and prioritized to elicit valuable, candid and useful feedback on board dynamics, operations, structure, performance and composition. Relevant evaluation topics and areas of focus should be drawn from:

- Analysis of board and committee minutes and meeting materials
- Board governance documents, such as corporate governance guidelines, committee charters and director qualification standards, as well as company codes of conduct and ethics
- Observations relevant to board dynamics, operations, structure, performance and composition
- Company culture, performance, business environment conditions and strategy
- Investor and stakeholder engagement on board composition, performance and oversight
The evaluation process should be designed to rigorously test whether the board’s composition, dynamics, operations and structure are effective for the company.

Forty percent of Fortune 100 proxy filers disclosed the general topics covered by the evaluation. These disclosures typically focus on core board duties and responsibilities and oversight functions, such as:

- Strategy, risk and financial performance
- Board composition and structure
- Company integrity, reputation and culture
- Management performance and succession planning

**Asking focused evaluation questions to elicit valuable feedback**

About 40% of Fortune 100 proxy filers disclosed use of questionnaires in their evaluation process, with 15% disclosing use of only questionnaires and 25% disclosing use of both questionnaires and interviews. Questionnaires are a key tool in the evaluation process but must be thoughtfully and carefully drafted to be effective. Questionnaire responses can be provided without attribution, which can promote candid and more detailed feedback.

Questionnaires are helpful because each director receives the same question set – even if there are separate questionnaires for the board, its committees and individual directors. This approach facilitates comparison of director responses and can help indicate the magnitude of any actual or potential issues as well as variances in director perspective and perception.

Evaluation questionnaires often put questions in the form of a statement, such as “The board is the right size,” which calls for a response along a numerical scale. The larger the numerical scale, the more variance, which allows for a relatively more nuanced response. More specific and candid feedback can be obtained by prompting directors to provide detailed freestyle commentary to explain a response on a numerical scale or to a “yes” or “no” question.

Well-drafted, targeted questions – or questions in the form of a statement – should be written specifically for the board, its committees and individual directors, as applicable, with the goal of eliciting valuable and practical feedback about board dynamics, operations, structure, performance and composition. High-quality feedback is what enables boards and directors to see how they can better perform and communicate, with the result that the company itself better performs and communicates.

Template evaluation questionnaires often do not demonstrate the strong potential of a well-drafted questionnaire. Many template questionnaires seem overlong and include unnecessarily hard-to-answer or unclear questions, such as “Does the board ensure superb operational execution by management?” These types of questions don’t seem to lend themselves to eliciting practical feedback. Complicated or unclear questions should be revised to be more practical or omitted from the questionnaire. Overlong questionnaires should be streamlined to be more relevant and effective in eliciting valuable and useful information.

Template evaluation questionnaires also often include numerous questions about clearly observable or known board and director attributes, practices and requirements. A short set of common examples includes:

- I attend board meetings regularly.
- Advance meeting materials provide sufficient information to prepare for meetings, are clear and well-organized, and highlight the most critical issues for consideration.
- I come to board meetings well-prepared, having thoroughly studied all pre-meeting materials.
- The board can clearly articulate and communicate the company’s strategic plan.
- The board discusses director succession and has implemented a plan based upon individual skill sets and overall board composition.
When evaluation questionnaires include numerous questions on observable practices or required duties and responsibilities, the evaluation becomes more of a checklist exercise than a serious effort to elicit valuable and useful information about how to improve board dynamics, operations, performance and composition. Overlong, vaguely worded, generic, checklist-type questionnaires can lead to director inattention and inferior feedback results, further impairing the evaluation process.

More effective questionnaires are purposefully and carefully drafted to focus director attention on matters that cut to the core of board and director performance. This may be facilitated when the questions focus succinctly on agreed-upon board goals and objectives or requirements and director qualifications considered together with the company’s performance and short- and long-term strategy.

For example, a written evaluation questionnaire need not ask whether the board and its directors have discussed and made a plan for director succession because the directors already know the answer. A better approach might be to recognize that such action did not take place and to ask each director, during a confidential interview process, “What factors or events distracted or prevented the board from discussing and implementing a plan for director succession?” Candid responses to that interview question should provide feedback that can uncover practices or leadership that should change in order to improve board performance.

