EY Center for Board Matters

Cybersecurity oversight disclosures: what companies shared in 2024

Following the SEC's approval of new cybersecurity disclosure requirements, many companies continue to increase their voluntary cybersecurity oversight disclosures to inform investors.

It is often a balancing act, as companies aim to disclose relevant information to the investment community on risk mitigation and responses to material incidents, while limiting information that could be exploited by adversaries and bad actors.

Disclosures play an important role in communicating with the investor community and stakeholders more broadly. In the quarter century since cyber risk became a core item on the board agenda, directors have recognized that it is an ever evolving issue, requiring constant diligence and a focused approach to enable effective oversight. The past year has seen an increase in the sophistication in cyber threats, which has prompted companies to improve their cybersecurity frameworks, but also helped adversaries improve the sophistication of attacks.

Notable developments in cybersecurity risks

New technologies are enabling growing threats

Generative AI (GenAI) is now being used in some way by nearly every company (93%), and many report that they have plans to use GenAI to improve cybersecurity[1] by helping companies identify potential cyber risks, detect vulnerabilities and breaches, and prioritize cybersecurity efforts. However, cyber threats continue to grow. Last year the FBI saw a 10% increase in complaints and a 22% increase in losses suffered — now $12.5b per year.[2] Nearly a third (32%) of these incidents involve some type of extortion scheme, such as ransomware.[3]

Employees play a role in most cyber breaches

More than two thirds of breaches include some involvement by company workers through phishing, behavior manipulation or other methods to obtain and exploit employee credentials.

Third-party cyber risks are growing

Reliance on third parties for increasingly complex IT operating environments is expanding the threat surface area — the places where an adversary may attack. It also may create single points of failure in critical systems that can be disrupted.

Growing use of external advisors

Due to its continuously evolving nature, cybersecurity is an area of constant diligence for directors and boards. Disclosures about the company's use of an external independent advisor more than doubled from 43% in 2023 to 87% in 2024 and 10% reported that their boards engage with one.

[1] "The State of Security 2024: The Race to Harness AI," Splunk.

[2] "Federal Bureau of Investigation, Internet Crimes Report 2023," Internet Crimes Complaint Center, FBI.

[3] "We've seen the data on how they're getting in," Verizon business, 2024.

[4] "Technical Line — A closer look at the SEC's new rules on cybersecurity disclosures," EY, September 19, 2024.

2024 cyber disclosure trends

Since we started tracking cyber disclosures in 2018, there has been a steady increase in voluntary cybersecurity disclosures. The SEC now requires publicly listed companies to disclose a wide variety of cybersecurity risk management and oversight information, including how the board is governing cyber risk.[4]

Overall public companies continue to disclose greater amounts of information about cybersecurity. Every aspect of cybersecurity we track in disclosures has increased since we began this effort in 2018. An analysis of cybersecurity oversight disclosures made by Fortune 100 companies reveals the following:

- Audit committees continue to oversee cyber. Despite an increasingly heavy workload, 81% of Fortune 100 companies report that cybersecurity oversight falls to the audit committee, up from 61% in 2018.
- Although the SEC cyber disclosure rule does not require companies to report on the cyber expertise of board members, our review of company filings show that cyber expertise is in demand. Nearly three quarters (72%) of companies disclose cyber as an area of expertise sought in the board and nearly as many (71%) disclose cybersecurity in at least one director biography, up from 34% in 2018.
- Dedicated cyber risk experts are engaging with the boardroom. 70% of companies report that the Chief Information Security Officer (CISO) provides the board cyber risk information — up from just 9% in 2018.
- Dedicated board time on cyber. More than half (57%) report the frequency of meeting with management on cybersecurity as at least annually or quarterly. The remaining are less specific, saying frequently or periodically. This is more than four times those with a similar disclosure in 2018.
- Preparedness exercises are common. Nearly half of companies (47%) now report performing simulations, tabletop exercises, or response readiness tests as part of their preparation efforts — up from just 3% in 2018.

