AI and the New Cyber Risk Landscape

Disclosure Gaps in the S&P Europe 350

06 FEBRUARY 2026

This publication analyzes how S&P Europe 350 companies describe and position AI-related risks in their annual reporting, identifying the most frequently disclosed risk types, sector-specific patterns, and how disclosure has evolved since 2023.

Trusted Insights for What's Ahead®

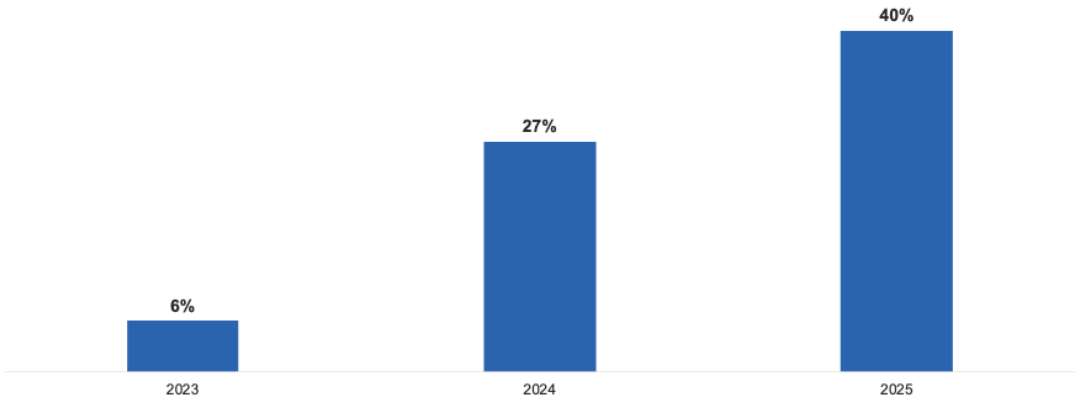
- AI-related risk disclosure among S&P Europe 350 issuers has accelerated since 2023 as EU requirements turn AI governance, documentation, transparency, and vendor controls into foreseeable compliance risks.
- The post-2023 rise in AI risk disclosure is driven largely by European financials, with industrials and IT also accelerating disclosure—broadly consistent with trends in the US and reflecting how AI-enabled decisioning and automation are moving fastest in operationally and regulatorily sensitive environments.
- Companies most frequently frame AI as a cybersecurity threat multiplier, expanding the attack surface through new AI systems and third-party dependencies.
- Reputational risk is described as a transmission channel, as biased, incorrect, or misleading AI outputs and associated privacy concerns can rapidly erode trust and trigger heightened regulatory and litigation scrutiny.
- Privacy risk is increasingly inseparable from AI governance, with companies highlighting generative AI (genAI)-specific safeguards (e.g., limiting data use and tightening controls) as prerequisites for scaling AI adoption.

AI Risk Disclosure Trends in S&P 350 companies

Figure 1

Disclosure of AI as a material risk has surged since 2023

Share of S&P 350 companies disclosing one or more AI-related risks in their annual reports, 2023–2025



Note: Some companies disclose more than one AI risk.
Source: The Conference Board/ESGAUGE, 2026

The reporting of AI as a material risk has surged since 2023 among S&P Europe 350 issuers. The acceleration is amplified by an increasingly stringent regulatory environment, with the European compliance framework now materially more prescriptive. For example, the EU AI Act entered into force on August 1, 2024 and its obligations phase began in 2025, turning AI governance, documentation, testing, transparency, and vendor controls into foreseeable compliance risks rather than discretionary best practices. That shift is reinforced by the legislation's penalty regime since administrative fines can reach up to 7% of worldwide annual turnover for certain infringements, raising the materiality stakes for large multinationals.

In parallel, adjacent EU regimes raise the baseline for technology-risk governance in the cloud-dependent, data-intensive environments where AI runs: the Network and Information Security Directive required national transposition by October 17, 2024 and expands cybersecurity accountability across critical sectors, while the Digital Operational Resilience Act applies from January 17, 2025 and tightens ICT resilience and third-party oversight in financial services, both of which increase pressure to describe AI-enabled attack surfaces and supplier concentration as principal risks rather than generic IT issues. Finally, Europe's privacy and fundamental-rights regime continues to pull AI into the risk-factor perimeter as regulators clarify how General Data Protection Regulation (GDPR) principles apply in the context of AI models and associated processing, reinforcing that data provenance, lawful basis, and automated decisioning can drive investigations, remediation costs, and operational constraints.