Conducting confidential one-on-one interviews to elicit more candid feedback

Conducting well-planned, skillful interviews as part of the evaluation process can elicit more valuable, detailed, sensitive and candid director feedback as compared to questionnaires. The combined use of questionnaires and interviews may be most effective and, as noted above, was the approach disclosed by about one-quarter of Fortune 100 proxy filers. Fifteen percent of Fortune 100 proxy filers disclosed use of interviews only.

Interviews are particularly effective when there is an actual or potential issue of some sensitivity to address, as directors may prefer to discuss rather than write about sensitive topics. If boards believe interviews will be helpful, they should carefully consider who should conduct them — with the key criteria being that the interviewer is:

- Well-informed about the company and its business environment as well as board practices
- Highly trusted – even if not well-known – by the interviewees
- Skilled at managing probing and candid conversations

Special considerations may arise when the interviewer is also part of the evaluation process. Where sensitivities like this are perceived, using an experienced and independent third-party interviewer can be effective.

While interviews do not enable anonymity, a trusted and skilled interviewer may still confidentially elicit valuable and sensitive feedback. Interviewer observations and interviewee feedback can be presented to the board without attribution.

Individual director self-and peer evaluations

Individual self- and peer evaluations — whether through questionnaires or interviews — can improve an evaluation process, especially one that is already generally successful as applied to the board as a whole and its committees. When directors understand and see value in evaluations at a collective level, they often perceive enhanced value in individual evaluations — both of themselves and of their peers.

Self-evaluations call for directors to be introspective about themselves and their performance and qualifications. Interestingly, simply being asked relevant questions about performance can lead directors to strive harder. The goal of self-evaluation is to enable directors to consider and determine for themselves during the evaluation process —
and every other day — what they can proactively do to improve personal performance and better contribute to optimal board performance. Approximately one-quarter of Fortune 100 proxy filer boards included individual director self-evaluations in their evaluation process.

Peer evaluations increasingly are seen as critical tools to develop director skills and performance and promote more authentic board collaboration. A successful peer evaluation can also help improve director perspective. While some suggest that peer evaluations, even if provided anonymously, can be uncomfortable to provide and receive, a key characteristic of an effective board is that the board’s culture inspires and requires active, candid, relevant and useful participation from all members, as well as healthy debate and rigorous and independent yet collaborative decision-making. Where the board culture and dynamic is healthy, directors should see peer evaluation as important and beneficial guidance and coaching from esteemed colleagues. Ten percent of Fortune 100 proxy filer boards included peer evaluations in their evaluation process.

Using a third party

Use of third-party experts, such as governance advisory firms or external counsel, to facilitate the evaluation process is increasing. Twenty-two percent of Fortune 100 proxy filers disclosed having a third party facilitate their evaluation at least periodically, typically stated as every two or three years.

A third party can perform a range of evaluation services, from leading the evaluation process to conducting interviews to providing evaluation questions and reviewing questionnaire responses. Third parties can also help oversee implementation of evaluation action items.

Where the third party is independent of the company and the board, its participation in the evaluation process can meaningfully enhance the objectivity and rigor of the process and results. Third-party experts can provide new and different perspectives, both gained from work with other companies as well as simply being from outside the company, which can lead to improved action-item development and evaluation results.

The use of a third party may be especially helpful when:

- The board wants to test or improve its existing evaluation process.
- Directors may not be forthcoming and candid with an internal evaluator.
- The board believes an independent third party can objectively bring new perspectives and issues to the board’s attention.
- The board is new or has undergone a significant change in composition and its directors are not yet poised to conduct an effective evaluation.
- The board has not seen significant change in composition over a period of time and new perspective is desired on board composition and performance.
- The company and its board are facing and addressing a crisis.

Intra-year evaluations and feedback

Board evaluations generally are performed annually. Common evaluation topics, however, relate to board practices and director attributes that are observable either in real-time, over a three- or six-month period, or with reference to board agendas and minutes. In such cases, boards should formally encourage real-time or prompt feedback to constructively address actual or potential issues. Indeed, doing so allows directors themselves to embody the “see something, say something” culture needed to promote long-term corporate value.

