DAC BEACHCROFT

Technology
Predictions 2027



England and Wales

Aviation

Growth of UK air cargo set to extend beyond traditional hubs

UK air cargo is likely to become more strategic, technology-driven and geographically diverse. Rather than remaining concentrated at London airports, Heathrow in particular, growth is increasingly being driven by regional gateways benefiting from available capacity and lower congestion. Recent developments at airports such as Glasgow Prestwick, driven by cross-border e-commerce and direct freighter services to China, suggest that cargo activity is becoming more widely distributed across the UK air freight network. Cross-border e-commerce is expected to remain the principal driver of growth. As consumers continue to demand faster international deliveries, cargo operators are likely to increase capacity on routes connecting the UK with key manufacturing centres in Asia. This is expected to support further investment in cargo facilities, automation technologies and customs processing capabilities. For insurers, the growth of regional cargo gateways may bring greater focus on supply-chain resilience, high-value freight movements and operational dependencies across interconnected logistics networks. As the sector develops, the UK's air cargo network may become both more geographically diverse and more strategically important to international trade and supply-chain resilience.

The regulatory roadmap for autonomous aviation to take shape

Following the Law Commission's final report on aviation autonomy, published in May 2026, 2027 may mark the transition from legal review to regulatory planning for the development of autonomous aviation in the UK. The report sets out a framework for future reform. Its recommendations include clearer legal definitions and harmonised terminology for autonomous and remotely piloted operations, legislative changes to facilitate traffic management services for uncrewed aircraft systems, measures to protect passengers travelling on remotely piloted or future autonomous aircraft and the reallocation of certain pilot responsibilities in fully autonomous operations. The report also examines wider issues such as aviation-related criminal law and the legal framework required if a single remote pilot is permitted to oversee multiple aircraft or if operations transition between remotely piloted and autonomous flight. For insurers, manufacturers, operators and regulators alike, the central question may become less whether autonomous systems can operate safely and more how responsibility should be allocated when they do not. As autonomy increases, established concepts of operational control, pilot responsibility and liability are likely to be tested in new ways.

Space debris moves from environmental concern to commercial risk

Space debris is likely to evolve from being viewed predominantly as an environmental concern to a significant commercial and insurance risk. In 2025, the European Space Agency (ESA) reported that approximately 40,000 objects were being tracked by space surveillance networks, and the number of space debris objects exceeding 1cm was estimated at over 1.2 million. As launch activity expands and satellite constellations proliferate, operators will be expected to demonstrate credible debris mitigation and end-of-life disposal strategies. The influence of the voluntary ESA Zero Debris Charter is also likely to become more pronounced, reflecting a broader shift towards debris-conscious mission design and responsible space operations. The success of Artemis II provides a useful example, with major mission components recovered or deliberately removed from orbit. For insurers and reinsurers, the issue extends beyond environmental stewardship. Space debris presents a classic accumulation risk, with a single collision event capable of generating thousands of additional debris objects and materially altering risk exposure across entire orbital regimes. Insurers are likely to scrutinise debris mitigation measures, disposal planning and collision-risk management more closely when assessing risk. By the end of 2027, the key question may no longer be whether debris reduction matters, but how quickly environmental expectations translate into commercial and insurance consequences.

For further information or enquiries, please contact:

Hans Allnutt, UK
Partner
hallnutt@dacbeachcroft.com

Richard Breavington, UK
Partner
rbreavington@dacbeachcroft.com

Rowena McCormack, Republic of Ireland
Partner
rmccormack@dacbeachcroft.com



Bermuda Market

Sports betting operators to face addiction-related litigation

The widespread availability of mobile betting applications has transformed access to sports gambling. Concerns about user addiction are expected to drive litigation in the United States by state attorneys general and individual gamblers who lose money and suffer from emotional distress as a result of these platforms. Betting markets range from match outcomes to parlays, with sports leagues increasingly partnering with betting companies to promote their services. Estimates are that approximately 95% of regular online sports gamblers lose money over time. In some cases, gambling debts can become substantial. The concept of liability arising from allegedly addictive digital products is already familiar in the United States. In August 2026, Meta agreed to a $17.1 billion settlement with 51 state attorneys general to resolve claims that Meta engineered Instagram and Facebook to be addictive for teens.

Casualty

AI-assisted litigants will increase pressure on courts

Increased use of AI by litigants in person will lead to more procedural errors, satellite disputes and court delays. Generative AI is making legal information more accessible than ever before, but accessibility does not guarantee accuracy. As more unrepresented litigants use AI tools to prepare pleadings, submissions and legal arguments, courts are likely to encounter a growing number of inaccurate authorities, procedural misunderstandings and poorly evidenced claims. This may generate additional hearings, costs disputes and challenges around case management. While AI has the potential to improve access to justice by enabling individuals to navigate legal processes without specialist representation, its misuse is likely to place further pressure on already stretched court resources and increase complexity for all parties involved in litigation.

Pet insurance will become increasingly personalised

Pet insurance will become more personalised as technology-driven underwriting and claims processes reshape the market. The growing use of pet activity trackers, GPS collars and health-monitoring devices is providing insurers with access to richer behavioural and health data. Much like telematics transformed motor insurance, these technologies are likely to support increasingly tailored pricing and risk assessment. At the same time, greater integration between insurers and veterinary providers will streamline claims handling, reducing reliance on traditional reimbursement models. Over time, pet insurance may begin to resemble private medical insurance, with more direct treatment pathways, faster claims decisions and increased emphasis on preventative healthcare and ongoing health management.

Construction and Engineering

Rooftop solar rollout set to increase insurance risks

Government plans to encourage millions of homes to be fitted with solar panels (the so-called 'rooftop revolution') are creating greater risks for insurers that all stakeholders need to consider. It has previously been predicted that this would lead to more claims, and recent statistics appear to bear this out, with the rate of fires increasing faster than the rate of installations. Plug-in solar panels are now legal for residential use, yet it remains unclear whether the absence of battery storage will reduce the fire risks associated with traditional rooftop solar panels. Their adoption may also introduce risks associated with unsuitable roofs, inadequate isolation arrangements, loose wiring and installation by inexperienced or unqualified individuals. Although homeowners can act as installers, devices must still be registered with the Energy Networks Association, providing insurers with a potential source of information when assessing risk and investigating claims. As the industry works through these issues, both property and Construction All Risks underwriters should assess their exposure carefully and ensure policy wordings and premiums properly reflect the risks involved.



D&O and Financial Institutions

AI governance set to become a boardroom priority

AI has moved from an innovation issue to a governance and accountability issue. As organisations increasingly embed AI and AI agents into core business functions, boards will face growing scrutiny over how these systems are governed, monitored and controlled. Potential areas of exposure include AI system failures, inaccurate or biased outputs, confidentiality breaches, intellectual property concerns, regulatory non-compliance and allegations of 'AI-washing' (overstating AI capabilities). Directors are now expected to be AI-literate and understand how AI is being deployed and what controls are in place. Poorly conceived AI investment, inadequate oversight and weak governance may expose organisations to shareholder and regulatory scrutiny, reputational harm and potential litigation. In this environment, directors should ensure robust AI oversight and clear accountability processes are in place to mitigate the risk of scrutiny. Crucial to risk management is the scope of any D&O insurance cover. Corporates and their boards must ensure that they have appropriate D&O provisions in place to protect against evolving AI risks.