In *C-Suite Outlook 2026: Uncertainty and Opportunity*, among societal, demographic, and technological shifts, "AI" was the leading source of downside risk cited by CEOs around the globe for the upcoming year, with 34.5% of Europe-based CEOs flagging it as a headwind (vs. 35.8% in North America). This reflects concern about the execution and organizational disruption risks of rapid adoption, such as uneven returns on investment, data governance demands, and the challenge of scaling AI without undermining trust and accountability

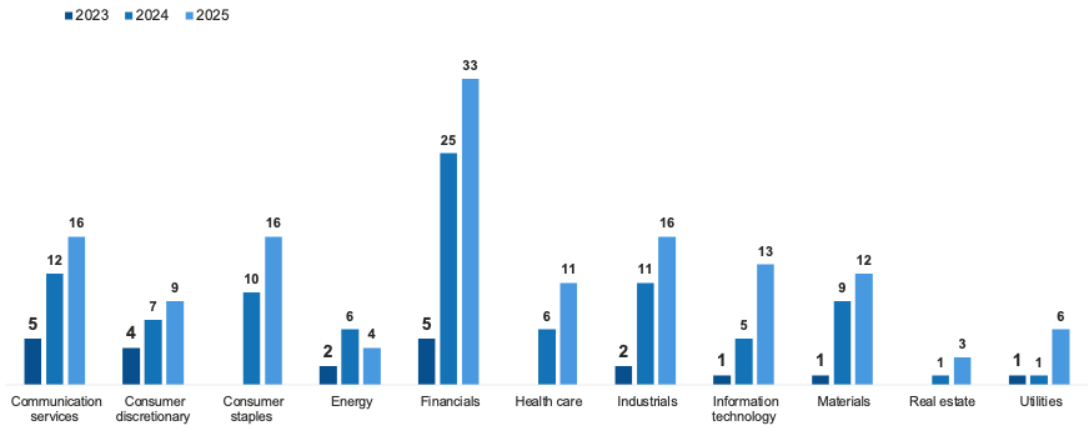
By contrast, US issuers are converging on similar levels of AI risk disclosure for more market-driven reasons than regulatory prescriptiveness. *AI Risk Disclosures in the S&P 500: Reputation, Cybersecurity, and Regulation* from The Conference Board® reveals that US companies' AI risk disclosures surged as the technology moved from experimental pilots to business-critical use, affecting customers, operations, compliance, and brand value; and as boards anticipate heightened scrutiny from investors, regulators, and other stakeholders, driving more explicit disclosure.

AI Risk Disclosures by Sector

Figure 2

The growth in reporting of AI risks is driven by financial, industrial, communication services, and IT firms

Number of S&P 350 companies disclosing one or more AI-related risks in their annual reports, 2023–2025



Note: Some companies disclose more than one AI risk.
Source: The Conference Board/ESGAUGE, 2026

Across S&P Europe 350 companies, there is a clear post-2023 inflection in the disclosure of AI as a material risk. This is directionally consistent with the US, where AI quickly shifted from an emerging technology to a mainstream enterprise risk disclosure.

In both regions, the rise in disclosures is led by sectors with the most immediate exposure to AI-enabled decisioning, automation, and regulated data environments: European financials are the largest contributor, with the acceleration in industrials and IT also mirroring US trends, where the jump is concentrated in financials, health care, industrials, IT, and consumer-facing firms.

The European mix, however, leans relatively more toward consumer staples and materials consistent with the EU's faster-moving governance-and-compliance agenda around AI and adjacent regimes, including the EU AI Act's phased obligations beginning in 2025–2026.

In the C-Suite Outlook 2026 survey, AI was increasingly framed as a governance and compliance risk: "evolving AI regulation and governance requirements" was flagged by 25.3% of Europe-based CEOs (vs. 24.9% North America). The survey highlights growing complexity from diverging expectations on transparency, accountability, and data governance for AI used in operational and customer-facing decisions.

AI Technologies Explicitly Referenced in S&P 350 Company Annual Reports

GenAI and genAI copilots. GenAI is a major technology shift, adding vector-based search capabilities and helping developers write code. Risk-sensitive companies are also moving toward internal genAI deployments within enterprise environments.

Machine learning (ML) and advanced analytics. ML is used across research and development and operations, including predictive modelling, as well as in modelling and optimizing energy use in buildings, factories, and data centers. AI and ML tools are considered as essential parts of data/technology-driven change affecting underwriting, pricing, and claims.

