Shumaker

APRIL 13, 2026 | PUBLICATION

Client Alert: Artificial Intelligence (AI) Is Supposed to Reduce Risk. Why Does It Feel Like the Opposite?

Last month, I wrote about a question many general counsel are beginning to hear from business leadership: *If our outside counsel is using AI, should our legal spend be going down?*

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

Lloyd J. Wilson

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The response to that article confirmed something many legal leaders already know: AI has changed how legal work is done, but it has not simplified the expectations placed on legal departments.

There is a parallel question starting to surface alongside that cost discussion, one that is broader and potentially more consequential:

If AI is making legal, privacy, and cybersecurity functions faster and more efficient, why does the organization's overall risk profile feel higher than ever?

For many companies, AI investments were expected to reduce exposure by improving detection, consistency, and responsiveness. In practice, risk has not disappeared. In some cases, it has become harder to assess, harder to explain, and harder to contain.

Understanding why requires a closer look at how AI changes, not eliminates, risk.

Efficiency Changes How Work Is Done, Not Who Is Accountable

AI is now embedded in many core risk functions. Organizations rely on AI-enabled tools for security monitoring, data classification, incident detection, compliance assessments, document review, and internal investigations. Much like AI-assisted drafting and research at law firms, these tools often operate quietly in the background, supporting decisions that carry real legal consequences.

AI unquestionably makes certain tasks more efficient. It can process more data, operate continuously, and surface issues more quickly than traditional manual approaches. Those efficiencies are valuable, and in many cases necessary, given the increasing complexity of regulatory and threat environments.

But efficiency does not change accountability.

When an AI-enabled system flags an incident, classifies data incorrectly, escalates an alert, or triggers a response, the organization remains responsible for the outcome. The decision may be faster, but the obligation to defend it does not change.

Speed Alters the Risk Profile

One effect of AI that is often overlooked is that it accelerates not only correct decisions but also incorrect ones.

AI-driven systems can act at scale and at speed. A classification error, a flawed assumption, or an incomplete model can affect large volumes of data or trigger actions across multiple systems before human review ever occurs.

This does not mean AI is unsafe or inappropriate. It means that mistakes propagate differently in an AI-enabled environment. Legal and security teams may gain broader coverage, but they also inherit greater downstream consequences from isolated failures.

As AI expands what teams can review and act upon, the scope of potential impact expands as well.

The Growing Attribution Problem

As AI becomes more deeply integrated into operational workflows, a practical question emerges after incidents and near misses: *How was this decision made?*

That question matters because regulators, auditors, boards, and plaintiffs do not differentiate between decisions made by people and decisions made with the assistance of AI. They focus on whether reliance was reasonable, supervised, and defensible.

Legal teams are increasingly asked to explain:

- Why an AI-enabled system was relied upon
- How its outputs were validated
- What limitations were understood at the time
- Where human oversight was applied

These are governance questions, not technical ones. And they often land squarely with legal leadership.

Cheaper Decisions, More Concentrated Exposure

AI changes the economics of decision making. Once deployed, the cost of additional analysis, review, or monitoring drops significantly. That can be a genuine advantage, particularly in resource-constrained environments.

But lower marginal cost also means more decisions are made, more often, and sometimes with less friction. Over time, risk becomes more concentrated. A small number of systems influence a wide range of outcomes.

When those systems perform well, they enhance consistency and responsiveness. When they perform poorly, the impact is rarely limited.

This helps explain why organizations can feel operationally stronger while simultaneously feeling more

exposed.

Why This Becomes a Legal Issue

Legal departments sit at the intersection of cost control, operational reliance, and accountability. Legal teams do not design most AI systems, but they are often responsible for approving disclosures, overseeing incident response, supporting audits, and communicating risk to senior leadership and boards.

As AI becomes embedded in upstream workflows, legal teams inherit not only the results but the obligation to stand behind them irrespective of whether technology is deployed internally or through third‑party vendors.

This is not about slowing innovation. It is about ensuring that reliance keeps pace with governance.

Questions Worth Asking

General counsel do not need to master AI technology to manage this shift. But asking the right questions internally can materially change how risk is understood and managed:

- Where are we relying on AI outputs without meaningful human validation?
- Which decisions would be difficult to explain after an incident?
- How do we document oversight and escalation paths?
- Are we clear about when AI is appropriate and when it is not?

These are the same types of questions legal departments already ask about outside counsel and key vendors. AI simply introduces a new context in which those questions matter.

Conclusion

AI can make legal, privacy, and cybersecurity functions faster and more efficient. It can improve coverage, consistency, and responsiveness in an increasingly complex environment.

But efficiency is not the same as risk reduction, and speed does not eliminate accountability. In many cases, AI shifts risk rather than removing it, concentrating responsibility in fewer, more consequential decision points.

For legal leaders, the goal is not to resist AI but to ensure that governance evolves alongside reliance. When expectations are set clearly and oversight is intentional, AI can strengthen outcomes without quietly expanding exposure.

Shumaker