Building a better working world

EY Center for Board Matters

What companies are sharing about cybersecurity risk and oversight

Cybersecurity attacks are among the gravest risks that businesses face today. The EY 2019 CEO Imperative Survey found that CEOs ranked national and corporate cybersecurity as the top global challenge to business growth and the global economy.

In this environment, stakeholders want to better understand how companies are preparing for and responding to cybersecurity incidents. They also want to understand how boards are overseeing these critical risk management efforts. Some of the answers can be found in public disclosures.

The U.S. Securities and Exchange Commission (SEC) issued guidance in 2018 promoting clearer and more robust disclosure about cybersecurity risks and incidents and how boards discharge their cybersecurity risk oversight responsibility. Our 2018 Cybersecurity disclosure benchmarking report explored how companies were responding to this guidance.

We undertook the same research this year to help inform stakeholders of emerging trends and developments. We analyzed three areas of cybersecurity-related disclosures in the proxy statements and Form 10-K filings of Fortune 100 companies from 2018-2019: board oversight (including risk oversight approach, board-level committee oversight, and director skills and expertise), statements on cybersecurity risk, and risk management (including cybersecurity risk management efforts, education and training, engagement with outside security experts and use of an external advisor). We found that many companies are enhancing their cybersecurity disclosures, with the most significant changes related to board oversight practices.

We also found that the depth and nature of these disclosures vary widely, and do not necessarily capture the entirety of a company's cyber-risk management and oversight activities. For example, only a few companies disclosed they are obtaining an assessment of their cybersecurity risk management program from an independent third party or conducting tabletop exercises (i.e., breach simulations) to enhance cyber incident preparedness by the board and C-suite. These are practices we are routinely observing in the market.

Our market observations

The EY Center for Board Matters frequently conducts education and insight sessions for boards. Based on these meetings and the work being done by our cybersecurity advisors around the globe and across industries, we have identified the following leading practices for overseeing cybersecurity risks:

- Having unfiltered board discussions with the chief information security officer (CISO) in executive sessions
- Gaining insights into how management is validating the operational effectiveness of its cybersecurity risk management program
- Regularly infusing cyber in boardroom conversations with all C-suite executives and division leaders to help create accountability for their role in supporting the cybersecurity environment
- Asking questions about cybersecurity impacts when contemplating any new product, initiative, partnership or business deal, and overseeing that cyber resiliency is embedded into the foundation of company practices and process (i.e., trust by design)
- Upskilling the full board via concentrated cybersecurity education and periodic training sessions with outside experts, certification courses and peer-to-peer director exchanges
- Overseeing that a third party is periodically evaluating the design and effectiveness of the company's cybersecurity risk management program, and engaging directly with that third party to help challenge internal bias
- Overseeing, and periodically participating in, tabletop exercises and simulations as part of the company's cybersecurity incident response and recovery planning

"

National and corporate cybersecurity was ranked number one by CEOs as the biggest challenge for the global economy in the next 5-10 years.

EY CEO Imperative Study

SEC guidance

The SEC's 2018 Commission-level guidance, which reinforced and built on the SEC staff's 2011 cybersecurity guidance, clarified companies' obligations to disclose cybersecurity risks, material breaches and the potential impact of the breaches on business, finances and operations — the goal being to enable investors to make more risk-informed investment decisions. The guidance reminded companies that a number of existing SEC disclosure requirements could require disclosure of cybersecurity matters, including description of the business, legal proceedings, MD&A, board role in risk management, and risk factors.

It expanded the prior guidance by highlighting two new topics: (i) the importance of strong disclosure controls and procedures to enable timely and accurate disclosures of cybersecurity risks and incidents, and (ii) insider trading prohibitions related to cybersecurity incidents.[1] Although the SEC reiterated its expectation that companies provide timely disclosure of cybersecurity risks and incidents that are material to investors, the guidance clarifies that companies need not make disclosures that could compromise their cybersecurity efforts and acknowledges that an ongoing investigation by law enforcement of a cybersecurity incident may affect the scope of the disclosure about the incident.