What follows is an analysis of Fortune 100 company disclosures. As of May 31, 2024, 79 of these companies filed their proxy forms and 10-Ks, and these companies formed the universe for this analysis. The work reflects observations across company filings for the past seven years. Because of the timing of fiscal years, some now-required cyber disclosures appear to be less than 100 percent. For voluntary disclosure, just because a matter is not disclosed does not mean it is not performed. It simply means that the company did not include disclosures about the activity in their filings.

Fortune 100 company cybersecurity disclosures, 2018–24

Board oversight category	Topic	2024	2022	2020	2018
Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters*	95%	89%	85%	76%
	Disclosed that the audit committee oversees cybersecurity matters	81%	72%	67%	61%
	Disclosed oversight by non-audit focused committee (e.g., risk, technology)	29%	28%	24%	19%
	Disclosed oversight by a risk committee	13%	11%	10%	9%
	Disclosed oversight by a technology committee	10%	9%	8%	9%
	Disclosed oversight by another committee (e.g., compliance)	8%	8%	8%	3%
Director skills and expertise	Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	85%	68%	61%	42%
	Cybersecurity disclosed as an area of expertise sought on the board	72%	51%	35%	19%
	Cybersecurity cited in at least one director biography	71%	56%	49%	34%
Management reporting to the board	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters**	96%	78%	57%	51%
	Identified at least one management role providing cybersecurity insights to the board (e.g., the CISO or CIO)	84%	42%	25%	18%
	Chief Information Security Officer is specifically mentioned (CISO)	70%	28%	16%	9%
	Chief Information Officer is specifically mentioned (CIO)	28%	16%	10%	8%
	Chief Technology Officer is specifically mentioned (CTO)	11%	4%	0%	8%
	Included language about frequency of management reporting to the board or committee (most of this language was not specific)	95%	70%	46%	34%
	Disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like “regularly” or “periodically”	57%	44%	18%	13%
Response preparation	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	100%	99%	95%	85%
	Disclosed alignment with external framework or standard**	57%	20%	4%	2%
	National Institute of Standards and Technology (NIST)	47%	14%	3%	1%
	International Organization for Standardization (ISO)	20%	4%	1%	1%
	Other**	14%	6%	0%	0%
	Referenced response readiness, such as planning, disaster recovery or business continuity considerations	95%	73%	65%	53%
	Stated that preparedness efforts include simulations, tabletop exercises or response readiness tests	47%	9%	6%	3%
	Stated that the company maintains a level of cybersecurity insurance	25%	20%	13%	8%
	Included cybersecurity in executive compensation considerations	11%	10%	6%	1%
Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	82%	47%	28%	15%
Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	28%	14%	10%	6%
Use of external advisor	Disclosed use of an external independent advisor	87%	34%	16%	15%

Percentages are based on total disclosures by companies. Data based on the 79 companies on the 2024 Fortune 100 list that filed Form 10-Ks and proxy statements for this year through May 31, 2024.

* Some companies delegate cybersecurity oversight to more than one board-level committee.

**Some companies disclose more than one external framework or standard to which they seek to align. Such frameworks or standards cover different scopes and may not cover all aspects of the enterprise; some, but not all, include external certification or attestation. Other frameworks or standards not broken out here include the Payment Card Industry Data Security Standards, Health Information Trust Alliance, System and Organization Controls 1 and 2, and more.

Committee with oversight responsibility

In 2018, approximately three out of four companies (76%) disclosed that at least one committee is charged with overseeing cyber risk, compared to 96% today. Consistent with prior years, 81% report that the audit committee oversees cybersecurity. Just 13% had cyber risk sitting in a stand-alone risk committee — many of these are in financial services, where a board-level risk committee may be a regulatory requirement. Even fewer located cyber risk in a technology committee (10%) or another committee (8%) such as compliance.

Emerging technologies are poised to transform business models in the years ahead and many, such as GenAI, have implications for cybersecurity. Further, the increasing sophistication of phishing and social engineering attacks could mean that topics outside of traditional threat and response could become part of the board agenda. This might include more robust discussion on cyber risk culture and cyber risk appetite.

Questions for the board to consider

- How does the board determine if its board and committee portfolios are best aligned to oversee the company's evolving cybersecurity needs?
- Does the committee currently overseeing cyber risk have adequate time and resources to do its job?
- 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?

