RESOLÜT PARTNERS

Governing AI in the Boardrooms

AI Governance, Liability and Disclosure

13 August, 2026

Session Background

AI now sits inside several layers of corporate decision-making - screening job applicants, drafting board presentations, assessing risk, managing customer queries, and writing code. Oversight has to be built into the workflow, not added after the fact.

Session Questions:

01

How does this use of AI create exposure for the company and for directors personally?

02

What should a board ask before and after a system goes live?

03

What steps on policy, contracts, insurance and records actually reduce that exposure?

Shadow AI and the Loss of Confidentiality

What is Shadow AI?

Shadow AI is the use of AI tools by employees without formal approval from / integration with IT-systems of an organization. It comes with certain key risks

- Loss of data confidentiality – can even be publicly accessible depending upon the model used
- Uncertain retention period for model training
- Loss of confidentiality directly leads to loss of privilege

‘Public’ does not only mean accessible to the general public in this context. Sharing data with third party service providers without confidentiality covenants can also cause data to be considered public.

***Lessons**: No ability to recall as confidentiality is lost immediately upon upload; absence of organization-wide protocols for confidentiality; employee intent may not exist, which complicates punishment.*

Samsung's Three Leaks in Three Weeks

LEAK 1

Semiconductor Source Code

An engineer pasted proprietary semiconductor source code into ChatGPT to speed up debugging. The code (a core trade secret) was retained as training data.

LEAK 2

Defect-Detection Algorithm

A second engineer uploaded confidential defect-detection code seeking optimization suggestions.

LEAK 3

Internal Meeting Recording

A third engineer fed a recording of a confidential internal meeting into a public AI tool to auto-generate minutes.

Why Do Employees Do This?

Deadline pressure, no sanctioned equivalent, and a genuine belief that a chatbot is like a search engine.

Is this a practice prevalent even within HR functions?

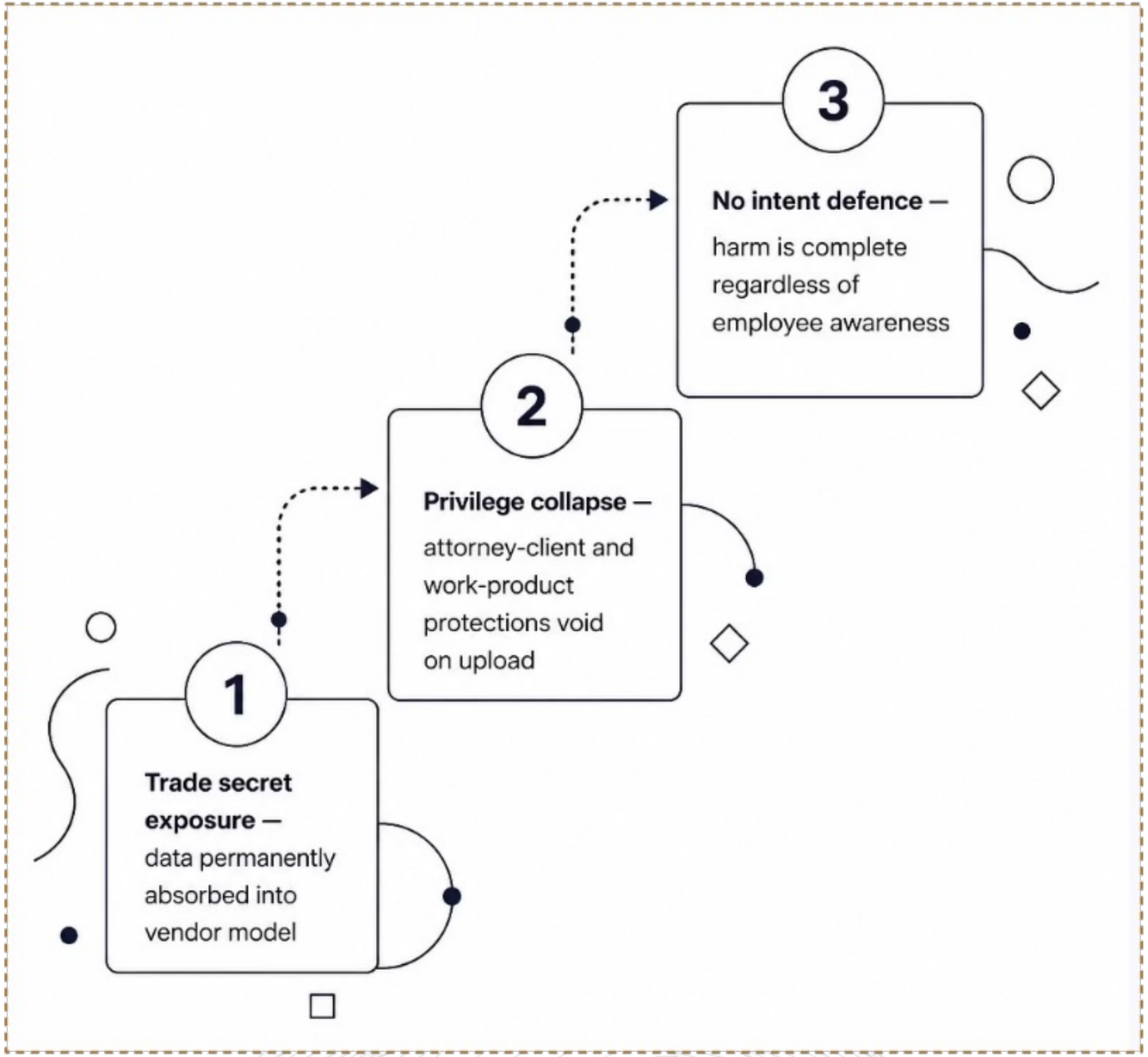
Are HR teams using AI to review performance notes, etc.?

