RESOLÜT PARTNERS

Analysis

Governing AI in boardrooms: 10 things board of directors must avoid to stay ahead and stay protected



Governing AI in boardrooms: 10 things board of directors must avoid to stay ahead and stay protected

Click here to listen to an AI-generated (unedited and unreviewed) podcast of this article.

Key Takeaways

- AI now drives core functions like hiring, capital allocation, customer service and compliance, so overseeing its use is a board-level fiduciary duty
- The greatest risk comes from "shadow AI", where employees input sensitive data into public tools, as seen in Samsung's 2023 data leaks[1]
- Data entered into public AI tools can lose both confidentiality and legal privilege permanently[2]
- Regulators and courts treat AI outputs as evidence; prompts can be discoverable, and cases involving bias and misleading AI claims are increasing
- D&O Insurers are introducing strict AI-related exclusions in D&O policies, making formal governance and documentation essential[3]

[1] Business Today, Samsung employees accidentally leaked company secrets via ChatGPT April 13, 2026 - Link.
[2] United States v Heppner, No 25 Cr 503 (JSR), 2026 WL 436479 (SDNY, 17 February 2026) (Rakoff J).
[3] Medium, The First AI Liability Insurance Product Has $25 Million in Coverage. Five Exist Worldwide, 22 March, 2026 - Link.

AI could now be a board-level risk

Until recently, artificial intelligence was looked at as a productivity tool to be bought, installed, and tested. This testing phase may now be approaching its end. Agentic AI and Generative AI now run through ordinary business operations. They screen job applicants, draft board notes, price risk, answer customers, and write production code etc. The increased functionality and usage has also increased the risk exposure. While the system can increase efficiency and revenues, it can potentially also leak a trade secret or trigger customer claims overnight.[4]

Across the world, the courts and regulators are rewriting the rules on confidentiality, liability and disclosure for a world run by AI. Hence, the board of directors need to be fully conscious of the exposure AI can potential bring both upon the businesses and themselves personally.

How companies are using AI

Currently, AI is being used in companies in two primary ways. The first is sanctioned, i.e. systems for hiring, fraud detection, customer service, forecasting, and software development, usually bought under a formal vendor contract. The second is "*shadow AI*", and it is the more dangerous of the two whereby employees are increasingly using consumer tools like ChatGPT, Gemini, and Claude to get work done faster.[5]

Shadow AI is where governance is most vulnerable. In 2023, within weeks of letting its engineers use a public chatbot, Samsung had three separate leaks. An engineer pasted in proprietary semiconductor source code to speed up debugging. Another uploaded defect-detection code to get optimisation suggestions. A third fed in a recording of a confidential internal meeting to turn it into minutes. Because the tool kept those inputs as training data by default, the trade secrets were given away leading to serious consequences. The episode taught some hard lessons i.e. the damage is done the moment the data is entered, it makes no difference that the employee meant no harm, and the consequences could be irreversible.[6]

The new risk landscape

Confidentiality and the collapse of legal professional privilege

The biggest risk to sharing of data is with respect to legal professional privilege. Increasingly, employees consult, brainstorm, and finalise legal strategy with a generative AI tool before ever approaching a lawyer. This can have serious ramifications for both confidentiality and privilege.

In *United States v. Bradley Heppner* (Southern District of New York, 2026), the court held that neither the prompts a user types into a public AI tool nor the answers it gives back are protected by attorney-client privilege or the work-product doctrine. The court reasoned that an AI tool is not a lawyer, and privilege depends on a relationship of trust with a licensed professional. Typing

[4] Forbes, Samsung Bans ChatGPT Among Employees After Sensitive Code Leak - Link.
[5] IBM, What is shadow AI? - Link.
[6] Financial Express, Samsung's trade secrets have reportedly leaked because employees shared a bit too much info with ChatGPT, 7 April, 2023 - Link.

sensitive facts into a commercial platform whose terms let it keep and share that data means the information is no longer confidential. Further, the court observed that the problem cannot be fixed after the fact by forwarding the material to a lawyer.[7] For a company, this can be a hard lesson, a manager who made a note about a regulatory investigation or a contractual claim in a consumer chatbot may end up losing all confidentiality.

