EY Center for Board Matters

How cyber governance and disclosures are closing the gaps in 2022

Cybersecurity is reaching an inflection point. Risks are growing and broader regulations are looming. Some companies are keeping pace, but others are lagging, both in disclosures and warding off threats. To close these gaps, directors should foster a culture of cooperation while elevating the tone at the top.

This is the year for directors to double down on closing the gaps in the company's cybersecurity defense and disclosure practices. The risks companies face, already high, are multiplying and accelerating, marked this year by potential threats tied to the war in Ukraine. Meanwhile, more guidance on cyber oversight and disclosure is here or on its way, from the Securities and Exchange Commission (SEC or commission), which proposed new rules earlier in 2022; and from Congress, which recently passed far-reaching legislation. Additionally, Institutional Shareholder Services Inc. (ISS) added 11 new cyber risk factors to its Governance QualityScore in 2021.

In our latest analysis of cyber-related disclosures in the proxy statements and Form 10-K filings of Fortune 100 companies, we found more companies providing information about how they are rising to the challenges. Yet in some areas, the gaps in information are nearly universal. For instance, only 9% disclosed performing response readiness simulations.

With the stakes so high, directors' tone at the top must continue to elevate the importance of managing cybersecurity risk on a company-wide basis, and not just as an IT matter, and ensuring proper disclosure. Enhanced disclosures clarify for investors and other stakeholders the rigor of the board's oversight, and management's role in assessing and managing cybersecurity risks. But to build better defenses against evolving threats, organizations also need to break out of their silos and echo chambers and promote a culture of cooperation, both internally and with other organizations. Independent outside parties can also help expand knowledge bases, strengthen capabilities and identify blind spots in security and risk management.

In brief

- Growing risks and greater stakeholder demands are leading companies to carefully address what they disclose about governance and management of cybersecurity.
- The SEC prioritized cybersecurity and is expected to finalize rules in early 2023 that will require new cybersecurity disclosures from public companies.
- Fortune 100 companies continue to increase disclosures in certain categories of cybersecurity risk management and oversight.

Fortune 100 cybersecurity disclosures, 2018–22

New this year: References to SEC and ISS denote disclosure areas included in the SEC's proposed rules and ISS's list of risk factors. Note that some elements of the SEC's proposals, notably those relating to material breaches, are not reflected in the chart.

Area of focus	Topic	Disclosure	2022	2021	2020	2019	2018
Category: Board oversight							
	Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	95%	88%	89%	86%	76%
SEC ISS	Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	88%	89%	86%	81%	72%
		▸ Disclosed that the audit committee oversees cybersecurity matters	70%	69%	68%	62%	57%
		▸ Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	28%	28%	24%	26%	18%
SEC ISS	Director skills and expertise	Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	61%	65%	57%	49%	35%
		▸ Cybersecurity disclosed as an area of expertise sought on the board	46%	42%	36%	27%	20%
		▸ Cybersecurity cited in at least one director biography	51%	55%	46%	39%	28%
SEC	Management reporting structure	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	74%	65%	61%	58%	54%
		▸ Identified at least one "point person" (e.g., the chief information security officer or chief information officer)	49%	41%	35%	32%	23%
SEC ISS	Management reporting frequency	Included language on frequency of management reporting to the board or committee(s)	68%	54%	47%	43%	36%
		Disclosed reporting frequency (e.g., annually, quarterly)	39%	31%	15%	15%	11%
Category: Statements on cybersecurity risk							
	Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%	100%	100%
		Included data privacy as a risk factor	99%	99%	99%	97%	93%
Category: Risk management							
SEC ISS	Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	99%	97%	93%	91%	85%
		Disclosed alignment with external framework or standard	18%	9%	3%	3%	1%
		Referenced response readiness, such as planning, disaster recovery or business continuity considerations	66%	65%	61%	57%	53%
		Stated that preparedness includes simulations, tabletop exercises or response readiness tests	9%	5%	7%	3%	3%
		Stated that the company maintains a level of cybersecurity insurance	51%	43%	36%	36%	31%
		Included cybersecurity in executive compensation considerations	7%	11%	5%	1%	0%
ISS	Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	45%	36%	30%	26%	18%
	Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	15%	12%	11%	12%	7%
SEC ISS	Use of external advisor	Disclosed use of an external independent advisor	28%	22%	15%	12%	15%
		Disclosed board engagement with an external independent advisor	7%	7%	4%	3%	1%
		Disclosed that the external advisor provided attestation	14%	8%	4%	4%	4%

Percentages based on total disclosures by companies. Data based on the 74 companies on the 2022 Fortune 100 list that filed Form 10-Ks and proxy statements in 2018, 2019, 2020, 2021 and 2022 through May 31, 2022. Areas of focus were referenced in the SEC proposed rules and/or by ISS in its list of Governance QualityScore cyber risk factors released in February 2021.
*Some companies delegate cybersecurity oversight to more than one board-level committee.

Our refreshed analysis of the proxy statements and 10-K filings, the fifth in an annual series, was designed to identify emerging trends and opportunities for enhanced communication. We looked at filings from 74 Fortune 100 companies that filed from 2018 through May 31, 2022. We cited sample language from their disclosures and also examined the current US regulatory and public policy cyber landscape.

To be sure, the latest proxy statement and 10-K filings provide a look back. By contrast, the SEC's proposed rules, among others, will shape the future. They have the potential to expose gaps in defenses and disclosures while serving as a roadmap for closing them. Companies shouldn't wait to use that map. This is the year to get moving.

> "The range of criminal, cyber and counterintelligence threats we face as a nation has never been greater or more diverse.
>
> FBI Director Christopher Wray, testifying before a Senate Appropriations subcommittee, May 25, 2022

The SEC's proposed rules: to be finalized in 2023

Under Chair Gary Gensler, the SEC has prioritized cybersecurity in its agenda. In 2022, the commission issued a couple of cyber-related rulemakings, illustrating its commitment to addressing cyber threats in the capital markets.

