DAC BEACHCROFT

Technology
Predictions 2026

AVIATION

Cyber threats targeting avionics and air traffic systems will prompt broader cyber coverage adoption

The aviation sector faces escalating cyber risks as digitalisation deepens across flight operations, maintenance, and passenger services. Cyber threats are becoming increasingly sophisticated, targeting critical systems such as avionics software, flight planning tools, and airport IT infrastructure. A successful breach could disrupt navigation, compromise safety, or ground entire fleets, leading to severe financial and reputational losses. Regulators are tightening cybersecurity compliance, pushing operators to invest in robust defences. Insurers are responding by expanding cyber liability offerings, often bundling them with traditional aviation policies, while introducing stricter risk assessment protocols and premium adjustments for operators with inadequate cyber resilience.

Launch of the UK eVTOL Delivery Model anticipates commercial flight operations

In September 2025, the UK Civil Aviation Authority published the electric Vertical Take-Off and Landing (eVTOL) Delivery Model in anticipation of commercial flight operations by the end of 2028. The Delivery Model provides a regulatory framework addressing certification, pilot licensing, vertiport integration, and operational approvals. The pioneering technology of eVTOLS represents a bold step toward a cleaner, smarter future for aviation – one that not only accelerates decarbonisation but redefines how we connect and move across the globe. eVTOL assembly and battery production facilities have been established in the UK to support certification and early production. By positioning itself at the forefront of aerospace innovation, the UK seeks to unlock new possibilities for sustainable travel and economic growth. As we edge towards commercial eVTOL operations, this is dialling up a need for a range of tailored advanced air mobility (AAM) insurance cover to include hull liability, war, passenger, cargo, third party liability, spares, hangar keeper and product liability insurance. In 2026, we will see the London and global aviation insurance market continuing to evolve, to respond to the needs of emerging AAM technology.

Autonomous flight: futureproofing laws and regulation

With ongoing advances in aviation automation and autonomous flight there is a need to reconsider related legal and regulatory frameworks. The UK Civil Aviation Authority, in conjunction with the Law Commission of England and Wales, is undertaking a three-year review of existing liability models relating to the future of flight modes including electric Vertical Take-Off and Landing (eVTOL), drones, novel air traffic management and air navigation services to uncrewed aircraft. A final report is scheduled to be published in early 2026. Included in the review are current mechanisms for attributing criminal and civil liability. In particular, the Law Commission is considering (i) where the law allocates responsibilities to a human (e.g. a pilot) and the issues that arise if functions are performed by autonomous systems and (ii) how to allocate civil and criminal responsibility where functions are performed by a system or shared between a human and a system. Meanwhile, in its general Discussion Paper ('AI and the Law') published in July 2025, the Law Commission, in provoking debate, suggested that the option of granting some AI systems legal personality is increasingly likely to be considered. One key objection against that argument is that AI systems might be used as 'liability shields' protecting those at fault from criminal and/or civil accountability. In the field of aviation, where safety, responsibility and accountability are paramount, we predict any such future proposals will be met with strong resistance.

CASUALTY

AI will identify potential athlete welfare issues before they arise

The rise of AI shows no signs of abating, and the potential use cases are exponential. For athletes, data will increasingly be used alongside AI to prevent welfare issues, be they physical, mental or emotional. From mental health monitoring to bio-mechanical data to detect the risk of injury, and from wearables that warn of fatigue and poor recovery to instrumental mouthguards capable of detecting potential head injuries, expect technology to become increasingly prevalent in proactively managing welfare in elite sports. Technological change, particularly where it is likely to filter down from elite to lower and grass-roots level, will be a game changer for individuals, clubs and associations.

CONSTRUCTION AND ENGINEERING

Innovation will meet risk in the race to build smarter

The growing incorporation of technology in the construction industry and pressure to reduce energy wastage has led to increasing numbers of buildings utilising smart technology. Smart buildings include analytical tools which can predict the needs of those using the building and monitor parts and systems, flagging them for repair or maintenance. Sensors in a smart building's infrastructure can have a positive effect in terms of reducing energy usage and carbon emissions. However, smart buildings are challenging to design and build, often requiring sophisticated construction techniques and complex mechanical and electrical infrastructure which can lead to claims against the contractor and professional team if they do not meet requirements. Smart buildings are also more at risk from cyberattacks than legacy buildings: a hacker who gains access to a building's system can cause chaos.

For further information or enquiries, please contact:

Hans Allnutt
Partner
hallnutt@dacbeachcroft.com

Charlotte Halford
Partner
chalford@dacbeachcroft.com

Rowena McCormack
Partner
rmccormack@dacbeachcroft.com

DAC BEACHCROFT

Technology
Predictions 2026

New Code will minimise water escapes

A new-ish but under-used industry Code will be written into more policies as the frequency and severity of water damage incidents on construction sites increases. Recognising the need for robust risk management, experts from both the insurance and engineering industries have developed a Joint Code of Practice for Escape of Water (EoW) Prevention and Management on Construction Sites and Buildings Undergoing Refurbishment. The Code applies across the supply chain to both permanent and temporary water systems and puts in place a collaborative risk-based approach that addresses the root causes of EoW during pre-construction and construction phases and mitigates the effect when it occurs. The focus on prevention includes the incorporation of modern technology to detect anomalous flow rates and then automatically isolate pipework and inform the planned emergency response. EoW incidents can lead to costly claims due to delayed handovers, damaged materials and wasted resources but they can also adversely impact a project's environmental and sustainability goals to monitor and reduce water consumption. Risk management is key and insurers should write in Code compliance to ensure that good practice is stringently followed.

