NEWS & INSIGHTS · INSIGHTS

Cyber Insurance Market 2025: Buyer-Friendly Pricing Meets Rising Resilience Expectations

December 3, 2025 · 4 min read

Cyber insurance entered 2025 in a buyer-friendly position—ample capacity, competitive pricing, and broader appetite—yet the underlying threat environment stayed turbulent. As we move into 2026, most credible market commentary points to a familiar pattern: rate softness for well-controlled buyers, but greater differentiation where ransomware exposure, third-party reliance (cloud/IT suppliers), social engineering, and operational disruption risks are not well managed. Regulators and major risk frameworks are also pushing "resilience" higher up the agenda, which is increasingly shaping underwriting questions and coverage structure.

What Happened in 2025: Prices Eased, Underwriting Stayed Disciplined

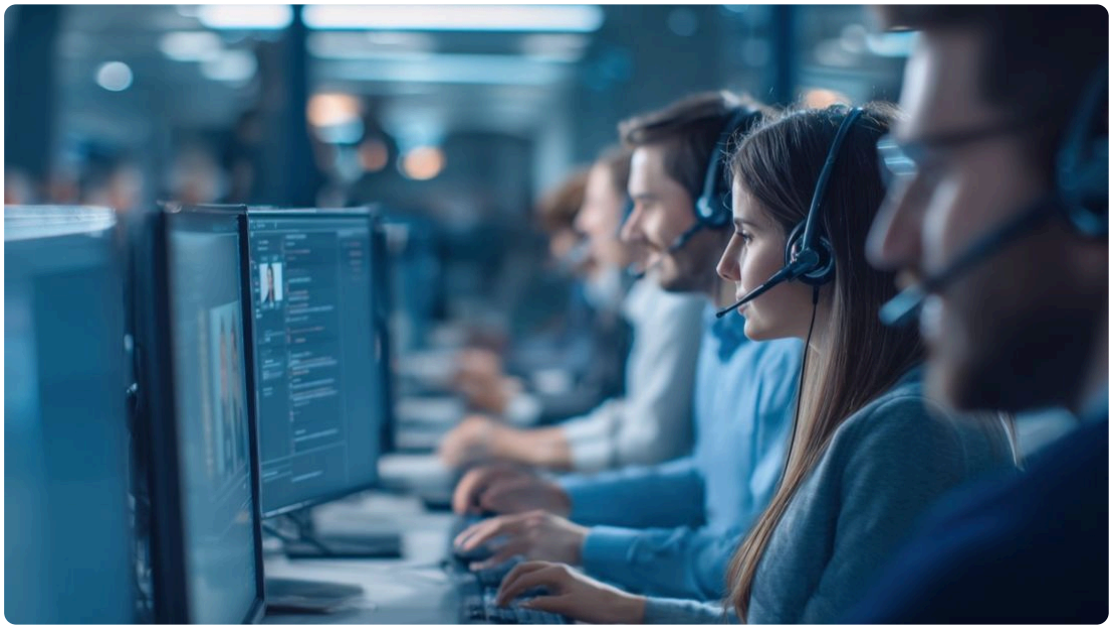
Across 2025 market updates, cyber remained broadly competitive, supported by surplus capacity and intense insurer competition—often translating into flat to falling rates and improving buyer options. At the same time, the claims picture did not "go away."

Ransomware continued to drive both frequency and severity, and attackers increasingly targeted less-well protected organisations, while using more sophisticated tactics and AI-enabled methods.

A key tension emerged: softening rates vs. volatile losses. S&P Global Ratings explicitly warned that stagnant/declining cyber rates combined with a sharp increase in claims could erode profitability—driving the need for clear wording, selective pricing, careful management of limits and retentions, and stronger insured controls through 2025–2026.