Director skills and expertise

Because cyber threats and defenses are constantly evolving, boards seek to continuously improve the skills and expertise of board members. This year, 72% of boards disclosed cybersecurity as an expertise sought on the board. A third of companies disclosed that at least one director had prior experience as a CISO, Chief Information Officer (CIO) or Chief Technology Officer (CTO). However, just 29% disclosed that their board had participated in cybersecurity-related education or training.

There are several ways to add cyber expertise in the boardroom. Some aim to have a cyber expert with deep, relevant and recent experience in the boardroom. Others focus on upskilling current board members through briefings with internal and external experts, conference attendance or certification, and have created formal or informal advisory boards to serve as an always-on resource for the company board or its committees to tap into.

Questions for the board to consider

- How do the board's current cyber skills and expertise map to the company's current and future needs?
- If expert knowledge by the board is needed, how would it get it?
- How does the board view the importance of a single cyber expert vs. a broad set of board members with cyber expertise?

Board and management relationships

This year we continued to see an increasing number of companies specify in their disclosures that the Chief Information Security Officer (CISO) provides information to the board, 70% this year compared to just 9% in 2018. In 2018, 8% disclosed the Chief Information Officer as the company point person for cybersecurity and another 8% the Chief Technology Officer. By 2024 these had risen to 28% for the CIO, and 11% for the CTO. Another 57% disclosed the frequency of these interactions as at least annually or quarterly — the remaining simply saying that they met often, regularly or periodically.

Questions for the board to consider

- How does the board ensure that it is receiving the right information from management on cyber risk?
- How does the board ensure that it is hearing from the right voices on cyber risk?
- Does management provide a holistic perspective on cyber risk ranging from threats and response to the state of the company's cyber risk culture?

Incident response preparation and use of external advisors

Because of the high likelihood — in fact near certainty of a cyber incident — being prepared to respond is exceptionally important. In 2018, just one company disclosed an external framework or standard used for cybersecurity. This has now changed. This year, 47% disclosed using NIST and 20% using ISO. In addition to following external standards, nearly half of firms (47%) report using simulations, tabletop exercises or response readiness tests. These have increased significantly in popularity, with disclosures growing by 3.5 times over the last proxy reporting cycle. While the specifics of any simulation are unlikely to match a real life scenario, the exercise can help to pressure test internal processes and procedures and develop the right muscle memory should a critical break occur.

To support response preparation and gain insight across a dynamic cybersecurity landscape, an increasing number of firms are disclosing the use of independent external advisors. This year, 87% of companies disclosed use of an independent external advisor, more than twice as many as last year, and 10% reported that their boards engage with one.

Questions for the board to consider

- Which external cybersecurity framework is used, why was it chosen, and would management choose it again if making the decision today?
- How does the board know that the company's cyber crisis response plans are up to date and relevant?
- What roles and responsibilities does the board have during a cyber risk event and which are the responsibilities of management?

Leading practices in cybersecurity oversight

Based on EY discussions with directors, industry groups, cyber leaders and public policy professions, we have identified these 10 leading practices to help boards oversee cyber risk.

