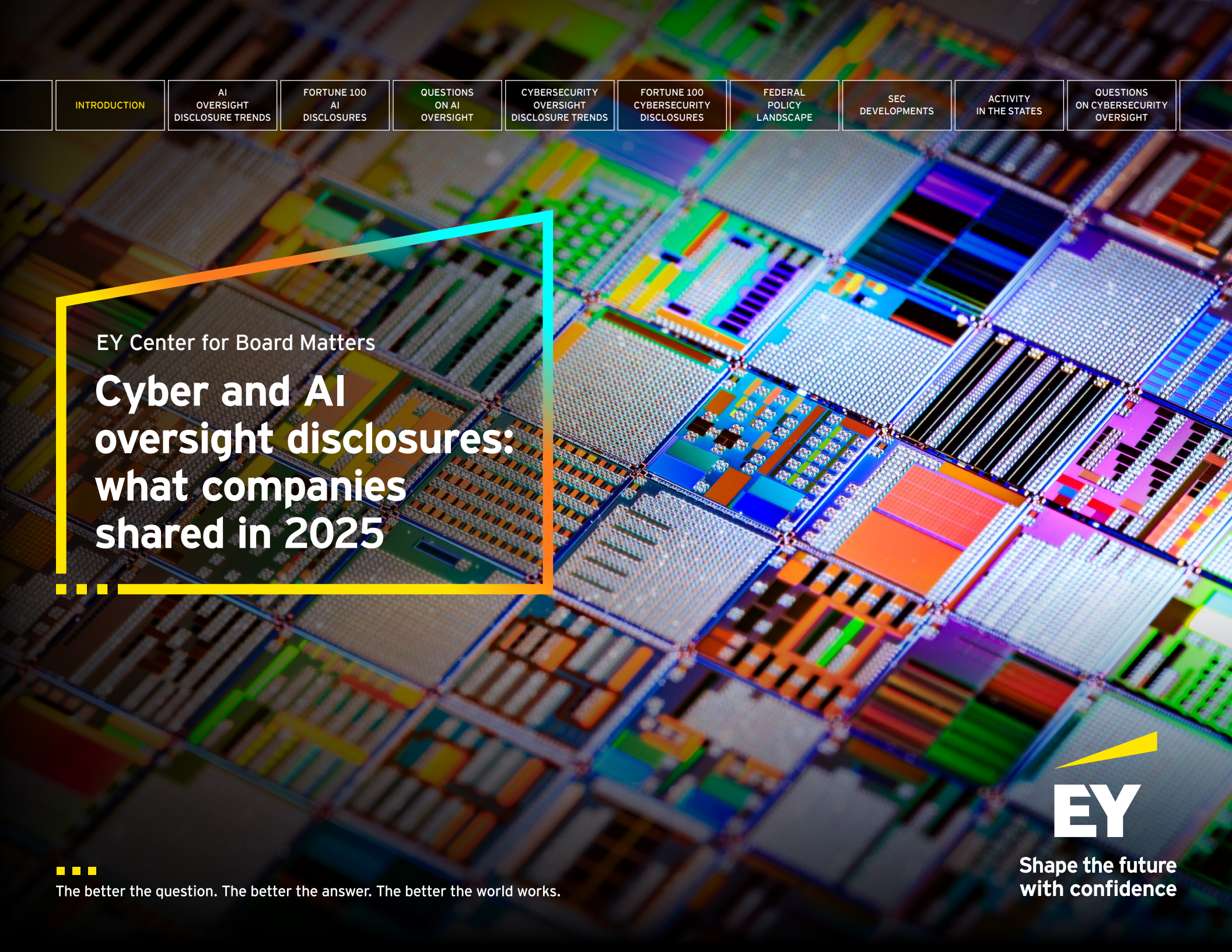


EY Center for Board Matters

Cyber and AI oversight disclosures: what companies shared in 2025

Introduction

Public disclosures reveal how leading boards are overseeing AI and cybersecurity

In today's fast-changing and high-stakes digital environment, boards are elevating their oversight approach. Voluntary disclosures around AI and cyber are not just more common — they're also more robust, doubling in scope across several critical areas.

