Brighton
You insure, We ensure

INSIGHTS

SEPTEMBER 2025

TRADE UNDER FIRE

Insurance in an Age of Maritime Conflict

Embedded Insurance: Challenges and Opportunities in Asia

Cyber Insurance in 2025: A Year of Adjustment

What Happens When AI Becomes A Liability?

Editor's Note

Dear Readers,

Every era has its own kind of risk. What's shifting today is not just the nature of those risks, but the speed at which they emerge and how interconnected they've become.

This September, we look at four narratives that capture the shifting boundaries of insurance. From the world's trade routes to the world's algorithms, risk is no longer confined to familiar terrain. The shipping industry, once defined by weather and war, now navigates geopolitical flashpoints.

Embedded insurance is slipping quietly into everyday life, transforming how consumers experience protection. Cyber insurance, once the industry's crisis child, is maturing and showing signs of discipline and uneven resilience rather than chaos. And then there's artificial intelligence, the newest disruptor and insurer's puzzle, turning questions of efficiency into questions of accountability.

Together, these narratives paint a portrait of an industry in constant motion—one that doesn't merely react to global change but anticipates and absorbs it. In doing so, insurance continues to serve its quiet, essential purpose: making progress possible in an uncertain world.

I hope you find the insights in this issue valuable and that they spark new conversations among your teams and networks.

Annie Undikai

Annie Undikai
Managing Editor

Brighton
INSIGHTS
SEPTEMBER 2025

IN THIS ISSUE

DRIVING SUCCESS

At Brighton, we provide exceptional solutions with cutting-edge software and dedicated support to advance your business in the competitive insurance industry.

TRUSTED STRENGTH

Rated **LECA1** by RAM Ratings, Brighton represents the pinnacle of capability and performance. We also stand at the forefront of global standards with the successful compliance to **IFRS 17**.

EXCELLENCE ENSURED

You insure, we ensure — driving your future forward with confidence and exceptional performance.

OUR SOLUTIONS

- LICENSING & COMPLIANCE
- ACCOUNTING SERVICES
- WEBBIE, CLOUD-BASED ACCOUNTING SOFTWARE
- PAYROLL SERVICES
- GST/SST REPORTING
- E-INVOICING
- WORK PERMIT APPLICATION
- CORPORATE TAX SUBMISSION
- INTERNAL AUDIT
- SHARIAH ADVISORY
- COMPREHENSIVE CAPTIVE MANAGEMENT
- RUN-OFF MANAGEMENT
- SERVICED OFFICE FACILITIES

For more information, visit us at www.brighton.asia or scan the QR code

TRADE UNDER FIRE

Insurance in an Age of Maritime Conflict

The shipping industry has always operated against a backdrop of uncertainty, but in recent years that risk has taken on an unfamiliar edge.

Trade routes that once seemed stable have become flashpoints, and marine underwriters are recalibrating cover in ways not seen since the height of Somali piracy. For shipowners and insurers alike, the challenge is no longer just weathering storms of nature but the brewing storms of geopolitics.

Under Seige

The numbers alone capture the scale of the challenge. According to UNCTAD, more than 80% of global trade by volume moves by sea, with about 11% of seaborne trade passing through the Suez Canal. When Houthi attacks on commercial vessels escalated in late 2023 and early 2024, shipping volumes through the canal fell by more than 40%.

Ships were forced to reroute via the Cape of Good Hope, adding up to 14 days of sailing time and millions of dollars in extra fuel costs per voyage. What used to be a predictable artery of trade suddenly became a war risk zone.

War risk insurance, which was once a specialist product, is now at the centre of boardroom discussions. Over the last two years, the Joint War Committee (JWC) in London has consistently broadened its list of high-risk maritime regions.

The Red Sea, the Gulf of Aden, and parts of the Black Sea are already there. Each new designation carries weight for shipowners, operators, and underwriters, because it reshapes the balance between commercial viability and safety.

The cost of insuring ships through the Red Sea has now more than double. Previously a crucial route for oil and commodities, this waterway has experienced a significant decrease in traffic since the attacks off Yemen's coast commenced in November 2023.

War risk premiums, which hovered at fractions of a percent before the conflict, have now climbed to 1% of a vessel's value. For shipowners, that translates into hundreds of thousands of dollars in additional costs for every journey.

War risk premiums, which hovered at fractions of a percent before the conflict, have now climbed to 1% of a vessel's value.

