LARRIDIN

A Practical Guide to Managing AI-Related Directors & Officers Liability

The AI Impact on D&O Insurance Risk Management Guide for CFOs

December 2025

Co-authored by:

Michael Levine
Partner at Hunton Andrews Kurth

Russ Fradin
CEO of Larridin

Table Of Contents

Executive Summary 3

Section 1: What Most Directors Don't Know About Their AI Exposure 4

Section 2: The Insurance Coverage Crisis 6

Section 3: What Insurance Carriers Need to See 8

Section 4: Practical Risk Mitigation Strategies 10

Section 5: Engaging with Insurance Carriers 13

Section 6: What Directors Should Do This Quarter 15

Conclusion: The Window for Proactive Risk Management 17

Resources and Next Steps 18

Executive Summary

The Challenge:

D&O insurers cannot quantify AI-related risks, creating coverage gaps precisely when AI adoption accelerates. With AI spending reaching $644 billion in 2025 (up 76% from 2024 per Gartner), directors and officers face new liability exposures without clear insurance protection.

The Gap:

Most CFOs and directors believe they understand their company's AI usage. They don't. For every AI tool a company knowingly purchases, employees are using one to two additional AI applications that leadership has never heard of. Even more concerning: two-thirds of employees use personal accounts for AI tools instead of the enterprise versions their companies paid for.

The Urgency:

Major insurers are responding to their inability to price AI risk by introducing broad AI exclusions. As Mark Benioff observes, "We're probably looking at three to twelve trillion dollars of digital labor getting deployed." Directors who fail to establish visibility and governance frameworks now may find themselves personally liable for consequences they never saw coming.

Section 1: What Most Directors Don't Know About Their AI Exposure

The Visibility Problem

> "I'll ask CFOs if their company is using AI," **explains Michael Levine, Partner at Hunton Andrews Kurth.** "Most now say yes. Next question is how. And that's where the conversation usually ends. They don't know."

This isn't a hypothetical concern. When companies deploy AI discovery capabilities, they consistently find:

- **Shadow AI usage:** 1-2 unauthorized AI tools for every known, purchased application
- **Personal account usage:** Two-thirds of employees use personal ChatGPT, Claude, or other AI accounts instead of enterprise versions, despite company BPAs and data retention agreements
- **Pervasive embedding:** AI in manufacturing systems, HR platforms, accounting software, iPhones, desktop applications—often without IT awareness

Why This Creates D&O Liability

Directors bear fiduciary responsibility for corporate risk management. Courts and regulators will not accept "we didn't know" as a defense when AI-related incidents occur. The exposure includes:

Governance Failures:

- Inadequate board oversight of AI deployments
- Failure to implement appropriate AI risk management frameworks
- Insufficient monitoring of AI-related compliance obligations

Disclosure Violations:

- SEC requirements for material AI risk disclosures
- Misrepresentations about AI capabilities or usage ("AI washing")
- Inaccurate financial reporting implications of AI implementations

Operational Incidents:

- Employment discrimination from AI-driven HR decisions
- Consumer harm from AI product failures or advice
- Data breaches through unauthorized AI tool usage
- Intellectual property violations from AI content generation

Real Cases Already in Litigation

CVS Health

Class action in Massachusetts for using AI facial expression analysis during interviews without required consent under state lie detector laws.

"AI Washing" Suits

Multiple companies facing derivative shareholder suits for misstatements about AI capabilities, triggering stock drops.

Personal Injury Cases

OpenAI and Character AI facing wrongful death claims related to chatbot advice.

Professional Malpractice

Legal sanctions for AI-generated hallucinations in court filings.

Section 2: The Insurance Coverage Crisis

Why Insurers Can't Price AI Risk

> "The major insurers have not jumped into affirmative coverage of AI," **Levine notes**. "They don't know how to quantify and therefore can't price that risk. It's the biggest challenge."

Without historical claims data or established frameworks for assessing AI-related liability, carriers face impossible underwriting decisions. The response has been predictable: defensive postures rather than comprehensive coverage.

The Exclusion Problem

Traditional insurers are introducing broad AI exclusions to avoid uncertainty. These exclusions create unexpected coverage gaps. Consider this scenario:

Your company uses Microsoft Word—with its embedded AI grammar and style suggestions—to draft SEC disclosures. A D&O claim arises from an allegedly inaccurate statement. If your D&O policy includes an exclusion for "any claim arising from the use of generative AI," that claim could be excluded entirely.

> "It's severe, and it may not be what the intent was," **Levine warns**, "but unfortunately, that's how the insurance industry works. Underwriters sell policies—they want the money. Then months later, a claim happens. It goes to a different side of the company, and they read the policy. They're like, 'Oh, you used AI, you got an exclusion, claim denied.'"