Companies are putting the spotlight on their technology governance, signaling an increasing emphasis on cyber and AI oversight to stakeholders.

In the past year, according to company disclosures, the increased sophistication of cyber threats has prompted companies to enhance their cybersecurity defenses, while adversaries have also advanced their attack methods. Ransomware attacks rose by over a third, and generative AI (GenAI) — rather than traditional AI — is emerging as a key feature of the threats, often in the form of deepfakes, and the company response.

Deepfakes are just one example of threat actors' using GenAI for malicious purposes and are now the second most common type of cybersecurity incident, behind malware.[1] However, some argue that today's biggest risk is the loss of sensitive company information when employees use unapproved AI services.[2]

One recent survey of full-time employees across industries and regions in the United States found that 78% of employees report using AI tools in the office and 58% admit to providing sensitive company information to large language models.[3] At the same time, organizations are increasingly using GenAI as part of their toolkit to respond to cyber risks.[4] Board oversight of these areas is critical to identifying and mitigating risks that may pose a significant threat to the company.

This article explores how technology oversight disclosures and related governance practices are evolving to meet the challenges of this moment. We aim to help boards and management teams understand the disclosure landscape and the underlying governance practices it reflects and identify opportunities to strengthen and better communicate the rigor of their governance approach in an area of stakeholder focus.

OUR METHODOLOGY

What follows is an analysis of Fortune 100 company technology oversight disclosures. As of July 31, 2025, 80 of these companies had filed proxy statements and Form 10-K filings, which serve as the basis for this analysis. The analysis includes observations on companies' cybersecurity oversight disclosures since 2019 and AI oversight disclosures since 2024. Given the critical challenges at the intersection of cyber and AI, we chose to include voluntary disclosure trends for both.

> "Some argue that today's biggest risk is the loss of sensitive company information when employees use unapproved AI services.

[1] Isms.online, State of Information Security Report, 2024 p.4
[2] Verizon, 2025 Data Breach Investigations Report – Executive Summary, p. 8.
[3] New Data Reveals Widespread, Risky AI Use at Work, 5 August 2025
[4] State of AI and Security Survey Report | CSA

2025 AI oversight disclosure trends: four key findings

1 **AI is showing up in disclosures about board oversight of enterprise risk. Nearly half (48%) specifically cited AI risk as part of the board's oversight of risk — triple the 16% that did last year.**

The depth of these disclosures varies widely. Some mention it as one of many risks overseen by the board, while others offer more detailed insights into the board's AI risk oversight practices. For example, a few companies have dedicated subsections addressing AI governance in their proxy statement. These sections emphasize the importance of board oversight of risks and opportunities related to AI strategies, development and usage.

2 **More director bios and skills matrices list AI. Close to half (44%) now mention AI in their description of director qualifications, a significant jump from 26% in 2024**.

Directors' AI experience ranges from developing AI software to earning certifications in AI ethics. Most companies that updated directors' biographies to include their AI experience did so for existing board members over the past year. New directors with AI backgrounds include examples such as a CEO of a company specializing in AI, a venture fund partner investing in AI-native companies, and a leader in AI product development and computational design. Notably, several companies disclosed AI education under their "board and director evaluations" section, noting that recent input has prompted enhanced discussions and deep dives on AI.