Since the 2018 guidance was issued, SEC Chairman Jay Clayton has made public statements emphasizing the importance of cybersecurity disclosures.[2] SEC Director of Corporation Finance William Hinman also has discussed the need for companies to comply with the guidance and noted that companies are responding to the guidance, as the SEC staff is seeing fewer boilerplate cybersecurity-related disclosures.[3] The Commission staff also has asked questions about the sufficiency of cybersecurity disclosures in comment letters to issuers.

The SEC staff looks at and comments on cybersecurity-related disclosures as part of its regular reviews of public company filings. The staff also monitors news reports of cyber breaches to assist in this process.[4] The SEC staff has said it does "not second-guess good faith exercises of judgment about cyber-incident disclosures. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action could be warranted."[5] One such case has already been brought.[6]

---

1 See also How the SEC views cybersecurity disclosures and board's oversight role.

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

3 Ibid.

4 Ibid.

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

6 Ibid.

Investor perspectives

Most investors consider cybersecurity to be a critical component of risk oversight and are engaging with portfolio companies to better understand how cybersecurity risk is governed and managed. We heard this consistently in late 2018 in conversations with governance specialists from more than 60 institutional investors representing over US$32 trillion in assets under management.

As part of our annual EY Center for Board Matters investor outreach, we asked investors about the top risk issues they are raising in their engagements with companies, and 61% said cybersecurity, regardless of sector, was among those elevated risk issues, even though investors characterize cyber risk as a pervasive and standard risk impacting all companies. Some of the key themes we heard from those conversations were:

- An interest in understanding how boards are structuring oversight (i.e., is a committee or the full board charged with that responsibility)
- How directors are developing competence around and staying up-to-speed on cyber issues
- Who in management is reporting to the board and how often
- Key features of how management is addressing cyber risk
- Interest in data privacy issues and compliance with new privacy laws and regulations

While some investors said they are focused on companies where a cyber incident has occurred, they also said that given the current environment where cybersecurity attacks are inevitable, they are specifically focused on companies' response and recover mechanisms.

What we found

We conducted an analysis of cybersecurity-related disclosures in the proxy statements and annual reports on Form 10-K of the 82 companies on the 2019 Fortune 100 list that filed those documents in both 2018 and 2019 through September 5, 2019. The analysis was based on cybersecurity-related disclosures on the following topics:

- Board oversight, including risk oversight approach, board-level committee oversight, and director skills and expertise
- Statements on cybersecurity risk
- Risk management, including cybersecurity risk management efforts, education and training, engagement with outside security experts, and use of an external advisor

Overall, we observed modest year-over-year increases across most of the disclosures tracked, though the depth and company-specific nature of the disclosures continued to vary widely, including the level of detail. This reveals continued opportunity for enhancement in how risk management activities and responsibilities, response preparedness and board oversight around cybersecurity issues are communicated.

The most significant changes relate to the area of board oversight, including risk oversight approach, board-level committee oversight, and the identification of director skills and expertise as well as officers reporting to the board on cybersecurity. Specifically:

- 89% of companies disclosed a focus on cybersecurity in the risk oversight section of their proxy statements, up from 80% last year.
- More boards assigned cybersecurity oversight to non-audit committees, 28% this year up from 21% in 2018.
  - A portion of these, 9% overall, assigned cyber responsibilities to both a non-audit committee and the audit committee. Most companies, 56% overall, assigned cybersecurity oversight to the audit committee alone. Some companies, 10% overall, indicated that the full board retained cybersecurity oversight, and a small number, 6% overall, did not explicitly disclose how they allocate oversight.
  - Only a few of these boards moved cybersecurity oversight responsibilities from the audit committee to another committee; in most cases cybersecurity oversight responsibilities were newly assigned to a non-audit committee.
- More than half (54%) included cybersecurity as an area of expertise sought on the board or cited in a director biography, up from 40% last year.
- Thirty-three percent identified at least one "point person" from management (e.g., the CISO or the chief information officer) who reports to the board, up from 26% last year

The percentage of companies that disclosed the use of an external independent advisor regarding cybersecurity matters held fairly steady at 12% in 2019 versus 13% last year. Nine percent stated that their preparedness includes simulations, tabletop exercises, response readiness tests or independent assessments.