D&O AND FINANCIAL INSTITUTIONS

AI is transforming the financial services industry but its rapid adoption is not without risks

AI is increasingly being used by financial services companies to drive operational efficiencies through automation and advanced analytics. It has fundamentally changed loan and investment decision-making by enabling the rapid analysis of vast amounts of data about a particular sector, supporting swift, robust and informed decisions. AI has also revolutionised fraud detection, customer service, risk management, and regulatory compliance. While AI delivers significant efficiencies and innovation, its widespread adoption raises concerns about overreliance. Where investors suffer a loss, this can lead to claims against financial institutions that deploy these technologies (as seen in Tyndaris v VWM). Oversight and ongoing monitoring are essential to mitigate these risks and ensure responsible use of AI in the financial sector.

DATA, PRIVACY AND CYBER

Pseudonymisation: ambitious data use will require robust safeguards

As the sector seeks to unlock the value of its datasets for analytics and AI training, the tension between anonymisation and pseudonymisation is becoming ever more pressing. True anonymisation remains the gold standard but often strips away the richness that gives data its value. Pseudonymisation preserves that utility but keeps data within the scope of data protection law. The CJEU's SRB decision brings welcome nuance, confirming that whether pseudonymised data counts as personal depends on the realistic means of re-identification available to the controller, not theoretical possibilities. This more contextual approach could open new space for innovation, provided businesses can show re-identification risks are genuinely low. Those in the sector that invest early in verifiable safeguards and governance frameworks will be best placed to harness data confidently and compliantly in the age of AI.

Agentic AI will intensify data protection risks

Agentic AI (systems made up of autonomous agents that are capable of independent interaction and decision making) poses heightened data protection risks. Although it brings notable benefits in terms of efficiency and innovation, representing another evolution beyond generative AI, it also introduces new challenges. Unlike some earlier AI systems, many typical agentic AI system use cases rely heavily on processing personal data, including special categories of personal data or other sensitive categories such as financial information. Although many organisations have so far managed to apply governance controls to the use of generative AI in the workplace, the reduced human oversight evident in agentic AI significantly increases the challenge of implementing the same controls. As a result, data protection risks are likely to intensify.

The integration of AI solutions will increase the adoption of privacy enhancing technologies

Over the next 12 months, we will see greater adoption of privacy enhancing technologies (PETs) and their closer integration with AI systems. For several years, PETs have been highlighted as having the potential to aid data protection compliance, in a variety of different contexts. In its 2023 guidance on PETs, the ICO specifically cited privacy by design and by default; data minimisation; security; and secure data sharing as capable of being supported by PETs. However, since then we have seen only intermittent PET adoption by organisations. In the coming year, PETs such as homomorphic encryption and federated learning will be used increasingly to train AI models.

DAC BEACHCROFT

Technology
Predictions 2026

Quantum computing will be the next frontier

As quantum technology develops, we expect cyber insurers to start considering the potential systemic risks associated with the post-quantum era. Developments in quantum technologies are advancing rapidly and will offer huge opportunities to improve our lives. However, quantum computing will also pose the next significant challenge to cybersecurity and organisations are being urged to take steps to prepare for this now. The National Cyber Security Centre has already published guidance on the timeline for the migration to post-quantum cryptography (PQC) which starts now by identifying information, systems and cryptography which is at risk and ends in 2035 with the complete migration to PQC for systems, services and products.

INSURANCE ADVISORY

Expect regulatory intervention to follow AI innovation

The insurance sector has embraced AI at speed, deploying it across underwriting, claims and customer engagement. Yet regulation is struggling to keep pace with the technology's rapid evolution. Current frameworks were not designed with self-learning systems or generative models in mind, leaving gaps around accountability, transparency and bias. For now, regulators are watching closely, with guidance rather than enforcement. But history tells us that regulatory intervention often comes after the first high-profile failures or consumer harms. When that moment arrives, we can expect tighter controls on explainability, governance and oversight of AI. For the sector, the message is clear: use this breathing space to build robust controls now, before regulators mandate them.

MARINE, ENERGY AND TRANSPORT

Batteries will store problems as well as power

The ever growing prevalence of lithium ion batteries across a wide range of products is increasing the risk of fire losses to vessels and cargoes. Batteries have been identified as the cause of a recent spate of scrap fires on vessels leading to major casualties. The problem stems from hazardous materials, particularly batteries, being present in supposedly inert scrap cargoes due to improper disposal in household waste streams. These batteries can spontaneously ignite or cause fires during handling and transportation, leading to intense, difficult-to-extinguish blazes that endanger ships and crews. Insurers and safety organisations are issuing warnings and recommending better screening and handling procedures for scrap metal cargoes. Incidents of battery fires on mega yachts are also on the rise. Mega yachts use an increasing number of lithium-ion batteries to power their advanced electronics, luxury amenities, and growing fleet of electric tenders and water toys. Incorrect use and maintenance coupled with insufficient crew training can lead to significant losses.

MEDICAL MALPRACTICE

AI transcription brings risks as well as efficiencies

As anticipated, the use of AI in clinical practice continues to become more prevalent, with an increasing trend in both primary and secondary care being the use of AI-assisted medical transcription tools for transcribing patient appointments. While there are benefits to the use of this technology – active listening, better quality consultations and reduced administration time, particularly for a reducing GP workforce – its greater use does lead to the increased risk of transcription errors and associated claims for compensation from any patients coming to harm, as well as an increased risk of claims based on alleged breaches of data protection laws. Healthcare providers and insurers dealing with any such claims will need to be alive to the ongoing uncertainty as to who has responsibility, or where the accountability lies, when something goes wrong with AI products generally. Given this uncertainty, it is entirely possible that certain jurisdictions will seriously consider the merits of a strict liability regime to deal with claims arising from AI errors. Indeed, this is already happening; in the European Union, for example, the new Product Liability Directive that came into force in December 2024 is a strict liability regime enabling consumers to pursue a claim where a defect in a product has caused personal injury or property damage. The scope of this directive is now wider in scope than previously and specifically includes software and AI.

