Insights, News & Events

DANIEL PEPPER DISCUSSES PROTECTING THE AI SUPPLY CHAIN FROM CYBERATTACKS

News
Sep 2, 2026

In an article with the *Cybersecurity and AI Law Report*, **Daniel Pepper** discussed how AI middleware has become an attractive target for ransomware attacks, following a two-stage ransomware attack discovered in July 2026 that exploited software widely used to develop and operate AI systems and destroyed a trained AI model. Daniel cautioned that instead of destroying or locking up AI models, ransomware purveyors might start making modifications to produce malicious AI models that could affect the wider operational environment unless the victim pays the ransom.

"If the training data and the datasets that are used for fine tuning become poisoned and you have a compromised model, there are no alarms that go off. There's no indication of a compromise. The integrity of that data now is lost," he said.

To read the article visit *Cybersecurity and AI Law Report* (subscription required).

Related People

Daniel Pepper, CIPP/US
Partner

303.218.3661

Service Focus

Data Protection and Cybersecurity

Related Offices

Denver