Fortune 100 company cybersecurity disclosures
2018–19

Topic	Disclosure	2018	2019
Board oversight			
Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	80%	89%
Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	78%	84%
	Disclosed that the audit committee oversees cybersecurity matters	62%	65%
	Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	21%	28%
Director skills and expertise	Cybersecurity included among areas of expertise sought on the board and/or cited in at least one director biography	40%	54%
	Cybersecurity included among the areas of expertise sought on the board	23%	32%
	Cybersecurity cited in at least one director biography	30%	40%
Management reporting structure	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	52%	54%
	Identified at least one "point person(s)" (e.g., the chief information security officer or chief information officer)	26%	33%
Management reporting frequency	Included language on frequency of management reporting to the board or committee(s), but most of this language was vague	39%	43%
	Disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like "regularly" or "periodically"	12%	16%
Statements on cybersecurity risk			
Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%
Risk management			
Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	82%	89%
	Referenced response planning, disaster recovery or business continuity considerations	49%	55%
	Stated that preparedness includes simulations, tabletop exercises, response readiness tests or independent assessments	9%	9%
Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	18%	26%
Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	6%	11%
Use of external advisor	Disclosed use of an external independent advisor	13%	12%

*Percentages based on total disclosures for companies. Data based on the 82 companies on the 2019 Fortune 100 list that filed Form 10-K filings and proxy statements in both 2018 and 2019 through September 5, 2019. *Some companies designate cybersecurity oversight to more than one board-level committee.*

Risk oversight approach

The depth of these disclosures varies widely. Companies on one end of the spectrum only listed cybersecurity among a variety of specific risks incorporated in the board's risk oversight. Companies on the other end provided more in-depth information regarding how the board exercises its cybersecurity risk oversight responsibilities. For example, companies in the latter group disclosed information about how often management is reporting to the board, which member(s) of the management team is meeting with the board, and some of the specific topics discussed.

Director skills and expertise

This year, 33 companies cited cybersecurity in the biography of at least one director, up from 25 companies last year. The meaning of this data is difficult to interpret. For example, a few companies explicitly cited cybersecurity experience in certain director biographies one year but not the other. In sum, the disclosures may at least indicate that companies are paying more attention to noting director experience or expertise in cyber.

Response readiness simulations and tabletop exercises

Nine percent of companies stated that their cybersecurity preparedness includes simulations, tabletop exercises, response readiness tests or independent assessments. This nine percent is weighted to the independent assessments; of the few companies that specifically disclose that they are performing simulations, drills or response readiness exercises at the management level, none disclosed whether the board is involved in these exercises.

Simulations are a critical risk preparedness practice that EY and others believe boards should prioritize. Among other critical benefits, such exercises help companies develop and practice action plans related to data privacy issues. Cyber breaches can — and often do — result in the loss of personal data. These events require compliance with a host of complex state and federal laws (all of which call for prompt notice to states, regulators and affected persons), and may require compliance with the laws of non-US jurisdictions. Preparation is key to promoting compliance.

If companies are performing cybersecurity breach simulations, they should, as a best practice, disclose that, and if not, boards should make this an agenda item in the near term.

Use of external independent advisor

This year, the portion of companies that disclosed the use of an external independent advisor to support management held fairly steady at 12% versus 13% last year. Among the 10 companies that made the disclosure in 2019, only one made clear that the board meets directly with the independent third party. Our research did not identify any discussion of the scope of the external assessments provided or whether an attestation opinion was obtained utilizing the American Institute of Certified Public Accountants' System and Organization Controls for Cybersecurity framework, which provides for an entity-wide examination of the company's cyber risk management program.