Data, Privacy and Cyber

AI-generated DSARs will change complaint handling

A surge in AI-generated data subject access requests (DSARs) and data protection complaints is currently driving organisations to reconsider their approach to managing these requests. AI tools have made it easier than ever for data subjects to generate detailed complaints, DSARs and follow-up correspondence, often referred to as 'agentic flooding'. Organisations are increasingly facing lengthy and disproportionate submissions, large volumes of information to review and near-instantaneous data subject responses, some of which are speculative, unsupported or based on misunderstandings or misapplications of data protection law. As the administrative and financial burdens on organisations grow, they are likely to push back more readily. Rather than engaging with every assertion and request, organisations will concentrate on scoping and proportionality, make greater use of available exemptions and challenge unreasonable demands where appropriate. The result will be a shift from simply responding to complaints and DSARs as received towards actively managing and triaging them in order to seek resolution of the true underlying issue.

The UK's innovation-first AI approach faces growing pressure

The UK's pro-innovation approach to the regulation of AI will be challenged in response to industry and public concerns over the safety risks associated with the development of artificial general intelligence and superintelligent systems. Reported incidents of agentic AI systems executing unsanctioned actions and demonstrating deceptive behaviour have emphasised the risks associated with the development of increasingly advanced AI models. A Private Member's Bill, the Artificial Superintelligence Bill, was introduced into Parliament in September 2026. While unlikely to pass, the Bill's proposal to prohibit artificial superintelligence systems and introduce monitoring and control powers illustrates the growing political appetite for more prescriptive regulation of advanced AI. Further significant AI-related incidents, whether involving misinformation, cyber security, critical infrastructure, autonomous decision-making or widespread workplace disruption, will quickly shift public sentiment and political priorities. As AI becomes more deeply embedded across sectors, the UK Government may face mounting pressure to change its approach and consider introducing a legislative framework to ensure that AI is developed and used safely and responsibly.

The AI era forces a rethink of data retention

Data deletion and retention will rise to the top of the boardroom agenda as insurers seek to reduce risk, improve data governance and prepare for an AI-enabled future. For many in the data and privacy sector, historic approaches to retaining data are becoming increasingly difficult to justify. Growing volumes of legacy data increase cyber exposure, storage costs and regulatory risk, while also raising questions around compliance with data protection principles. At the same time, firms are looking to harness AI and advanced analytics, placing greater scrutiny on the quality, provenance and governance of the data they hold. We expect firms to move beyond policy reviews and launch more ambitious retention and deletion programmes. The challenge will be balancing legal, regulatory and business requirements to retain information against increasing pressure to justify why data is kept in the first place.



Cyber risk in the supply chain will remain a board-level concern

Cyber risk in the supply chain will remain a board-level concern as firms become increasingly dependent on complex networks of technology providers, outsourced services and data partners. Recent years have demonstrated that organisations are often only as resilient as their weakest supplier. As the sector continues to adopt cloud services, AI solutions and digital platforms, the potential for operational disruption, cyber incidents and data breaches originating within the supply chain will continue to grow. We expect increased regulatory scrutiny of supplier oversight, contractual risk allocation and incident management arrangements. Firms will be expected not only to understand their critical dependencies, but also to demonstrate that appropriate governance, due diligence and ongoing monitoring processes are in place throughout the supply chain.

Insurance Advisory

The FCA to take a more interventionist approach to AI

The Financial Conduct Authority (FCA) will take a more interventionist approach to AI, increasing its scrutiny of how firms govern, test and oversee AI systems. While the regulator has consistently stated that existing regulatory frameworks remain fit for purpose, its focus is shifting from understanding AI adoption to assessing whether firms can demonstrate appropriate accountability, effective governance and positive customer outcomes. The FCA is already engaging with industry on issues such as model testing, explainability, monitoring outcomes and the fair treatment of vulnerable customers, while its work on frontier AI signals a growing interest in the risks posed by more advanced AI systems. For insurers deploying AI across underwriting, claims and customer engagement, the challenge will be less about complying with new AI-specific rules and more about evidencing that existing regulatory obligations are being met in an AI-enabled environment.

Insurers will innovate to close protection gaps

As climate, cyber, AI and other emerging risks continue to evolve, traditional insurance products will not always provide adequate protection. In response, insurers will accelerate the development of innovative products and alternative risk-transfer solutions to address growing protection gaps across both commercial and personal lines. Expect further growth in areas such as parametric insurance, bespoke and structured risk-transfer solutions, and products targeting previously underinsured or uninsured risks. Innovation will extend beyond product design, with insurers exploring new sources of data, technology-enabled underwriting and more flexible approaches to risk assessment and pricing. As customers seek protection against increasingly complex and interconnected risks, insurers that can demonstrate a clear understanding of emerging exposures and adapt their offerings accordingly will be best placed to meet changing market demand.

Third-party risk moves to the top of the resilience agenda

Third-party dependencies will drive the next phase of operational resilience, as regulators increase their scrutiny of operational incidents, material third-party arrangements and concentration risk across the insurance sector. The Prudential Regulation Authority and Financial Conduct Authority are introducing new reporting requirements for operational incidents and material third-party arrangements, reflecting growing concern about firms' reliance on a relatively small number of critical service providers. For the sector, the focus will extend beyond traditional outsourcing arrangements to cloud infrastructure, technology platforms and other critical services that underpin key business operations. As dependence on global technology providers grows, firms will be expected to demonstrate a clear understanding of their critical dependencies, robust oversight of third-party risk and effective contingency planning. Operational resilience will increasingly be judged not only by how firms manage their own systems, but by how well they manage their external dependencies.



International and Complex Casualty

Social media addiction litigation set to gain momentum

In 2027, the UK will see social media addiction litigation gain momentum, mirroring the trajectory seen in the United States over the past year. In July 2026, a claimant firm announced a potential action on behalf of individuals in the UK who have allegedly suffered significant harm linked to prolonged social media use. Although the current regulatory framework focuses on online safety and harmful content, there is growing attention on the impact of platform design features, such as infinite scrolling, algorithmic recommendations and engagement-driven notifications. The UK Government has already announced plans to restrict access to major social media platforms for under-16s from spring 2027. The UK action involves a collaboration with the trial lawyer who led the landmark K.G.M. action in the United States, resulting in a $6 million award to a plaintiff. The first significant action of this nature in Australia was also announced in October 2026. Heavily publicised settlements in the United States have also produced agreements on changes to the operation of certain platforms. Similar allegations are likely to be tested before UK courts. As with other large-scale actions, significant legal hurdles remain, but insurers need to start assessing social media addiction claims as an active source of exposure for technology-related litigation in the UK.

Gaming addiction litigation gains momentum

Gaming addiction may emerge as the next frontier in technology-related collective redress in the UK and Europe. Early claims originated in the United States, where major game developers have been targeted for allegedly designing their products intentionally to encourage compulsive use. However, these claims remain an emerging yet unproven form of action in the United States, with many cases still developing. There is growing regulatory scrutiny in the UK and Europe of loot boxes, persuasive design features, in-game monetisation and the impact of excessive gaming on children. These developments will assist in framing gaming-related harms as a consumer protection and product safety issue rather than an issue of personal responsibility for users and their parents. The recognition of gaming disorder by the World Health Organisation arguably provides claimants with an increasingly credible medical framework for establishing injury. Although significant causation hurdles will arise in such actions, claimant firms will be watching developments closely. For insurers, gaming addiction litigation must be considered alongside the possible technology risks associated with claims alleging harm caused by social media.