The Black Sea Conundrum

The situation in the Black Sea highlights a different kind of complexity. Since Russia's invasion of Ukraine in 2022, ports like Odesa and Mykolaiv have faced blockades, missile strikes, and shifting corridors negotiated under fragile agreements.

The UN-brokered Black Sea Grain Initiative briefly provided a lifeline, enabling Ukraine to export more than 32 million metric tons of grain before collapsing in mid-2023. Each voyage out of those ports involved a tangle of geopolitical calculations: Was the ship flagged in a neutral country? Would insurers provide cover for a cargo corridor exposed to missile strikes?

Lloyd's Market Association data shows that in the first year of the war, premiums for transiting the Black Sea jumped more than tenfold. Some operators withdrew altogether, leaving trade flows disrupted and insurance markets straining to adapt.

The Black Sea situation revealed vulnerabilities in global supply chains, impacting grain traders, shipping lines, and insurers. Delayed or rerouted shipments led to rising grain prices and supply bottlenecks, contributing to inflation in food-importing countries in Africa and the Middle East. This highlights how localized conflicts can escalate into global economic challenges.

Expanding Risk Map

The Middle East provides the clearest case study of how fast risks can escalate. The Houthi drone and missile campaign against vessels in the Red Sea has not only disrupted Suez Canal traffic but also highlighted how non-state actors can wield asymmetric power over global trade.

Unlike traditional state-to-state wars, these conflicts do not have either predictable ceasefires or negotiated maritime corridors. For insurers, that unpredictability complicates actuarial models. How do you price risk when the aggressor isn't a government with territory to defend but a group using mobile missile launchers and drones? Data becomes scarce, and underwriters often rely on intelligence briefings as much as actuarial tables.

This unpredictability filters down into the day-to-day operations of shipping companies. Consider container shipping as an example: in early 2024, Maersk and Hapag-Lloyd halted services through the Red Sea, opting for longer Cape routes despite incurring higher costs.

Their choices were not solely based on commercial factors; they also took into account the availability and affordability of war risk coverage. If underwriters refuse to support a voyage or if the premiums render it unfeasible, vessels are unable to set sail.

That, in turn, reshapes global supply chains. Goods take longer to reach markets, costs rise, and inflationary pressures ripple through economies already strained by energy shocks and currency volatility.

Insurance as Arbiter of Trade

For insurers, these aren't just temporary fluctuations but long-tail exposures that ripple through balance sheets. War risks intersect with other lines of cover: hull and machinery, cargo, and even liability if crews are injured or detained.

In the latest Allianz Safety & Shipping Review, it is highlighted that political risk and conflict are emerging as increasingly significant drivers of maritime loss in an era of heightened geopolitical tension. Against this backdrop of conflict and economic fragmentation, global shipping is facing a reshaped landscape of risk exposure.

This shift is already visible in how fleets move. Greek and Norwegian operators, long dominant in tanker trades, are recalibrating routes to avoid high-risk zones. Asian fleets are spreading exposure across multiple regions, using diversified chartering strategies to reduce concentration risk.

The insurance sector sits at the center of this transformation. War risk cover enables trade to continue in hostile waters, offering a financial buffer that keeps supply lines alive. Yet, when premiums surge or coverage is withdrawn, entire routes can shut down overnight. Insurers, in this sense, are no longer neutral observers; they're de facto gatekeepers of global trade.

A 2024 Marsh report revealed that in several conflict zones, the availability of insurance alone determined whether cargoes moved at all. In this context, the ability to insure became the ability to trade.

Looking ahead, two patterns seem inevitable. First, geopolitical flashpoints are multiplying, not consolidating. Beyond Ukraine and the Red Sea, the South China Sea remains tense, with near-daily confrontations between Chinese coast guard vessels and ships from Vietnam and the Philippines.

The stakes are immense: over $3.4 trillion in trade passes through these waters each year, according to the Center for Strategic and International Studies. Even a temporary disruption could dwarf the economic shock of the Suez Canal blockage

Second, the tools of conflict at sea are changing. Drone warfare has lowered the barrier to entry for non-state actors, while cyber vulnerabilities present new ways to disrupt shipping without firing a shot. In 2017, Maersk's systems were paralysed by the NotPetya cyberattack, costing the company an estimated $300 million.

That was only a glimpse of what future conflicts could bring. A well-targeted cyber strike on navigation systems or port logistics could cause the same paralysis as a physical blockade.

For underwriters, this convergence of physical and digital risks is reshaping the entire model of marine insurance. Traditional war risk frameworks weren't built for this hybrid reality.