MOTOR

The increase in vehicle technology will positively impact road traffic claims volumes

Influenced by increasingly strict safety homologation rules within the European Union, expect the percentage of vehicles with Advanced Driver Assistance Systems to continue to increase. These rules require manufacturers to gain approval from a national authority for a vehicle's entire type, regardless of where components are sourced, therefore confirming compliance with safety, environmental, and market surveillance standards. It allows vehicles to be registered and sold across the EU single market which will accelerate the incorporation of advanced safety systems which is expected to lead to a continued reduction in road traffic claims.

DAC BEACHCROFT

Technology
Predictions 2026

The increase in vehicle technology will negatively impact the cost of road traffic claims

Despite the lower claims numbers, claims costs will continue to rise faster than the Consumer Prices Index. Concerns regarding the integrity of electric vehicle (EV) batteries post-collision, and the need to recalibrate Advanced Driver Assistance Systems will result in increased complexity and cost, for both labour and parts. Insurers and the motor repair sector continue to highlight skills shortages for repairing EVs and cars with sophisticated safety systems post-accident. This increases repair times and with it, costs.

POLICY WORDINGS

The ban on ransomware payment in the public sector will drive changes to cyber underwriting appetite

It is likely that the government's proposed ransomware payment ban, impacting public sector bodies and operators of Critical National Infrastructure (CNI), will come into force in 2026 and marks a significant shift in the UK's national cyber policy. The exact scope of the legislation remains to be seen, particularly whether the ban will extend to privately owned organisations within the public and CNI sectors, as well as their suppliers. In response, insurers will likely reassess underwriting appetite to reflect a changed risk exposure where ransom payments are no longer a viable recovery option. The objective of the legislation is to reduce the attractiveness of public and CNI sector targets to ransomware groups. However, this theory is untested and the removal of ransom payments as a recovery option could increase the financial exposures of the sector. In the short term, this could lead to an impact on the availability of cyber insurance capacity, limits of indemnity, and amendments to policy conditions, or the emergence of separate specialised cyber products for public bodies and operators of CNI.

The risk of silent AI will continue to generate product development

Policy wordings are evolving to reflect the increased role of AI in day-to-day business operations. Policyholders, and indeed brokers, continue to seek clarification on the adequacy of their insurance programmes and be keen to see policy wordings affirming AI-related risks. We expect to see more product innovation in the market, as well as insurers seeking to limit or condition riskier AI-related exposures. Policyholders should review policies for AI-specific exclusions, ensure ethical AI practices, and stay informed about how insurers use AI in pricing, risk assessment and claims handling.

POLITICAL RISK, TRADE CREDIT AND POLITICAL VIOLENCE

Drone warfare will lead flight to political violence insurance

The exponential rise of the use of drones in the theatres of combat will raise the awareness (and need) for political violence insurance far beyond the front lines. The increase in use is driven by advancements in AI and lower costs, making them a cheaper and 'safer' alternative to manned aircraft for both surveillance and offensive strikes. Unmanned aerial vehicles have become the main weapon of the war in Ukraine, now accounting for up to 80% of all Russian and Ukrainian casualties. The technology is causing mayhem far beyond the front lines, with Ukraine using quadcopters (drones with four rotors) to mount a devastating attack on airfields deep inside Russia, including one in eastern Siberia some 3,000 miles from Kyiv. But their recent usage demonstrates how neighbouring countries, and insureds therein, are also exposed to the threat of this technology. In September 2025, 19 Russian drones flew over Poland overnight, of which up to four were shot down - the wreckage of 16 were found scattered across the Polish countryside, smashing into homes and damaging cars. It marks the first time Russian drones have been downed over the territory of a NATO state. The provision of political violence cover within a country actively engaged in a war is likely difficult (and expensive). However, drone warfare will mean that those insureds that consider the epicentre of conflict to be far from their property would be well advised to consider their political violence coverage, including whether it extends to perils such as War, Warlike Operations and Hostile Acts of sovereign entities, to name just a few potentially applicable perils.

PRODUCT SAFETY, LIABILITY AND RECALL

UK reform is likely to align with the European Union on product liability

The UK's anticipated product liability reform will likely create some form of alignment with the updated EU Product Liability Directive. Such a move will promote regulatory stability for businesses operating within both jurisdictions. The Law Commission announced a review of the law relating to product liability in July 2025, emphasising technological developments that require an updated regime in the UK. Any legislation introduced because of the Law Commission project and any subsequent government consultation is likely to contain similar provisions to the Product Regulation and Metrology Act. That Act ensures that UK law could be updated to recognise new or updated EU regulations on product safety. Similar provisions in any product liability legislation may consider alignment on issues such as a wider definition of product, the burden of proof, and when a product is considered to be defective.

DAC BEACHCROFT

Technology
Predictions 2026

Expect lithium-ion batteries sold online to be the focus of new regulation

Measures will be introduced to regulate the sale of lithium-ion batteries used in e-scooters and e-bikes via online marketplaces. Much of the discussion surrounding the passing of the Product Regulation and Metrology Act focused on the ability of the government to introduce measures to help with growing safety concerns over fires caused by lithium-ion batteries purchased online. While a private member's bill sought to address this issue, the Product Regulation and Metrology Act now offers the legal basis for specific lithium-ion battery regulations, particularly for e-bikes. Beyond the well-reported concerns around lithium-ion batteries and micromobility, insurers will also need to continue to be mindful of developing risks in other areas. In particular, the use and storage of lithium-ion batteries has been linked to several fires in residential properties, personal and business storage facilities and marine cargo.