In March, the commission proposed rules that would, among other things, require cybersecurity incident reporting, and periodic reporting by public companies of their cybersecurity risk management, strategy and governance. The SEC's regulatory agenda indicates it will finalize the proposed rules in spring 2023. As drafted, the rules would require registrants to disclose the following information:

- Whether there is cybersecurity expertise on the company's board of directors and, if so, the nature of such expertise
- Whether the entire board, specific board members or a board committee oversees cybersecurity risks; how the board is informed about those risks, including the frequency of its discussions on the topic; and how the board or relevant board committee considers the risks as part of its oversight of business strategy, risk management and financial oversight
- Policies, procedures and strategies, if any, for identifying and managing cyber threats
- Management's role in assessing and managing cybersecurity risks and in implementing the registrant's cyber policies, procedures and strategies, including whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, and whether the registrant has a designated chief information security officer (CISO)

The proposal also requires disclosure of a material cybersecurity incident in Form 8-K within four business days of determining that it is material, and that registrants provide updates in periodic reports about previously disclosed material incidents. In addition, registrants must disclose when a series of previously undisclosed individually immaterial cyber incidents becomes material in the aggregate.

See page 10 for further information on key US regulatory and public policy developments.

What we found: mixed results

In comparing the proxy statements and Form 10-K filings of Fortune 100 companies over the past five years, we have seen steady and significant increases in the percentage of disclosures in certain categories of cyber management and oversight. One aspect relating to disclosing director cybersecurity skills and expertise, for example, had a 61% disclosure rate in 2022, up from 35% in 2018.

Other areas of noteworthy increases in disclosure rates in the 2022 filings:

- Providing insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters (74% in 2022, up from 54% in 2018), and identifying at least one point person (e.g., the chief information security officer (CISO) or chief information officer (CIO)), 49%, up from 23%
- Frequency of management reporting to the board or committee(s), 68%, up from 36%
- Maintaining cybersecurity insurance, now 51%, up from 31%

Another one of the biggest increases came in disclosing the use of education and training efforts to mitigate cyber risk. In 2022, 45% of the companies we reviewed made such a disclosure, up sharply from 18% in 2018, but still leaving 55% silent in this fundamental area, which could leave investors with uncertainty as to whether the company provides cybersecurity education and training.

By contrast, some areas have only a few registrants making disclosures. For example, the rate of disclosures of tabletop exercises and response readiness tests has grown from only 3% in 2018 to 9% now.

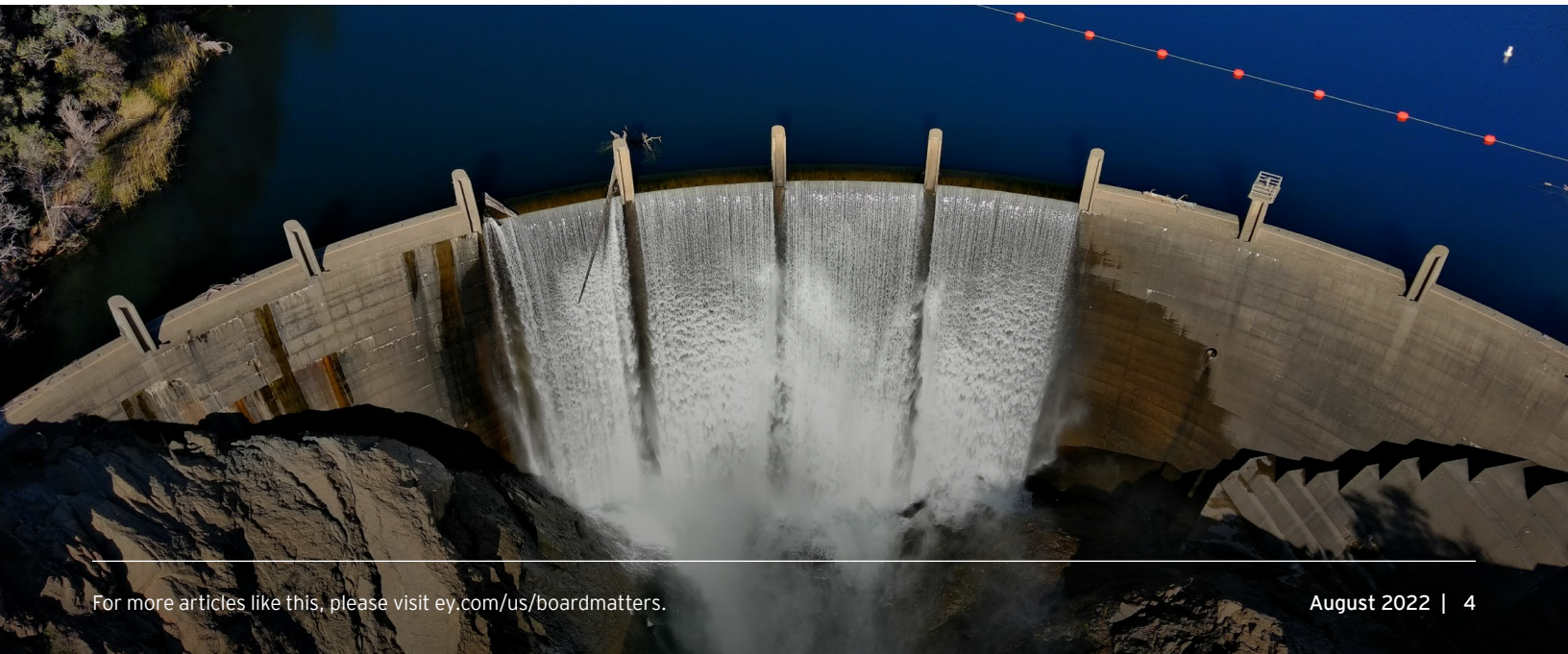
That said, we continue to see a broad range of opportunities for more companies to disclose practices that are vital to enhancing their cyber resiliency. Such practices include collaboration with peers, industry groups or policymakers, and, of course, the use of cyber readiness simulations. They also include the use of external expertise and adding cybersecurity responsibilities to executive compensation considerations.

What follows is our analysis of the latest disclosures and five-year trends. In certain key areas, we provide a comparison with the proposed SEC rules, underscoring the gaps that some companies will need to address in their practices and disclosures.

Identification of director skills and expertise

Disclosing whether directors have expertise in cybersecurity, which would be a new requirement under the SEC's proposed rules, represents one of the more significant shifts in disclosure rates that we've observed since initiating this analysis five years ago. In 2022, 46% of companies disclosed cybersecurity as an area of expertise sought on the board, up from 20% in 2018. More than half of the companies now cite cybersecurity experience in at least one director biography, up from 28% in 2018.