Practice	Actions to take	Questions to consider
Elevate the tone	Establish cybersecurity as a key consideration in all board matters. If technology is a cornerstone of most business decisions, then cyber risk considerations should be part of board and management discussions about strategy, product and service growth plans, digital transformation, and so on.	▸ What parts of our business are most vulnerable to cybersecurity disruptions? ▸ What critical single points of failure are existential risks to the company?
Stay diligent	Address new issues and threats stemming from remote work and the expansion of digital transformation.	▸ How does the company assess, monitor and improve its cyber risk culture? ▸ Who is in the best position to provide this information to the board?
Determine value at risk	Reconcile value at risk expressed in dollar terms against the board's risk tolerance, including the efficacy of cyber insurance coverage.	▸ What metrics can best show the company's value at risk? ▸ How well does the company's risk tolerance match its value at risk?
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).	▸ How does management determine which risks should be elevated to boardroom conversation? ▸ How confident is the board that it's having discussions about the right risks?
Embed security from the start	Embrace a "secure by design" philosophy when designing new technology, products and business arrangements. Last year, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and international partners published secure-by-design and -default principles and approaches.	▸ What is the company's approach to secure by design? ▸ How does the board know that this approach is being followed?
Independently assess	Obtain a rigorous third-party assessment of the company's cyber risk management program (CRMP), including testing of critical systems and processes.	▸ How did management determine who to partner with for a third-party assessment? ▸ What are the most important areas of disagreement with the third-party review and what are the planned action steps?
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.	▸ What third parties represent a single point of failure to critical systems? ▸ What do we know about the risks posed by third parties and their downstream suppliers and providers?
Test response and recovery	Enhance enterprise resilience by conducting rigorous simulations and arranging protocols with third-party specialists before a crisis.	▸ What experience does the board have with realistic and complex simulation exercises? ▸ How are the outcomes of the simulations incorporated into the company's crisis response planning?
Understand escalation protocols	Have a defined communication plan for when the board should be notified, including incidents involving ransomware.	▸ Under what conditions is the board notified and how long should it take? ▸ What is the board's role in the plan and how will the board be notified if it changes?
Monitor the regulatory and public policy landscape	Stay attuned to evolving oversight practices, disclosures, reporting structures and metrics and understand implications for how the company is staying in compliance with requirements.	▸ Who is responsible for monitoring the regulatory and public policy landscape? ▸ How are relevant groups notified and processes updated with relevant changes?

Cybersecurity — public policy landscape

Over the past year, there has been no final legislation and relatively few regulatory developments relating to cybersecurity at the federal level, while state legislatures have been highly active. Some developments that may impact boards and companies are discussed below.

At the federal level, regulatory agencies have advanced cybersecurity policy on several fronts. For companies that are in critical infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) released a Notice of Proposed Rule Making (NPRM) to implement the Cyber Incident Reporting for Critical Infrastructure Act. The Act imposes reporting requirements on critical infrastructure entities for cyber incidents, including ransomware payments. CISA is expected to release an updated version of the proposed rule for additional consideration.

The Federal Communications Commission (FCC) launched its Cyber Trust Mark Program, a "voluntary cybersecurity labeling program that would provide consumers with clear information about the security of their Internet-enabled devices" to help inform purchasing decisions. Similar to the "Energy Star" program administered by the Environmental Protection Agency, the program will allow labeling of internet connected devices that meet the FCC's cyber criteria. The FCC issued a proposed rule on implementation of the program in July 2024, with a program launch possible late in the year.

SEC

SEC Chair Gary Gensler continues to be vocal about cybersecurity risks. In June 2024 remarks, Gensler stated, "Cyber threats represent an ever-increasing threat to the agency and our markets alike."

The SEC has issued several pieces of staff guidance relating to the cybersecurity disclosure rule. This includes guidance for public companies on where to report cybersecurity incidents at different stages of determining the significance of the incidents. Other recent guidance for issuers emphasizes the need for companies to evaluate and report material cybersecurity breaches involving ransom demands, even if the incident seems resolved after paying the ransom.

The SEC also adopted amendments to Regulation S-P in May 2024, which require broker-dealers, investment companies and other securities industry actors to implement an incident response plan to identify and manage potential data breaches. These entities also are obligated to promptly inform individuals whose sensitive information may have been compromised or is at a reasonable risk of unauthorized access or use.

The SEC continues to take enforcement action against companies for cybersecurity-related failings. According to its FY23 Enforcement Results report, the SEC acted against companies for misleading statements about customer data protection and insufficient disclosures regarding major ransomware attacks impacting thousands. More recently, the Commission has charged companies for failing to protect client securities and funds, downplaying cybersecurity risks, and not reporting cyber intrusions, among other issues.

Activity in the states

In 2024, state legislatures have introduced 132 bills and considered over 250 bills (including bills that carried over from 2023) related to cybersecurity. Twenty-seven bills were signed into law, including measures requiring insurers to investigate and notify the insurance commissioner of cybersecurity events, protecting election systems and electronic grids, providing for security measures in procurement, and funding for cybersecurity training and education. Bills have been enacted in Alaska, Arizona, California, Florida, Indiana, Iowa, Kansas, Louisiana, Maryland, Massachusetts, Minnesota, Mississippi, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Utah, Virginia, Washington, and West Virginia.