Marine, Energy and Transport

Data centres set to become a defining insurance opportunity

With annual data centre investment projected to top $1 trillion next year, and comprehensive insurance a prerequisite for securing financing, the global data centre insurance market is set to grow strongly, with premiums doubling to $24 billion by 2030. This is a major opportunity, but the scale and complexity of these crucial infrastructure assets pose challenges. Once warehouse-like facilities, data centres are now hyperscale campuses housing multiple tenants, utilities and on-site infrastructure, with construction costs totalling tens of billions of US dollars. This concentration of value and accumulation of risk raises the prospect of a single event triggering claims across property, construction, business interruption, liability and cyber covers all at once. Success and the continued insurability of these assets will require coordinated, transparent risk management, tailored covers and a focus on risk mitigation throughout the design, construction and operation phases.

Autonomous vessel systems will accelerate as fleets grow and seafarer numbers fall

The difficulties in seafarer recruitment will continue as the industry faces a shortage of personnel and increased demand from growing fleets. Technology will need to fill that gap, with autonomous systems being used to support crew decision-making and increasingly taking over certain crew tasks altogether, allowing for lower manning levels. The adoption of the long-awaited International Maritime Organization Maritime Autonomous Surface Ships (MASS) Code in July 2026, together with confirmation from the International Group of P&I Clubs that liabilities arising from MASS are covered across all modes of operation, has removed two significant obstacles to wider deployment of autonomous systems. Human crew and intelligent machines can be expected to work more closely together than ever before, challenging long-standing concepts of seaworthiness and crew competence and raising novel legal issues regarding subrogation that are likely to lead to new areas of dispute.



Medical Malpractice

The rise of the AI-enabled claimant

AI is widely used by healthcare providers and clinicians, but patients and prospective claimants will increasingly use it too. Insurers and defendant lawyers are seeing growing evidence of litigants in person using AI tools to prepare complaints and pursue claims against healthcare providers. That trend is expected to accelerate over the next couple of years, placing pressure on providers to respond to increasing volumes of increasingly sophisticated complaints. AI may also create new sources of dispute. Cosmetic surgery providers have reported growing numbers of patients presenting AI-generated images of themselves as a basis for treatment expectations. Where those expectations are unrealistic or inadequately managed, the risk of dissatisfaction, complaints and subsequent litigation is likely to increase.

Motor

Automated Passenger Service pilots will expose tomorrow's insurance questions today

Automated Passenger Service (APS) trials will generate more insurance and liability questions than answers. The first APS deployments represent a significant milestone in the journey towards commercial automated vehicle deployment. Yet their greatest value may lie in revealing the practical challenges ahead. Data access, accident investigation, software updates, attribution of fault, product liability and recovery strategies will all come under closer scrutiny. Claims professionals will increasingly find themselves operating at the intersection of motor, product liability and cyber risk, with ever more focus on the interpretation and analysis of data.

Growth of Chinese original equipment manufacturers will drive repair inflation

New Chinese vehicle entrants to the UK motor market will have a disproportionate impact on motor claims costs. Repair networks and parts supply chains will struggle to keep pace with sales figures. The debate will move from the extent to which Chinese manufacturers will take market share to whether the UK's repair ecosystem can keep pace. New brands bring unfamiliar repair methodologies, limited parts infrastructure, evolving distribution networks and greater reliance on overseas supply chains. Combined with increasingly sophisticated Advanced Driver Assistance Systems and electric vehicle technology, this creates longer repair lifecycles, higher mobility costs and greater claims inflation. Some insurers may discover that their pricing assumptions have become outdated before the market stabilises.

Micromobility claims will outpace regulation

The Government is expected to continue to avoid comprehensive regulation of micromobility, leaving stakeholders and the judiciary to deal with the consequences. The proliferation of high-powered e-bikes that fall outside Electrically Assisted Pedal Cycle requirements is becoming increasingly difficult to ignore. However, micromobility risks remain politically awkward, and a further year of policy inertia is expected, despite growing evidence of serious injury, fire and property damage risks. The result will be an increasing number of claims involving uninsured or effectively untraceable users, coupled with greater uncertainty around liability, recovery prospects and product safety. The question is no longer whether reform is needed, but whether policymakers are prepared to prioritise it.

Policy Wordings

US social media disputes expose gaps in liability wordings

Insurers should address whether their liability wordings provide clarity on whether harm caused by digital products and algorithms is treated as an insured event for the purposes of coverage. Claims against social media platforms and other digital providers are expected to increase in the UK and elsewhere. A 2026 coverage dispute in the United States between a social media platform and its liability insurers considered this issue. The court held that the insurer had no duty to defend claims brought against the platform because the allegations concerned intentional, rather than accidental, conduct. This decision is subject to appeal. Nonetheless, discussions in respect of policy coverage for emerging claims involving social media addiction and digital harms are only likely to increase.



Ransomware payment ban to drive cyber underwriting changes

A proposed UK-wide ban on ransomware payments by public sector bodies and operators of critical national infrastructure (CNI) will prompt insurers to reassess their underwriting appetite to reflect increased exposure where ransom payments are no longer available as a recovery option. Initially proposed in 2025, such legislation would be intended to make the public and CNI sectors less attractive to ransomware groups. However, this approach remains untested and could increase their financial exposure. This could constrain cyber insurance capacity, reduce indemnity limits and tighten policy conditions. It may encourage the development of specialist products for public bodies and operators of CNI, but in the absence of formal legislative proposals, there remains a lack of clarity on whether the ban extends to privately owned organisations operating in the public and CNI sectors.

Policy wordings will race to keep pace with emerging risks

Insurers will increasingly reassess both policy wordings and underwriting strategies to ensure they remain fit for purpose as emerging risks such as cyber and climate change continue to develop. Traditional coverage structures are often unable to adequately cover novel or rapidly evolving exposures, creating opportunities to provide greater contractual clarity while maintaining sustainable risk selection and pricing. Insurers are likely to address these concerns via several routes, such as tailored wordings, specialist endorsements and parametric solutions designed to balance increasing demand for protection with the need for underwriting certainty. Underwriters may also place greater emphasis on understanding new risk characteristics, identifying potential accumulation exposures and assessing where protection gaps exist.

Political Risk, Trade Credit and Political Violence

Critical infrastructure will become a political violence priority

Energy, telecommunications and transport infrastructure will attract enhanced underwriting scrutiny across political violence portfolios. Critical infrastructure has become a focal point for both state-sponsored and non-state actors seeking to maximise economic and political disruption. Energy networks, submarine cables, ports, logistics facilities and communications infrastructure are increasingly viewed as strategic assets and therefore potential targets. In many jurisdictions these risks extend well beyond active conflict zones. Political violence insurers are likely to demand more granular information regarding security arrangements, supply chain resilience and business continuity planning. Premiums and capacity may increasingly reflect the strategic importance of an insured asset rather than simply its geographic location.