A closer look at these changes over the past few years shows that, in most cases, the increases in director experience are related to either a new person joining the board or some companies starting to add cyber-related experience to longer-standing board member bios. The new arrivals have included former CISOs and senior information technology executives, the head of a cybersecurity company, and former leaders in federal intelligence agencies or the military.



Management reporting to the board

Another new requirement in the SEC proposed rules is disclosing how the board is informed about cyber risks and the frequency of its discussions on this topic. Over time, we've seen disclosure enhancements regarding management reporting on such risks to the board. This year, 74% of companies provided insights into management reporting to the board and/or committee overseeing cyber matters, up from 54% in 2018.

While that change is notable, the real change we're seeing is around who is providing that information and how often it is conveyed. In 2022, 49% identified at least one person who is reporting to the board on cybersecurity, most often the CISO or CIO, up from 23% in 2018. Similarly, 39% disclosed this year that management is reporting to the board on cybersecurity at least annually or quarterly, up from 11% in 2018. Many other companies include language on the frequency of management reporting, but typically that language is not specific, alluding to reports to the board that occur "regularly" or "periodically."

As the proposed rules indicate, the commission is looking for more disclosures in management reporting practices and the senior executives' level of expertise. As noted earlier, the proposed disclosure requirements include disclosing whether the registrant has a designated CISO or employs someone comparable; details about that person's credentials; and identifying the person to whom that executive reports. The disclosure would also say whether and how frequently the CISO or equivalent briefs the board or a board committee on cybersecurity risk.

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

Board-level committee oversight

Under the proposed rules, the SEC wants companies to disclose whether the entire board, specific members or a board committee is responsible for cybersecurity oversight. In our research, 88% of companies this year charged at least one board-level committee with oversight, up from 72% in 2018. Since 2018, we've observed a significant increase in boards assigning oversight to non-audit committees, most often risk or technology committees. This year, 28% of boards chose a non-audit committee, up from 18% in 2018. Among the boards making that choice, 86% added cyber responsibilities to the committee charter. Separately, Gartner reports that less than 10% of boards currently have a dedicated cybersecurity committee, but predicts that 40% will establish one by 2025.[1]

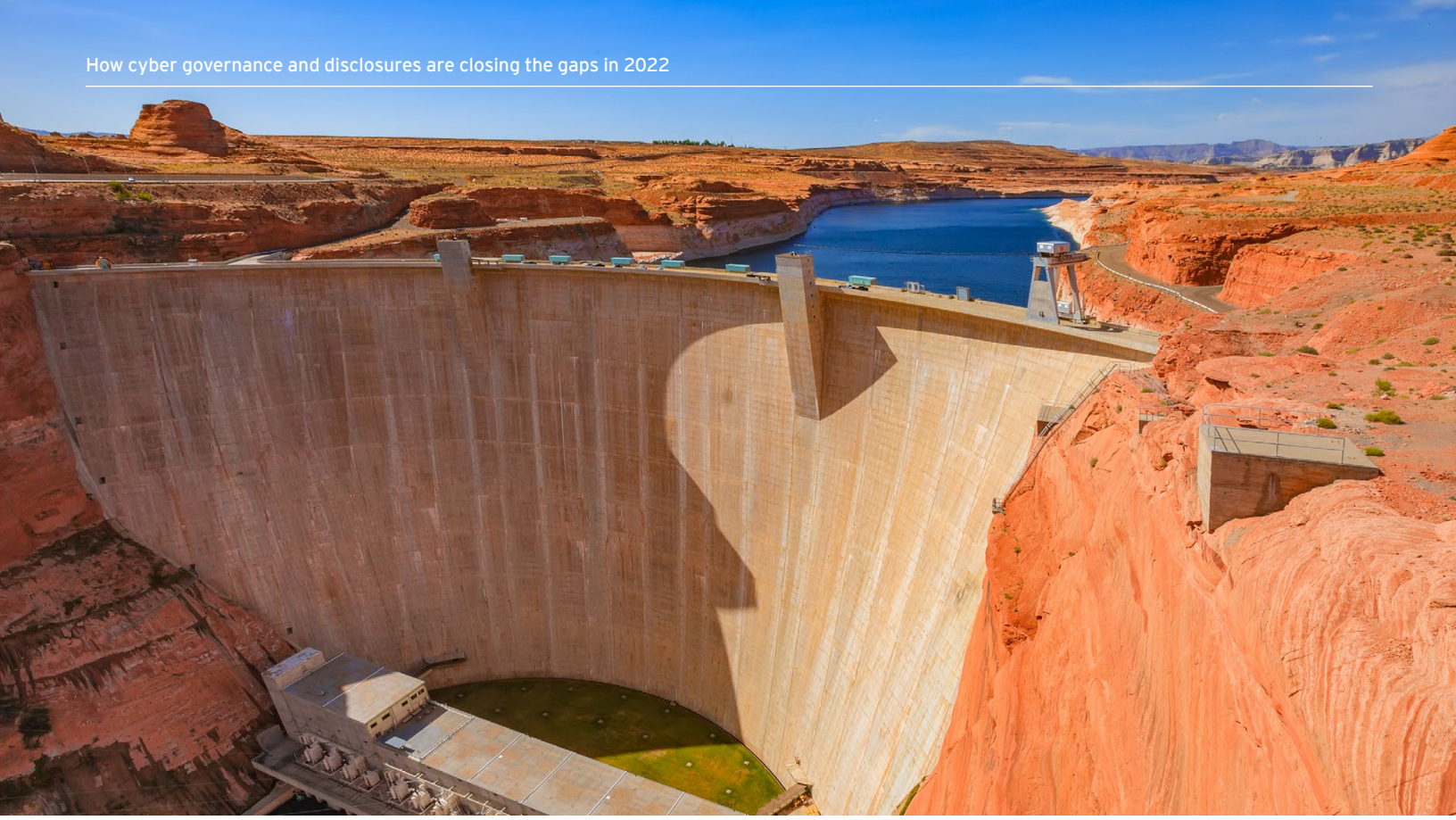
For now, at least, audit committees remain the primary choice to oversee cybersecurity risk. This year, 70% of the boards chose audit, up from 57% in 2018. One company disclosed this year that it had shifted oversight from audit to an ad hoc committee. Among the boards that chose the audit committee, 69% formalized that responsibility in the committee charter. Given proposed ESG disclosure rules coming in the near term, it remains to be seen whether audit committees can absorb both incremental cyber and ESG reporting obligations and governance responsibilities within their respective charters.