National Commission set to regulate AI in healthcare

A new National Commission will help accelerate safe access to AI in healthcare and across the NHS by advising the Medicines and Healthcare products Regulatory Agency on a new regulatory rulebook. With expertise from global AI leaders, clinicians and regulators, the Commission will immediately look at tech that is being held back due to regulatory uncertainty, like AI assistants for doctors. AI ambient voice technology or AI scribes can record and summarise discussions between doctors and patients. This reduces admin and means more people can be seen by clinicians and that they can spend more time focusing on patients. If cutting-edge AI technologies are to be safely and effectively integrated into everyday healthcare, AI regulation must ensure patient safety and public confidence by getting regulation right.

PROFESSIONAL LIABILITY

All professions: Professionals will continue to grapple with the rapid evolution of AI

AI has the potential to reduce the number of mundane tasks junior professionals must deal with, enhance efficiencies and reduce the incidence of human error, which is a significant cause of claims. The advantages are obvious, but they must be balanced against the risks, primarily through safeguards to check outputs. Recent well publicised cases have demonstrated the legal and regulatory risks inherent in using AI that will impact all professional services firms. As AI technology advances, professionals are having to keep pace with its developing capabilities and manage the risks through governance and risk management. Professional service firms should be acting now to assess their risks by developing internal policies, issuing guidance and training to their staff and structuring methods to ensure compliance. Firms will also be considering the cover that their professional indemnity insurance provides, how the policy will respond, for example to multiple errors caused by a failure in the technology, and whether there are any gaps in cover. AI is here to stay and the question therefore is just how we manage the potential risks.

Lawyers: AI remains high on the cost/benefit spectrum for lawyers

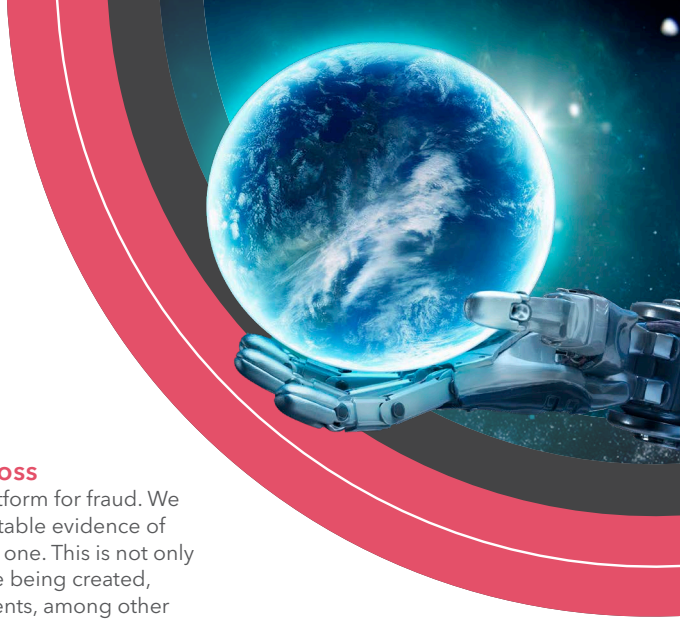
As lawyers continue to adopt AI, we have seen several cases that underline the need for careful governance and risk management. It is obviously imperative that lawyers keep up to date with technological advances and guidance from their regulatory bodies including the SRA and Bar Council. The misuse of AI can lead to negligence claims, regulatory issues and reputational damage. AI is already embedded in many law firms. Its use will only become more prevalent, including by the court and clients. Lawyers will need to review retainers to reflect how AI and clients' data will be used to avoid inadvertent disclosures, data breaches and the breach of client privilege and confidentiality. Leaders of law firms must ensure that all their colleagues who provide legal services understand and comply with their duties when using the AI tools that are available. Lawyers who fail to do so (for example, by relying upon non-existent case citations) risk severe sanctions which will also impact on their firms from a financial and reputational perspective. Supervision of output has never been so important.

Technology professionals: Cyber and AI-related technology and media claims will continue to rise

The ever increasing deployment of AI technology as part of the provision of many types of services will lead to an increase in errors resulting from inadequate checking or review of outputs and resulting claims. This development coupled with the rising fragmentation of technology services provision (where many technology products or services incorporate or rely on products or services from other providers) will increase the uncertainty in predicting risk based on the activities of an insured and bring the importance of properly drafted exclusions and limitation of liability clauses (and their effective incorporation into contracts) once again to the forefront of risk analysis.

DAC BEACHCROFT

Technology
Predictions 2026



PROPERTY

Insurers need to be alert to fraudulent AI-generated evidence of loss

Although AI tools have many benefits for the insurance industry, they also provide a platform for fraud. We have seen an increase in claim submissions that would historically be considered acceptable evidence of loss, but in fact have been created to generate a claim or inflate an otherwise legitimate one. This is not only impacting personal lines, where, for example, AI generated photographs of damage are being created, but also commercial lines, where AI is being used to generate fake invoices and statements, among other things. As access to these AI systems becomes easier, we envisage this trend in fraudulent claims will increase. Insurers need to scrutinise submitted evidence, even from commercial organisations that may on the surface appear successful, legitimate businesses.

REINSURANCE

Silent AI exposures will require reinsurance consideration

As policy wordings in the primary insurance market evolve to address the growing role of AI in business operations, insurers will increasingly look to their outward reinsurance arrangements to ensure that AI-related risks affirmed at the primary level are also adequately covered under their reinsurance programmes. Equally, reinsurers may seek to condition or exclude AI-related risks which may impact how reinsurance claims are adjusted.