The challenge now is adaptation. Some shipowners are turning to private security, though the legality and practicality of armed escorts remain disputed. Others are pressing for stronger naval protection, as seen with the US-led patrols in the Red Sea.

Drone warfare has lowered the barrier to entry for non-state actors, while cyber vulnerabilities present new ways to disrupt shipping without firing a shot.

For insurers, innovation will likely hinge on agility. Static models and annual policy renewals can no longer keep pace with rapidly shifting risk landscapes. The next frontier lies in modular cover structures that adapt dynamically to changing threat levels, with policies that flex with real-time data rather than fixed assumptions.

Underwriters are experimenting with parametric solutions that trigger payouts for predefined events, such as port closures or cyber intrusions. This approach minimises delays in loss assessment and enables quicker recovery for shipowners and traders.

Real-time risk analytics will become equally vital. Satellite tracking, open-source intelligence, and AI-driven risk mapping are beginning to feed directly into underwriting decisions. Assessing geopolitical, weather, and cyber threats in near real time may revolutionise premium settings and claims handling, especially in volatile regions where data-driven responses are essential for keeping trade routes insurable.

Partnerships are essential for insurers to manage risks effectively. Collaborating with geopolitical intelligence providers, defense analysts, and tech firms can enhance risk oversight. Some reinsurers are adopting predictive conflict modeling in portfolio management, merging traditional actuarial skills with national security tools.

In this environment, insurers have evolved from merely pricing risk to interpreting uncertainty. They analyze fragmented data, political signals, and market movements to influence global commerce. During crises, their decisions determine the continuity of trade routes, shipping, and economic connections.

Adapting to Uncertainty

There is no easy solution to the complex relationship between sea and land politics. Despite the myth of neutrality at sea, the maritime and insurance industries have proven resilient amid wars and piracy. The challenge now is to adapt to unpredictable conflicts, with war risk insurance turning political chaos into manageable risks, enabling ongoing trade. Insurers and shipowners should prioritize flexibility in operations and risk models as maritime contention persists in today's geopolitical climate.

Embedded Insurance

CHALLENGES AND OPPORTUNITIES IN ASIA

The integration of insurance into non-insurance products is rapidly reshaping the way consumers engage with coverage. This growing trend, known as embedded insurance, is transforming sectors such as automotive, travel, healthcare, and even retail. While the concept isn't new, it has gained significant momentum in recent years, with insurers and tech companies leveraging new platforms and data insights.

In Asia, where digitalisation is accelerating and consumer behaviours are shifting, embedded insurance is poised for significant growth. However, along with this expansion come unique regulatory and commercial challenges that need careful navigation.

The Rise of Embedded Insurance

Embedded insurance refers to the seamless integration of insurance products into the purchase process of goods or services, where the coverage is automatically included in the price or as an optional add-on. This model allows customers to purchase insurance without the need for a separate transaction or in-depth understanding of insurance policies. It can take the form of trip insurance with flight bookings, health coverage with wellness apps, or auto insurance bundled with vehicle purchases.

According to a recent report by the Asia Insurance Review, the embedded insurance market in Asia is expected to grow at a compound annual growth rate (CAGR) of 18.5% between 2023 and 2030. This growth is largely driven by the increasing digitalisation of industries, the rise of e-commerce, and changing consumer expectations.

The Asia-Pacific region, in particular, is seeing a rapid shift toward embedded insurance solutions, especially in countries like China, India, and Southeast Asia, where large portions of the population are becoming more tech-savvy and open to digital insurance offerings.

One of the biggest drivers of embedded insurance is the increasing use of data. With the rise of Internet of Things (IoT) devices, AI, and big data analytics, insurers are able to collect real-time information that can be used to assess risk more accurately. In turn, they can offer personalised products that are tailored to the unique needs of consumers.

For instance, a car rental company can offer usage-based insurance (UBI) based on the exact number of miles driven or the type of driving conditions, making the coverage more relevant and cost-effective for the consumer.

Key Challenges

While the potential for embedded insurance is immense, there are several challenges that insurers, regulators, and service providers must address to unlock its full potential.

1. Regulatory Complexity

The regulatory landscape for embedded insurance is often fragmented and complex, particularly in Asia, where each country has its own set of insurance laws, requirements, and standards. This creates an added layer of complexity for insurers trying to navigate different jurisdictions.

For example, in countries like Singapore and Hong Kong, regulatory frameworks are relatively clear and supportive of digital insurance innovations, encouraging insurers to experiment with embedded solutions.

However, in markets such as India and Indonesia, regulatory environments can be more restrictive, especially when it comes to data privacy and cross-border data flow, which are critical for embedded insurance solutions that rely heavily on customer data.