Event disruption risks will drive convergence between contingency and political violence cover

The distinction between contingency cover and political violence cover will continue to blur. Large sporting events, entertainment venues, conferences and public gatherings face an increasingly complex threat landscape. Organisers must contend with risks including terrorism, activist disruption, cyber incidents, drone activity and major public disorder. As a result, event-related insurance programmes are likely to require greater integration between contingency, cyber and political violence products. Underwriters will increasingly rely upon sophisticated security assessments, intelligence analysis and real-time monitoring to assess exposure. Hybrid insurance solutions that address multiple causes of disruption within a single programme are likely to become more prevalent.

Grey-zone conflict will become the defining political violence exposure

Political violence insurers will face increasing claims arising from grey-zone conflict that falls short of conventional war. States are increasingly pursuing strategic objectives through cyber operations, sabotage, proxy actors, disinformation campaigns and covert attacks rather than formally declared armed conflict. These activities often create significant physical and economic damage while generating uncertainty regarding the application of war exclusions and political violence wordings. Recent years have demonstrated the vulnerability of locations including energy infrastructure, telecommunications networks, logistics hubs and transport systems. Over the next year, insureds and insurers will increasingly focus on whether policy wordings adequately address state-linked but deniable acts. Coverage disputes concerning attribution and causation are likely to become more common as geopolitical competition intensifies.



Product Safety, Liability and Recall

Battery recalls will become a defining risk

The continued growth of electric vehicles, e-bikes, consumer electronics and energy storage systems, together with increased domestic solar power generation, will ensure that lithium-ion batteries remain a significant source of product safety concerns and recalls. Although battery technology continues to improve, the risk of thermal runaway, where a battery overheats and potentially catches fire or explodes, cannot be eliminated entirely. There have also been high-profile examples of other performance issues, such as loss of power, which have raised significant vehicle safety concerns. Complex global supply chains, increasing production volumes and pressure to reduce manufacturing costs may further increase the potential for defects. Lithium-ion battery defects continue to account for some of the largest and most costly automotive recalls, with individual recall campaigns often affecting tens of thousands, and occasionally millions, of vehicles due to concerns over fire risk, overheating and battery system failures. As regulators increasingly focus their attention on battery safety, manufacturers are likely to face greater scrutiny regarding product testing, quality control and post-sale monitoring. In response, recalls may become more frequent in the short term, particularly where even a small number of incidents suggest a serious fire risk.

Digital traceability to transform product recalls

Digital supply chains are likely to transform product recalls from broad, reactive exercises into highly targeted and proactive interventions. By integrating technologies such as Internet of Things sensors, RFID (radio frequency identification) tags and GPS technology, companies will gain real-time visibility over products from manufacture to end use. Rather than recalling entire batches, businesses will be able to identify the precise components, production runs or individual units affected by a defect. This enhanced traceability should significantly reduce recall costs, minimise disruption to customers and limit unnecessary waste, all while improving safety. Ultimately, this could shift recalls from a crisis-management reaction to a real-time, targeted intervention. Traditional supply chains often rely on fragmented systems, manual reporting and limited visibility. By contrast, a digital supply chain creates a continuous flow of real-time information between manufacturers, suppliers, distributors, retailers and customers. This is not entirely without risk or cost. In many industries, particularly the automotive and pharmaceutical industries, this level of traceability is becoming a regulatory expectation. There are also challenges around supply chain interdependence and the preservation of evidence in an environment in which there is a huge amount of data, as well as the threat of cyberattacks. The implications for insurance could potentially include a reduction in the cost of cover, but also the emergence of coverage issues around knowledge and reaction speed.

Professional Liability

AI will continue to impact all professions

AI is increasingly being adopted by professionals to enhance efficiency, manage data and reduce the incidence of human error. A key challenge for insurers and their customers will be to keep up to date with the various use cases and technological developments to understand the nature of the potential risks and exposures. Users ultimately remain responsible for the output generated by AI. Professionals must therefore check the work product to mitigate the potential risks. Law firms have already faced claims and regulatory scrutiny as a result of AI hallucinations and the inadvertent loss of privilege that occurs when client information is uploaded to an open AI model. Claims might also arise in the future if professionals fail to use AI for a task it would have completed more efficiently or to a higher standard. All professionals must keep up to date with regulatory guidance and understand the operation and limitations of any AI they use.

Technology professionals: The rise of the AI litigation battlefield

Increasing AI use by parties and practitioners will lead to further proliferation of court documents in both number and length. This proliferation will itself require and expand the use of AI by other parties and the court in order to work through them. As a result, the capability and potency of law firms' AI systems will become increasingly important. The courts will also have to expand their AI usage in order to manage the volume of materials before them. Technology and other complex claims will likely be disproportionately affected by this development, due to the number of documents ordinarily relevant to such claims and the natural prevalence of AI usage in these contexts.



Property

Utility infrastructure risks will prompt review of policy extensions

Growing cyber and infrastructure resilience risks to utility providers should prompt insurers to carefully review their underwriting appetite for policy extensions covering associated risks. A cyber incident in mid-2026 that resulted in a four-day operational shutdown of an electricity-generating facility in the UK acutely demonstrated this growing risk. Although this incident did not affect the wider electricity system or grid stability, similar incidents in the future could cause significant financial loss for affected businesses. Ordinarily, without physical damage to their own property, standard business interruption (BI) cover would not respond to such a claim. However, utilities extensions are frequently added as extensions to BI policies, providing cover for BI losses flowing from damage to or interruptions in supply from utilities infrastructure (depending on the wording). As scrutiny of grid reliability and security intensifies, businesses will want to seek BI policies that cover utilities and supply failure extensions as part of their wider resilience planning. Insurers will also wish to review their potential aggregated exposure under these wordings.

Reinsurance

Silent AI will come under increasing reinsurance scrutiny

Insurers will increasingly expect their outward reinsurance arrangements to respond to AI-related risks affirmed at the primary level, reflecting the evolution of primary-market policy wordings to address the growing use of AI in business operations. Reinsurers are likely to respond with more explicit AI exclusions, sub-limits and coverage conditions, bringing AI-risk allocation to the forefront of renewal negotiations. As a result, AI is likely to follow the path of cyber risk, moving from a largely silent exposure to a specifically underwritten, priced and managed risk across the reinsurance market. Potential gaps between primary and reinsurance coverage may also create new opportunities for disputes over claims and aggregation.

Parametric insurance will move further into the reinsurance mainstream

With the volume of reinsurance claims likely to trend upwards, reinsurers and cedants will look to solutions to better manage this evolving risk outlook. One such solution will be the fast-tracking of parametric risk transfer solutions. One major project announced in recent months was the launch of a parametric cover to respond to wildfires using satellite data. Products of this nature will be crucial as claims arising from incidents such as natural catastrophes increase, meaning that reinsurers are now facing margin pressure due to both increased loss activity and softer market conditions. The sector will remain profitable, but with heightened volatility and a greater focus on risk selection and capital management.

Data centre risks will become a major reinsurance accumulation risk

The rapid growth of data centres, driven by the ever-accelerating adoption of AI, will pose challenges to the sector. The potential exposures are significant. Data centres are expensive to build, operate and maintain, while the expansion of the sector has led to shortages of vital parts, especially semiconductors, making repairs more expensive and prone to delay, with the potential for substantial business interruption losses. The tendency to cluster data centres geographically also increases the risk of multibillion-dollar claims. It is estimated that 40% of data centres in the United States are located in areas at high risk of tornadoes, raising the prospect of a single weather event affecting multiple facilities simultaneously. Significant fire risks also arise from their reliance on large-scale lithium-ion battery systems. Adding to this increasingly complex risk profile, property reinsurers are being asked to provide cover for war and terrorism exposures alongside more traditional property risks.