SPORTS AND ENTERTAINMENT

Contingency insurers will leverage climate-related technology to price risk and pay claims

Extreme and unpredictable weather – including storms, wildfires, floods and extreme heat – is on the rise due to climate change, and outdoor events and festivals have been hit hard by associated disruptions and costs. Insurance premiums and deductibles have necessarily increased as severe weather claims account for a larger proportion of cancellation claims. Contingency insurers will need to continue to utilise technology, including climate-modelling tools and AI – rather than relying on historical weather patterns which may no longer be reliable – to assess and manage risk. We are likely to see a rise in hybrid policies whereby traditional event cancellation cover is combined with automatic, parametric insurance to compensate risks such as low attendance due to wind, temperature or rainfall.

Contingency insurers will use technology to respond to emerging risks

Across the whole insurance market, investment is being made into technology solutions to improve underwriting models, risk management and claims processes. The contingency market is no exception, with obvious efficiencies and pricing advantages to be gained, for example from using AI predictive modelling to forecast weather-related and other risks. Deployed effectively, technology can also be used to improve the customer experience, for example by offering swift, automatic claim payments via parametric policies. Enhanced data analytics and InsurTech also have the potential to assist with the challenge of calculating ascertained net loss. The contingency market is becoming increasingly dynamic and innovative in using technology to respond to a post- pandemic boom in demand for event insurance.

TRANSACTIONAL LIABILITY

AI-powered solutions are accelerating the M&A process

Although M&A activity has slowed in recent years, the deals going through demand increasingly complex due diligence. Buyers must assess a wide range of factors including the target's exposure to economic and geopolitical volatility, regulatory compliance, tax, environmental, social and governance performance, and litigation risk. AI technologies are now playing a pivotal role in streamlining this process. Advanced AI tools enable enhanced due diligence by rapidly reviewing vast datasets, identifying financial crime and anti-money laundering compliance issues, and flagging inconsistencies or potential risks for further investigation by the buyer and its legal team. This not only improves accuracy and efficiency but also frees up valuable human resources, allowing deal makers to focus on strategic elements such as negotiation and stakeholder engagement. With appropriate oversight, the integration of AI into the M&A lifecycle offers transformative potential, reshaping how transactions are assessed, executed and managed.

DAC BEACHCROFT

Technology
Predictions 2026

Transactional risk insurers must adapt to stay ahead in a competitive market

Challenging market conditions have led to a slowdown in M&A activity, but high-value premiums remain within reach for insurers as buyers seek greater certainty in the volatile deal making landscape. To maintain a competitive edge, transactional risk insurers are evolving their product offerings. The market is responding to growth sectors - notably technology, renewable energy, and life sciences - where emerging risks tied to intellectual property (IP) and AI are central to the target's value and asset base. In these sectors, insurers are developing innovative solutions to address complex exposures, including bespoke coverage for IP infringement and AI-related risks. Buyers are increasingly demanding tailored representations and warranties that explicitly cover these areas, seeking robust protection and risk mitigation as part of the transaction structure. As a result, transactional risk insurance is becoming more sophisticated, with a sharper focus on the unique attributes of cutting-edge technologies.

REPUBLIC OF IRELAND

Demand for cyber insurance and related services will grow in Ireland in the year ahead

It is anticipated that cyber insurance will be an area of growth in Ireland. Regulatory compliance is driving demand (notably NIS2 and the Digital Operational Resilience Act), along with increased media coverage of major breaches. It is expected that more modular policies will be available, allowing businesses to select options such as cover for regulatory fines, third-party liability, and IT provider coverage. The modularity will help businesses align coverage with their risk profiles and compliance obligations. Further it is expected that cyber policies will increasingly address AI-specific risks. Demand for risk mitigation services is also likely to increase to try and prevent incidents. This will include vulnerability scanning of IT infrastructure, employee training, and dark web monitoring. Similarly, predict-and-prevent services will increase with options to include supply chain scanning, employee credential monitoring, and breach simulations.

FRANCE

Generative AI will generate major risks for professional liability and cyber lines in France

The rise of generative AI exposes French companies to a diverse range of risks: errors, discrimination, illicit content and deepfakes are all likely to result through increased use. Early court decisions show that both the designers and end-users of AI will be targeted, even without specific legislation. Insurers must adapt cyber and professional liability policies to cover or limit these new exposures. Further, the growing use of AI to generate deepfakes or manipulate images exposes companies to major legal risks as a result of the actions of third parties. These AI creations raise the prospect of privacy actions, defamation and identity theft. Insurers must adapt media liability, cyber and PI covers to address these new exposures.

GERMANY

Stricter EU cybersecurity regulation to create emerging D&O risks in Germany

The introduction of the NIS2 Directive will create greater liability risks for directors and officers, and increase their risk profile for insurers. The Directive introduces stricter and more detailed technical and organisational cybersecurity requirements for companies in Germany. Although most businesses still do not fall directly within the scope of the Directive, the ongoing trend towards tighter regulation will significantly impact non-binding security standards and any contractually-owed standards of care. Importantly for those in scope, the Directive introduces accountability on the part of directors and other senior managers for ensuring compliance. This takes the form of monetary and other sanctions, which may create additional risks for D&O insurers through coverage issues such as regulatory defence costs and possible financial penalties (such as may be insured). Although the obligations introduced by NIS2 are not new, having already been part of many risk management duties, especially for companies heavily reliant on data processing and digital operations, insurers may seek to ensure that their policyholders are familiar with any obligations.

The AI revolution will drive new risks and new regulation in 2026

Developing and implementing AI technology at all levels of the business will be challenging for general counsel at insurers. New liability claims for damages based on using AI technology should be anticipated. In addition, additional regulatory frameworks should be expected and monitored, again also raising the risk of bringing with them new liabilities.