The concept of real-time or intra-year evaluation of board and director composition and performance is not new, even if not now widely practiced. A few (just under 10%) of proxy filers in the Fortune 100 disclosed that they carry out phases of the evaluation process on an ongoing basis, at every in-person meeting, quarterly, biannually or otherwise during the year.
Disclosing the evaluation process and evaluation results

A vast majority, 93%, of Fortune 100 proxy filers provide at least some disclosure about their evaluation process, but we observed wide variances in the scope and details of the disclosures. Given the attention to board effectiveness, we expect companies will expand their disclosures relating to board evaluation and effectiveness.

About 20% of Fortune 100 proxy filers disclosed, at a high level, actions taken as a result of their board evaluation.

Some examples include:
- Enhanced director orientation programs
- Changes to board structure and composition
- Changes to director tenure or retirement age limits
- Expanded director search and recruitment practices
- Improvements to the format and timing of board materials
- More time to review key issues, such as strategy and cybersecurity
- Changes to company and board governance documents
- Improved evaluation process

Companies with more detailed disclosures often use graphics to explain their evaluation process, such as in this example:

### Our board’s evaluation process

<table>
<thead>
<tr>
<th>Determine format</th>
<th>Conduct evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The formal self-evaluation may be in the form of written or oral questionnaires, administered by the board members, management or third parties. Each year, our governance and nominating committee discusses and considers the appropriate approach and approves the form of the evaluation.</td>
<td>Members of our board and each board committee participate in the formal evaluation process, responding to questions designed to elicit information to be used in improving board, committee and director effectiveness.</td>
</tr>
<tr>
<td>Review feedback</td>
<td>Respond to evaluation feedback</td>
</tr>
<tr>
<td>Director feedback provided during the formal evaluation process is discussed during board and committee meetings, in executive session or with management present when appropriate.</td>
<td>Following discussion of director feedback, the board and its committees work with one another and management to take specific steps to improve policies, processes and procedures to improve board, committee and director effectiveness.</td>
</tr>
</tbody>
</table>
Conclusion

Investors, regulators, other company stakeholders and governance experts are challenging boards to examine and explain board performance and composition. Boards should address this challenge – first and foremost through a tailored and effective evaluation process. In doing this, boards can work to identify areas for growth and change to improve performance and optimize composition in ways that can enhance long-term value. Boards can also describe evaluation processes and high-level results to investors and other stakeholders in ways that can enhance understanding and trust.

Observations about Fortune 100 company board evaluation practices

<table>
<thead>
<tr>
<th>Observation</th>
<th>% of total*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performed individual director self-evaluation, in addition to board and committee evaluation</td>
<td>24%</td>
</tr>
<tr>
<td>Used or considered using a third party at least periodically to facilitate the evaluation</td>
<td>22%</td>
</tr>
<tr>
<td>Used both questionnaires and individual director interviews to conduct the evaluation</td>
<td>26%</td>
</tr>
<tr>
<td>Provided board evaluation disclosures in their proxy statement</td>
<td>93%</td>
</tr>
<tr>
<td>Identified in the proxy statement general topics covered in the evaluation</td>
<td>40%</td>
</tr>
<tr>
<td>Disclosed in the proxy statement general actions taken as a result of the evaluation</td>
<td>21%</td>
</tr>
</tbody>
</table>

* Data based on the most recent proxy statements available for the 86 public companies on the 2018 Fortune 100 list.

Questions for the board to consider

- Has the most recent evaluation process enabled the board and individual directors to identify actions to optimize board and director performance and board composition?
- Has the company considered disclosing the evaluation process and summarizing the nature of actions taken to enhance stakeholder understanding of the board’s work and value?
- Does the board as a whole and each director have a common and clear understanding of the term “effectiveness” as applied to the board as a whole, its committees and each director individually?
- Has the board formulated clear goals, objectives and standards for itself, its committees and each director that can be referenced during and outside of the evaluation process? If the board has director qualification standards, should they be expanded in more specific ways to include standards and requirements that each director must consistently meet to earn renomination?
- Does the evaluation process include components that occur on a biannual, quarterly and/or real-time basis? If not, why not?
- Is the evaluation process appropriately synergized with the board’s annual governance review, orientation and education programs, director nomination process, succession planning and stakeholder engagement programs?
- Does the evaluation process provide validation to each director that he or she is the right director at the right time for the right company?
Today’s independent board leadership landscape

Board leadership structures have evolved dramatically over the past 20 years. Today, 92% of S&P 1500 companies have independent board leadership, up from just 10% in 2000. This change corresponds to a rise in independent directors, as well as the continuing separation of chair and CEO roles.