Sports and Entertainment

Mega-event cyber incidents will drive a rethink of contingency coverage

Cyber disruption will become one of the most significant drivers of contingency claims for major sporting and entertainment events. The increasing digitisation of major events has created a risk landscape that extends far beyond the physical venue. Ticketing systems, broadcasting infrastructure, payment platforms, venue operations and fan engagement tools all present attractive targets for cybercriminals and state-sponsored actors. Analysis undertaken in relation to the 2026 FIFA World Cup has highlighted credible concerns relating to ransomware, phishing campaigns, AI-enabled fraud, disinformation and attacks targeting critical infrastructure. As a result, insurers are likely to introduce increasingly granular underwriting requirements and seek clearer delineation between cyber and contingency coverage. The market may also witness the emergence of integrated products designed specifically for large-scale events, reflecting the growing convergence between operational disruption and cyber risk.



Athlete welfare and data claims will increase exposure

Concussion litigation has brought athlete welfare firmly into the spotlight, but the next wave of claims is expected to focus not only on head injuries and chronic traumatic encephalopathy, but also on psychological and digital welfare risks, including the impact of social media on athletes. Risks may arise both from athletes' own online activity and from the growing prevalence of online abuse and harassment directed at them. For junior athletes, these issues add a further dimension to existing safeguarding obligations, increasing the expectations placed on clubs, governing bodies and educational institutions. At the same time, the continued convergence of sport and technology is likely to raise complex questions around the collection, use, ownership and protection of athlete health and performance data. As organisations seek to leverage data to enhance performance and welfare, they will need to balance those opportunities against evolving legal, regulatory and reputational risks.

Transactional Liability

AI due diligence to test the boundaries of Warranty & Indemnity cover

AI is already transforming the transactional liability space, with insureds increasingly using the technology to draft notifications and insurers necessarily having to deploy AI in the underwriting and claims process simply to keep up. It remains to be seen how effective a tool this is in circumstances where every transaction and every set of facts is different. However, we foresee other problems arising. First, software as a service (SaaS) has been a mainstay of the transactional liability market but is one of the sectors most disrupted by AI. More fundamentally, where AI is used extensively in a due diligence exercise, how will this interact with an 'actual knowledge' exclusion, and is that exclusion as valuable as it once was?

Ireland

Ireland stays at the centre of European Big Tech regulation

As AI, data governance and digital regulation evolve, Ireland is expected to remain at the centre of Europe's most significant regulatory investigations and technology disputes. Ireland's Data Protection Commission (DPC) has imposed €4 billion in fines on major technology companies based in Ireland, underlining its central role in enforcing European data protection laws. Most recently, the DPC issued a €403 million fine to Google over its handling of location data. Many of those decisions remain subject to appeal, meaning only a small proportion of the headline fines (some €20 million) has so far been collected. Because many global technology companies maintain their European headquarters in Ireland, the DPC is likely to remain one of the continent's most influential regulators, exerting a significant impact on those companies' operations, with several major investigations continuing into 2027.

The Irish insurance sector enters the age of AI automation

With AI adoption now widespread across the insurance sector, the next phase will be the automation of routine decision-making and operational processes. Competitive advantage is increasingly likely to depend on effective implementation rather than adoption alone. Central Bank of Ireland surveys indicate that 85% of insurers already use generative or other forms of AI, although much of that use remains subject to human oversight. Insurers are expected to expand AI deployment across underwriting, pricing, claims handling, fraud detection and customer service, although shortages of specialist talent and the need for robust governance frameworks may constrain the pace of adoption.

Scotland

AI governance will reshape professional indemnity risk for Scottish firms

The Scottish professional services market will see increased deployment of generative and agentic AI, generating the need for an increasingly sophisticated professional indemnity (PI) insurance and regulatory response. Compared with many other jurisdictions, a relatively large proportion of Scotland's professional services sector consists of small and medium-sized independent firms that are not particularly well resourced. These smaller firms will need to consider how the productivity benefits of AI can be realised, but not at the expense of appropriate governance and risk controls. This will create the need for a stronger focus on AI governance, rather than AI itself. Firms that can demonstrate controlled and auditable use of AI, including strong cyber security and effective supervision, are likely to enjoy a competitive advantage. Those firms that treat AI as merely another useful software product, or as one that does not require enhanced safeguards, risk encountering regulatory issues and increasing difficulty in securing PI cover for any of their work that is heavily AI-assisted. From a PI insurance perspective, the first significant Scottish claim arising directly from negligent AI-assisted professional advice, and the market reaction to it, may well prove more influential than any forthcoming legislative developments.



France

New product liability regime in France will turn cyber failures into casualty claims

Cyber vulnerabilities and defective software will increasingly generate product liability claims rather than purely cyber losses. The implementation of the revised EU Product Liability Directive in France will bring software, AI systems and connected products within the strict liability regime, while extending potential exposure across manufacturers, importers, distributors, online platforms and other economic operators. Failures to provide security updates or comply with mandatory cybersecurity requirements may be relied upon as evidence that a product is defective. Insurers should therefore expect increasing overlap between product liability, cyber, technology errors & omissions (E&O) and directors & officers (D&O) policies, together with more complex allocation and aggregation disputes where a single software defect causes losses across multiple products and jurisdictions.

Germany

Regulators will look beyond AI adoption to AI governance in Germany

2027 will mark a turning point for the German insurance sector, as AI moves from experimentation to industrial-scale deployment. Success will be measured not only by technological capability, but by how robust AI governance is. Ahead of the AI Act's late-2027 compliance deadlines for standalone high-risk AI systems, operational resilience will become a commercial imperative rather than a purely compliance-driven objective. Insurers that fail to establish robust governance frameworks may face heightened regulatory risk. As European Union AI legislation takes effect and AI capabilities continue to advance, differences in insurers' AI maturity will become increasingly visible to the insurance ecosystem, influencing competitiveness, underwriting performance and market confidence.

Cybersecurity vulnerabilities will drive a new wave of product liability and supplier recourse disputes

As connected products become increasingly dependent on third-party software, cybersecurity vulnerabilities will drive disputes over who bears the resulting remediation, recall and liability costs. The EU Cyber Resilience Act (CRA) reinforces manufacturers' responsibility for the cybersecurity of finished products, including where vulnerabilities originate in a third-party component, such as software. However, regulatory responsibility does not automatically translate into a right to recover the costs of patches, recalls or other remediation from software suppliers. A recovery against the software supplier by the manufacturer may be limited where a vulnerability is corrected before it causes injury or damage, leaving manufacturers to rely largely on contractual claims through the supply chain. Disputes are likely to focus on agreed security standards and support periods, whether a vulnerability existed on delivery, and whether any field-action costs are recoverable. In preparation, manufacturers should review software supply agreements, update and support commitments, liability caps, and procedures for urgent remediation and timely defect notices.