Discovery — "prompts are documents."

There is an increasing trend of seeking disclosures about AI related work product in court / arbitration discovery processes. Hence, boards should be mindful that prompt histories and AI outputs can be demanded in discovery, and that they may expose a company's internal doubts and weak points in a case. In *Concord Music Group v. Anthropic*,[8] the court accepted that the lawyers' carefully written prompts could count as opinion work product, but held that the protection was waived once the party relied on the AI's performance as part of its case.

Algorithmic bias and tort liability

Companies have also started using AI for handling customer facing functions such as handling customer enquiries, after sales etc. Recently, when a company used AI in front of the public, courts treated the system as the company's agent. This meant that the company was answerable for the AI bot's mistakes. In *EEOC v. iTutorGroup*,[9] the US Equal Employment Opportunity Commission won a US$365,000 settlement in its first AI-discrimination case. The company's recruitment software had automatically rejected women over 55 and men over 60, in breach of age-discrimination law. The problem only surfaced because one applicant sent in two identical résumés with different dates of birth, and only the younger one was shortlisted. In another case *Moffatt v. Air Canada*,[10] a tribunal held the airline responsible for wrong information its own chatbot had given a customer. The chatbot's mistake was treated as the company's mistake.

Companies sign enterprise AI contracts assuming that the vendor carries the risk. However, these models are trained on enormous and undisclosed datasets. Hence, the vendors cannot promise that the output will not infringe someone else's rights thereby ensuring they remain protected themselves. They exclude or cap IP indemnities, often at twelve months' fees. They reserve the right to train on customer inputs, which can also quietly strip the data of its confidential status.[11] They grant only a limited licence to the output, and they restrict audit rights. If AI-generated marketing, code or designs turn out to infringe a third party's IP, the liability may land with the company that used the tool, not the vendor that supplied it.

Regulatory and disclosure risk

Regulators are also increasingly paying close attention to what companies say about their AI usage. The US Securities and Exchange Commission's "*AI-washing*" cases against *Delphia*[12] and

---

[7] *United States v Heppner*, No 25 Cr 503 (JSR), 2026 WL 436479 (SDNY, 17 February 2026) (Rakoff J).
[8] *Concord Music Grp., Inc. v. Anthropic PBC*, 2025 U.S. Dist. LEXIS 201671 (Northern Dist. Cal. October 12, 2025).
[9] Press Release, U.S. Equal Employment Opportunity Commission, EEOC Sues iTutorGroup for Age Discrimination, 5 May, 2022 - Link.
[10] *Moffatt v. Air Canada*, 2024 BCCRT 149.
[11] Reuters, AI-focused procurement playbook refresh, 10 April, 2024 - Link.
[12] Sec. Exch. Comm'n, I*n the Matter of Delphia (USA) Inc.*, File No. 3-21894 at 2 (18 March 2024).

Global Predictions punished firms for overstating their use of AI to investors.[13] Similarly, for listed Indian companies, AI that has a material effect on revenue or operations may trigger disclosure obligations under the SEBI Listing Regulations.

D&O Insurance policies are excluding AI related liabilities

As the exposure grows, the insurance companies are moving the other way. Insurers like Berkley have added "absolute" AI exclusions to directors-and-officers and errors-and-omissions policies, and others exclude named tools outright.[14] Thus, the directors must ensure that such exclusions are properly negotiated and considered in their D&O policies going forward.

Conclusion

As seen from above, AI use can multiply a company's liabilities faster than any technology, if used carelessly. However, governed properly, it is yet another enterprise level tool that can increase efficiencies by leaps and bounds. Thus, the boards must be cautious and push for a safe and compliant AI usage such that they are ready to meet the risks.

10 Things the Board of Directors Must Not Do

1. **Do not treat AI as a low-risk IT tool**: it poses serious enterprise-level risk, so don't operate without proper policies and governance frameworks around AI usage.

2. **Do not leave AI oversight to one function**: don't run AI without a cross-functional governance committee comprising legal, IT, security, HR and the business with clear mandate to drive policy, escalation and reporting to the board.

