ERMIS

Newsletter

October 2026 - Issue No 8

In this Issue

Global Market Dynamics of Cyber Insurance 1
The ERMIS Marketplace: Final Release 2
ERMIS presented at TechEx Europe 2026 2
ERMIS Marketplace Validation: Validating the ERMIS Marketplace in real-world pilot environments 2

Global Market Dynamics of Cyber Insurance

For risk managers, chief information security officers, and executive boards, the memory of the recent cyber insurance hard market remains vivid. Staggering rate increases, sudden capacity pullbacks, and aggressive sub-limits on critical exposures (e.g. ransomware, wire fraud) defined corporate renewals for years.

The current global market landscape presents a markedly different environment. As underwriting discipline takes hold and capital flows back into the sector, the industry is experiencing a phase of market stabilization, with rates flattening or showing modest single-digit relief for preferred risks.

Beneath this softening, however, the global market is far from uniform. Evolving regulatory pressures, distinct loss drivers across geographies, and contrasting strategies among key insurers and reinsurers are reshaping how risk is transferred and priced.

The Transatlantic Divide of US and Europe

The United States remains the largest and most mature cyber insurance market, accounting for the majority of global premium volume. Having undergone aggressive price corrections during earlier cycles, the US market is currently defined by buyer-friendly rate conditions and ample primary capacity.

Underwriting scrutiny in North America has shifted heavily toward high-frequency, operational claims. While traditional ransomware severity persists, business email compromise, funds transfer fraud, and wrongful collection claims (e.g. privacy litigation stemming from tracking pixels and data scraping) are driving significant loss activity. Underwriters are rewarding organizations that present verified technical controls, particularly hardware-backed multi-factor authentication, endpoint detection, and isolated backup architecture.

In contrast, the European cyber market is undergoing rapid expansion, catalysed by sweeping regulatory mandates. The Digital Operational Resilience Act (DORA) and the NIS2 Directive have forced corporate boards across the European Union to elevate operational resilience and third-party risk management into core governance obligations.

With strict incident reporting timelines, often requiring initial notifications within 24 to 72 hours, and potential personal accountability for directors, European mid-market enterprises are increasingly turning to cyber insurance. They view policies not merely as balance sheet protection, but as an operational framework providing access to pre-approved incident response retainers, forensic specialists, and legal counsel.

Market Positioning of Global Carriers and Brokers

Marsh & Aon: Strategic Advisory and Data-Driven Placements

Global insurance brokers Marsh and Aon emphasize that current market softening must be navigated with discipline. Marsh's market tracking highlights that carriers are increasingly moving away from static, annual underwriting questionnaires. Instead, underwriters are leveraging continuous threat monitoring and external attack surface telemetry to evaluate risk profiles in real time.

Aon's cyber risk analyses point to the growing impact of systemic single-point-of-failure events, such as widespread cloud service disruptions or software supply chain compromises. Both brokers advise policyholders to use today's favourable capacity environment to negotiate broader policy terms, eliminate restrictive sub-limits, and establish clearer coverage triggers before market cycles pivot again.

Gallagher: Market Growth and AI Exposure Scrutiny

Projections from Gallagher highlight a rapidly expanding market, forecasting global cyber premiums to scale toward $30 billion to $50 billion over the coming years as adoption deepens across non-US regions.

Gallagher's market research underscores an emerging focus among underwriters: artificial intelligence. As threat actors utilize AI to execute hyper-realistic social engineering and automated vulnerability exploitation, insurers are beginning to evaluate corporate AI governance. Underwriters are asking detailed questions regarding internal AI tool inventories, model security, and data handling protocols, establishing AI management as a new baseline for top-tier insurability.

Allianz Commercial & AXA XL: Technical Risk Engineering and Sector Realities

Major European primary carriers such as Allianz Commercial and AXA XL are balancing market competition with disciplined loss prevention. Allianz notes that while claims frequency has stabilized, data exfiltration without encryption now features prominently in large-scale extortion claims. Consequently, carriers are placing increased emphasis on data governance, exposure management, and cloud backup security.

AXA XL and Allianz both emphasize sector-specific risk segmentation. While general commercial lines enjoy flat rates, high-exposure sectors such as healthcare, education, and critical manufacturing continue to face cautious underwriting. For these verticals, carriers demand deeper visibility into operational technology, legacy systems, and third-party vendor dependencies before committing capital.

Lloyd's of London & Munich Re: Systemic Risk Boundaries and War Exclusions

At the reinsurance and specialty market level, Lloyd's of London and Munich Re play a central role in setting structural boundaries for catastrophic risk.

Lloyd's has led the industry in refining policy language around state-sponsored cyber operations and systemic risk aggregation. Market mandates have established clear exclusionary wording to differentiate routine, criminal cybercrime from nation-state cyber warfare capable of paralyzing physical or financial infrastructure. Reinsurers such as Munich Re remain highly focused on managing single-point-of-failure exposure, ensuring that syndicates maintain sufficient capital buffers against catastrophic cloud provider outages or cascading supply chain compromises.

Zurich Insurance & Coalition: Active Risk Mitigation and Tech-Enabled Underwriting

Zurich Insurance and technology-driven MGAs represent a growing trend toward active risk transfer. Zurich has integrated pre-breach risk engineering, continuous vulnerability monitoring, and embedded incident response capabilities directly into its corporate cyber policies.