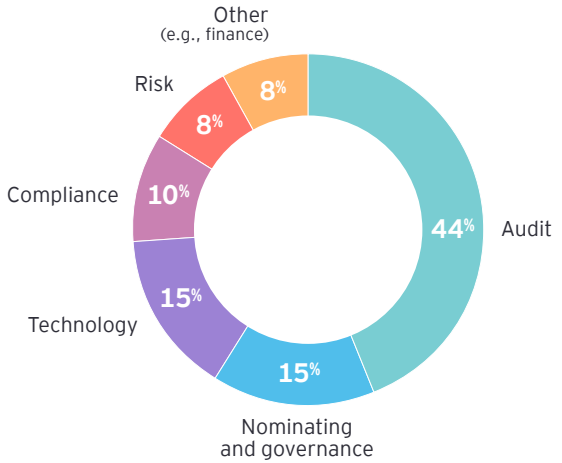
3 **AI oversight responsibilities are being assigned to committees. Around 40% disclosed charging at least one board-level committee (usually the audit committee) with AI oversight responsibilities, almost four times the 11% that did so in 2024.**

The audit committee is board members' preferred location for AI oversight. However, disclosures about the committee's focus tend to be more robust when overseen by non-audit committees such as technology or nominating and governance (e.g., reviewing the company's approach to responsible AI development and AI governance, overseeing the responsible and ethical application of AI). Further, more non-audit committees formalize these responsibilities in their charter than when the audit committee is charged with overseeing AI.

4 **AI is increasingly showing up as a risk factor. More than a third (36%) now disclose AI as a separate 10-K risk factor, up from 14% last year.**

New AI risk factors covered topics similar to last year's such as regulatory challenges, cybersecurity threats, operational disruptions, reputational issues, consumer expectations and technological hurdles.

AI oversight by board committees



Source: Analysis by EY Center for Board Matters. Chart reflects only the subset of Fortune 100 companies that have disclosed committee oversight of AI.

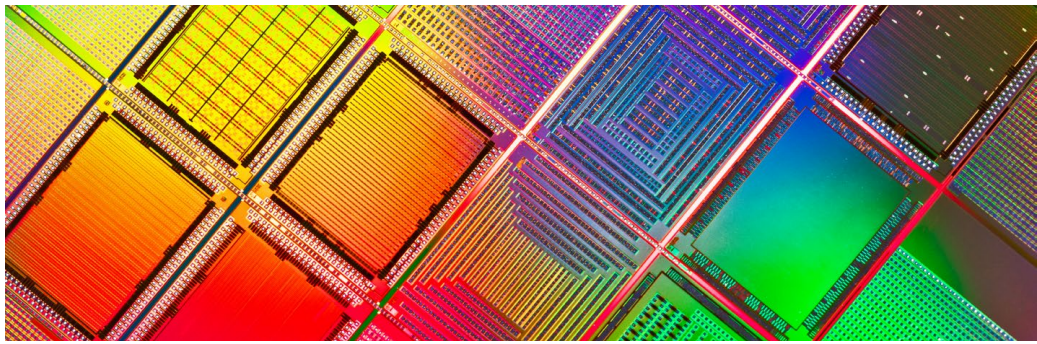
Fortune 100 company AI disclosures, 2024–2025

Topic	Disclosure	2025	2024
Category: Board oversight			
Risk oversight approach	Disclosed a focus on AI in the risk oversight section of the proxy statement	**48%**	**16%**
Board-level committee oversight	Disclosed that at least one board-level committee was charged with oversight of AI matters*	**40%**	**11%**
	▪ Disclosed AI oversight by the audit committee	**21%**	**8%**
	▪ Disclosed AI oversight by a non-audit committee	**25%**	**8%**
Director skills and expertise	AI disclosed as an area of expertise sought on the board or cited in at least one director biography	**44%**	**26%**
	▪ AI disclosed as an area of expertise sought on the board	**15%**	**8%**
	▪ AI cited in at least one director biography	**35%**	**23%**
	Board-level education and training efforts on AI	**11%**	**8%**
Management reporting structure	Provided insights into management reporting to the board and/or committee(s) overseeing AI matters	**16%**	**6%**
	▪ Identified at least one management role providing AI insights to the board (e.g., the CISO or CTO)	**8%**	**4%**
	▪ Included language on frequency of management reporting to the board or committee(s)	**9%**	**5%**
Category: Statements on AI risk			
Risk factors	Included AI as a stand-alone risk factor	**36%**	**14%**
	Included AI as a risk factor	**89%**	**69%**

