Insights: Publications

5 Key Takeaways | Faulty Intelligence: Responding to an AI Incident

August 13, 2025

Kilpatrick's **Greg Silberman** recently led a session at the 21st annual **KTIPS (Kilpatrick Townsend Intellectual Property Seminar**) on "**Faulty Intelligence: Responding to an AI Incident**", focusing on how legal, security, and product teams should prepare for and manage model-driven failures. The discussion examined incident classification through a four-element lens (risk domain, failure mode, lifecycle, and ownership) and provided strategies for rapid stabilization, evidence preservation, remediation, and recovery amid evolving regulatory expectations.

Greg provides these key takeaways:

1. AI Incidents are not the same as Cybersecurity Incidents. Adopt AI-specific incident response plans that address the broader range of harms and failure modes unique to AI. Pre-configure first-hour controls so teams can activate safe mode or human review, rate-limit or geofence features, disable risky tool calls, and bind retrieval to trusted sources on demand. Define clear escalation triggers for disablement, executive and board notice, insurer engagement, and regulatory or customer notifications, aligned to your severity schema.

2. AI Governance is Key. Formal AI governance is critical to both regulatory compliance and enables faster, more effective incident response. Demonstrating responsible AI governance is also becoming a commercial necessity in some industries. At a minimum, maintain an inventory of all AI uses within the company and implement baseline policies governing development, deployment, and use.

3. Review your Insurance Coverage. Verify coverage, panel requirements, and notice periods for AI incidents so the team knows exactly what to report and when. Do not assume that cybersecurity insurance will cover AI-related events or that the same notice periods and evidentiary requirements will apply.

4. Strengthen AI Vendor Terms. Build AI-specific diligence and contractual protections into vendor assessments and agreements. Require restrictions on data use, regulatory-mandated bias testing and documentation (where applicable), assurances of data security, cooperation during incident investigations, and reasonable transparency regarding the vendor's AI supply chain.

5. Practice your AI Incident Response Plan. A written plan is only the starting point. Conduct tabletop exercises with AI-specific scenarios involving cross-functional stakeholders. Recognize that many AI incidents will not involve cybersecurity breaches. After an incident, hold blameless post-mortems and add targeted red-team tests to prevent recurrence.

For more information, please contact:
Greg Silbermann, gsilbermann@ktslaw.com

Related People

Gregory P. Silberman

t 650.462.5310

gsilberman@ktslaw.com