Takeaways for board oversight

Directors and boards should have an understanding of key concepts of cybersecurity risks and mitigation steps to effectively oversee the challenges and opportunities that new and legacy technologies might present. Leading boards prioritize cybersecurity oversight by embedding it in all appropriate board-level conversations, remaining engaged with a variety of voices from management and external experts, ensuring that relevant skills are in or accessible to the board room, and engaging in response exercises — and incorporating lessons learned into company playbooks. Further, they stay current on the evolving regulatory environment and are increasingly transparent and timely in their cyber disclosures about how the company is identifying and addressing key cybersecurity risks.

Examples and sample language from public cyber disclosures

Charters

Charters for board committees should accurately reflect the committee's responsibilities and be updated as needed. The Citigroup Inc. Technology Committee charter and the Humana Inc. Technology Committee charter are two 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 Lockheed Martin 2024 proxy statement does both on pages 29–37. A skills matrix notes the directors' general experience and skill, and each skill has a clear definition. 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 matter.

> *Cybersecurity risk is overseen by management-level committees, which report to the Firm Risk Committee and subsequently to the Operations and Technology Committee as well as the Board. The Operations and Technology Committee has primary responsibility for oversight of operations, technology and operational risk, including information security, fraud, vendor, data protection and privacy, business continuity and resilience, and cybersecurity risks (including review of cybersecurity risks against established risk management methodologies). In accordance with its charter, the Operations and Technology Committee receives regular reporting at each quarterly meeting from senior officers in the Technology Department (Technology), Operations Department (Operations) and Non-Financial Risk on operational risk and the steps management has taken to monitor and control such exposures. Such reporting includes updates on the Company's cybersecurity program, the external threat environment, and the Company's programs to address and mitigate the risks associated with the evolving cybersecurity threat environment.*
>
> *The Operations and Technology Committee also receives an annual independent assessment of key aspects of the Company's cybersecurity program from an external party and holds joint meetings with the Audit Committee and Risk Committee, as necessary and appropriate. The Board or the Operations and Technology Committee reviews and approves the Global Cybersecurity Program Policy, the Global Information Security Program Policy and the Global Technology Policy at least annually. The Chair of the Operations and Technology Committee regularly reports to the Board on cybersecurity risks and other matters reviewed by the Operations and Technology Committee. In addition, the Board receives separate presentations on cybersecurity risk and in accordance with the Corporate Governance Policies all Board members are invited to attend Operations and Technology Committee meetings and have access to meeting materials.*
>
> *Senior management, including the senior officers mentioned above, discuss cybersecurity developments with the Chair of the Operations and Technology Committee between Board and committee meetings, as necessary. The Operations and Technology Committee meets regularly in executive session with management, including the Head of Non-Financial Risk, and senior officers from Technology and Operations.*

Response readiness

> *The program includes managing the Firm's global cybersecurity operations centers, providing training, conducting cybersecurity event simulation exercises, implementing the Firm's policies and standards relating to technology risk and cybersecurity management, and enhancing, as needed, the Firm's cybersecurity capabilities.*