Topic	Disclosure	2025	2024
Category: Risk management			
Responsible use	Disclosed the use of AI frameworks, principles or guidelines	**25%**	**11%**
Shareholder engagement	Included AI under shareholder engagement topics	**21%**	**11%**
Compensation	Included AI in executive compensation considerations	**31%**	**25%**
Education and training	Disclosed use of education and training efforts on AI matters	**13%**	**5%**

Percentages are based on total disclosures by companies. Data based on the 80 companies on the 2025 Fortune 100 list that filed Form 10-Ks and proxy statements for this year through July 31, 2025.

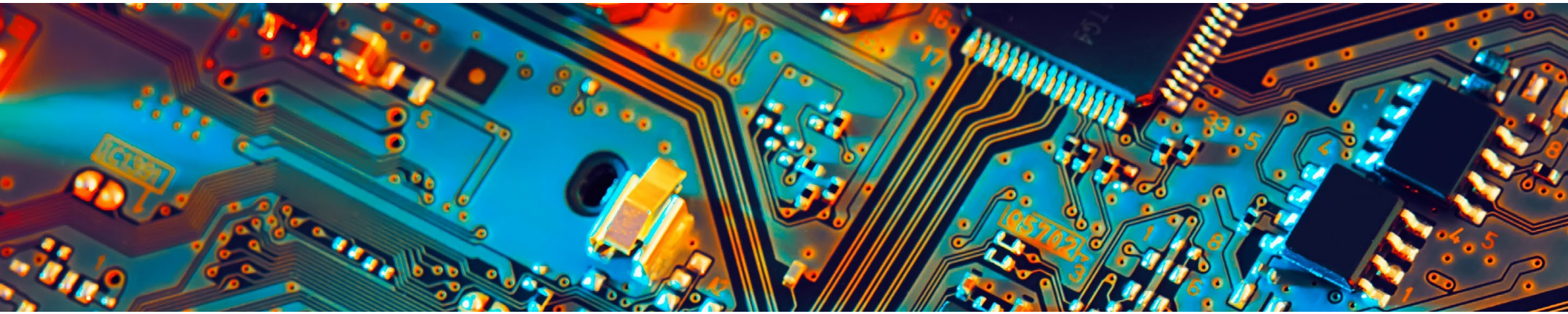
*Some companies delegate AI oversight matters to more than one board-level committee.



Questions for the board to consider regarding AI oversight

- How should AI be integrated into the board's overall risk management oversight process?
- Should an existing board committee oversee AI risks, or is it necessary to establish a new technology-focused committee?
- Could the board form an ad hoc or working group to ensure that AI receives adequate attention? Alternatively, can optimizing the complementary roles of committees and the full board ensure effective oversight of all critical aspects of AI solutions?
- Is the board knowledgeable in technology and AI and related risks and opportunities for the business? How is it regularly enhancing that knowledge (e.g., accessing AI experts)?
- How effective are the company's disclosures in providing stakeholders with a window into the rigor of the board's AI governance approach and demonstrating the board's depth of experience and engagement on this topic?
- How would disclosing more about the board's ongoing AI education boost investor confidence in its AI oversight?

"Should an existing board committee oversee AI risks, or is it necessary to establish a new technology-focused committee?