Chatbots and large language model (LLM) conversational assistants. AI digital-assistant chatbots are used for engagement and product information, as well as in supporting employee productivity, including customer contact centers.

Network/telecom automation and autonomous networks. AI is framed as foundational for future autonomous telecom networks, defined as networks that can monitor, decide, and act (often using AI/ML) to meet service objectives with minimal human intervention. This includes AI-driven radio access network initiatives (including large-scale pilots) and AI-driven network management (e.g., predictive operations)

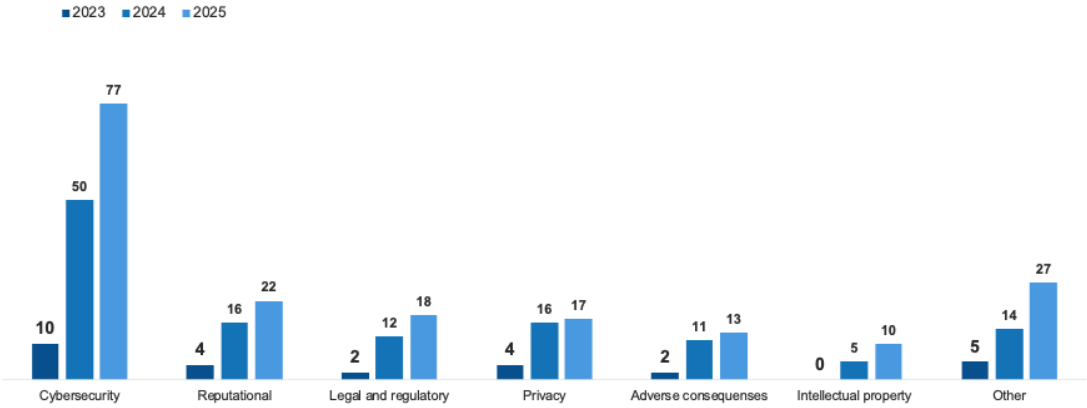
Industrial and internet of things (IoT) platforms enabling AI. Companies describe industrial platforms as the enabling layer that connects IoT data, provides secure access to applications, and makes AI repeatable at scale. In practice, these platforms support digital twin capabilities and operational analytics, enabling use cases such as energy monitoring and optimization, asset performance management and predictive maintenance, and performance analytics (comfort, utilization, benchmarking).

AI Risk Categories: What S&P 350 Companies Flag as Material

Figure 3

Most AI risks relate to cybersecurity and reputational, legal and regulatory, and privacy concerns

Number of S&P 350 companies disclosing AI-related risk in annual reports by risk category, 2023–2025



Note: Some companies disclose more than one AI risk.
Source: The Conference Board/ESGAUGE, 2026

Cybersecurity

Across disclosures, companies consistently frame AI as a threat multiplier for cybersecurity, arguing that ML and generative capabilities increase the scale, speed, and sophistication of malicious activity, ranging from AI-enabled malware and automated phishing/social engineering to deepfakes that undermine identity verification and facilitate fraud. They also describe technical, model-specific vulnerabilities, including adversarial ML and manipulation of AI systems, as expanding the attack surface as AI is embedded into operations and decision-making. A recurring concern is that AI adoption extends risk beyond the company itself through vendors and AI supply chains, where third-party tools and integrations can propagate weaknesses and elevate exposure.

In materiality terms, firms link AI-related cybersecurity risks to operational disruption and loss of sensitive or confidential data. Some disclosures even extend such risks beyond IT systems to physical facilities and infrastructure, framing cyber incidents as capable of disrupting production, logistics, or other operational environments—not only digital services. In C-Suite Outlook 2026, AI risk was also flagged as a workforce issue: “impact of automation, including AI” was cited as a human capital challenge by 18.7% of Europe-based CEOs (vs. 24.0% in North America), reinforcing that material AI exposure extends beyond models and systems to talent, skills, and operating model readiness.

Furthermore, AI-related incidents can lead to heightened regulatory scrutiny and compliance pressure, potentially significant financial impacts (incident response costs, litigation, penalties), and reputational harm and stakeholder trust erosion. Several disclosures also note governance and control responses such as updated policies, training, audits, and recurring AI risk assessments as these threats evolve.