Use of external independent advisor and board engagement

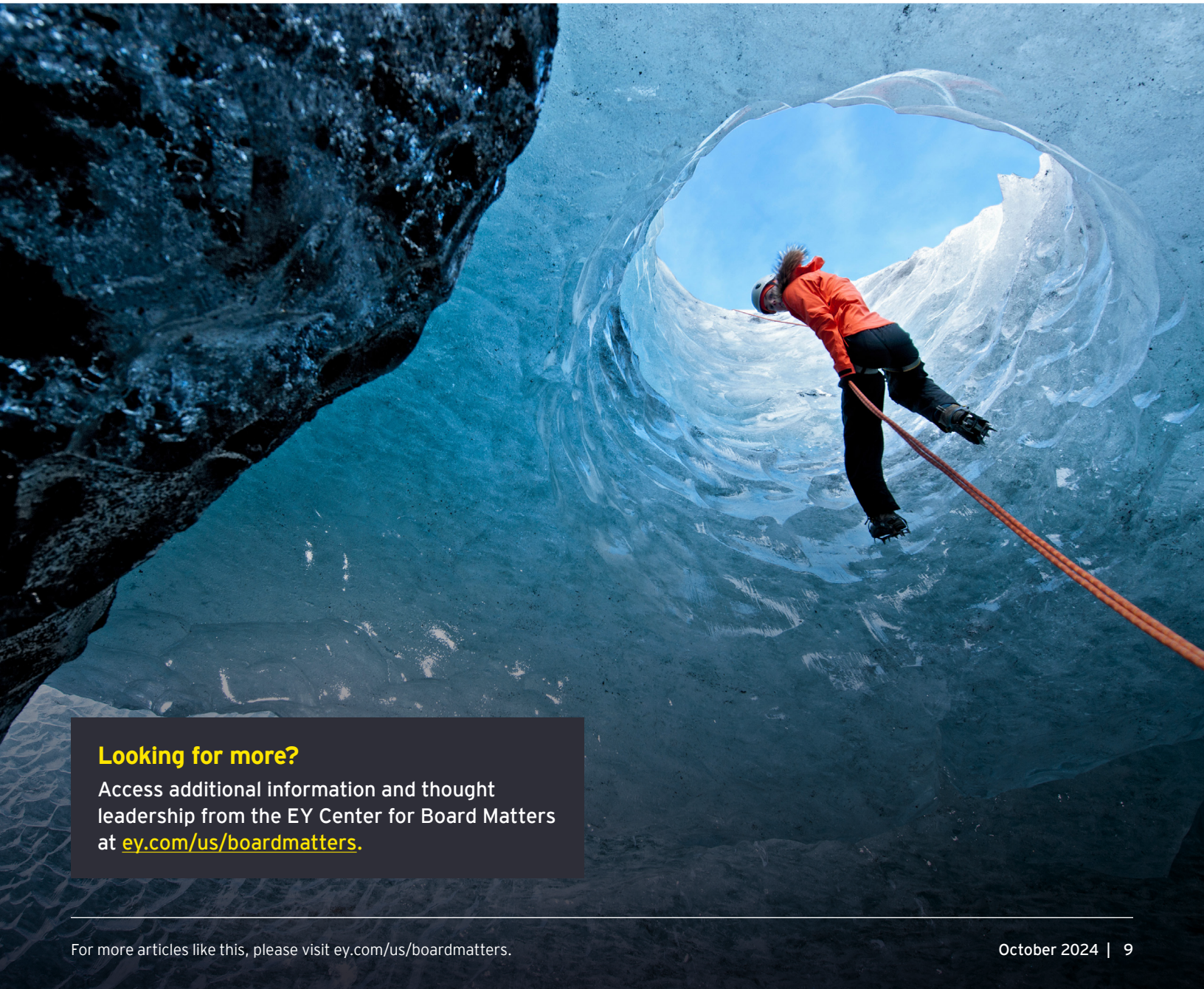
> *We also maintain a documented Information Security Program (the Program) that includes risk assessments regularly conducted by the Company and third-party experts to evaluate potential security threats that may have a negative impact on the organization, to detect potential vulnerabilities, and to mitigate any identified security risks. The Program is informed by industry standards and frameworks and is designed to protect the confidentiality, integrity, and availability of information assets and systems that store, process, or transmit information.*

Alignment with external framework or standard

> *On an annual basis, we conduct risk assessments and compliance audits, both internally and by independent third parties, against standards including the National Institute of Standards and Technology security framework (NIST) and Payment Card Industry Data Security Standards (PCI DSS), and regularly benchmark and evaluate program maturity with industry leaders.*

Training

> *Security Awareness and Training. Events and education activities are hosted throughout the year, such as the Cybersecurity Awareness Month, expos, videos, training programs and frequent phishing simulations. [The company] continuously trains workforce members on the importance of preserving the confidentiality and integrity of customer data. All new hires have mandatory information protection and privacy training as part of their onboarding, and all workforce members complete an annual cybersecurity refresh training.*



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. 24735-241US
2409-13294-CS

ED None

ey.com/us/boardmatters