2025 cybersecurity oversight disclosure trends: four key findings

1 **Audit committees remain the primary spot for cybersecurity oversight. Most (78%) companies report that cybersecurity oversight falls to the audit committee, about the same as reported over the last three years.**

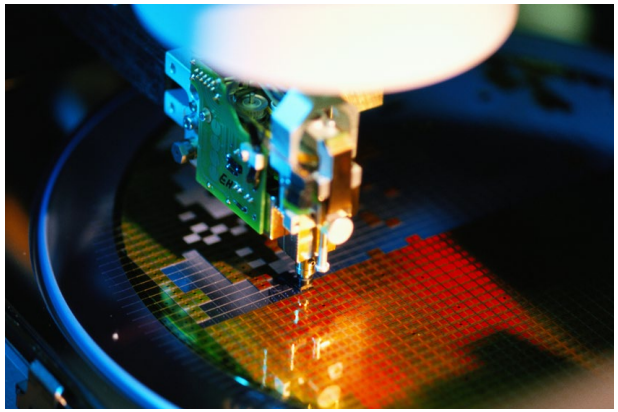
Emerging technologies like GenAI are set to change business models and impact cybersecurity. As phishing and social engineering become more advanced, boards may need to address broader cyber risk issues, including risk culture and risk appetite. This could prompt a reassessment of how cyber risk oversight is handled at the board level to keep discussions relevant.

2 **Most companies now say they are aligning to an external framework. Nearly 3 in 4 (73%) companies now disclose alignment with an external framework such as NIST CSF 2.0, ISO 27001, or something similar.**

This is up from 57% last year and 4% in 2019. Many companies have found it valuable to clearly articulate the external framework used to assess and improve their abilities to respond to cyber events. This helps to demonstrate a structured and proactive approach to regulators, investors and other stakeholders.

3 **A majority of companies report doing cyber preparedness exercises. More than half (58%) report that their cybersecurity preparedness includes simulations, tabletop exercises or response readiness tests — up from just 3% in 2019.**

Nearly every company (99%) references some kind of response readiness, such as planning, disaster recovery or business continuity. Such exercises can be important when not only planning for a specific incident but exercising the more general skills that can help a firm effectively respond to the unexpected.



4 **Cyber expertise continues to be in demand in the boardroom. Most companies (86%) disclose cybersecurity as an area of expertise that a director has or that the board seeks — a 62% increase since 2019.**

Companies may choose to introduce cyber expertise into the boardroom through various approaches. For example, current board members may enhance their cyber knowledge by participating in briefings with internal or external specialists, attending industry conferences, or obtaining professional certifications. In addition, companies may establish formal or informal advisory boards to provide ongoing resources and guidance for the board, or its committees as needed. Some companies have onboarded cybersecurity advisors to provide those specific insights to the board.

Fortune 100 company cybersecurity disclosures, 2019–2025

Topic	2025	2023	2021	2019
Category: Board-level committee oversight				
Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters*	96%	92%	87%	81%
▪ Disclosed that the audit committee oversees cybersecurity matters	78%	77%	68%	62%
▪ Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	35%	30%	28%	24%
▪ Disclosed oversight by a risk committee	13%	13%	10%	9%
▪ Disclosed oversight by a technology committee	11%	10%	9%	9%
▪ Disclosed oversight by another committee (e.g., compliance)	13%	9%	9%	8%
Category: Director skills and expertise				
Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	86%	78%	70%	53%
▪ Cybersecurity disclosed as an area of expertise sought on the board	73%	62%	43%	27%
▪ Cybersecurity listed in at least one director biography	74%	66%	59%	46%

Topic	2025	2023	2021	2019
Category: Management reporting to the board				
Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	100%	84%	66%	57%
▪ Identified at least one management role providing cybersecurity insights to the board (e.g., the CISO or CIO)	89%	56%	32%	27%
▪ Chief information security officer (CISO)	78%	41%	22%	16%
▪ Chief information officer (CIO)	24%	20%	11%	13%
▪ Chief technology officer (CTO)	15%	5%	1%	0%
Included language about frequency of management reporting to the board or committee	99%	77%	56%	44%
▪ Disclosed reporting frequency of at least annually or quarterly; the remaining companies used terms such as "regularly" or "periodically"	60%	49%	34%	18%

Percentages are based on total disclosures by companies. Data is based on the 80 companies on the 2025 Fortune 100 list that filed Form 10-Ks and proxy statements for this year through July 31, 2025.