Cyber insurers face a widening gap between price and risk in Germany

In 2027, German cyber insurers will face a growing disconnect between falling premiums and progressively complex risks. As capacity continues to expand and competition intensifies, insurers will increasingly underwrite complex and emerging risks, including AI exposures, at even thinner margins. At the same time, ransomware remains a significant threat, while systemic cyber exposures are becoming harder to model and quantify. One of the biggest shifts will be the growing importance of third-party and supply-chain risk. As larger organisations strengthen their own cyber defences, attackers are increasingly pursuing alternative targets such as their suppliers, cloud providers and other external partners. Managing cyber risks will therefore require greater visibility beyond an organisation's own IT environment. Expanding cybersecurity regulation will add a further layer of complexity, requiring insurers to integrate regulatory compliance into underwriting and risk assessment. The challenge for cyber insurers will not be deploying capacity but ensuring that pricing adequately reflects increasingly connected and systemic risks.



Italy

Enhanced anti-fraud reporting to target emerging fraud risks

Detecting AI-enabled fraud in casualty claims will become a central component of anti-fraud reporting frameworks in Italy. The rapid deployment of AI has created new liability exposures arising from algorithmic errors, bias, lack of transparency and regulatory breaches. Insurers are increasingly required to assess exposures linked to AI-driven products and services. However, the use of AI is not limited to new risks, as the use of deepfakes, synthetic identities and AI-generated documentation is increasing the sophistication of insurance fraud schemes. In 2026, the Italian insurance regulator, IVASS, consulted on reforms to its anti-fraud reporting framework to account for these risks, which we expect will lead to enhanced anti-fraud reporting and greater regulatory visibility over emerging fraud typologies. In response, we expect insurers to continue investing in advanced fraud detection and claims verification tools.

Netherlands

Class actions in the Netherlands will increasingly target alleged digital harms

Class actions in the Netherlands will increasingly focus on large-scale digital harms. These actions demonstrate that collective redress is moving beyond traditional privacy and data protection claims into platform design, consumer protection and health-related harms. This may create novel coverage and aggregation issues for insurers. The recent claim brought by the consumer group Stichting Massaschade & Consument against the social media platform Snap over alleged social media addiction illustrates how digital harm class actions may create complex, cross-line exposures arising from alleged harm at scale.

Spain

Data centre expansion creates new multi-line risks in Spain

Data centres will become a significant multi-line insurance risk in Spain as the country consolidates its position as one of Europe's leading data centre markets. Continued investment in digital infrastructure will create increasingly complex underwriting and claims exposures across the construction and operational phases of these facilities, spanning property, construction, cyber, liability and business interruption risks. At the same time, the sector is entering a period of heightened regulatory scrutiny. Following the public consultation launched by the Ministry for the Ecological Transition on a draft Royal Decree intended to implement aspects of the EU Energy Efficiency Directive, operators may face additional energy efficiency, sustainability and reporting obligations. The proposed framework also links compliance with certain requirements to access to electricity transmission and distribution networks, increasing the importance of energy and environmental considerations in the development of new facilities. Insurers should therefore exercise greater scrutiny of operational resilience, energy dependency and regulatory compliance when assessing data centre risks.

AI liability moves from emerging risk to active claims

As AI becomes embedded in everyday business operations, insurers will increasingly face AI-related claims across cyber, professional liability, product liability and D&O lines. Spain has been at the forefront of these developing risks; the AEPD (Spanish data protection authority) publicised the first reported data breach executed autonomously by an AI agent using a large language model in September 2026. Claims are likely to arise from defective AI systems, inaccurate or misleading outputs, regulatory breaches, cybersecurity incidents and failures in governance and oversight. Regulatory changes such as the updated Product Liability Directive (when formally transposed into Spanish law) are expected to lower the barriers to recovery and broaden the range of potential defendants. Spanish insurers should expect to pay close attention to underwriting and risk allocations across supply chains, particularly in sectors involving connected products. AI-related disputes will move increasingly from theoretical risk scenarios to real-world claims.



Cyber supply chain risk becomes a major driver of insurance losses

Cyber incidents originating within technology supply chains will become a major source of insured losses in Spain. Spanish organisations' dependencies on third-party technology providers mean that cyber events involving software vulnerabilities, managed service providers, cloud platforms or outsourced IT services are likely to generate significant business interruption losses, recovery costs and regulatory exposure. Recent years have demonstrated that cyber incidents increasingly originate within digital supply chains rather than within the affected organisation itself. European cybersecurity legislation, including NIS2 and the Cyber Resilience Act, has increased expectations regarding cybersecurity standards and supply chain security. As these frameworks become fully operational, they are likely to influence how regulators, courts and claimants assess whether reasonable cybersecurity measures were in place. Insurers should therefore expect greater scrutiny of third-party dependencies, vendor management and supply-chain security controls during underwriting, as well as more complex claims involving multiple affected insureds arising from a single cyber event.

Sweden

Cyber insurance enters the Swedish mainstream

Cyber insurance will become an increasingly standard component of corporate risk management in Sweden. As cyber attacks continue to grow in frequency and severity, insurers are responding with higher premiums, increased deductibles and tighter policy terms. Organisations seeking cover will need to demonstrate a higher level of cyber resilience. Basic safeguards such as incident response plans and staff training will become prerequisites for cover, not optional extras. In July 2026, Swedish organisations faced an average of 2,352 cyberattacks per week, a 36% increase since last year, making Sweden the most targeted country in the Nordics. Municipalities remain the prime target, followed by the finance sector and healthcare. This is coupled with a rise in cyber extortion against Swedish small businesses of 188% in 2026.

Software liability forces a repricing of product risk in Sweden

Insurers are likely to move swiftly to reprice and reassess product liability exposures following the introduction of Sweden's new Product Liability Act. This will result in a harder, more document-driven product liability market ahead of the Act's planned entry into force, particularly around software development and AI-heavy manufacturers. The Act transposes the updated EU Product Liability Directive into Swedish law and significantly broadens the scope of product liability exposure. The Act will expand liability to cover traditional tangible products, as well as standalone software and digital files such as apps and AI systems. The range of potentially liable parties is also broadened. In addition, the Act expands compensation for property damage, introduces economic loss arising from the destruction or corruption of data as a new recoverable head of loss and makes it easier for claimants to establish liability in technically complex cases.

United States

Data centre development in the US to face growing regulatory resistance

Opposition to the expansion of data centre development in the United States is expected to intensify during 2027. Several states and municipalities have already imposed moratoriums on data centre development and construction. Further moratoriums are expected in 2027, as concerns grow over their environmental and societal costs. In 2024, data centres in the United States were estimated to consume approximately 192 TWh worth of electricity, which is approximately 4% of the country's total electricity consumption. That number reportedly rose to 312 TWh for 2025, and lawsuits are underway to prevent data centre owners and developers from passing those energy costs to ratepayers. Data centres also can consume substantial volumes (between 300,000 and 5,000,000 gallons) of water daily and generate sustained noise levels (between 85 and 100 dB) that affect surrounding communities. The noise pollution produced has already generated lawsuits from residents close to data centres seeking damages for the effect on their daily lives. Further challenges may target planning and regulatory approvals that opponents argue lacked sufficient transparency or public consultation.



Sports betting operators to face addiction-related litigation

The widespread availability of mobile betting applications has transformed access to sports gambling. Concerns about user addiction are expected to drive litigation in the United States by state attorneys general and individual gamblers who lose money and suffer from emotional distress as a result of these platforms. Betting markets range from match outcomes to parlays, with sports leagues increasingly partnering with betting companies to promote their services. Estimates are that approximately 95% of regular online sports gamblers lose money over time. In some cases, gambling debts can become substantial. The concept of liability arising from allegedly addictive digital products is already familiar in the United States. In August 2026, Meta agreed to a $17.1 billion settlement with 51 state attorneys general to resolve claims that Meta engineered Instagram and Facebook to be addictive for teens.