> "Gartner reports that less than 10% of boards currently have a dedicated cybersecurity committee, but predicts that 40% will establish one by 2025.

Alignment with an external framework or standard

The number of companies that disclosed the alignment of their cybersecurity program and information security practices with an external security process or control framework increased to 18% this year, double the percentage from 2021 and up from just 1% in 2018. The framework of the National Institute of Standards and Technology (NIST) was cited by 10 companies, more than any other. Among the others chosen were the International Organization for Standardization (ISO) 27001 and HITRUST. A number of companies also disclosed that certain portions of their controls were covered by the American Institute of Certified Public Accountants (AICPA) System and Organization Controls for Service Organizations: Trust Services Criteria (SOC 2) service audit reports.

[1] Gartner, Inc. news release dated January 28, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-.



Compensation incentives

This year, we observed a modest decrease in companies specifically disclosing performance related to cybersecurity or privacy issues as a consideration in determining executive pay. Seven percent of companies did so, down from 11% last year; in 2018, the percentage was zero. Nonetheless, companies generally cited cyber considerations (e.g., driving and responding to policy initiatives on cybersecurity and data privacy in the face of escalating threats) among a host of other nonfinancial company or individual performance considerations in executive pay decisions.

Response readiness simulations and tabletop exercises

The percentage of companies disclosing that they performed cyber incident simulations or conducted tabletop exercises with management and/or the board remains very low, increasing to just 9% this year, from 5% in 2021 and 3% in 2018. Of the companies that disclosed such exercises, several disclosed that the board participated, and one specified it was a ransomware simulation.

Simulations are a critical risk preparedness practice that Ernst & Young LLP (EY) and others believe companies should prioritize. Yet in one of our recent polls of directors, 86% said their board had not participated in a breach or ransomware simulation exercise in the last 12 months.[2]

If cybersecurity breach simulation plans are not practiced and a breach occurs, the reaction by the board and management is largely improvised. Well-designed incident simulations and tabletop exercises can stress-test the organization and improve readiness by providing clarity of roles, protocols and escalation processes and can include third parties (e.g., a public relations firm, forensic specialists). Policies on ransomware should also be established ahead of time, including whether the company and board would approve payment and under what circumstances. Management should conduct these exercises to test the company's significant vulnerabilities and identify where the greatest financial impact could occur. Boards should consider participating in these simulations so that their insights and experiences can be incorporated to elevate the company's ability to respond and recover.

Further, such exercises help companies develop and practice action plans related to data privacy issues. Cyber breaches can — and often do — result in the loss of personal data. These events require compliance with a host of complex state and federal laws (all of which call for prompt notice to states, regulators and affected persons), and may require compliance with the laws of non-US jurisdictions. Practice is key to ensuring effective preparation and responses.

[2] Survey of directors during the EY cybersecurity webcast "Ransomware," October 8, 2021.

Use of external independent advisor

The percentage of companies disclosing the use of an external independent advisor to support management grew to 28% this year, from 22% the year before and 15% in 2018. Among the companies that made the disclosure this time around, five indicated that the board received reports from the independent third party. One company disclosed that the audit committee receives semiannual reports from its independent cybersecurity advisor.

The National Association of Corporate Directors (NACD) and the Internet Security Alliance's Director's Handbook on Cyber-Risk Oversight encourages boards to have deep-dive briefings from independent third-party experts validating whether the company's cyber risk management program is meeting its objectives. In the absence of a cyber expert on the board, retaining an independent expert (or organization) to regularly advise the board on cyber matters may become a growing practice, as boards already avail themselves of similar expertise on matters such as executive compensation and fairness opinions.

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

Disclosure of cyber incidents

There appears to be a gap between disclosures around material cybersecurity incidents, including the depth of the disclosures, as compared with the number and scale of cyber incidents reported in the news media and third-party reports. For example, the SEC rule proposal cites that a total of 74,098 Form 8-K filings were made in 2020 involving 7,021 filers, out of which 40 filings reported material cybersecurity incidents.[3] Yet, the 2020 Verizon Data Breach Incident Report stated there were 3,950 confirmed data breaches in 2020[4] but did not address the materiality of these breaches.

Even when ransomware is involved, most breaches stay under the radar. "We believe that only about a quarter of ransomware intrusions are actually reported," Eric Goldstein, Executive Assistant Director of the Cybersecurity & Infrastructure Security Agency (CISA), told *The Washington Post* last year.[5] CISA is a unit of the Department of Homeland Security (DHS).

[3] SEC's Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, March 9, 2022, page 62.

[4] 2020 Verizon Data Breach Incident Report, page 5.

[5] "Many ransomware attacks go unreported. The FBI and Congress want to change that," *The Washington Post*, July 27, 2021.

A report by Audit Analytics, Trends in Cybersecurity Breach Disclosures, examining breaches affecting public companies, found that the number of reported incidents climbed to a high of 188 in 2021, up from 28 in 2011. The report noted that, in 2021, 43% of the incidents were disclosed in a filing with the SEC. Most commonly, the disclosure appeared in the risk factors section of a periodic report.

In the proposed rules, the SEC requires disclosure of a material cybersecurity incident in Form 8-K within four business days of determining that it is material, and that registrants provide updates in periodic reports about previously disclosed material incidents. The SEC states the information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important."[6] In addition, the proposed rules would require companies to disclose in periodic reports when a series of previously undisclosed individually immaterial incidents become material in the aggregate.

In its Governance QualityScore rating solution, ISS includes several factors that address disclosures of information security breaches (see sidebar). These include: Has the company experienced a breach in the last three years, how long ago did the most recent breach occur (in months), net expenses incurred from breaches over the last three years relative to total revenue, and net expenses incurred from breach penalties and settlements in the last three years relative to total revenue.

Disclosures range from stating the occurrence of an incident to providing a more in-depth account, including the number of account holders affected; the nature of the data; costs and insurance offsets; and remedial steps taken to fix the security vulnerability.

> "Information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important.'