A recent Deloitte report on regulatory challenges in embedded insurance noted that inconsistent regulations on data protection are a major hurdle. Countries such as China and Japan have stringent rules on data privacy that make it difficult for foreign insurers and tech companies to operate seamlessly across borders.

The General Data Protection Regulation (GDPR) in Europe provides a solid framework. But in Asia, the lack of harmonised data protection laws means that companies may face challenges when offering embedded insurance in multiple countries.

2. Trust and Consumer Protection

While embedded insurance offers convenience, it also poses risks when it comes to transparency and consumer protection. A significant challenge is ensuring that consumers fully understand the terms of the coverage they are purchasing, especially when it is bundled with other products.

In some instances, customers may not even realise they have insurance coverage or may not know how to make a claim. This can be particularly problematic in markets where the insurance penetration rate is still low, due to limited financial literacy, and lack of trust in insurers. As embedded insurance becomes more prevalent, insurers and distributors will need to prioritise clear communication and transparency, ensuring that customers are fully informed about their coverage.

The Asia Pacific Insurance Forum recently highlighted that educating consumers is a crucial step in overcoming trust barriers. Only 42% of consumers in emerging Asian markets are confident in their understanding of embedded insurance products, compared to 58% in more mature markets like Japan and South Korea. This gap points to the need for insurers to work with their distribution partners to provide more accessible, understandable information.

3. Integration with Existing Infrastructure

The seamless integration of embedded insurance into the current commercial platforms presents several challenges. Many businesses, particularly smaller ones, often lack the necessary infrastructure and expertise to incorporate insurance offerings into their products or services.

Furthermore, ensuring a seamless insurance delivery at the point of sale requires collaboration among multiple stakeholders, such as insurers, technology providers, and distribution partners.

One example of this challenge is in the e-commerce sector. Major players like Shopee and Lazada in Southeast Asia are increasingly offering embedded insurance options, such as product protection for consumer electronics or shipping insurance.

However, integrating these offerings into the checkout process without overwhelming consumers with options or adding complexity to the transaction process remains a significant hurdle.

Ensuring a seamless insurance delivery at the point of sale requires collaboration among multiple stakeholders,

Unlocking New Opportunities

Despite these challenges, the opportunities presented by embedded insurance in the Asian region are significant.

1. Expansion into Underserved Markets

Embedded insurance provides an excellent opportunity to expand coverage into underserved markets, where traditional insurance distribution channels are limited. In many parts of Asia, especially in rural areas, insurance penetration is still relatively low. The ability to offer micro-insurance products that are easy to purchase and use through mobile phones or digital platforms can help bridge this gap.

In India and Bangladesh, micro-insurance schemes that address agricultural risks and health expenses are becoming increasingly popular. By integrating these insurance products into mobile applications or collaborating with local retailers, insurers can offer affordable coverage to individuals who might otherwise have limited access.

The Microinsurance Network reported that over 500 million people in Asia are already covered by micro-insurance products, a number that is expected to rise with the continued growth of embedded solutions.

2. Leveraging Data for Personalisation

As previously noted, data utilisation is a crucial factor in the growth of embedded insurance. With the increasing prevalence of connected devices, insurers can acquire more profound insights into consumer behaviour, allowing them to customise their products. This innovation paves the way for highly personalised and adaptable insurance offerings, encompassing health, life, auto, and home coverage.

In countries like China, where tech giants like Alibaba and Tencent dominate the digital space, considerable advancements have been made in utilising big data for tailored insurance solutions.

For example, Ant Financial, the financial arm of Alibaba, has been offering embedded insurance in the form of coverage for mobile phones and other electronics purchased on its platform. These policies are powered by data analytics, which helps assess risk more accurately and set premiums that are competitive and fair.