Today, 60% of S&P 1500 companies have separate individuals serving as chair and CEO, more than doubling the 27% that separated the roles in 2000. But while the shift toward independent board leadership is clear, the form that leadership takes, and the responsibilities assigned to those leaders, differ among companies.

We reviewed S&P 1500 companies and found that, among the various independent leadership structures, independent board chairs have been experiencing the fastest increase since 2000. We also found marked differences between the levels of authority commonly assigned to the different independent leadership roles, as well as emerging disclosure and engagement trends that raise the profile and highlight the strength of independent board leaders.

Continuing trend toward independent chairs

When it comes to independent board leadership, views on best practice vary. Corporate disclosures differ on why one type of leadership structure may be more effective for a particular company. Also, what works best may change over time based on company-specific circumstances and board dynamics. Views among investors differ too. For some investors, there is no substitute for an independent board chair, while others find lead directors to be sufficient provided the responsibilities are clearly defined and robust.

The evolving independent board leadership landscape reflects this varied approach. While overall more S&P 1500 companies are appointing independent chairs, S&P 500 companies are still far more likely to have lead directors. The practice of appointing presiding directors, who are often viewed as having a more passive role, continues to decline.

Boards should use the annual self-evaluation process or a time of transition as an opportunity to reconsider the appropriate board leadership structure given the company’s specific circumstances.

Evolving board leadership practices, S&P 1500
% of companies

<table>
<thead>
<tr>
<th>Year</th>
<th>Independent board chair</th>
<th>Lead director</th>
<th>Presiding director</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>7%</td>
<td>3%</td>
<td>0%</td>
</tr>
<tr>
<td>2013</td>
<td>30%</td>
<td>45%</td>
<td>11%</td>
</tr>
<tr>
<td>2015</td>
<td>37%</td>
<td>49%</td>
<td>7%</td>
</tr>
<tr>
<td>2018</td>
<td>40%</td>
<td>49%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Increase in independent board leaders parallels rise in independent directors

The shift to independent board leaders goes hand-in-hand with another governance shift over the same time period: a significant increase in independent directors. In 2000, 65% of S&P 1500 directors were considered independent vs. 83% in 2018.

Most S&P 1500 boards today include only one or two directors who are not independent, going well beyond listing standards that require a majority of independent directors. Even controlled companies, which are not required to have a majority independent board, usually comply with or exceed this threshold.

**A note about the data**

Not all companies have independent board leadership, and a small number of companies have both independent chairs and lead or presiding directors. While a majority of S&P 1500 companies separate the chair and CEO positions, most have a non-independent director (often a current or former company executive) serving as chair.
Companies continue to identify ways to use the proxy as an effective tool for engagement and communication with stakeholders.

Title matters: how key responsibilities differ

Lead director positions serve as a kind of compromise in terms of board leadership structures. They maintain the unified leadership of the combined CEO/chair while providing an independent counterbalance to management’s leadership on the board. They do not command the same authority as a board chair, but their role is generally more robust than that of a presiding director.

Our review of the key responsibilities assigned to independent chairs, lead and presiding directors at companies in the 2018 Fortune 100 illustrates this differentiation among the roles. The role of independent chair is distinct in regards to responsibilities related to calling and chairing meetings of the full board and shareholder meetings. Most lead directors have many of the same powers as that of an independent chair, such as calling and chairing meetings of the independent directors and approving board meeting agendas, schedules and information. The authority of presiding directors is generally more limited.