DAC BEACHCROFT

Technology
Predictions 2026

NETHERLANDS

(Online) consumer protection will increasingly attract attention

Dutch courts are showing a willingness to protect consumers. This is triggered by European law and seen across the legal landscape where disputes with consumers are involved. Often it concerns online transactions: travel, energy contracts, purchases etc. Caselaw shows this trend is also present in real estate where homes are rented out. Claims, or defences, that are based on general terms and conditions get the full attention of the courts. They are, as a matter of course, checked by the courts as to their fairness to the consumer.

SPAIN

Mandatory electric scooter insurance will take effect in January 2026

As part of the reform of the Motor Vehicle Insurance Law, Spain has introduced a mandatory civil liability insurance requirement for electric scooters and other personal mobility vehicles. From 2 January 2026, all personal mobility vehicle owners must have valid insurance. This includes obtaining a 'certificate of circulation' and ensuring the vehicle is registered with the Directorate General of Traffic. The law defines a personal mobility vehicle as a vehicle weighing up to 25 kg and capable of speeds between 6 and 25 km/h. Vehicles exceeding these specifications may fall under different regulatory categories. The introduction of mandatory insurance is expected to impact the insurance sector significantly, as insurers will have to develop specific products or policies for personal mobility vehicles, considering factors such as vehicle type, usage patterns, and risk profiles. Additionally, the establishment of a public registry by the Directorate General of Traffic will facilitate the monitoring and enforcement of compliance.

Supreme Court decision will shift liability in digital fraud cases

In a recent ruling by the Spanish Supreme Court, it was determined that banks are liable for unauthorised transactions resulting from digital fraud, such as phishing or SIM swapping, unless they can demonstrate gross negligence on the part of the customer. This ruling reinforces the quasi-objective liability framework established by Directive 2015/2366 on Payment Services, shifting the burden of proof to financial institutions to demonstrate that the transaction was authorised or that the customer acted with gross negligence. The decision is based on the special duty of care that banks must exercise when, among other matters, opening a bank account (e.g. verifying the ID or the contracting party's information is accurate) or monitoring certain operations (such as unusually timed large transfers by a user). This legal precedent could have significant implications for the insurance sector, particularly regarding policies held by banks. Liability insurers of banks may face an increase in claims related to digital fraud, as banks are more likely to be held responsible. Additionally, insurers should reassess the risks covered and the security measures implemented by banks. Underwriters should consider the adequacy of cybersecurity protocols and banks' incident response capabilities when evaluating risks.

SWEDEN

Expect rising cyber insurance demand in 2026

Cyberattacks are becoming increasingly frequent and severe in Sweden, affecting both businesses and municipalities. Despite being one of the most digitally advanced countries, many organisations remain vulnerable to ransomware, data breaches, and other cyber threats. In December 2023, the prominent Swedish retail chain Coop was hit by a cyberattack that disrupted operations and left payment systems offline for several days. In August 2025, a large-scale ransomware attack compromised systems in numerous municipalities, raising concerns over data breaches and operational disruptions. As these attacks continue, cyber insurance is becoming an essential tool for managing risk. More organisations are expected to adopt coverage to protect operations and recover swiftly after incidents. Implementing basic safeguards, such as response plans and staff training, is becoming standard practice. With digital threats on the rise, the importance of cyber insurance in Swedish risk management will only grow.

UNITED STATES

Increased integration of AI into day-to-day business decisions will similarly increase litigation and coverage risks

AI is becoming increasingly prolific, spanning an increasing spectrum of industries. With that comes a simultaneous increase in AI-related litigation risks. For example, AI companies have been named in numerous lawsuits alleging they infringed copyrights in constructing their large language models. We also foresee malpractice claims against doctors who rely too heavily on AI and misdiagnose patients, and differences in federal and state regulation of employers' use of AI in hiring decisions could lead to an increase in employment discrimination lawsuits. All these developments will have downstream effects on insurance.

DAC BEACHCROFT

Technology
Predictions 2026

BRAZIL

Open insurance could accelerate market innovation

By 2026, the ongoing rollout of Brazil's open insurance framework may foster a wave of innovation and competition across the sector. If data-sharing protocols and interoperability standards are widely adopted, consumers could benefit from more personalised products, easier policy comparisons, and improved movement between insurers. New entrants, including fintechs and insurtechs, might leverage open data to offer tailored solutions and challenge established players. However, the pace and impact of open insurance will depend on regulatory clarity, industry collaboration, and consumer trust in data privacy and security. If these factors align, open insurance could reshape how Brazilians interact with insurance providers and drive broader financial inclusion.

Digital channels are set to boost insurance distribution

Digital channels may become the leading mode of insurance distribution in Brazil, with a growing share of new policies sold and managed online or via mobile apps. This potential shift could be influenced by regulatory support for digital onboarding, the rise of insurtechs, and increasing consumer demand for convenience and transparency. Traditional brokers and agents are likely to respond by offering hybrid digital-human services, while the market may gradually favour seamless, self-service digital experiences. If this trend accelerates, insurers that do not invest in robust digital platforms and data-driven personalisation could risk losing market share to more agile competitors. However, the pace and extent of digital adoption will depend on consumer preferences, regulatory developments, and the ability of incumbents to adapt.

CHILE

New fintech law will promote parametric insurance for earthquakes

In January 2023, Law No. 21,521 came into force, promoting financial competition and inclusion through innovation and technology in the provision of financial services, known as the Fintech Law. This law introduces the concept of parametric insurance and the simplification of the design of policies and settlement procedures. Moreover, the regulator has established a list of risks that can be insured using a parametric model, the variables that activate cover, and the minimum content of insurance policies. We expect this will appeal to the property sector for losses related to natural catastrophes, and, in particular earthquakes, given Chile's history.