Are companies concerned about the loss of personal data on this count?

What is being done to mitigate use of shadow AI?

What tools are needed to fix this problem: Enrolment-style training, and making the safe route the easy route.

Privilege and Discovery



Privilege and Discovery

- Employees now consult AI tools on legal strategy before approaching counsel, skipping the protected conversation entirely.
- Brainstorming and finalizing strategy with generative AI erodes legal professional privilege, the AI is not counsel, and the conversation is not protected.
- Data shared with AI tools loses confidentiality protections. Once disclosed to a third-party system, privilege may be permanently waived.
- This is no longer just a data privacy concern, It is where the issue can pivot from data privacy problem to legal privilege.

Privilege and Discovery

United States v. Heppner (2026)	Concord Music Group v. Anthropic (2025)
The court held that an AI tool is not a lawyer, and privilege depends on a relationship of trust with a licensed professional. Typing sensitive facts into a commercial platform whose terms let it keep and share that data means the information is no longer confidential. The court observed that the problem cannot be fixed after the fact by forwarding the material to a lawyer. Neither the prompts nor the outputs of a public AI tool are protected by attorney-client privilege or work product.	The court accepted that carefully drafted lawyer prompts could qualify as opinion work product, but held that protection was waived once the party relied on the AI's performance as part of its case.

Prompt histories are documents. They expose a company's internal doubts and weak points in a case, and can be demanded in discovery and arbitration.

How discovery and disclosure practice here is likely to absorb this, and the position on privilege under the Indian framework.

Privilege and Discovery – Board Action

- How concerned are HR teams about this issue today?
- Do companies have a mechanism to manage the fallout once this happens?
- What is the Day-1 action after an employee is found to have used AI this way?

Board Action

- Do not route sensitive analysis through AI, and do not wait for a dispute to crystallize before involving counsel.
- Question for management: If we were served a disclosure request tomorrow, could we produce or defend withholding - our prompt histories?

Liability for AI Mistakes

RESOLÜT PARTNERS

Liability for AI Mistakes

EEOC v. iTutorGroup

The company's recruitment AI automatically rejected women over 55 and men over 60 - a clear breach of age-discrimination law. The flaw was only discovered because one applicant submitted two identical résumés with different birth years, only the younger profile was shortlisted.