3. Enhancing Customer Experience

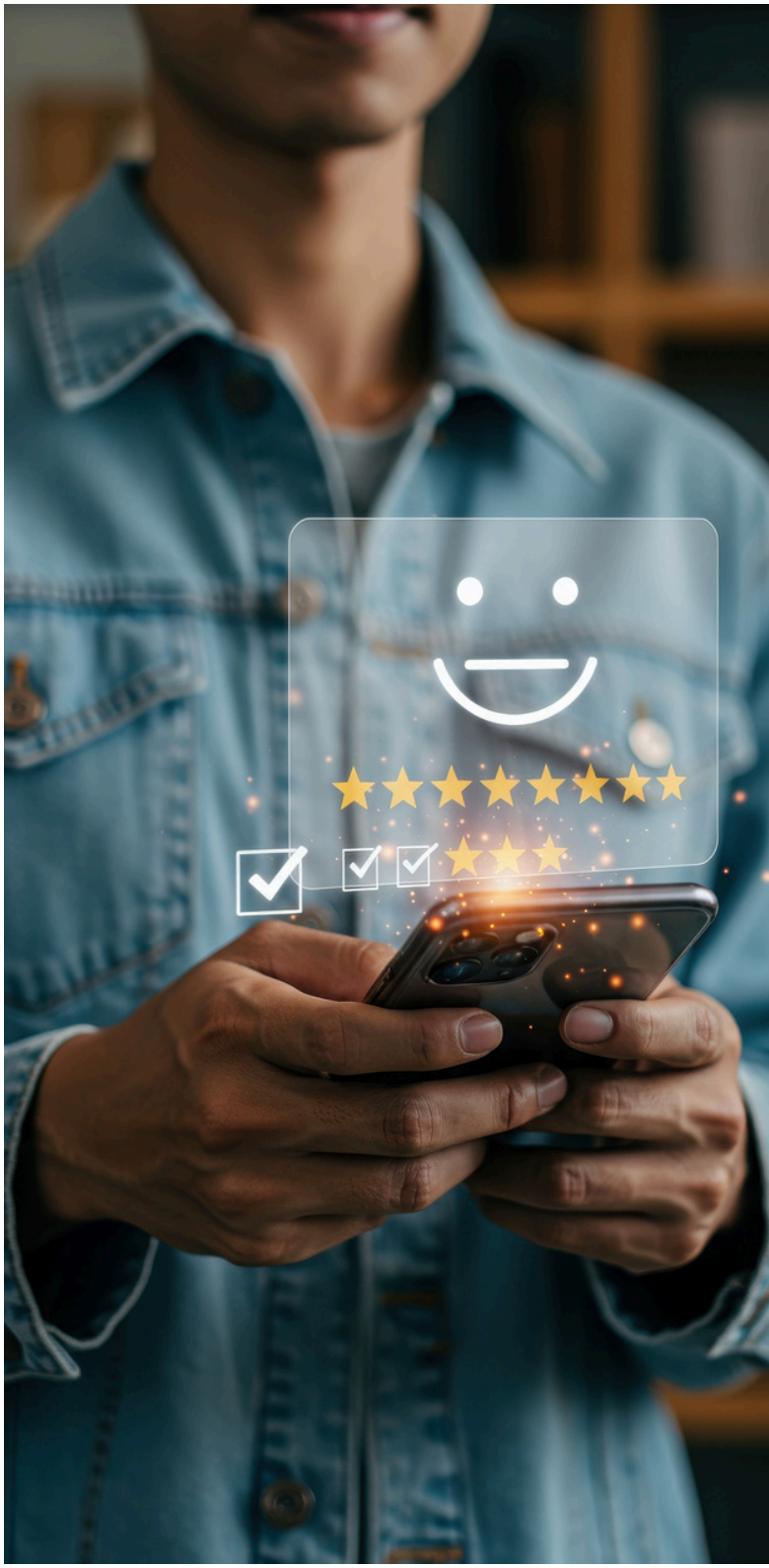
Embedded insurance can also improve the overall customer experience. The convenience of having insurance bundled with other services or products can make it easier for customers to obtain coverage without the hassle of separate applications or forms. This frictionless experience can drive greater customer satisfaction and loyalty.

For example, travel insurance that is automatically included in a flight booking or ride-hailing service can be a game-changer for frequent travelers. According to a McKinsey survey, 72% of consumers in Asia are more likely to purchase embedded insurance when the process is seamless and integrated into their existing purchase experience.

This underscores a crucial insight: the more intuitive and invisible the process, the stronger the relationship between insurer, distributor, and customer. As digital ecosystems grow and partnerships between insurers and non-insurance platforms deepen, this seamless model could become the new benchmark for customer-centric insurance delivery.

A Growing Frontier

Embedded insurance in Asia is nascent but holds great growth potential. Despite existing challenges, the opportunities for innovation are substantial. As digitalisation advances, embedded insurance will be crucial for enhancing financial inclusion and catering to changing consumer needs.



CYBER INSURANCE IN 2025

A Year of Adjustment and Uneven Resilience

Cyber risk has become a fact of life for businesses. Every company connected to the internet is a potential target, and the frequency of attacks continues to test the limits of preparedness. Yet, 2025 is shaping up to be a year of quiet adjustment rather than crisis with fewer large losses, smarter defences and more selective underwriting. The numbers tell a story of resilience, but also of uneven protection across industries and regions.

