THE JOURNAL RECORD

Gavel to Gavel: Cyber insurance in 2025 – Why coverage is no longer enough

By: Jason Seay // GableGotwals // July 1, 2026

Jason Seay

For years, cyber insurance was viewed as a financial safety net – something organizations purchased in case the unthinkable happened. As cyber threats become more sophisticated and losses more systemic, cyber insurance is evolving from a back-office risk transfer tool into a strategic business decision.

The market continues to expand rapidly, with double-digit annual growth fueled by increasing cyber incidents, regulatory expectations, and rising awareness of digital exposure. Yet growth alone does not mean organizations are adequately protected. Many businesses, particularly small and mid-sized companies, remain underinsured or misunderstand what their policies actually cover.

Modern cyber policies generally address two categories of risk:

- first-party losses, which often include business interruption, ransomware response, forensic investigations, data restoration, and crisis communications and
- third-party liability, which typically focus on privacy claims, regulatory actions, network security liabilities, and technology-related errors.

But the greatest challenge for buyers today may not be what policies include, ***but what they exclude***.

Insurers are tightening policy language in response to large-scale losses and emerging threats. Exclusions tied to nation-state attacks, widespread infrastructure failures, prior vulnerabilities, contractual obligations, and digital assets are becoming increasingly common. Organizations may assume they are protected only to discover significant gaps after an event occurs.

Recent incidents have highlighted the complexity of these exposures. The debate around war exclusions following major cyberattacks and the widespread business disruption caused by technology outages have forced insurers to reconsider how they model and limit catastrophic cyber risk.

At the same time, artificial intelligence is introducing a new generation of uncertainty. AI-enabled phishing, deepfake fraud, and autonomous attack tools are challenging

traditional underwriting assumptions. Meanwhile, organizations deploying AI internally may face liability exposures that standard cyber policies were never designed to address.

Insurers are responding with more rigorous underwriting expectations. Multi-factor authentication, endpoint monitoring, tested backups, privileged access controls, and formal incident response plans are increasingly becoming prerequisites for coverage, not recommendations.

Looking ahead, the industry may move toward continuous risk monitoring, AI-assisted underwriting, parametric policy structures, and even government-supported cyber backstops for systemic events.

The takeaway for business leaders is clear: cyber insurance can no longer be treated as an annual procurement exercise. Effective protection now requires aligning policy language, cybersecurity practices, and enterprise risk strategy before a claim ever occurs.

Jason Seay is Of Counsel at GableGotwals. He is an experienced technology lawyer focused on data privacy, security and governance.

Gavel to Gavel: Cyber insurance in 2025 – Why coverage is no longer enough | The Journal Record