New cyber and data protection regulation will drive uptake of cover and notification of losses

While the new cyber regulation has been in place for the last year, the new Data Protection regulation will come into force by the end of 2026, both of which establish standards of protection for systems and data respectively, also requiring notice of breaches and setting out fines and penalties for those who do not comply. Consequently, it is expected that notification of cyber losses to insurers will increase, along with interest in cyber-related insurance by large corporations.

ECUADOR

Data protection enforcement will reshape insurer obligations

Ecuador's Organic Law on the Protection of Personal Data, now fully in force, will significantly impact the insurance sector in 2026. As the national data authority begins active enforcement, insurers will face growing scrutiny over how they collect, store, and process sensitive data - particularly health, biometric and financial information. Non-compliance may lead to reputational damage, fines and regulatory injunctions. Insurers will need to update consent frameworks, automate access requests, and implement robust breach response protocols. Additionally, cross-border data transfers, common in reinsurance and regional claims handling, will require new contractual safeguards.

From cash to claims: E-money will drive embedded insurance uptake

Ecuador's rapid adoption of mobile wallets like Bimo and DeUna! will drive insurers to embed microinsurance and personal accident coverage into digital payment flows in 2026. These embedded offerings, tied to transactions or account balances, will expand protection for underserved populations. However, regulators will face pressure to adapt consumer protection rules, ensure fair disclosure, and define the roles of fintech platforms in distribution. Legal clarity on licensing, data sharing, and cross-border transactions will be crucial. This convergence of finance and insurance marks a shift toward more inclusive, tech-enabled coverage models.

Financial institutions face mandatory cyber resilience requirements in 2026

By 2026, all financial institutions in Ecuador will be required to comply with mandatory cybersecurity standards. The regulator is aligning local regulation with international norms, imposing obligations on data protection, technology risk management, business continuity plans, and cyber incident reporting. This rule will encourage banks and insurers to adopt cyber insurance, strengthening the financial system's resilience against digital attacks and ensuring the continuity of critical operations. The measure demonstrates a regulatory commitment to technological stability and market trust.

DAC BEACHCROFT

Technology
Predictions 2026

Satellite surveillance will become a standard in agricultural claims

In Ecuador, the use of satellite imagery will become standard for verifying agricultural insurance claims, especially in parametric policies. This technology enables validation of climate events like droughts or floods, speeds up payouts, and reduces fraud. Insurers will need clear frameworks on data privacy and collaboration with technology providers. Initiatives such as CampoSeguro indicate that Ecuador is following the global trend toward agricultural digitalisation, combining operational efficiency and transparency for both farmers and insurers.

PERU

AI will expand both in depth, tackling empathy, and in reach, accessing rural areas

AI will not only automate repetitive tasks but will also advance toward understanding emotions and contextual information, turning chatbots and virtual assistants into more empathetic, accurate and efficient tools. Businesses will increasingly rely on AI to customise services and enhance user experience, while workplaces will benefit from AI-driven platforms that optimise workflows in real time. These developments will foster productivity and innovation across multiple sectors. At the same time, Peru continues to expand its digital infrastructure to improve internet access in rural and underserved regions, which will open new opportunities for telemedicine, remote education, and e-government services. Strategic alliances, such as Huawei's collaboration with the government on mobile classrooms for digital literacy, will further narrow the digital divide.

Cyber insurance will become a critical pillar of risk management in Peru

In 2026, the rise in cyber threats and digital dependence will push Peru to adopt stronger cybersecurity frameworks and to expand the market for cyber insurance policies. Companies in banking, telecommunications, and critical infrastructure will increasingly seek cyber risk coverage to safeguard against ransomware, data breaches, and business interruption caused by digital attacks. These policies will become essential not only to mitigate financial losses but also to strengthen corporate resilience and regulatory compliance. Additionally, government institutions will be urged to enhance co-operation with the private sector in order to build more robust cyber defence mechanisms. Cyber insurance is expected to evolve into a critical pillar of risk management, particularly as businesses accelerate their digital transformation and AI adoption.

AUSTRALIA

Cyber class actions and privacy tort will escalate liability exposure

In 2026, insurers face mounting exposure from cyber-related class actions, driven by high-profile breaches such as Medibank, Optus and Latitude. Plaintiffs are increasingly seeking damages for emotional distress, reputational harm, and costs incurred in mitigating identity theft. Quantifying loss remains complex, often relying on market-based causation (e.g. share price drops) or aggregated damages across affected groups. The introduction of a statutory tort for serious invasions of privacy adds a new layer of risk. Individuals can now sue for misuse of personal data or intrusion upon seclusion, with courts empowered to award damages, injunctions, and apologies. This tort broadens the pool of potential defendants and may trigger claims under cyber, D&O, and professional indemnity policies. Insurers must reassess coverage wording, exclusions, and aggregate limits, while preparing for increased litigation and regulatory scrutiny. Proactive client engagement and scenario modelling will be essential to manage this rapidly evolving liability landscape.