Signs of Stabilisation

Allianz Commercial's Cyber Security Resilience Outlook 2025 reported roughly 300 cyber claims in the first half of the year, almost identical to 2024. What changed was not the number of incidents, but their impact. The severity of claims fell by more than 50%, and large losses were down around 30%.

Allianz attributes this to stronger detection and response capabilities among large insured companies. Many now have dedicated cyber response teams and better network monitoring, which helps contain attacks before they spiral into multi-million-dollar losses.

Findings from other research echo this trend. NetDiligence's 2025 Cyber Claims Study, which reviewed more than 10,000 incidents, found that average claim costs fell 6% year-on-year, while the share of catastrophic losses declined.

Marsh's Global Insurance Market Index also noted that cyber insurance pricing eased for three consecutive quarters through mid-2025 as loss ratios improved. These signals suggest the market is maturing after several years of sharp volatility.

However, Allianz anticipates that total claims for the year will approach 700, particularly with the usual year-end surge during the online shopping season. This pattern is familiar: a consistent flow of risk intermingled with sudden spikes in activity, as attackers exploit the heightened retail traffic and staffing shortages during the holiday season.

Marsh's Global Insurance Market Index also noted that cyber insurance pricing eased for three consecutive quarters through mid-2025 as loss ratios improved.

Rise of Double Extortion

Ransomware remains the single largest driver of insured losses, making up about 60% of large claims in Allianz's dataset for the first half of 2025. IBM's X-Force Threat Intelligence Index 2025 supports this, noting a trend towards shorter, impactful campaigns. The "double extortion" tactic, involving both encryption and data theft, was used in 40% of Allianz's large claims, up from 25% the previous year.

The shift signifies a wider transformation in criminal strategies. Previously, attackers aimed to disrupt operations, but now they are after reputational leverage. A compromised customer database or confidential contract can cause significantly more harm than just temporary downtime.

IBM revealed that in 2024, the average global cost of a data breach approached nearly $4.9 million, a figure influenced by tighter privacy regulations and longer remediation timelines. For smaller businesses, even one breach can represent a significant existential risk.

The Growing Divide

A key theme across recent research is the widening resilience gap between large enterprises and smaller firms. Verizon's Data Breach Investigations Report 2025 found that ransomware played a role in 88% of breaches at small and mid-sized businesses, compared with just 39% at larger organisations. The numbers highlight a pressing reality: smaller firms remain far more exposed, often without the resources or recovery plans their bigger counterparts can afford.

Smaller companies are often easier targets due to outdated systems, limited IT staff, and inconsistent data backup practices make them vulnerable. In its Cyber Resilience Report, Aon reported a 22% increase in cyber insurance claims in Asia Pacific, driven mainly by attacks on mid-sized firms.

Many of these companies are either self-insure or maintain only minimal cyber coverage. For them, the financial repercussions of a significant breach such as ransom payments, forensic investigations, and lost revenue can surpass their annual profits. Moreover, the complexity of digital supply chains and outsourcing practices increases the risk, creating intricate interdependencies that are difficult to secure.

Industry Patterns

Certain industries continue to bear the brunt of cyber losses. Manufacturing generated one-third of Allianz's large cyber claims over the past five years, followed by professional services (18%) and retail (9%). Manufacturers are often targeted for their operational technology, where downtime directly affects production lines. Professional service firms hold sensitive client data, making them attractive for data theft. While, retailers face both volume and timing risks, as attacks often coincide with peak sales periods.

Software updates gone wrong, system misconfigurations, and accidental data leaks serve as reminders that some of the most costly breaches can originate from within.

AXA XL's 2025 cyber report reached similar conclusions. It found that manufacturing accounted for the highest average claim cost, while healthcare and financial services faced the longest recovery times. Across all sectors, ransomware and business email compromise remained the top two causes of loss.

Not all cyber incidents stem from malicious intent. Allianz data shows that in 2024, technical failures and improper data handling accounted for 28% of large claims by value. Software updates gone wrong, system misconfigurations, and accidental data leaks serve as reminders that some of the most costly breaches can originate from within, i.e. through human error or technical missteps rather than external attacks.

View from Asia Pacific

Asia Pacific has become the world's most active region for cyber incidents, accounting for 34% of global attacks in 2024, according by IBM. The region's growing digital economy, extensive use of third-party providers, and uneven regulatory frameworks make it fertile ground for attackers. Furthermore, Allianz reported that ransomware accounted for all of its reported cyber losses in Asia during the first half of 2025.