3. **Do not lose track of your AI systems**: don't operate without a single register of every AI system in use, whether built in-house, bought from a vendor or running unofficially.

4. **Do not allow consumer AI for sensitive work**: don't let employees use unapproved consumer tools that reuse data or lack proper encryption, and don't rely on a one-off memo in place of real training.

5. **Do not put privilege at risk**: don't route sensitive analysis through AI or wait until a dispute has formed before involving counsel.

6. **Do not go live without testing for bias**: don't deploy AI in hiring, lending or other high-stakes decisions without independent bias testing and regular monitoring.

7. **Do not sign vendor contracts blindly**: don't assume the vendor carries the risk. Thorough review of IP indemnities, training-data rights, ownership of output and audit rights should be undertaken.

---

[13] Press Release 2024-36, U.S. Securities Exchange Commission, SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence, 18 March, 2024 - Link.

[14] Medium, The First AI Liability Insurance Product Has $25 Million in Coverage. Five Exist Worldwide, 22 March, 2026 - Link.

8. **Do not overstate your AI use**: don't tell investors or regulators anything about the company's AI usage that cannot be proven.

9. **Do not ignore your D&O insurance**: don't overlook AI exclusions in D&O and E&O policies.

10. **Do not leave AI discussions off the record**: don't let board minutes omit genuine discussion of AI risks and approval of AI policies without a contemporaneous record.

Authors



Prashant Khurana
Resolüt Partners



Mohammad Kamran
Resolüt Partners

The authors would also like to acknowledge and thank **Arya Mitkari** for his contribution to the article.

Join our Whatsapp Community

Click here or scan the QR code to join our WhatsApp community

Recent Research

TITLE	PRACTICE
M&A Considerations for Roads Secondaries in India | Beyond Traffic and Concession Life 11 June 2026 | Analysis	Listed M&A/ Securities Law
Tracking Debentures and the New ECB Framework: An Idea Whose Time Has Come 04 June 2026 | Analysis	Private Credit
Private Equity | Stress-Testing the Deal: Key Investor Protections in Downside Scenarios 16 April 2026 | Analysis	Private Equity/ M&A
GAAR Grandfathering Restored: CBDT Responds to Tiger Global, but Only Partly 08 April 2026 | Bottom Line	International Tax
Public M&A: Does conversion of >5% convertibles result in a new open offer if the original offer was triggered by both equity and the same convertibles? 02 April 2026 | Bottom Line	Listed M&A/ Securities Law

Click here or scan the QR to view other research

FT INNOVATIVE LAWYERS 2024 ASIA-PACIFIC

Only Indian law firm commended for Innovation in 'Dealmaking' category at the FT Innovative Lawyers Awards Asia-Pacific.

About Resolüt Partners

We are a firm focused on transactional law and global dispute resolution, and are built on four main foundations:

- *Mathematically sharp commercial approach*
- *Integrated legal, tax and dispute resolution advise*
- *Multi-jurisdictional understanding*
- *Problem solving through elimination of choices*

Simply, we believe that for us to be effective at what we do, we cannot confine ourselves to the theoretical exploration of the law and have to lean into the practical implementation...*read more*

About our International Disputes & Investigations Practice

International Arbitration and Dispute Resolution is a core specialism of the firm. Our practice operates at the intersection of transactional law and courtroom advocacy. The firm's deep expertise in structuring and executing complex cross-border transactions – particularly in the technology, infrastructure, renewable energy and financial services sectors – gives us a distinctive ability to understand the commercial and contractual context in which disputes arise, and to deploy that understanding with precision in the conduct of proceedings. We do not approach disputes in isolation from the deal. We approach them as informed insiders.

The team has appeared before and been appointed to tribunals under the SIAC, ICC, LCIA, MCIA, LMAA and ad hoc rules, handling arbitrations across major seats globally including London, Singapore, New York, Geneva, and across India.

The arbitrations we handle are complex, high-stakes and consequential. Our lawyers combine strong commercial acumen and a multi-jurisdictional approach with an in-depth understanding of the law to deliver and implement effective dispute resolution strategies that align with and achieve our clients' strategic objectives...*read more*