Argentina

Parametric insurance set for a regulatory breakthrough in Argentina

In 2027, Argentine regulators are expected to begin developing a framework for parametric insurance, marking an important step towards wider adoption of these products. Demand for rapid and transparent claims payments, particularly for agriculture, energy and climate-related risks, will increase interest in solutions triggered by predefined events rather than traditional loss adjustment processes. A clearer regulatory environment would provide legal certainty, support product innovation and improve protection against catastrophic and weather-related events.

Brazil

AI will move into core decisions under stronger governance

In 2027, it is expected that insurers and other supervised protection providers in Brazil will expand the use of AI in underwriting, pricing, claims, fraud detection and distribution. Competitive advantage will depend on data quality, human oversight and integration with established controls, not merely access to models. For example, insurance cooperatives and mutual protection administrators may use AI to scale member services and claims management, while facing the same expectations for governance and consumer safeguards set out by the Insurance Act and data protection regulation. As automated tools influence customer outcomes, market participants will need robust governance and transparent oversight. AI-assisted triage and generative tools may improve efficiency, but inaccurate, biased or insufficiently documented outputs could create legal, operational and reputational exposure. Responsible deployment will therefore become part of product and claims governance.

Chile

AI and digital infrastructure to drive Chile's next growth phase

Chile will strengthen its position as one of Latin America's leading technology and innovation hubs. Continued investment in digital infrastructure will support modernisation in both the public and private sectors, including cloud computing, data centres and AI. Demand for reliable digital services, combined with Chile's reputation for institutional stability, should attract further foreign technology investment. The mining, energy, and forestry sectors will accelerate the adoption of automation, robotics, predictive analytics and remote operations to improve productivity and sustainability. At the same time, policymakers will face increasing pressure to address data privacy, cyber security, digital inclusion and workforce reskilling. AI will become an increasingly significant driver of economic growth, public service delivery and business competitiveness.

Colombia

Cyber risk shifts to Colombia's SMEs and supply chains

Cyber exposure in Colombia will shift increasingly towards SMEs, service providers and interconnected supply chains in 2027. As larger organisations strengthen their defences, smaller businesses and third-party providers often lack comparable resources, controls and incident-response capabilities. More sophisticated attacks, including AI-assisted fraud and ransomware, may therefore generate losses beyond the initial target organisation through outsourced technology, digital platforms and dependent business relationships. These attacks will increase demand for accessible cyber products, but insurers may struggle to assess risks associated with smaller businesses and their shared reliance on service providers. Underwriting scrutiny will increasingly focus on minimum security standards and vendor management. Claims may also raise difficult questions regarding business interruption (BI) losses, data restoration costs and the interaction between cyber, crime and traditional property policies.



Ecuador

Privacy enforcement will test cyber cover in Ecuador

Ecuadorian privacy claims will put cyber wordings under pressure in 2027, addressing whether policies will respond to regulatory investigations and corrective measures in the absence of a cybersecurity breach. The data protection regulator's first enforcement action in December 2025, resulting in six-figure fines against two national sports bodies for processing user information without valid consent, demonstrates that possible insurance exposure extends to unlawful processing. Insurers are expected to revisit investigation triggers, defence costs and losses arising from orders to stop processing or delete data. AI-assisted underwriting and overseas claims handling will add scrutiny of decision records and data-sharing arrangements. Whether the policy responds to the alleged privacy violation will be the central coverage question, with fines and remediation costs requiring separate consideration under both the policy wording and applicable law.

El Niño to reprice Ecuadorian coastal risk accumulations

Coastal placements in Ecuador will face renewed scrutiny of flood and landslide risk accumulations in 2027. Ecuador remains one of the most El Niño-exposed economies in the region. The 1997-98 El Niño event, one of the most damaging natural disasters in Ecuador's recent history, caused widespread infrastructure and agricultural losses. Shrimp aquaculture and banana production, in particular, remain highly sensitive to rainfall and sea-surface temperature. Disputes are expected to concentrate on two issues: whether successive flooding and landslide events aggregate as a single occurrence under 'Loss Occurrence/Hours clauses', and whether business interruption cover responds where transport links and supply chains are disrupted without physical damage at the insured location. Reinsurers will press for separate flood sub-limits and clearer denial-of-access wording, while parametric and index-based products will gain traction for risks the traditional market is unwilling or unable to absorb.

Peru

Cyber insurance will become a core risk management tool

Cyber insurance uptake in Peru will accelerate as organisations confront increasingly sophisticated cyberattacks and AI-enabled fraud. Businesses will also be subject to evolving regulatory expectations regarding data protection. Coverage will no longer be viewed solely as a financial safeguard but as part of a broader risk management framework. Demand is expected to grow across various sectors including banking, telecommunications, energy, logistics and public infrastructure. Insurers are likely to supplement policies with additional services such as incident response, cybersecurity assessments and risk-prevention services. Cyber insurance will become a core component of corporate governance and resilience strategies.

Repeated climate shocks to accelerate parametric insurance adoption in Peru

Repeated severe weather events, compounded by the 2027 El Niño event, will accelerate interest in parametric insurance solutions in Peru. Traditional indemnity products often struggle to provide rapid liquidity following large-scale catastrophes, whereas parametric products can deliver swift payouts based on predefined triggers such as rainfall levels, river heights or temperature thresholds. As climate-related losses become more frequent and public authorities seek greater financial resilience, parametric solutions will expand beyond agriculture into the infrastructure and logistics sectors, becoming an increasingly important tool of public sector risk management.

Australia

AI liability moves from financial loss to bodily injury in Australia

AI-enabled decisions will generate a new wave of bodily injury and liability claims in 2027. As AI influences healthcare, transport, workplace safety and public services, claimants will test who is responsible when technology-assisted decisions cause bodily harm. The court system in Australia is likely to focus on the organisations, professionals and directors who selected, implemented or relied on the system, rather than the technology itself. Claims will raise difficult issues of causation, foreseeability, reliance and the standard of care. A single flawed algorithm may also affect many people, creating aggregation risk. Casualty insurers should review whether existing wordings respond clearly to AI-related injury and consider affirmative cover, defined endorsements or targeted exclusions for unintended systemic exposure.



Hong Kong

Hong Kong insurers to compete for leadership in AI coverage

Demand for AI-related provisions, whether to write back presently excluded cover or for full AI-specific policies, will increase exponentially in 2027. Meaningful progress in this debate will not be helped by an almost invisible claims history. However, the speed at which AI is improving, its already pervasive effects on our lives and work, and the challenges introduced by the inevitable exposure mean that AI-related risks can no longer be considered theoretical. As AI adoption accelerates, insurers in Hong Kong and beyond will face growing scrutiny of policy wordings and increasing demand for clarity on the scope of cover for AI-related losses. There will be significant opportunities for those insurers that take a leading position on AI-related coverage and focus on presenting attractive solutions to customers.