» *Major cyber incidents can depress company value for years, not just create a one-time IT expense. On average, firms experience abnormal stock underperformance of about 8.9% over one year and 14% over two years after an extreme incident; the two-year effect is statistically significant.*[1]

Reputation

Disclosing companies report that reputational harm can arise when AI becomes socially or politically contentious, when stakeholders scrutinize ethical and social impacts (including privacy and intellectual property concerns), or when AI is used in consequential decisions and fails to perform as intended. In this framing, trust erosion is driven less by AI in the abstract than by identifiable failure modes, incorrect or misleading algorithmic outputs, unintended effects, data misuse, and algorithmic bias—each of which can trigger public debate, heightened regulatory and litigation attention, and, ultimately, damage to brand credibility and customer relationships.

AI-related reputational damage can undermine a company's ability to attract and retain customers and create direct financial loss (e.g., through lost revenue due to customer churn, reduced sales), especially where AI is used in critical decision-making or where governance is seen as inadequate. In this framing, reputation functions as a transmission channel: technical errors, governance weaknesses, biased outcomes, or misuse incidents can quickly evolve into stakeholder distrust, heightened scrutiny, and enforceable accountability, ultimately straining customer relationships and increasing financial exposure.

In C-Suite Outlook 2026, Europe-based CEOs were more likely than their peers in North America to prioritize "AI in communications" (31.0% Europe vs. 20.6% North America), implying that firms see AI-enabled messaging as both an opportunity and a reputational risk requiring tighter oversight and controls.

Regulation

Across disclosures, companies describe AI regulation as rapidly evolving and difficult to anticipate, with meaningful ambiguity around how privacy, data protection, and related legal requirements will be interpreted when applied to AI systems. Companies also emphasize that this is not only an on-paper governance issue. They expect practical obligations that affect how AI is built and used, including transparency in decision-making, additional technical documentation and controls, and stronger expectations around accountability.

In some sectors, these requirements are reinforced by industry-specific regulator guidance, for example, in health care-related contexts. Several companies further warn that new rules may force changes to business practices, require retraining of algorithms, or limit the extent to which AI can be used to improve products and services.

The AI regulatory challenge is described as having clear potential financial and operational implications. Companies point to direct exposure to sanctions, including the possibility of significant fines and penalties, sometimes referenced as a percentage of global annual turnover under the EU AI Act. They also highlight knock-on risks such as civil claims and litigation, as well as the need for substantial compliance investment, including new controls, expanded documentation, and ongoing monitoring capabilities.

Beyond these direct costs, companies frame materiality in strategic and execution terms. Regulatory requirements may force the redesign of AI-enabled features, additional validation/testing, expanded documentation, and in some cases retraining or modification of algorithms. Companies also warn that regulation may restrict, limit, or prevent certain AI applications, reducing flexibility in how AI can be deployed across products and services. Finally, the rapidly evolving global regulatory landscape increases complexity for multinational operations, requiring coordination across legal, compliance, engineering, and product teams.

For example, in March 2023 Italy's data protection authority temporarily blocked ChatGPT while it investigated suspected GDPR breaches and set out remedial requirements for the service to resume. After concluding its investigation, it fined OpenAI €15 million and ordered a public information campaign, illustrating how the interpretation of privacy laws as applied to AI can translate into forced product/process changes and direct financial exposure.

Privacy

AI-related privacy concerns are framed by companies as a governance and trust challenge created by the acceleration of data-driven automation and new AI-enabled interactions with customers, employees, and third parties. Disclosures emphasize that AI can expand the collection, processing, and reuse of personal information, while increasing exposure to privacy breaches and misuse if systems are improperly designed, implemented, or controlled. Several reports highlight genAI as a distinct pressure point: privacy and security are described as barriers to adoption, and companies stress technical and procedural safeguards intended to limit exposure, such as constraining user/model interactions to the individual, preventing customer data from being used to train models, and relying on encryption and commercial-grade data protection configurations. Beyond product controls, firms also connect privacy to wider AI-risk vectors including deepfakes and emerging cyber threats. This highlights the need to embed privacy and security considerations throughout the AI system's lifecycle, reinforced by internal training and ongoing monitoring of AI use cases.

AI-related privacy risk is portrayed as an enterprise exposure that can cascade across reputation, cybersecurity resilience, and legal/regulatory compliance. Some companies explicitly elevate responsible AI and data privacy/security to the level of most material (unmitigated) financial risks, while others stress that privacy failures can directly constrain AI deployment by eroding user trust and slowing the adoption of AI-enabled services. Regulated firms, particularly in financial services and health care-related contexts, underscore uncertainty at the intersection of emerging AI rules and established privacy regimes (including GDPR-aligned expectations), implying heightened compliance burdens, supervisory scrutiny, and the prospect of enforcement if controls do not keep pace. Operationally, AI is positioned both as a privacy-protective control (e.g., AI-based security solutions designed to protect customer privacy) and as a force multiplier for cyber and data protection risk; in both framings, privacy is treated as inseparable from AI governance and therefore material to continuity, stakeholder confidence, and the permissibility of scaling AI across the business.