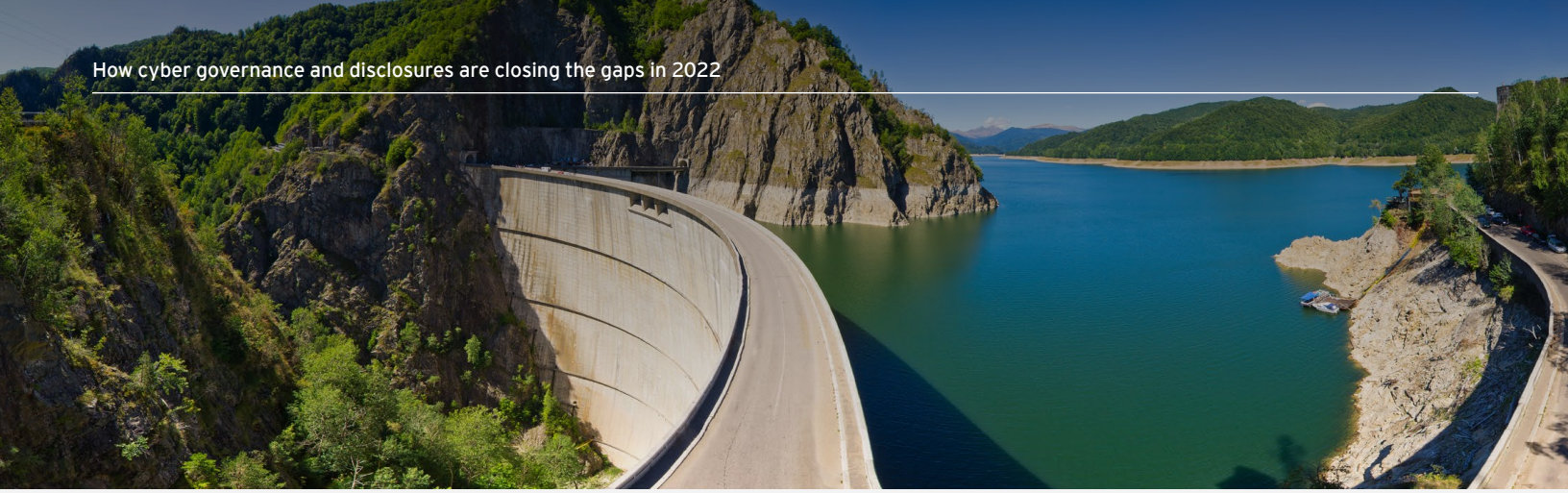
[6] SEC's Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, March 9, 2022, page 23.

Institutional Shareholder Services' Governance QualityScore cyber risk factors

In February 2021, ISS announced methodology changes to its Governance QualityScore rating solution, including the addition of the following 11 factors concerning information security risk oversight and management.[i]

1. What percentage of the committee responsible for information security risk is independent?
2. How often does senior leadership brief the board on information security matters?
3. How many directors with information security experience are on the board?
4. Does the company disclose an approach on identifying and mitigating information security risks?
5. What are the net expenses incurred from information security breaches over the last three years relative to total revenue?
6. Has the company experienced an information security breach in the last three years?
7. What are the net expenses incurred from information security breach penalties and settlements over the last three years relative to total revenue?
8. Has the company entered into an information security risk insurance policy?
9. Is the company externally audited or certified by top information security standards?
10. Does the company have an information security training program?
11. How long ago did the most recent information security breach occur (in months)?

[i] ISS ESG Unveils 2021 Methodology Enhancements for Governance QualityScore, February 8, 2021.



Our market observations

EY regularly engages with boards and hosts gatherings of directors and cybersecurity experts to discuss challenges and leading practices in overseeing cyber risk. During the past year, our programs included dialogues involving more than 500 directors, and a three-part webcast series attended by over 18,000 people. The webcasts covered these topics:

1. Ransomware
2. Leading practices for cyber oversight
3. Regulatory developments in cyber and data privacy

When cyber criminals strike, the main differentiator between failure and resiliently weathering the crisis is leadership. A proactive sense of urgency, readiness, presence and constant engagement must come from the top of the organization. Yet in one of our recent polls, only 23% of directors said their organization was "very ready" to respond to a ransomware attack.[7]

Even if ransomware attacks are inevitable, catastrophic damage is not. Influence, disruption and deterrence are proactive measures that each organization should take before incidents occur. That means focusing on early detection, isolating critical assets, making continuity plans for operating in crisis mode, complying with authorities while hedging against litigation, and communicating with employees, customers and investors.

Directors also need to be aware of a looming challenge spawned by the proliferation of artificial intelligence. When asked in one of our poll questions how much they understood of their organization's AI and robotic-related risks, more than a third (35%) said "not much," with another 51% saying only "somewhat well." Just 14% said they understood those risks "very well."[8]

Based on insights gained through these engagements with directors, as well as what EY cybersecurity leaders have learned from assignments around the globe and across industries and company sizes, we have identified these 10 leading practices to help boards oversee cyber risk:

1. **Elevate the tone.** Establish cybersecurity as a key consideration in all board matters.
2. **Stay diligent.** Address new issues and threats stemming from remote work and the expansion of digital transformation. And remember that every employee needs to be diligent, too — 82% of breaches involve a human element, according to Verizon's 2022 Data Breach Incident Report, issued in late May.
3. **Determine value at risk.** Reconcile value at risk in dollar terms against the board's risk tolerance, including the efficacy of cyber insurance coverage.
4. **Leverage new analytical tools.** Such tools inform the board of cyber risks ranging from high-likelihood, low-impact events to low-likelihood, high-impact events (i.e., a black swan event).
5. **Embed security from the start.** Embrace a "trust by design" philosophy when designing new technology, products and business arrangements.
6. **Independently assess your program.** Obtain a rigorous third-party assessment of your cyber risk management program (CRMP).
7. **Evaluate third-party risk.** Understand management's processes to identify, assess and oversee the risk associated with service providers and third parties involved in your supply chain. Supply chains were responsible for 62% of system intrusion incidents in 2021, according to Verizon's 2022 Data Breach Incident Report.
8. **Test response and recovery.** Enhance enterprise resilience by conducting rigorous simulations and arranging protocols with third-party specialists before a crisis.
9. **Understand escalation protocols.** Have a defined communication plan for when the board should be notified, including incidents involving ransomware.
10. **Monitor evolving practices and the regulatory and public policy landscape.** Stay attuned to evolving oversight practices, disclosures, reporting structures and metrics.

[7] Survey of directors during the EY cybersecurity webcast "Ransomware," October 8, 2021.

[8] Survey of directors during the EY cybersecurity webcast "Regulatory developments in cyber and data privacy," October 22, 2021.