Similarly, Coalition, San Francisco based MGA, utilizes real-time security scanning to alert policyholders to critical perimeter vulnerabilities during the policy period, actively preventing claims before they occur. This shift toward continuous risk management reflects a broader realization across the industry: the most effective cyber insurance strategy combines capital protection with active technical defence.

By Vasilis Kakariaris, Karavias Underwriting Agency

Capacity: the total maximum amount of capital or risk an insurer, syndicate, or the overall market is willing or able to commit to underwrite risks across a specific line of business.
Hard Market: an insurance cycle characterized by reduced carrier capacity, steep premium increases, tightened policy terms, and strict underwriting criteria. It occurs when carriers experience heavy cumulative losses and must rebuild profitability
Soft Market: the opposite phase
MGA: Managing General Agent**,** a specialized type of insurance intermediary granted delegated underwriting authority directly from a insurance carrier or Lloyd's syndicate. Unlike standard brokers, MGAs can quote, bind coverage, set terms, and issue policies directly on behalf of capital providers.
Sub-Limits: Specific policy caps embedded within a broader insurance policy that restrict the maximum amount payable for particular types of loss (e.g., a $5M total policy limit with a $250k sub-limit for BEC/wire fraud).

The ERMIS Marketplace: Final Release

With DEP-ERMIS reaching the end of its 36-month journey, the final release of the ERMIS Marketplace is now live. What began as an architecture and a set of use-case scenarios in 2024 is today an operational platform that brings together cybersecurity assurance and cyber insurance in a single, integrated offering.

What the platform does

The marketplace is connected with SPHYNX SPA suite, allowing a registered organisation to model its assets, run an evidence-based cybersecurity assessment, measure its certification and regulatory readiness and browse a catalogue of insurance and assurance bundles matched to its actual risk profile. From there it can express interest in a bundle and receive a quotation from the insurer, without the lengthy questionnaires that cyber insurance has traditionally required. On the supply side, cybersecurity solution providers and insurers register their tools and policies, opt in to bundling, and gain controlled visibility into the readiness status of prospective clients.

Validated in practice

The final release has been validated through two evaluation cycles in both pilots. The feedback from these cycles shaped the final version: a streamlined assessment workflow, shorter questionnaires, and a number of usability improvements across the platform.

Watch the platform in Action

A series of short videos walking through the ERMIS Marketplace is now available on the project's YouTube channel and website. More info can be found at the following link: https://www.youtube.com/@Dep-ERMISproject. As DEP-ERMIS concludes, the

Marketplace, the project deliverables and the video library will remain available at dep-ermis.eu, and the consortium partners will continue to build on the project's results in their own products and services.

By Antonis Paragioudakis, Sphynx Hellas



ERMIS presented at TechEx Europe 2026

ZELUS participated in TechEx Europe 2026, held at RAI Amsterdam on 19–20 October, presenting the ERMIS project and its cybersecurity assurance and cyber insurance marketplace.

At Stand T13, the ZELUS team introduced ERMIS to visitors and stakeholders, outlining how the marketplace brings together cybersecurity tools and services to support organisations with cyber risk assessment, security certification and cyber insurance.

The event also provided an opportunity to engage directly with small and medium-sized enterprises (SMEs) and secure the participation of additional companies into the final stage of the ERMIS piloting period. These discussions fed into the project's final evaluation cycle and helped strengthen engagement with potential marketplace users.

ERMIS Marketplace Validation: Validating the ERMIS Marketplace in real-world pilot environments

The DEP-ERMIS project has reached an important milestone with the successful completion of the ERMIS Marketplace validation phase, carried out through the project's pilot activities. This achievement marks a significant step towards demonstrating the Marketplace's functionality, usability, and potential to support innovative digital services and collaboration across the ERMIS ecosystem.

The validation process provided an opportunity to assess the Marketplace in realistic operational scenarios, bringing together technological capabilities, user requirements, and practical application needs. Through the ERMIS pilots, the project evaluated key Marketplace functionalities, including service discovery, accessibility, interaction between ecosystem participants, and the overall user experience.

The pilot activities also enabled the collection of valuable feedback from participating stakeholders, helping identify opportunities for improvement and ensuring that the Marketplace responds effectively to real-world requirements.

From Development to Real-World Validation

The completion of the validation phase represents an important transition from technical development towards operational readiness. By testing the ERMIS Marketplace through the project's pilots, the consortium has strengthened its understanding of how the platform can facilitate access to digital solutions, encourage collaboration, and support the broader adoption of ERMIS technologies.

Looking Ahead

Building on the outcomes of the pilot validation activities, the DEP-ERMIS project will focus on consolidating the results, incorporating lessons learned, and supporting the Marketplace's future exploitation and sustainability.

The successful completion of this milestone reinforces the DEP-ERMIS project's commitment to delivering practical, user-oriented, and innovative digital solutions with lasting impact.

By Nikos Piliouras, Nodalpoint Systems LTD

Contact	Project Coordinator	Zelus	Inquiries	I info@dep-ermis.eu









Disclaimer

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101128013.

The project is supported by the Ministry of Digital Governance of Hellenic Republic and the National Cyber Security Authority and is aligned with the Hellenic Cyber Security Strategy.

Consortium Partners