In a 2021 case involving a photo app that US regulators said misled users, the authorities alleged the company was not transparent about its facial-recognition feature or how it collected, used, and retained users' photos and videos. The resulting privacy enforcement action went beyond standard notice-and-consent fixes, requiring the company to delete the facial-recognition models and algorithms it had developed using media obtained under the challenged practices.

The EU and US: AI risk disclosure comparison

AI risk fillings of EU companies cluster most heavily around the same triad as their US counterparts: reputation, cybersecurity, and regulation. However, the relative emphasis differs: for US companies: reputational risk is the dominant category and is framed as an umbrella category for highly visible failure modes—such as consumer-facing errors, capability and implementation shortfalls, privacy lapses, hallucinations/inaccurate outputs, and bias/fairness concerns—that can quickly trigger customer, investor, regulator, and litigation impact.

On cybersecurity, US companies also describe AI as amplifying attacks and expanding the attack surface, with notable attention to third-party/cloud/vendor dependencies, closely matching how EU companies frame AI-risk exposure.

On regulation, both EU and US companies stress rapid change and uncertainty. US filings tend to focus on navigating fragmented, cross-border regimes, often explicitly flagging the EU AI Act, and on the difficulty of applying existing consumer and privacy laws to AI use cases. Meta, for example, paused plans to train LLMs on EU Facebook/Instagram user content after engagement with Ireland's Data Protection Commission, and has said it would not roll out certain multimodal AI offerings in the EU due to regulatory uncertainty. This illustrates how cross-jurisdiction compliance can delay deployment and reshape AI product roadmaps. EU issuers, by contrast, lean more heavily into the practical governance requirements likely to flow from evolving rules, such as transparency, documentation, controls, and accountability.

Conclusion

Looking ahead, AI risk disclosures by S&P Europe 350 issuers are likely to become more granular and control-focused as the EU AI Act's phased obligations begin and the wider EU regulatory framework raises expectations around governance, cybersecurity accountability, and third-party oversight. The dominant themes should remain consistent: AI as a cybersecurity threat multiplier, reputational harm as a transmission channel from identifiable AI failure modes, and uncertainty in rapidly evolving regulation, while privacy is increasingly treated as inseparable from AI governance.

As regulatory ambiguity hardens into practical obligations (transparency, technical documentation/controls, and accountability), the differentiator will be disclosure quality: whether firms can evidence credible governance and vendor controls behind the risk-factor language, not just describe the risks.

About This Report

This report analyzes how S&P 350 companies disclose AI-related risk factors in their annual reports, using 2023–2025 data compiled by The Conference Board® and data analytics firm ESGAUGE as of January 10, 2026. Disclosures are categorized by type: reputational, cybersecurity, legal and regulatory, intellectual property, privacy, adverse consequences and other. Sector-specific patterns and trends over time are also highlighted.

Explore Corporate Disclosure Trends with TCB Benchmarking

This report shares data from the TCB Benchmarking platform, powered by ESGAUGE. TCB Benchmarking provides access to a comprehensive library of corporate disclosure data from European and US public companies. To schedule a demo of TCB Benchmarking, please contact Anuj Saush (asaush@tcb.org) or Evi Angelidou (pangelidou@tcb.org).

About the Knowledge Partner

POWERED BY ESGAUGE INTANGIBLES AI

ESGAUGE is a data mining and analytics firm uniquely designed for the corporate practitioner and the professional service firm seeking customized information on US public companies. It focuses on disclosure of environmental, social, and governance (ESG) practices such as executive and director compensation, board practices, CEO and NEO profiles, proxy voting and shareholder activism, and CSR/sustainability disclosure. Our clients include business corporations, asset management firms, compensation consultants, law firms, accounting and audit firms, and investment companies. We also partner on research projects with think tanks, academic institutions, and the media. www.esgauge.com

About the Authors

Ioannis Siskos, Senior Research Fellow, Governance & Sustainability Center, Europe

Anuj Saush, Head, TCB Advisory International, Europe

Endnotes

[1] Matthew Ryan, et al., *The Impact of Extreme Cyberattacks on Market Valuations: An In-Depth Economic Analysis*, Australian Journal of Management, 2025.