The Moving Target Problem

Insurance applications increasingly ask specific questions about AI usage:

- What percentage of revenue derives from generative AI?
- Which systems incorporate AI capabilities?
- How is AI deployed across the organization?

> "That's a snapshot in time, and generally there's no duty to update that information," **Levine explains.** "When you get to the back end of that 12-month policy and that number has changed and you experience a loss, they're going to come back and say you misrepresented your revenue. We're not only going to deny your claim, but we're going to rescind the policy."

Policy rescission means the entire policy never existed—complete exposure with no coverage at all.

Emerging AI Insurance Market

A handful of specialized insurers are entering the market:

- **Armilla, Chaucer, Testudo:** Focusing exclusively on AI coverage
- **Munich Re:** "AI Sure" product warranty instrument guaranteeing AI function
- **Smaller Carriers:** More amenable to crafting custom language and definitions

These emerging options provide alternatives, but coverage remains limited and expensive compared to traditional policies.

Section 3: What Insurance Carriers Need to See

Documentation Requirements

Based on discussions with Berkeley, AXA, Munich Re, and other leading carriers, insurers evaluating AI risk want evidence of:

Governance Framework:

- Board-level AI oversight authority and regular reporting
- Written AI policies addressing usage, data handling, and risk tolerance
- Executive accountability structures for AI-related decisions
- Incident response procedures for AI failures

Visibility and Monitoring:

- Complete, current inventory of AI tools and applications
- Understanding of data flows through AI systems
- Usage monitoring across departments and business units
- Controls preventing unauthorized AI implementations

Risk Assessment Process:

- Systematic evaluation of AI deployments before implementation
- Regular compliance audits of AI systems
- Third-party AI vendor risk management
- Legal review of AI use in sensitive applications

Audit Trail:

> "I think an audit trail is very important," **Levine emphasizes**. "You always want to be able to point to hard documentation. If you have an issue about whether you were truthful or accurate in your application—'Yes, we were, because we weren't using this then, but now we do'—that timeline helps push things either into coverage or away from an exclusion."

However, traditional audit approaches fall short:

> "Here's what's interesting about an audit—the day it starts, it's out of date," **notes Russ Fradin**. "You're talking about the fastest-moving technology in the history of technology. You do an audit using a 1950s accounting practice to track 2025 technology."

Application Strategy

Don't Just Check Boxes

Provide narrative explanations of AI usage and anticipated evolution

Invite Dialogue

Make carriers partners in understanding your AI risk profile Document

Assumptions

Explain that AI usage will change during the policy period Seek Custom

Language

Negotiate exclusions and definitions that reflect actual usage

Section 4: Practical Risk Mitigation Strategies

Essential First Step: Establish Visibility

> "If you do not know what is actually happening in your company, you certainly can't have any plan to deal with it," **Fradin emphasizes**. Directors cannot manage risks they don't know exist.

Critical Questions to Answer:

- ? What AI tools are actually being used across all departments?
- ? Are employees using personal accounts instead of enterprise versions?
- ? What data is flowing through these systems?
- ? Where are unauthorized AI implementations creating exposure?

Approach 1: Continuous Monitoring Technology

Implementation: Implementation: Deploy AI discovery and monitoring platforms (such as Larridin Scout, or similar solutions) that provide real-time visibility into AI usage

Benefits:

- ✓ Identifies shadow AI usage and unauthorized tools
- ✓ Tracks personal account usage vs. enterprise versions
- ✓ Creates continuous audit trail for insurance documentation
- ✓ Enables proactive risk identification before incidents occur

Considerations: Technology investment required; change management for deployment

Approach 2: Restrictive Governance Framework

Implementation: Limit AI to pre-approved platforms with strict access controls and usage policies

Benefits:

- ✓ Maximum control and clear accountability
- ✓ Simplified compliance and insurance discussions
- ✓ Reduced risk exposure from unknown tools

Considerations: May limit innovation and competitive advantage; requires significant enforcement resources; employee resistance likely

Approach 3: Periodic Audits and Assessments

Implementation: Quarterly or semi-annual comprehensive AI usage reviews through internal teams or third-party consultants

Benefits:

- ✓ Lower cost than continuous monitoring
- ✓ External validation of governance effectiveness
- ✓ Suitable for organizations with limited AI usage

Considerations: Point-in-time visibility only; significant gaps between audits; becomes outdated immediately in fast-changing environment

Approach 4: Cross-Functional Governance Team

Implementation: Assemble key stakeholders across departments to continuously evaluate AI usage and risk

> "You have to partner with consultants," **Levine advises**. "Identify your key stakeholders within the company. The head of HR is not going to know how operations is using AI, or distribution, or procurement. They're all using different platforms in different ways. So you've got to get your key stakeholders across the company, get them all together, and continually evaluate what you're doing, how you're doing it, and what your exposure looks like."