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

Topic	2025	2023	2021	2019
Category: Response preparation				
Disclosed alignment with external framework or standard**	73%	30%	11%	4%
▪ National Institute of Standards and Technology (NIST)	64%	22%	9%	3%
▪ International Organization for Standardization (ISO)	23%	6%	3%	0%
▪ Other**	15%	9%	3%	0%
Referenced response readiness, such as planning, disaster recovery or business continuity considerations	99%	77%	68%	59%
▪ Stated that preparedness efforts include simulations, tabletop exercises or response readiness tests	58%	13%	5%	3%
Stated that the company maintains a level of cybersecurity insurance	31%	27%	16%	11%
Included cybersecurity in executive compensation considerations	10%	10%	9%	1%

Topic	2025	2023	2021	2019
Category: Education and training				
Disclosed use of education and training efforts to mitigate cybersecurity risk	86%	56%	37%	25%
Category: Engagement with outside security community				
Disclosed collaborating with peers, industry groups or policymakers	40%	16%	11%	11%
Category: Use of external advisor				
Disclosed use of an external independent advisor	99%	43%	23%	14%

Percentages are based on total disclosures by companies. Data is based on the 80 companies on the 2025 Fortune 100 list that filed Form 10-Ks and proxy statements for this year through July 31, 2025.

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

The federal policy landscape

Cybersecurity

The past year in Washington has been dominated by the transition from the Biden to Trump administration, with a new approach to cybersecurity issues. While no new federal legislation has been signed into law, the president and some regulators have taken some actions in recent months focused on cybersecurity concerns.

However, one important issue looms on the horizon. The Cybersecurity Information Sharing Act of 2015 (CISA 2015)[5] expired on 30 September 2025. CISA 2015 allows private sector entities to disclose cybersecurity threats and provides liability protections for businesses making disclosures in order to promote the sharing of information. A coalition of trade associations (including the American Institute of CPAs) has united to urge Congress to reauthorize CISA 2015 while the relevant congressional committees continue to consider legislation reauthorizing CISA at this writing.

Additionally, the Trump administration has made changes in cybersecurity personnel and shifted some policy priorities. On 6 June 2025, the president issued an executive order (EO) aimed at strengthening the nation's cybersecurity "by focusing on critical protections against foreign cyber threats and enhancing secure technology practices."

The Trump EO also makes significant changes to Obama and Biden-era EOs (14144 and 13694) while focusing on software supply chains and promoting the use of artificial intelligence (AI) technologies to promote cybersecurity. Notably, President Trump's EO eliminates a Biden directive encouraging the development and use of digital identity documents by federal and state governments.

The AI agenda released by the administration in July 2025 also included provisions recognizing the potential benefits and risks to cybersecurity posed by AI technologies. "Winning the Race: America's AI Action Plan" calls on the Department of Homeland Security (DHS) to establish an AI Information Sharing and Analysis Center (AI-ISAC) to "promote the sharing of AI-security threat information and intelligence across U.S. critical infrastructure sectors." The Action Plan further requires DHS to provide guidance to private sector entities on AI cyber threats, as well as to encourage the sharing of information of known AI vulnerabilities.

Artificial intelligence

Advancing AI technologies is a key priority of the Trump administration. As noted above, President Trump's AI Action Plan sets forth the administration's plan to promote the development and deployment of AI technologies through three pillars — Accelerate AI Innovation, Build American AI Infrastructure, and Lead in International AI Diplomacy and Security.

> "An industrial revolution, an information revolution, and a renaissance — all at once. This is the potential that AI presents. The opportunity that stands before us is both inspiring and humbling. And it is ours to seize, or to lose."
>
> **— "Winning the Race: America's AI Action Plan"**

The plan largely focuses on removing regulatory barriers to the development and deployment of AI systems and the infrastructure (including energy demands) necessary to support them. It also outlines the Trump administration's strategy on global AI governance initiatives, including pushing for regulatory frameworks that are less restrictive and limiting the influence of countries considered by the administration to be adversarial.