Key Indicators (2025 → 2026)

- **Market conditions: buyer-friendly in many segments, with ample capacity and competitive pricing.**
- **Top claims driver: ransomware remains the largest driver of major losses (commercial reporting highlights ~60% of value of large claims >€1m in 1H 2025).**
- **2026 underwriting direction: more emphasis on controls, wording clarity, and cautious management of limits/retentions to protect profitability.**



What to Expect in 2026: Selective Firming, More Scrutiny of Resilience and Dependencies

1) "Risk-Based Outcomes" Will Intensify

2026 is unlikely to be a blanket hard market. Instead, insurers will continue to reward well-controlled organisations while applying tougher terms where controls are weak or exposures are high—particularly around:

- ransomware readiness (containment + recovery)
- email/social engineering controls
- privileged access management
- patching cadence and vulnerability management
- third-party/outsourced IT dependencies (MSPs/cloud)

2) Business Interruption (BI) Will Remain a Core Underwriting Focus

BI is where cyber becomes "real money," and it is increasingly common for cyber events to drive operational downtime. Market commentary in 2025 notes turbulent incident activity despite favourable buying conditions—reinforcing why insurers scrutinise resilience and recovery capabilities.

3) Wording, Retentions and Sub-Limits Will Matter as Much as Headline Premium

Even in competitive pricing conditions, insurers are relying on:

- tighter definitions (events, outages, war/systemic triggers)
- sub limits for specific loss types (social engineering, dependent BI, funds transfer fraud)
- higher retentions/deductibles for frequent loss categories

Why This Matters to the Aviation, Marine and Traders Sector

Aviation (Operators, Managers, Service Providers)

Cyber losses increasingly convert into physical-world disruption: flight planning/ops systems, maintenance records, passenger handling, vendor ecosystems, and charter/management workflows. Underwriters will focus on operational continuity and the strength of identity controls, third-party access, and incident response playbooks.

Marine & Shipping (Owners/Operators, Ports, Ship Managers)

Modern fleets depend on a mesh of shore-side systems and vendors. Insurers will probe segmentation, remote access governance, patching discipline, and the "blast radius" of an event—especially where a single outage could affect multiple vessels or business units.

Commodity Traders

Traders face elevated exposure to payment instruction fraud, counterparty manipulation, and BI impacts across contract performance, documentation, and settlement. Expect closer attention on approval workflows, call-back controls, privileged access, and incident readiness—plus careful structuring of crime/cyber interfaces.

Logistics (3PLs, Forwarders, Warehouses)

Logistics sits at the intersection of cyber and physical operations—warehouse automation, TMS/WMS, scanners, port community systems, and carrier integrations. In 2026, insurers will look hard at dependent business interruption (supplier outages), ransomware resilience, and recovery time objectives—because downtime creates immediate contractual and reputational harm.

Orion View: A Practical "2026-Ready" Cyber Renewal Checklist

To get the best outcomes in 2026, we recommend clients prioritise the evidence insurers respond to fastest:

- MFA everywhere (especially privileged access) + conditional access
- Immutable/offline backups + tested restoration
- EDR across endpoints + 24/7 monitoring or credible MDR
- Patch and vulnerability KPIs you can actually show
- Supplier/third-party access governance (MSPs, cloud, contractors)
- An incident response plan with named roles, decisioning, and tabletop testing

As cyber insurers will be receptive to offering favourable policy terms to well-controlled organisations while applying tougher terms where controls are weak or exposures are high, Orion expects to close a partnership agreement in early 2026 with a Cyber Security company focused on delivering data analytics related to a client's cyber resilience.

The cyber security company's tools include continuous monitoring, exposure analysis, vendor / supply-chain risk analysis, domain/ certificate/ email/ IP reputation risk, alerting to vulnerabilities or zero-day exploits etc. This is invaluable information for an underwriter as Orion will be able to offer "a full end-to-end underwriting workbench," to support the insurer with underwriting decisions, exposure management (both single risks and accumulation across portfolios), and dynamic risk profiling. In short we hope to leverage favourable data on a client's cyber posture to obtain competitive cyber policy terms and avoid claim disputes.

Disclaimer: This commentary reflects Orion Insurance Group's general market view based on publicly available reports and market publications as at June–December 2025 and is subject to change as insurer appetite, claims experience and regulatory developments evolve through 2026. It is provided for general information only and does not constitute advice.