US public policy developments

Following up on President Biden's May 2021 executive order on cybersecurity, the administration has continued its efforts to strengthen the nation's cyber defenses, particularly in the wake of the war in Ukraine and related cyber threats. Disclosure of cyber breaches continues to be a major topic of consideration, both at federal agencies and in Congress.

In a statement issued on March 21, 2022, the president underscored the important role that US corporations must play in the fight: "You have the power, the capacity and the responsibility to strengthen the cybersecurity and the resilience of the critical services and technologies on which Americans rely."

The SEC's Division of Corporation Finance posted a sample comment letter on the SEC website to illustrate the types of comments it may issue to companies regarding disclosures on the direct and indirect effects of the war in Ukraine, the sanctions on Russia, and related supply chain issues. In the letter, the SEC staff reminded registrants that they have obligations to provide detailed disclosures, to the extent material or otherwise required, about new or heightened risk of cyber attacks.

Additional SEC cyber-related activity

In addition to the proposed cybersecurity disclosure rules for registrants, in February 2022, the SEC proposed rules on cybersecurity risk management applicable to registered investment advisors and funds. If adopted, these proposals would enhance advisor and fund disclosures related to cyber risks and incidents and require funds to adopt and implement written policies and procedures.

Chair Gensler has noted that the commission also is considering cyber issues relating to service providers that work with financial sector registrants (but are not necessarily registered with the SEC themselves) and cyber risks at the SEC itself.

The SEC's Division of Enforcement also has focused on cybersecurity matters. Division Director Gurbir Grewal has highlighted cybersecurity as "a critical issue in our securities markets and our economy as a whole," and further noted that the commission must remain vigilant in "both ensuring that market participants safeguard essential data and systems, and pursuing public companies that do not reasonably disclose material cybersecurity incidents." In recent months, the division has brought several actions against SEC registrants for cybersecurity-related issues, including inadequate disclosure controls and procedures.[9] To advance its cyber-related enforcement efforts, the SEC recently announced it has nearly doubled the size of the division's Crypto Assets and Cyber Unit. While it is expected to undertake enforcement activity relating to digital assets, the SEC press release indicates that the unit will also "continue to tackle the omnipresent cyber-related threats to the nation's markets."

Biden administration: a public-private effort

The administration has aimed to shore up protections for both the private sector and government. In an effort to increase cooperation between the two, a number of additional resources have been provided:

- NIST is in the process of updating its Framework for Improving Critical Infrastructure Cybersecurity. The framework "focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes." This will be the third updated version of the guidance.
- NIST also released a revised version of its Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, which "provides guidance on identifying, assessing and responding to cybersecurity risks throughout the supply chain at all levels of an organization."
- DHS established a Cybersecurity Review Board made up of 15 cyber leaders from both the public and private sectors. The purpose of the board is to review major cyber events, assess vulnerabilities in the nation's critical infrastructure and make recommendations for both sectors. Currently serving on the board are officials from DHS, the Department of Justice and the National Security Agency, along with representatives of Google, Microsoft and Verizon, among other experts in tech and telecom.

On March 21, 2022, the administration issued a warning about the "potential that Russia could conduct malicious cyber activity against the United States" in response to US sanctions after the Ukraine invasion, and urged companies to take specific steps to guard against attacks. CISA spearheaded efforts to share information on Russian threats and strategies, particularly with respect to critical infrastructure. CISA's "Shields Up" program serves as a central source of information about threats and actionable guidance for business leaders and individuals.

The administration has also taken a variety of actions aimed at strengthening the federal government's cyber defenses, as well as enacting specific requirements for federal contractors.

[9] See, e.g., *In the Matter of First American Financial Corporation*, June 14, 2021.

For example, the president's May 2021 executive order requires each federal agency to "develop a plan to implement Zero Trust Architecture," and CISA drafted the Zero Trust Maturity Model to assist agencies in their transition. Both the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) are adding specific requirements relating to cyber incident reporting and security, as mandated by Section 2 of the order. NIST also issued software supply chain security guidance to establish security standards for software procured by the federal government.

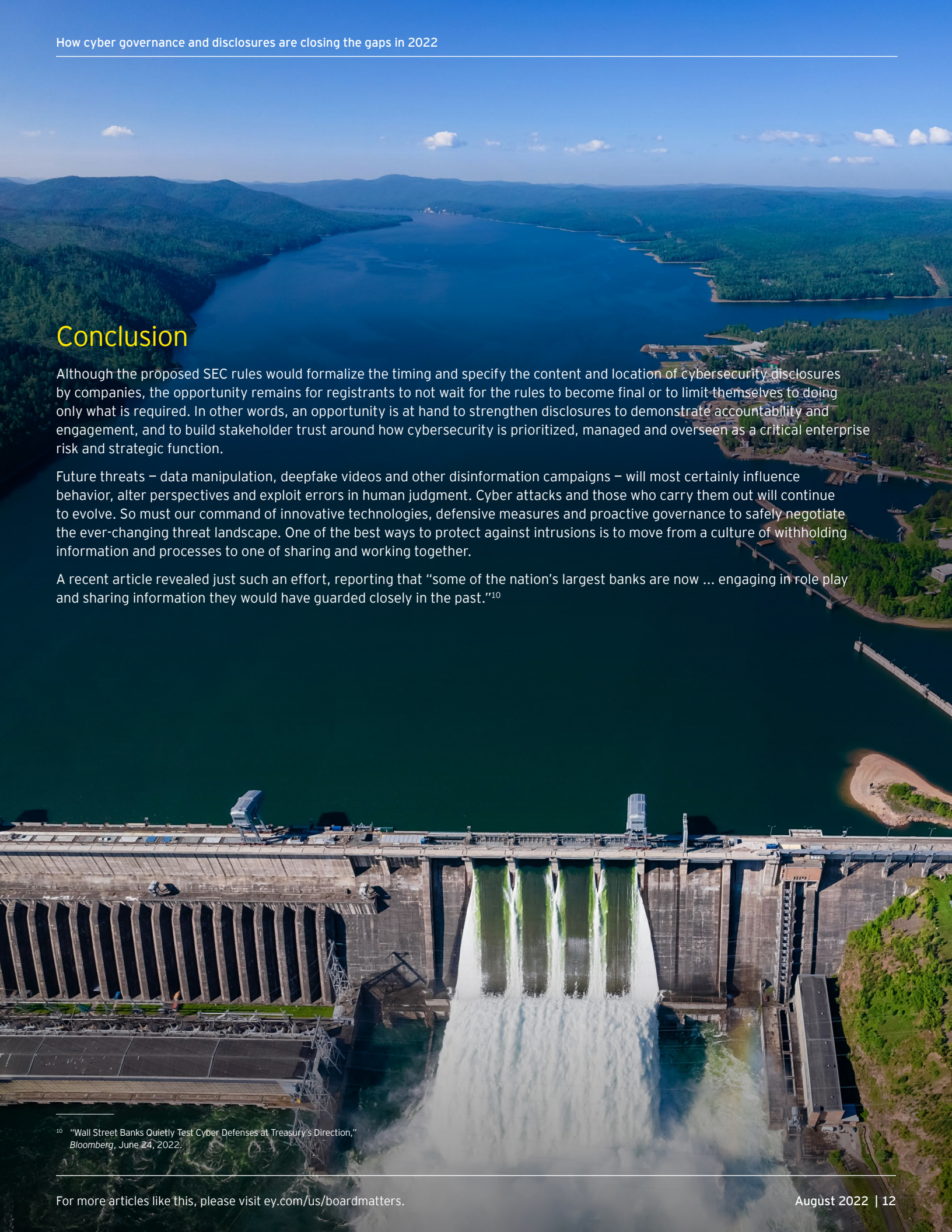
Congressional action: legislation and funding