Settlement: $365,000 paid by the Company

Moffatt v. Air Canada

Air Canada's chatbot provided a passenger with inaccurate bereavement fare information. The court held the airline fully liable for its AI's misinformation, the company could not disclaim responsibility for its own automated agent.

Precedent-setting liability for AI output

When a company puts AI in front of the public, courts treat the system as the company's agent.

In both cases, the problem could not be identified from inside the company and was found by accident. Therefore, an absence of complaints should not be treated as a complete lack of any issues.

Liability for AI Mistakes

- How are AI-tools for customer / employee facing functions actually adopted in an organization?
- What is the level of involvement of talent acquisition teams, services groups, and legal teams in onboarding such AI tools?
- For customer facing responsibilities, how can companies design protocols that ensure correct information is conveyed while cost optimization makes it necessary to use AI tools?

Structural Challenges with AI Tools

Structural Challenges with AI Tools

- ***IP Infringement Claims***. No AI vendor can warrant that output won't infringe a third party's IP - models are trained on enormous, undisclosed datasets. This risk exists with every AI tool.
- ***Liability Allocation***. If AI-generated marketing, code or designs infringe third-party IP, liability lands on the company that used the tool.
- ***Mitigating Risk***. In enterprise contracts: check for excluded or capped IP indemnities, any reserved right to train on customer inputs, and audit rights over data-sanitization methods.
- Enterprise agreements should bar the vendor from retaining data, prompts or training inputs, and should clearly define ownership of uploaded data.
- ***Future Outlook***. Expect these to become turnkey contracts over time, which increases the risk.

Structural Challenges with AI Tools

What are the dispute-resolution mechanisms for AI-related IP-infringement claims defences available to companies caught up in them?

Is there a criminal-liability angle worth flagging here?

Which of our AI contracts allow the vendor to train on our data, and what is our IP indemnity right actually capped at?

Disclosure, Regulation and Insurance

Disclosure, Regulation and Insurance

- **AI-washing**: The SEC's actions against Delphia and Global Predictions - both penalized for overstating their use of AI to investors.
- **India**: The DPDP regime applies to personal data processed through AI systems, including consent and purpose limitation where employee and customer data is involved.
- **D&O and E&O**: Insurers have introduced absolute AI exclusions, and others exclude named tools outright. Without cover, the company may face large payouts in shareholder litigation - or directors could be personally liable if the company can't indemnify them.
- **Directors should regularly and carefully review AI use with management, to demonstrate oversight and avoid negligence claims.**

SEC v. Delphia (USA) Inc. (2024)

The Company claimed it used AI/machine learning on clients' social media and banking data to power investment decisions. It never actually used any client data in its algorithm, despite years of marketing claims. Kept making the false claims even after admitting the truth to SEC examiners in 2021.

Penalty: $225,000 paid by the Company + censure + cease-and-desist order

SEC v. Global Predictions, Inc. (2024)

The Company falsely marketed itself as the "first regulated AI financial advisor" and claimed to offer "expert AI-driven forecasts" on its website, social media, and in client emails - capabilities it didn't actually have.

Penalty: $175,000 paid by the Company + censure + cease-and-desist order

Disclosure, Regulation and Insurance

- Regulatory statements can become evidence - watch the gap between what the annual report claims about AI and what the systems actually do.
- Can internal communications be tailored to explain AI tools, and their nuanced risks- clearly to employees?
- Should rewards be tied to employees' level of AI adoption, as is happening in some cases, or is that a misaligned incentive that encourages hastier use?

Conclusion

- Treat AI as an enterprise risk, not an IT issue.
- Stand up one cross-functional governance committee to own vendor onboarding.
- Keep a register of every AI system sanctioned for use.
- No consumer AI for sensitive work.
- Protect privilege.
- Test for bias and other inherent risks before deploying tools.
- Use checklists when negotiating AI vendor contracts.
- Check D&O and E&O policies for AI exclusions.
- Record board-level consideration of these issues to avoid negligence claims.


RESOLÜT
PARTNERS