Boards of directors

Boards are continuing to increase their engagement on the subject. The National Association of Corporate Directors (NACD) and the Internet Security Alliance first issued *The Director's Handbook on Cyber-Risk Oversight* in 2014, outlining five core principles for board-level cybersecurity oversight. NACD and ISA are expected to issue a third edition of the handbook in 2020, capturing the evolution of the threat environment and providing additional tools for directors.

In spring 2019, Ernst & Young LLP hosted a series of gatherings bringing together board members for discussions on the latest challenges and leading practices in overseeing cybersecurity risk. We engaged with over 100 directors who collectively represent more than 200 public companies. We issued a report, What boards are doing today to better oversee cyber risk, to share insights and takeaways from the conversations with these directors. Two of the key recommendations from this group were that boards should:

- Set the tone that cybersecurity is a critical business issue
- Stay attuned to evolving board and committee cybersecurity oversight practices and disclosures, including asking management for a review of the company's cybersecurity disclosures with peer benchmarking over the last two to three years

US public policy environment

In response to a growing number of high-profile cybersecurity attacks and breaches on US companies, Congress has increased its oversight and engagement on cybersecurity disclosure and cyber-risk management.

Legislators also have introduced legislation, including the Cybersecurity Disclosure Act, for the second straight Congress. The bipartisan bill introduced by Senator Jack Reed (D-RI) and Rep. Jim Himes (D-CT), 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. Differing from the bill introduced in previous legislative sessions, this version of the bill text permits a company to disclose why having cyber expertise on the board is not necessary due to other cybersecurity protocols put in place by the company.

While this bill and other proposed cybersecurity bills have failed to gain momentum in Congress (passing in the House and not receiving a Senate vote), interest in and scrutiny of how companies are managing cybersecurity risks will remain a key focus of Congress and other policymakers in Washington.

Conclusion

Recognizing the threat that cybersecurity attacks pose to companies, consumers, and our capital markets, a variety of stakeholders want to understand how companies plan for and respond to cybersecurity incidents – and how the board conducts oversight of these activities. This understanding is increasingly critical for building stakeholder confidence and trust as the cybersecurity risk landscape evolves and as technological innovations raise the stakes for data privacy and protections.

Public disclosures present an opportunity for companies to further this understanding and demonstrate engagement. By examining how disclosures are evolving and sharing perspectives and insights based on our market engagement, companies can identify opportunities for enhancement of both communications and practices related to this vital matter.

> “As our society increasingly relies on technology, businesses across all sectors of the economy must prioritize cybersecurity. A single cyberattack can cripple even the most sophisticated firms, and the public has a right to know whether companies are focused on preventing cybersecurity threats.[7]
>
> Senator Doug Jones (D-AL)

7 Key US Senators Lead Bipartisan Push for Stronger Cybersecurity by Public Companies, press release, 1 March 2019.

Questions for the board to consider

- Is the board allocating sufficient time on its agenda, and is the committee structure appropriate, to provide effective oversight of cybersecurity?
- Do the company's disclosures effectively communicate the rigor of its cybersecurity risk management program and related board oversight?
- Is the board communicating with C-suite executives beyond the CISO to gain insights into potential business impacts of cyber incidents, and how cybersecurity governance is integrated across all divisions?
- What resources is the board using to enhance its competency on cybersecurity topics and understand emerging threats?
- How is the board getting a pulse on the company's culture with respect to cybersecurity?
- Does management reporting to the board include: (1) metrics that report on the health of the cybersecurity risk management program, including visibility into the effectiveness of the program, and (2) the results of cyber breach simulations? Does the board periodically participate in those drills?
- Does the board understand the scope of work performed through any independent third-party assessments, and is the board having direct dialogue with that third party?
- Has the board considered the value of obtaining a cybersecurity attestation opinion to build confidence among key stakeholders?

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

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

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

US SCORE no. 07406-191US
CSG no. 1909-3271948

ED None

ey.com/us/boardmatters

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