Governments throughout the region are implementing stricter regulations in response. Amendments to Singapore's Cybersecurity Act, updates to Japan's data protection law, and Australia's mandatory breach reporting framework are reshaping corporate responsibilities.

However, there are still inconsistencies in enforcement and public awareness. Insurance penetration remains lower than in Europe or North America, with many smaller companies depending on self-insurance or minimal coverage.

A Market in Transition

Globally, the cyber insurance market is expanding but recalibrating. Allianz estimates it could more than double to nearly $30 billion by 2030. Demand is rising as boards recognise cyber risk as a core business issue rather than an IT problem.

At the same time, insurers are refining underwriting standards, requiring stronger controls before extending coverage. Multi-factor authentication, offline backups, and incident response planning have become baseline requirements for policy renewal.

The improved loss ratios in 2025 have brought some relief to insurers that faced steep payouts during the ransomware surge of 2020–2022. Yet the underlying risk continues to evolve. As generative AI tools lower the technical barrier for attackers and as geopolitical tensions drive state-linked cyber campaigns, the potential for systemic events remains a major concern.

The Road Ahead

If there's a single takeaway from 2025 so far, it's that progress in cybersecurity is evident yet inconsistent. However, cyber insurance will evolve to be more tailored, merging with cybersecurity services and offering pre-incident support. The lines between risk management and insurance are blurring, driven by collaboration among insurers, governments, and tech providers to adapt to new threats. Despite major fears not materialising, cyber risks will continue to evolve, exploiting any f complacency.

What Happens When AI Becomes a Liability?

Artificial intelligence isn't just reshaping how businesses work—it's redefining what risk looks like. Across industries, algorithms are writing marketing copy, screening job candidates, generating code, and helping doctors analyse scans. What once felt like science fiction is now embedded in everyday workflows.

But as AI systems grow more capable, companies are discovering a new kind of vulnerability: when technology makes its own mistakes, who bears the cost?

A new report by the Geneva Association found that more than two-thirds of firms are willing to pay at least 10% higher premiums for policies that explicitly cover Generative AI (Gen AI) risks.

Over 90% said they now need insurance tailored to AI-related exposures. The strongest demand comes from the technology and financial sectors, where automation and data-driven models sit at the heart of operations.

Consider the financial industry. Banks are using Gen AI to automate compliance monitoring and detect fraud in real time. If those systems produce a false positive, or worse, fail to catch a real issue; the consequences can include regulatory penalties and reputational damage.

In one well-publicised case, an AI-driven lending platform in the US was accused of discriminatory bias in loan approvals, triggering both legal scrutiny and public backlash. For insurers, such incidents represent a complex blend of liability, ethics, and cyber exposure.

In healthcare, AI tools are helping radiologists identify early signs of disease, but when algorithms misread an image or recommend the wrong course of action, questions of accountability arise. Is it the developer's fault, the hospital's, or the clinician's? These grey areas are exactly what insurers are being asked to navigate.

Even creative industries aren't immune. In 2024, several artists sued major AI companies for using copyrighted materials to train image-generation models without consent. The case exposed how easily intellectual property risks can escalate when data is scraped at scale and serve as a reminder that AI's efficiency often outpaces regulation.

