HINSHAW

News

# Scott Seaman Addresses a 2025 Cyber Insurance Landscape Confronting Growing AI Risks and Supply Chain Attacks

**February 11, 2025**

In a recent article by *SecurityWeek's Cyber Insights 2025*, Scott Seaman, a Chicago-based partner and co-chair of Hinshaw's global Insurance Services Group, was featured along with several experts to discuss artificial intelligence (AI) and cybersecurity. Seaman addressed the evolving landscape of cyber insurance amidst the growing complexity of cybersecurity threats.

First, Seaman pointed to the advancements in technology, particularly in generative AI, and how they pose heightened systemic risks for insurers in 2025. *SecurityWeek* excerpt:

> "The power of AI presents opportunities that companies cannot afford to ignore, yet the losses can be catastrophic," warns Scott Seaman, a partner at Hinshaw & Culbertson LLP. "We expect to see more generative AI coverage endorsements, both granting coverage and excluding coverage."
>
> Meanwhile, insurers must beware of how they use AI as well as how they cover it. Seaman also notes that in July 2024, the New York State Department of Financial Services (NYSDFS – never a laggard in regulating matters involving finance) adopted a final circular about the 'Use of Artificial Intelligence (AI) Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing'.
>
> "This Circular," says Seaman, "was issued as guidance to the insurance industry and imposes significant obligations on insurers using artificial intelligence systems or external consumer data and information sources for underwriting and pricing."

Seaman also noted the rising number of supply chain attacks as another key cybersecurity concern that insurers will need to consider and address in 2025. *SecurityWeek* excerpt:

> "The CrowdStrike incident has caused insurers to focus on outages as well as cyberattacks and to focus more on the need to limit supply chain exposures in dependent or contingent interruption and other coverages."
>
> But as insurers begin to better understand the complications and potential implications of supply chain risk, their only recourse to address any growing imbalance between income and claims will be to revert to

## Attorneys

Scott M. Seaman

## Service Areas

Privacy, Security & Artificial Intelligence

## Offices

Chicago

increasing either premiums or exclusions.

Lastly, Seaman addressed the impact of global geopolitical risks on the insurance industry at large, revealing that insurers are implementing updated War Exclusions to mitigate liabilities stemming from systemic or state-sponsored cyberattacks. *SecurityWeek* excerpt:

> Seaman delves deeper. "Insurers are adding updated War Exclusions, many are modeled on London [i.e., Lloyds] forms and other exclusions to preclude coverage for systemic or state-sponsored cyberattacks."
>
> "For the past couple of years," continues Seaman, "Lloyds has been requiring that standalone cyberattack policies exclude liability for losses arising from any state-backed cyberattack. There are at least four exclusion forms available. The exclusions must exclude losses arising from war (whether declared or not) and must apply to losses arising from state-backed cyberattacks that significantly impair the ability of a state to function or that significantly impair the security capabilities of a state. As you can envision, determining whether a cyberattack is attributable to a state may present difficulties."

Read the full article.

- "Cyber Insights 2025: Cyberinsurance – The Debate Continues" was published by *SecurityWeek's Cyber Insights 2025* on January 30, 2025.