Benefits:

- ✓ Organization-wide visibility and coordination
- ✓ Shared responsibility for AI governance
- ✓ Better understanding of varied AI use cases

Considerations: Requires ongoing coordination; potential for information gaps; dependent on stakeholder engagement

Recommended Hybrid Approach

Most organizations benefit from combining elements:

- **Technology foundation:** Continuous monitoring for baseline visibility
- **Policy framework:** Clear guidelines for approved usage
- **Cross-functional team:** Regular review and governance oversight
- **Periodic validation:** Third-party assessments for insurance documentation

Section 5: Engaging with Insurance Carriers

Preparing for Application and Renewal

Document Current State:

- Complete AI inventory with usage data
- Governance policies and enforcement mechanisms
- Risk assessments and mitigation plans
- Audit trails demonstrating oversight

Explain Evolution:

> "You can't just check boxes on the application," **Levine explains**. "You've got to provide a narrative. You've got to explain what we're doing, consult with experts to understand here's how we're using AI, here's what our runway looks like over the period of this policy, so the numbers that we give you today are not static. They're going to change. And invite a dialogue with the carrier."

Address Exclusions Proactively:

- Request specific definitions rather than broad AI exclusions
- Negotiate carve-outs for embedded AI in standard business tools
- Seek clarity on what triggers exclusions vs. coverage

Working with Specialized Counsel

> "You have to engage, preferably a lawyer who understands this stuff, because it's not as simple as checking boxes," **Levine notes.**

Insurance counsel with AI expertise can:

- Navigate complex application questions
- Negotiate appropriate policy language
- Create documentation strategies
- Prepare for potential coverage disputes

Managing the Policy Period

- Maintain continuous documentation of AI usage changes
- Notify carriers of material changes when appropriate
- Keep detailed records of governance decisions
- Prepare for potential claim scenarios

Section 6: What Directors Should Do This Quarter

Immediate Actions (Next 30 Days)

Assess Current Visibility

Ask: "Can we document all AI tools and applications in use across our organization right now?" If the answer is NO, you have a governance gap.

Review Existing D&O Coverage

Work with insurance counsel to examine:

- AI-specific exclusions in current policies
- Application representations about AI usage
- Coverage gaps for anticipated AI deployments

Establish Board-Level Oversight

Create or designate AI governance authority with regular reporting to board/ audit committee.

Strategic Initiatives (Next 90 Days)

Implement Visibility Solution

Deploy continuous monitoring, establish audit protocols, or create cross-functional oversight team—choose the approach that fits your organization's AI maturity and risk profile.

Develop Comprehensive AI Policies

Document governance framework addressing:

- Approved AI tools and usage guidelines
- Data handling and privacy requirements
- Risk assessment and approval processes
- Incident response and reporting

Prepare Insurance Documentation

Create comprehensive evidence package for next renewal:

- Current AI inventory and usage patterns
- Governance policies and enforcement
- Risk assessments and mitigation efforts
- Audit trails and oversight evidence

Ongoing Commitments

- **Quarterly governance reviews**: Update board on AI deployments and risks
- **Regular policy updates**: Keep pace with rapidly changing AI landscape
- **Continuous monitoring**: Maintain current understanding of actual AI usage
- **Insurance carrier dialogue**: Proactive communication about AI program evolution

Conclusion: The Window for Proactive Risk Management

The AI transformation represents the fastest technology adoption in corporate history. Directors who establish visibility, governance, and insurance strategies now will be better positioned than those who wait.

"You cannot manage what you do not measure," as the saying goes. In the AI era, what directors don't know will hurt them—and potentially expose them to personal liability.

The good news: establishing appropriate oversight frameworks is achievable. The key is starting now, before coverage becomes prohibitively expensive or unavailable, and before an AI-related incident creates a crisis.

Resources and Next Steps

For Insurance Coverage Guidance:

Michael Levine

Partner at Hunton Andrews Kurth
Insurance Recovery Practice
Washington, D.C.

For AI Visibility and Governance Solutions

Russ Fradin

CEO at Larridin
larridin.com
russ@larridin.com

Industry Data Sources:

- Gartner AI spending projections and market analysis
- SEC guidance on AI-related disclosure requirements
- Emerging insurance market coverage options and trends