Federal agencies are directed to take dozens of actions to promote the US as the global leader in AI which will continue to be implemented over the next year. For additional information on the plan, please see Ernst & Young LLP's Trump administration executive action alert on "Winning the Race: America's AI Action Plan and Executive Orders."

[5] Consolidated Appropriations Act, Pub. L. No. 114-113, Div. N, Title I – Cybersecurity Information Sharing Act, 129 Stat. 2935 (2015), 6 U.S.C. § 1501; S. Rep. No. 114-32, at 2 (2015).

SEC developments

SEC Chair Paul Atkins has signaled a clear departure from the previous chair's approach to cybersecurity and the use of AI in the capital markets.

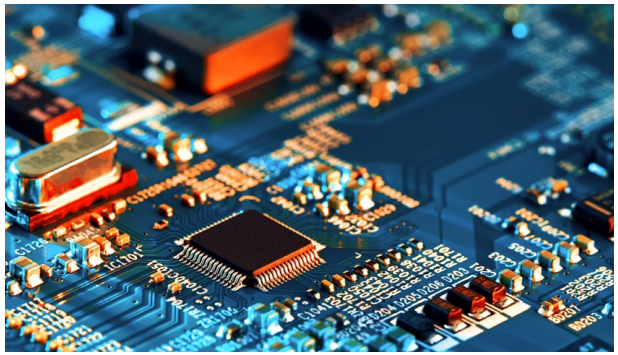
While former Chair Gary Gensler advanced several rulemakings to address cybersecurity and AI risks, so far Atkins has focused on supporting innovation in financial markets and taking steps to facilitate capital market access, such as by reviewing "increasingly complex" disclosure requirements. Atkins has stated that the SEC "should use its available authority and discretion to adapt to and accommodate new developments."

One of Atkins' early actions was to rescind several proposed rules relating to disclosure and other obligations for market participants that were issued during Gensler's tenure. These include:

- The "Cybersecurity Risk Management Rule for Broker-Dealers, Exchanges, and Other Market Infrastructure Entities," which would have required key market entities to implement, assess and disclose robust cybersecurity policies and incident responses to market participants.
- The "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies and Business Development Companies" rule, which would have mandated cybersecurity risk management policies and incident reporting.
- The "Predictive Data Analytics" rule, which would have required firms to remove conflicts of interest when using AI and predictive data tools in investor interactions.

Still pending from the previous administration is the compliance date for amendments to Regulation S-P, set for 3 December 2025 for larger companies. The amendments require written incident response programs that address risks posed by data breaches and mandate prompt disclosure to individuals whose sensitive information is compromised or is vulnerable to unauthorized access.

Atkins has indicated that the SEC will narrow its enforcement scope to focus on fraud and manipulation. Recently, the commission opened litigation against a startup for allegedly misleading investors by making false statements about the company's use of AI.



According to its FY 2024 enforcement results, the SEC took enforcement actions last year against companies for "AI-washing" and fraud.

Looking ahead, Atkins' goal of creating a friendlier environment for innovation aligns with the administration's AI plan. As noted above, the plan calls for the commission to revise or repeal regulations that block AI development or deployment. It also directs the SEC to establish regulatory sandboxes for testing AI tools.

These frameworks would be intended to allow enterprises to "rapidly deploy and test AI tools while committing to open sharing of data and results" while under regulatory supervision. Commission action to implement these concepts may be seen in the coming months.

> "So far Atkins has focused on supporting innovation in financial markets and taking steps to facilitate capital market access.

Activity in the states

In the absence of federal legislative actions on cybersecurity and AI, states remain highly active in both areas of policy.