Meanwhile, Congress has passed significant new cyber legislation and provided additional funding for cyber efforts.

The Infrastructure Investment and Jobs Act (IIJA), signed into law in November 2021, designates more than $2 billion for cyber resiliency and innovation. The law includes funds to reduce cyber vulnerabilities in public water systems and drinking/clean water technology. It also allocates funding to state and local authorities via grant programs for cyber functions that include detecting and recovering from cyber threats and emergencies.

On the policy front, the National Defense Reauthorization Act for fiscal year 2022 formally codified CISA's CyberSentry program, which had been launched as a pilot program in 2020. Through CyberSentry, CISA partners on a voluntary basis with critical private infrastructure providers to continuously monitor cyber threats and provide mitigation and remediation assistance in the event of an incident.

Most notably, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), thus far the most sweeping cybersecurity disclosure mandate applicable to the private sector. CIRCIA requires "covered entities" to disclose substantial cyber incidents to the federal government within 72 hours and ransom payments within 24 hours. CISA is directed to propose rules implementing the legislation within two years of enactment (i.e., by March 15, 2024); the rules then must be made final within 18 months. CIRCIA's coverage is expected to be broad and could apply to those critical infrastructure sectors identified by DHS, which range from communications and financial services to water systems.



Conclusion

Although the proposed SEC rules would formalize the timing and specify the content and location of cybersecurity disclosures by companies, the opportunity remains for registrants to not wait for the rules to become final or to limit themselves to doing only what is required. In other words, an opportunity is at hand to strengthen disclosures to demonstrate accountability and engagement, and to build stakeholder trust around how cybersecurity is prioritized, managed and overseen as a critical enterprise risk and strategic function.

Future threats — data manipulation, deepfake videos and other disinformation campaigns — will most certainly influence behavior, alter perspectives and exploit errors in human judgment. Cyber attacks and those who carry them out will continue to evolve. So must our command of innovative technologies, defensive measures and proactive governance to safely negotiate the ever-changing threat landscape. One of the best ways to protect against intrusions is to move from a culture of withholding information and processes to one of sharing and working together.

A recent article revealed just such an effort, reporting that "some of the nation's largest banks are now … engaging in role play and sharing information they would have guarded closely in the past."[10]

[10] "Wall Street Banks Quietly Test Cyber Defenses at Treasury's Direction," *Bloomberg*, June 24, 2022.

Appendix: Sample language from public disclosures

Security reports

Equifax released its 2021 Security Annual Report on March 23, 2022. The report, according to a company news release, "is part of the company's ongoing commitment to further transparency in cybersecurity. The report outlines the company's investments in top-tier cybersecurity capabilities and a security-first culture; how Equifax has innovated its security infrastructure in ways that make its business, customers and consumers more secure; and the steps taken to collaborate across the industry to be a force for good in cybersecurity."

Charters

Charters for board committees should be updated regularly and accurately reflect the committee's responsibilities. The General Motors Risk and Cybersecurity Committee charter is one of the better examples outlining a committee's cyber risk governance responsibilities.

Pointing out the board's cyber expertise

A leading practice for companies to disclose board director expertise is the use of a matrix and director bios in the annual proxy statement. The Morgan Stanley 2022 proxy statement, on pages 15–22, includes a matrix noting the directors' general experience, qualifications and skills and highlighting which members have a cyber, technology and information security background. The qualifications are listed in each of the directors' bios.

Information about the board's oversight of cyber risks, including how it is kept informed and how it or a relevant board committee considers the risks as part of its oversight of business strategy, risk management and financial matters

Example A

The Audit Committee is charged with oversight of data privacy and cybersecurity risks. Protection of our customers' data is a fundamental priority for our Board and management team. Our Chief Information Officer and our Chief Information Security Officer provide updates at each quarterly Committee meeting on our cybersecurity risks and actions taken to mitigate that risk to the Audit Committee and meet with the full Board at least annually. The Chief Information Security Officer reports on compliance and regulatory issues, continuously evolving threats and mitigating actions, and presents a NIST Cybersecurity Framework Scorecard to the Audit Committee.

Example B

The committee, which includes directors with technology and cybersecurity experience, met a total of five times during the year. At each of those meetings, the committee received updates from the company's Chief Information Officer and Chief Security Officer, among other members of management, on technology investments, IT programs and operations, and the company's information security programs, matters, and efforts.

Example C

Board oversight of cybersecurity. We are a global financial services company and understand the substantial operational risks for companies in our industry as well as the importance of preserving the trust of our customers and protecting personal information. To that end, we have an extensive cybersecurity governance framework in place. Our Board receives reports on cybersecurity at least once a year and our Risk Committee receives reports on cybersecurity at least twice a year, including in at least one joint meeting with the Audit and Compliance Committee, and all receive ad hoc updates as needed. In addition, the Risk Committee annually approves the Company's Information Security Program.