<table>
<thead>
<tr>
<th>Fortune 100 independent board leadership responsibilities*</th>
<th>Chair</th>
<th>Lead director</th>
<th>Presiding director</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority to call shareholder meetings</td>
<td>▲</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chair shareholder meetings**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chair board meetings**</td>
<td>▲</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority to call meetings of all directors</td>
<td>▲</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority to call meetings of the independent directors</td>
<td></td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Chair meetings of the independent directors</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Serve as liaison between management and independent directors</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Approve board meeting agendas and schedules</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Approve information sent to the board</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Be available, when appropriate, for consultation and direct communication with shareholders</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Lead CEO performance evaluation (often in coordination with compensation committee)</td>
<td>▲</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lead annual board performance evaluation (often in coordination with nominating/governance committee)</td>
<td>▲</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Based on the most recent proxy statements, corporate governance guidelines and bylaws of 86 public Fortune 100 companies that file proxy statements. Yellow triangles indicate that a majority of companies with such position specifically assigned the responsibility; gray triangles indicate that at least a quarter of companies with such position assigned the responsibility.

** Reflects primary responsibility for chairing board and shareholder meetings. Most lead and presiding directors have responsibility for presiding over board meetings in the chair’s absence, and some lead directors have responsibility for presiding over shareholder meetings in the chair’s absence.
Spotlighting independent board leaders in disclosures and engagement

U.S. Securities and Exchange Commission rules require companies to disclose in the proxy statement their board leadership structure, including why that structure was determined to be appropriate for the company, how the structure and the board’s risk oversight responsibilities relate to each other, and whether the same person serves as CEO and board chair. Where the CEO and chair positions are combined, companies must disclose whether they have a lead independent director and, if so, explain the specific role the lead director plays in the leadership of the board.¹

Companies continue to identify ways to use the proxy as an effective tool for engagement and communication with stakeholders. One way they are accomplishing this is with letters to shareholders from the independent board leader, or the full board itself, which communicate the board’s message around prominent governance topics, such as board composition and effectiveness, board oversight of strategy, shareholder engagement, and key governance and pay changes.

Having such a letter come from the independent board leader highlights that individual’s role and can showcase the strength and authority of that independent position vis-à-vis the CEO. In 2018, 15% of S&P 500 companies included a letter to shareholders either from the independent board leader alone or jointly from the independent board leader and the CEO, which is three times the number in 2015. Around 60% of these letters were from lead directors and around 40% were from independent chairs, which may reflect additional efforts by lead directors to more clearly demonstrate independent leadership on a board that is chaired by the CEO.

Direct engagement with shareholders, as appropriate, is another avenue for building shareholder trust in the strength of independent board leadership, including by raising the profile of the independent board leader and showcasing that individual’s qualifications and expertise. And the practice is on the rise: this year 14% of S&P 500 companies disclosed that the board’s independent leader was directly involved in engagement conversations with shareholders over the past year, up from 4% in 2015. More than a third (36%) of the lead directors and almost half (47%) of the independent chairs involved in these engagement conversations also wrote letters to shareholders in the proxy statement.

Other emerging trends that highlight the strength of independent board leadership include discussion in the proxy statement of how the current independent board leader is uniquely qualified for the role based on his or her relevant expertise and leadership qualities and key focus areas or activities of that leader over the previous year.

Letters to shareholders from independent board leaders and shareholder engagement involving independent board leaders, S&P 500

% of companies

<table>
<thead>
<tr>
<th>Letter from independent board leader</th>
<th>Joint letter from independent board leader and CEO</th>
<th>Shareholder engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>4%</td>
<td>9%</td>
</tr>
<tr>
<td>1%</td>
<td>6%</td>
<td>14%</td>
</tr>
<tr>
<td>4%</td>
<td>4%</td>
<td></td>
</tr>
</tbody>
</table>

Where are the women?

Only 8% of independent board leadership positions at S&P 1500 companies are held by women (with only 21% of S&P 1500 directorships overall held by women). And title matters: lead director roles are almost twice as likely to be held by women as independent board chairs.

This year 14% of S&P 500 companies disclosed that the board’s independent leader was directly involved in engagement conversations with shareholders over the past year, up from 4% in 2015.