Cybersecurity

In 2025, state legislatures considered nearly 250 bills related to cybersecurity. Fifty bills were signed into law, including many measures to strengthen state-level cybersecurity systems. These bills include the creation or expansion of state cybersecurity offices, the establishment of IT infrastructure oversight mechanisms, protection of state-issued devices, requirements for incident response planning, protection of critical infrastructure, and mandates for risk assessment and cybersecurity insurance coverage.

Artificial intelligence

In 2025, state legislatures considered more than 1,000 bills related to AI. Of those, 136 were signed into law in 40 states, most of them relating to deepfakes. Laws were enacted to prohibit certain sexual deepfakes, regulate political deepfakes during election season and criminalize the use of deepfakes for fraudulent activities.

Other enacted laws related to the use of AI in health care, prohibiting certain services such as nursing or therapy without human oversight, and regulating the use of AI in utilization review management by insurers. Specifically, Texas enacted an AI law that prohibits certain uses of the technology and creates an AI sandbox program.

Most recently, California enacted the Transparency in Frontier Artificial Intelligence Act, which establishes transparency requirements for large AI developers, requires the reporting of critical safety incidents to the state's attorney general, and provides whistleblower protections for employees who report potential risks.

New York's legislature also passed its own AI regulatory framework earlier this year, and the governor must decide by the end of the year whether to amend the AI bill to match California's law, sign the bill in its current form, or veto the legislation.

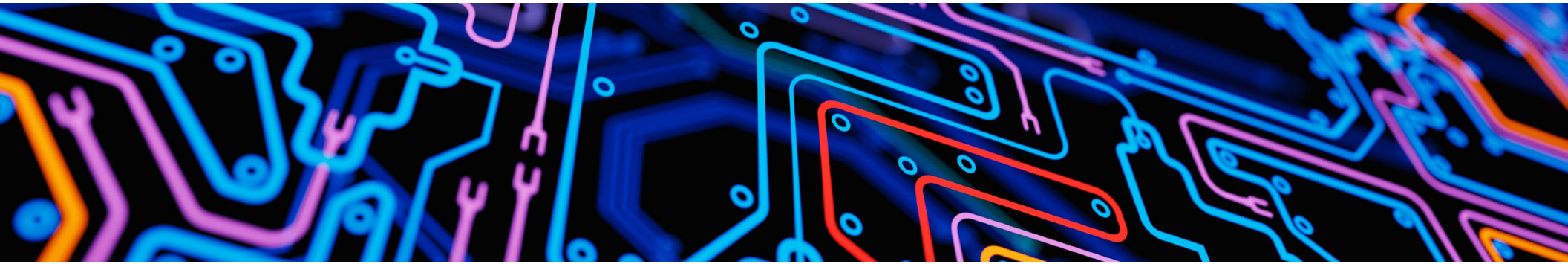
These developments are expected to add to the ongoing discussions at the federal level.

"Other enacted laws related to the use of AI in health care, prohibiting certain services such as nursing or therapy without human oversight, and regulating the use of AI in utilization review management by insurers.

Questions for the board to consider regarding cybersecurity oversight

- How does the board ensure its structure supports evolving cybersecurity needs?
- Does the committee overseeing cyber risk committee have sufficient time and resources?
- What information has management given to identify vulnerable business assets and partners, including third parties?
- Do current board cyber skills meet present and future company requirements?
- If expert knowledge is needed, how will the board obtain it?
- What is the board's view on having a single cyber expert vs. a diverse set of skills?
- Which external cybersecurity framework is used, why was it chosen, and would management select it again?
- How does the board confirm crisis response plans are current and effective?
- What roles does the board and management have during a cyber event?
- How effective are the company's cybersecurity disclosures in balancing the need for confidentiality with the need to demonstrate rigorous, structured oversight to stakeholders?

"What information has management given to identify vulnerable business assets and partners, including third parties?



RETURN HOME

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

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. 28533-241US
CS no. 2509-10116-CS

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.