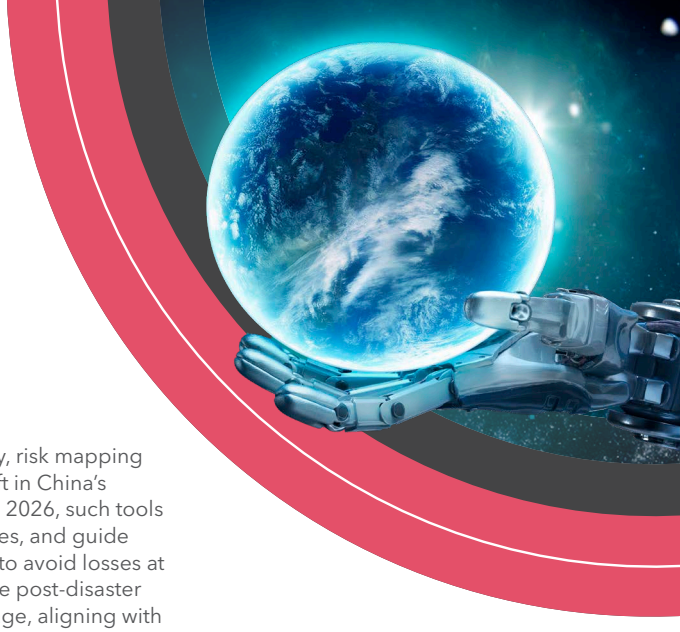
MAINLAND CHINA

Low-altitude economy insurance will expand

In 2025, major Chinese insurers launched products covering drones and other low-altitude aircraft, reflecting Beijing's policy drive to develop the 'low-altitude economy'. With strong regulatory support for drones, logistics applications, and urban air mobility, the insurance sector is moving quickly to roll out liability and property covers tailored to this emerging field. Likely claims scenarios include bodily injury to third parties, property damage in congested cities, and product liability linked to drone components or software systems. A systemic failure in air-traffic management could result in multiple simultaneous incidents, exposing reinsurers to concentrated, catastrophe-style losses. Going forward we expect litigation to test the scope of exclusions relating to 'experimental flight' activities, cyber-hacking, and other technology-driven risks. Courts may also face challenges in allocating liability where responsibility is split between operators, manufacturers, and system providers. The rapid expansion of this sector underscores both the opportunities for insurers to capture growth and the heightened legal and underwriting complexities that will shape market practice.

DAC BEACHCROFT

Technology
Predictions 2026



Catastrophe risk management will be digitised

In 2025, Ping An P&C launched the EagleX Global platform, integrating satellite imagery, risk mapping and AI-powered alerts. Its early success during the Beijing hailstorm demonstrates a shift in China's insurance sector from reactive compensation to proactive prevention. Looking ahead to 2026, such tools are set to become mainstream, enabling insurers to mobilise adjusters faster, cut disputes, and guide businesses and households to act early - whether closing factories or moving vehicles - to avoid losses at source. The impact reaches beyond claims efficiency: by reducing the need for extensive post-disaster reconstruction, EagleX also helps conserve resources and mitigate environmental damage, aligning with the broader push for green development. Reinsurers are likely to make these capabilities a precondition for capacity. Insurers, in turn, must strengthen governance through customer consent, encryption and deletion protocols. Those able to deliver a 'detect–decide–deploy' cycle within 24–48 hours will stand out not only on cost and client retention, but also on their environmental and social credentials.

HONG KONG

New laws will protect critical infrastructure in Hong Kong

Hong Kong recently saw the passage of the Protection of Critical Infrastructure (Computer System) Ordinance into law, the provisions of which will come into effect on 1 January 2026. The new laws aim to protect local infrastructure in certain sectors designated as critical. Banks and financial institutions (in addition to those operating in other prescribed sectors) will be required to implement measures to prevent and report security breaches. Failure to do so may attract a fine of up to HK$5 million (US$640,000). We expect increased regulatory activity in encouraging organisations to bolster the security and reporting any breaches of their computer systems in 2026.

SINGAPORE/SOUTHEAST ASIA

Higher demand for electric vehicles is likely to result in an increase in product recalls/ product liability claims

Attractive government incentives, falling prices and a global focus on decarbonisation is resulting in an ever-increasing demand for electric vehicles (EVs), with the United States and Europe in particular seeing significant growth in sales. In an attempt to meet this demand, new entrants to the EV manufacturing market are using developing technologies to produce EVs quickly and at significantly reduced prices. Production of EVs (and EV parts) is likely to remain predominantly in Asian jurisdictions such as China, Taiwan and South Korea, requiring them to continue to balance this high demand against the increasingly stringent safety standards of the West. While the EV manufacturing market continues to develop rapidly, we anticipate an increase in product recalls and product liability claims, particularly in the United States and Europe. With many EV manufacturers supplying parts to multiple car manufacturers, the risk of significant claims arising out of a product defect substantially increases. In light of this rise in EV-related product recalls and product liability claims, we are seeing insurers taking a more cautious approach to risk by offering higher premiums or different terms for those products sold to the United States and Europe.

Developments in AI will lead to more sophisticated cyberattacks

With the advancement of AI, we expect to see an increase in the sophistication of cyberattacks. Gone are the days of simple phishing emails sent to unwitting employees asking them to change their password, which often contain obvious errors that are easily detected. Threat actors are now using AI to create sophisticated attempts, such as deepfakes, to deceive employees into handing over their credentials. One recent example was an employee who transferred large sums of money following receipt of a deepfake video showing the company's senior executive instructing employees do so. We also anticipate that threat actors will use AI to assist with password decoding and data mining of large datasets to determine the value of the data that they have accessed and possibly exfiltrated. Datasets that were traditionally thought to be difficult to translate in Asia, e.g. Japanese or Korean, can now be easily and accurately translated with the improvement in AI-assisted translation tools. As a result, we anticipate that through the use of AI, attacks based on deception and abuse of confidence will become more sophisticated and increasingly convincing, which is likely to result in an increase in cyber claims of this nature.

Scan here to view our full suite of predictions for 2026.

insurance.dacbeachcroft.com
dacbeachcroft.com
Connect with us: DAC Beachcroft LLP
Follow us: DACBeachcroft