### Independent board leadership varies by sector

<table>
<thead>
<tr>
<th>Independent board leadership roles</th>
<th>% independent chairs</th>
<th>% lead directors</th>
<th>% presiding directors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer discretionary</td>
<td>35%</td>
<td>49%</td>
<td>5%</td>
</tr>
<tr>
<td>Consumer staples</td>
<td>24%</td>
<td>58%</td>
<td>8%</td>
</tr>
<tr>
<td>Energy</td>
<td>41%</td>
<td>51%</td>
<td>4%</td>
</tr>
<tr>
<td>Financials</td>
<td>38%</td>
<td>58%</td>
<td>2%</td>
</tr>
<tr>
<td>Health care</td>
<td>44%</td>
<td>48%</td>
<td>5%</td>
</tr>
<tr>
<td>Industrials</td>
<td>37%</td>
<td>53%</td>
<td>4%</td>
</tr>
<tr>
<td>Information technology</td>
<td>52%</td>
<td>42%</td>
<td>4%</td>
</tr>
<tr>
<td>Materials</td>
<td>43%</td>
<td>53%</td>
<td>3%</td>
</tr>
<tr>
<td>Real estate</td>
<td>32%</td>
<td>59%</td>
<td>3%</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>36%</td>
<td>36%</td>
<td>0%</td>
</tr>
<tr>
<td>Utilities</td>
<td>43%</td>
<td>55%</td>
<td>6%</td>
</tr>
</tbody>
</table>

*Based on S&P 1500 companies. Not all companies have independent board leadership, and a small number of companies have both independent chairs and lead or presiding directors.

### Questions for the board to consider

- How is the independent board leader selected and his or her performance evaluated? Are those processes robust?
- Do the key responsibilities assigned to the independent board leader sufficiently empower that individual to provide strong independent leadership? And are those responsibilities clearly defined in the company’s governance documents and communicated to investors?
- Does the board understand how key shareholders view its leadership structure? And how is it addressing any related shareholder interests or areas of focus?
- Are there opportunities to better communicate the strengths of the board’s current leadership structure and the effectiveness of the current independent board leader?
- What is the process for evaluating the board’s leadership structure? Are there opportunities to enhance that evaluation?
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.

Does your board know what questions to ask about cybersecurity – and how to assess the answers?

The cyber threat dominates today’s risk landscape, and the scale of that threat is expanding dramatically. By 2021, the global cost of cybersecurity breaches will reach US $6 trillion by some estimates, double the total for 2015. It has never been more difficult for organizations to map and protect the digital environment in which they operate, and the board’s role in overseeing cybersecurity has never been more critical. Access the replay of our webcast to learn how boards can be a strategic partner to management in making cybersecurity an enterprise-wide risk management priority, and hear about steps boards can take to move their cybersecurity oversight to the next level.

Next-generation enterprise risk management

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.

If crisis strikes today, is your board ready?

A corporate crisis in today’s world accelerates more quickly with a larger impact than ever before. The 24-hour news cycle and prevalence of social media contribute to the risk of destabilization. While prevention must always remain a priority, advance crisis preparation has become imperative for companies – and boards have a critical role to play. We invited Karen Golz, Chair of USA Gymnastics and an audit committee member of Analog Devices, Inc., and others to discuss their perspectives on how boards can help prime their organizations to react and recover from a crisis with resiliency and strength.

Access any of our on-demand webcasts at ey.com/boardmatters.
EY Center for Board Matters (CBM) contacts

EY Americas CBM Leader
Stephen Klemash
+1 412 644 7461
stephen.klemash@ey.com

Americas Regional CBM Leaders

Canada
Fred Clifford
+1 416 943 2489
fred.clifford@ca.ey.com

FSO
Paul Haus
+1 212 773 2677
paul.haus@ey.com

Latin America North
Lupita Castaneda
+52 555 283 8691
guadalupe.castaneda@mx.ey.com

Latin America South
Guilherme Sampaio
+55 11 2573 5253
guilherme.sampaio@br.ey.com

Northeast
Chris Bruner
+1 215 448 2289
chris.bruner@ey.com

Southeast
Cigdem Oktem
+1 404 817 4203
cigdem.oktem@ey.com

Southwest
Steve Macicek
+1 713 750 1253
steven.macicek@ey.com

West
Lee Dutra
+1 415 894 8220
lee.dutra@ey.com

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

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.

© 2018 Ernst & Young LLP. All Rights Reserved.
SCORE no. 05332-181US
1812-2974829
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

About this publication
Board Matters Quarterly is published four times a year and includes articles previously published online and distributed electronically to our subscribers. To access or sign up to receive similar content relevant to board members, please visit ey.com/boardmatters.