Our cybersecurity program is designed to protect the confidentiality, integrity and availability of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The program is built upon a foundation of advanced security technology, a well-staffed and highly trained team of experts, and robust operations based on the National Institute of Standards and Technology Cybersecurity Framework. This consists of controls designed to identify, protect, detect, respond to and recover from information and cybersecurity incidents. The framework defines risks and associated controls which are embedded in our processes and technology. Those controls are measured and monitored by a combination of subject matter experts and a security operations center with our integrated cyber detection, response and recovery capabilities.

Example D

The full Board absorbed the Technology Committee's duties and responsibilities, including reviewing the company's cybersecurity risks, policies, controls and procedures and overseeing the company's technology strategy. The Board believes that all directors should be responsible for oversight of these matters given the increasing importance of cybersecurity to our risk profile as well as the significant role our technology strategy plays in our strategic priorities. Both our Chief Information Officer and our Chief Information Security Officer regularly report to the full Board.

At least two times per year, the Chief Information Security Officer meets with the Board to report on the company's internal and external cybersecurity risks, our actions and responses and related information. Management also timely briefs the Board on policy and regulatory cybersecurity matters.

Example E

On a quarterly basis, or more frequently as needed, the Audit Committee and/or the full Board receives detailed reports on data protection and cybersecurity matters from senior members of our IT department, including our Chief Information Officer and Chief Information Security Officer. The topics covered include risk identification and management strategies, consumer data protection, the Company's ongoing risk mitigation activities, results of third-party assessments and testing, updates on annual associate training and other specific training initiatives, and cybersecurity strategy and governance structure.

Example F

Protecting the security and integrity of the information and systems under our control and safeguarding the privacy of our customer and employee information has long been a priority. In fact, cybersecurity and privacy risks are among the core enterprise risks for Board-level oversight identified through our annual Enterprise Risk Management ("ERM") assessment.

Our cybersecurity strategy, policies and practices are overseen by a Cybersecurity Leadership Council, headed by our Chief Financial Officer and Chief Legal Officer. Other members include the Chief Information Security Officers ("CISOs"), Chief Technology Officers ("CTOs"), Chief Financial Officers and General Counsels of our divisions, along with our head of Internal Audit. Our information security programs cover a comprehensive range of capabilities, including network security, endpoint security, vulnerability management, antivirus and malware protection, encryption and access control.

We are committed to data protection, perform annual third-party certifications/audits where appropriate, and engage an independent firm to perform a cyber capability maturity assessment every three years. Our Board, including through our Audit Committee, reviews and discusses our cybersecurity risks, practices and protections with our CISOs and CTOs at least twice per year. In addition, our Audit Committee receives regular updates on our cybersecurity posture throughout the year from our head of Internal Audit as appropriate.

Example F, continued

We also have a Privacy Council, which includes our Chief Legal Officer and our Chief Compliance Officer, and the Chief Privacy Officers and General Counsels of our divisions, that reviews and assesses privacy risks throughout our businesses and shares best practices. We respect the privacy rights of individuals and have implemented tailored privacy compliance programs for our businesses. Our Board, through our Governance and Corporate Responsibility Committee, reviews and discusses our privacy program, processes and priorities with our Chief Privacy Officers.

Response readiness and tabletop exercises

The Board remains committed to ensuring that we are prepared for whatever may come next. Last September, the Board held a full-day strategy session to assess the execution of the company strategy and concluded that the company was on track. Directors also participated in an intensive cyber resilience and crisis management simulation session, including a simulation to demonstrate the company's response readiness in the event of a cyber-crisis incident.

Use of external independent advisor and board engagement

Example A

The audit committee receives semi-annual reports from its independent cybersecurity advisor.

Example B

Each quarter, the Risk and Cybersecurity Committee reviews management's Cybersecurity Maturity Scorecard, which leverages both the National Institute of Standards and Technology cybersecurity framework and the Federal Financial Institutions Examination Council maturity rating.

Example C

The Company's information technology systems are assessed by independent parties for the following on an enterprise basis: Payment Card Industry Data Security Standards ("PCI DSS"); HIPAA; SOC 1; and National Association of Insurance Commissioners ("NAIC"). Also, certain of the Company's business units are assessed by independent parties for the following: SOC 2; SOC 2 Type 2; NIST 800-53; and HITRUST. As a backstop to its strong information security programs, policies and procedures, the Company annually purchases a cyber security risk insurance policy that would defray the costs of an information security breach.

Alignment with external framework or standard

The company has a comprehensive cybersecurity and information security framework that includes risk assessment and mitigation through a threat intelligence-driven approach, application controls, and enhanced security with ransomware defense. The framework leverages International Organization for Standardization (ISO) 27001/27002 standards for general information technology controls, International Society of Automation (ISA) / International Electrotechnical Commission (IEC) standards for industrial automation, the National Institute of Standards and Technology (NIST) Cyber Security Framework for measuring overall readiness to respond to cyber threats, and Sarbanes-Oxley (SOX) for assessment of internal controls.

Questions for the board to consider

- **Has management performed an analysis comparing the company's current cybersecurity disclosures with the SEC's proposed rules and shared the results with the board?**
- Do the company's disclosures effectively communicate the rigor of its cyber-risk management program and related board oversight?
- Is the board allocating sufficient time on its agenda, and is the committee structure appropriate, to provide effective oversight of cybersecurity and ESG disclosure requirements?
- Have appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis and given a dollar value?
- What kind of threats is the company most concerned about? How does the company monitor the evolving threat landscape? Has the company been the target of a major cyber attack?
- What information has management provided to help the board assess which critical business assets and partners, including third parties and suppliers, are most vulnerable to cyber attacks?
- How does management evaluate and categorize identified cyber and data privacy incidents and determine which ones to escalate to the board?
- What kind of policies has the company established on ransomware? How have the company and board approached the issue of payment?
- Has the board participated with management in one of its cyber breach simulations in the last year? How rigorous was the testing?
- Will new or pending privacy regulations and frameworks impact the organization's strategy, competitive position, and business models and practices?
- Has the board leveraged a third-party assessment, as described in the NACD's cyber-risk oversight handbook, to validate that the company's cyber risk management program is meeting its objectives? If so, is the board having direct dialogue with the third party related to the scope of work and findings?
- Has the board considered the value of obtaining a cybersecurity attestation opinion to build confidence among key stakeholders?

Looking for more?

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

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

About the EY Center for Board Matters

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

US SCORE no. 16917-221US
CS no. 2206-4055730

ED None

ey.com/us/boardmatters