Hong Kong's low-altitude economy to create new insurance opportunities

The coming year is likely to see a focus on the capacity of the insurance market to provide innovative solutions in support of the development of the low-altitude aviation economy in Hong Kong. In his 2024 Policy Address, the Hong Kong Chief Executive set out plans to develop the low-altitude economy by establishing a working group led by the Deputy Financial Secretary. The group was intended to explore low-altitude flying application scenarios, review relevant regulations and plan for low-altitude infrastructure. The Civil Aviation Department has now approved over 140 project applications under its regulatory sandbox scheme. Proposals would extend the framework to cover cross-border logistics within the Greater Bay Area and non-traditional aircraft, including passenger-carrying models. The intention is to position Hong Kong as the Asia-Pacific hub for innovative low-altitude applications. With significant financial and intellectual capital being deployed alongside technological advances, the potential benefits to insurers in Hong Kong and the region are clear.

Mainland China

Chinese companies' overseas expansion will demand more insurance cover

In 2027, insurance demand is expected to follow the overseas operating footprint of Chinese businesses. China's 2026 technology insurance measures will encourage support for businesses operating overseas, while Shenzhen's 2026–2028 action plan expressly promotes overseas property, engineering and liability cover. Companies establishing foreign production and distribution networks will seek protection extending beyond cargo and payment to wider property and liability risks. This shift should deepen collaboration between mainland and international insurers, reinsurers and claims specialists. For international market participants, this presents an opportunity to support Chinese clients beyond their home market, particularly for those who can combine an understanding of Chinese clients with local market knowledge, effective claims handling and access to specialist legal support.

China's low-altitude economy will move towards commercial scale

China is expected to move beyond pilot projects towards broader commercial deployment of drone logistics, urban air mobility services and advanced aerial operations. One of the clearest signals emerged from the China Air Transport Association's 15th Five-Year Development Plan (2026–2030), which emphasised the strategic importance of the low-altitude economy. Regulatory and industry standards, along with infrastructure investment, are likely to mature rapidly. This will position China as the global test bed for next-generation aviation services. As the sector develops, a wide range of organisations such as aviation technology firms, drone manufacturers, software providers and aerospace service companies are likely to find new opportunities to scale their operations. For insurers and aviation stakeholders, the continued growth of the low-altitude economy will raise questions about how these operations are authorised and insured, and where liability lies when things go wrong. As commercial deployment accelerates, the supporting legal and regulatory frameworks will face increasing scrutiny, particularly where cyber risk intersects with operational and coverage issues.



Judicial guidance will shape China's AI landscape

China's new Supreme People's Court Opinions signal an intention to govern AI-related disputes through existing laws, rather than a standalone AI liability regime. In 2027, Chinese courts will play an increasingly important role in defining the legal and practical boundaries of AI development and deployment across areas including personal information, consumer protection and automated vehicles. The Opinions provide a roadmap for allocating responsibility, linking liability to factors such as fault, transparency, control and preventive measures. They also place significant emphasis on evidence, with courts expected to scrutinise training records, governance processes and technical documentation. As AI-related disputes increase, these principles will become an important mechanism for balancing innovation with accountability while strengthening legal certainty. For businesses operating in China, effective governance will be essential to support AI innovation. Organisations deploying or developing AI systems should expect courts to examine whether their governance arrangements provide meaningful oversight and risk management. Businesses that can demonstrate transparency, preserve relevant evidence and maintain accountability for their systems will be better placed to defend AI-related claims as litigation grows.

Singapore and Southeast Asia

Cyber in Southeast Asia to remain both fast-growing and volatile

Cyber incidents in Southeast Asia are expected to rise, driven less by traditional ransomware and more by AI-enabled fraud, business email compromise, deepfakes, cloud compromise and supply chain attacks. As local businesses across the region, particularly SMEs, continue to increase their digital engagement to drive efficiency and growth, phishing, cyber fraud and social engineering attacks are likely to become more prevalent. For insurers, one of the primary concerns will be systemic losses, such as a cloud provider outage or a service provider breach affecting multiple insureds simultaneously. At the same time, we anticipate greater scrutiny of cyber controls at underwriting, particularly for sophisticated and well-resourced insureds, for whom a robust standard of cyber hygiene is increasingly expected.

Greater regulatory scrutiny to drive increased exposure for businesses in Southeast Asia

Businesses in Southeast Asia will face intensified regulatory scrutiny, particularly in relation to financial services, cybersecurity and ESG-related governance. Illustrating this trend, the Malaysian Anti-Corruption Commission is now conducting a new investigation every week; implementation of the Philippines National Cybersecurity Plan 2023–2028 is driving more formalised compliance practices; and the Indonesian Financial Services Authority has mandated sustainability reporting for public companies and financial institutions, with its regulatory framework expected to expand further during 2027. Regulators across the region are expected to move beyond guidance towards more active enforcement, with larger penalties and more onerous remediation becoming increasingly common. From an insurance perspective, a key challenge will be the gap between growing regulatory expectations and the level of awareness and preparedness among many insureds.

AI-enabled products to drive liability and recall claims

Increasing use of AI in consumer and industrial products is likely to increase product recall exposures and regulatory scrutiny across Southeast Asia. Manufacturers are rapidly integrating AI-enabled functions into a wide range of products from consumer electronics to motor vehicles. As these products become more autonomous and increasingly rely on software-driven decision-making, questions of product safety, causation and responsibility will become more complex. Recent developments in Asia, particularly China's increasing regulatory and judicial focus on autonomous and driver-assistance vehicle technologies, highlight growing concerns around AI-driven product safety and manufacturer responsibility. Insurers will face more product liability and recall claims arising from allegations that AI-enabled products have malfunctioned, made flawed decisions or failed to operate as intended. Given the scalability of software-based defects, a single flaw may affect thousands of products simultaneously, creating the potential for large-scale recalls, regulatory action and cross-border liability claims.



Data centre failures to drive high-value property and BI claims in Asia

The rapid expansion of Asia's data centre sector is expected to generate more high-value property damage and business interruption (BI) claims. Driven by growing demand for AI and other digital services, significant investment continues to flow into data centres across Singapore and the wider region. These highly integrated facilities depend on resilient power and cooling systems, with even minor failures capable of generating substantial losses. This growth is occurring alongside increasing pressure on regional power infrastructure, prompting operators to invest in complex combinations of back-up generation, battery storage and uninterruptible power supply systems. As reliance on interconnected infrastructure grows, so too does the potential for equipment failures and cascading losses. Given the critical services data centres support, even short disruptions can have significant operational and financial consequences. Insurers are likely to see increasing claims from failures in power resilience infrastructure, together with fires, water damage and consequential BI losses.

Scan here to view our full suite of predictions for 2027.

insurance.dacbeachcroft.com

dacbeachcroft.com

Connect with us:
DAC Beachcroft LLP

DAC Beachcroft publications are created on a general basis for information only and do not constitute legal or other professional advice. No liability is accepted to users or third parties for the use of the contents or any errors or inaccuracies therein. Professional advice should always be obtained before applying the information to particular circumstances. For further details please go to www.dacbeachcroft.com/en/gb/about/legal-notice. Please also read our DAC Beachcroft Group privacy policy at www.dacbeachcroft.com/en/gb/about/privacy-policy. By reading this publication you accept that you have read, understood and agree to the terms of this disclaimer. The copyright in this communication is retained by DAC Beachcroft. © DAC Beachcroft 2026. Prepared November 2026.