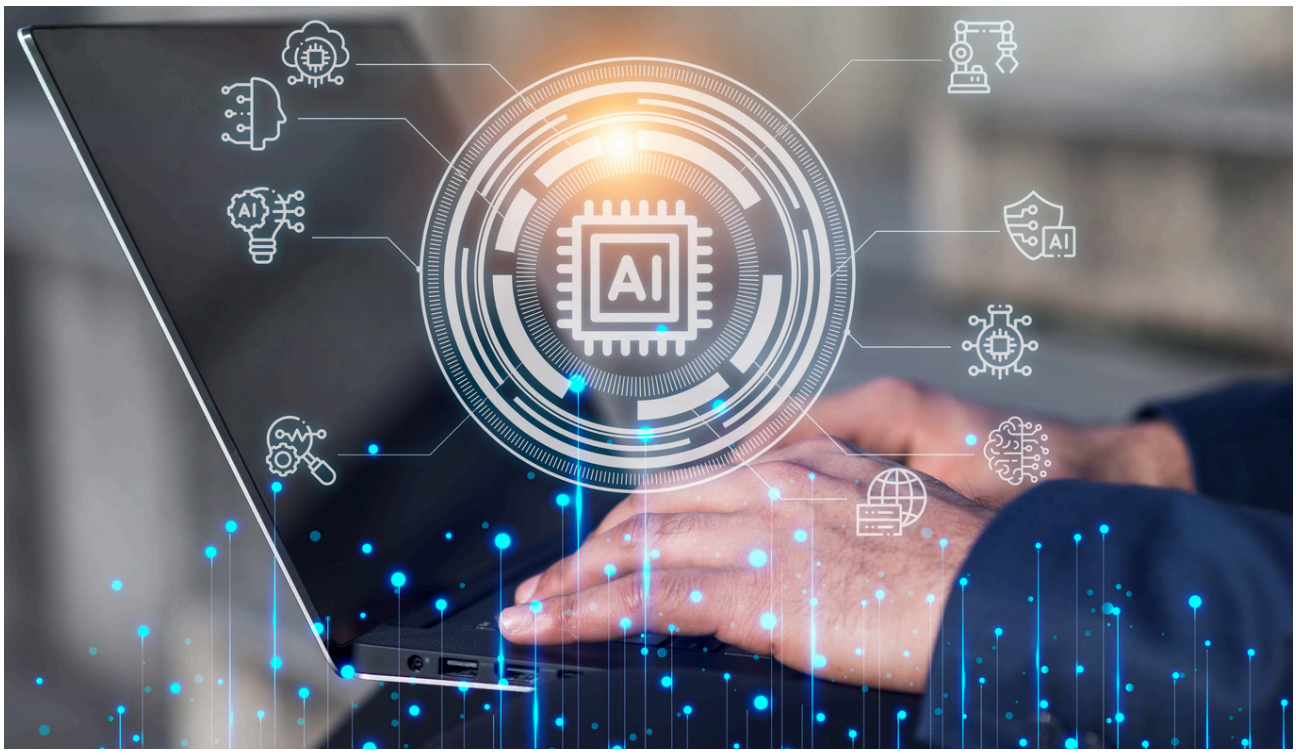
Legal challenges reveal a trend where advanced AI tools intersect with outdated laws and norms. Issues like copyright, moral rights, attribution, and commercial use are prompting creative industries to rethink their production, sharing, and protection strategies in an AI-driven environment.

Despite these risks, businesses aren't backing away from AI. They're moving forward with caution, investing in both technology and protection. The Geneva Association's survey shows that cybersecurity remains the top concern, cited by more than half of respondents. Third-party liability and operational disruption follow closely. While reputational damage ranks lower, experts warn that it can be the hardest to recover from.

For underwriters, Gen AI introduces challenges that feel familiar yet distinct. Evaluating how companies govern AI models or safeguard data isn't as straightforward as assessing fire or flood exposure. Many organisations hesitate to share detailed technical information, leaving insurers to make educated guesses.

This information gap leads to what economists refer to as asymmetry; in other words, when one party possesses more knowledge than the other. As a result, insurers may be compelled to adopt conservative pricing strategies or even restrict coverage entirely.

The industry is already adapting. Traditional cyber and professional liability policies are being reworked to include AI-related losses. Some carriers are experimenting with parametric insurance, where payouts are triggered by defined events, such as an algorithmic malfunction or data leak linked to an AI system. Others are developing new due diligence tools that measure how responsibly clients deploy AI, much like environmental audits in sustainability reporting.



A few insurers are even piloting standalone AI coverage. These policies bundle protections for cyber breaches, intellectual property violations, and errors in automated decision-making. They're still niche, but they signal a direction: the insurance market is beginning to treat AI as a distinct category of risk rather than an extension of existing ones.

The Geneva Association's report calls on insurers to act now, before claims patterns fully emerge. It suggests defining clear AI risk boundaries, creating modular policy extensions, and collaborating with technology firms and regulators to build standardised assessment models. It's a lesson learned from the early days of cyber insurance, when uncertainty and inconsistent wording left both insurers and clients exposed.

The study, based on insights from 600 corporate insurance buyers across China, France, Germany, Japan, the UK, and the US; found striking regional contrasts. Companies in China and the US report the highest confidence and adoption levels, reflecting their advanced digital maturity. European firms, meanwhile, are more cautious, often prioritising regulatory compliance and ethics over speed of deployment.

The road ahead is clear. Organisations are starting to view AI not just as a driver of innovation, but also as a potential source of financial and reputational risk. In a era when algorithms have the capability to create, predict, and make decisions; forward-thinking companies are acknowledging the necessity of protecting not only their physical assets but also their intellectual capital.