BEALE&CO

INSURANCE TRENDS 2026

REGULATORY SHIFTS AND EVOLVING EXPOSURES

International Construction and Insurance Law Specialists

INTRODUCTION

Another year on, the pressures shaping the market have not only persisted but become increasingly complex

In last year's report, we highlighted the economic headwinds and regulatory pressures shaping the market. Twelve months on, those challenges remain firmly in place, albeit with new considerations. Conflicts around the globe, simmering political tensions, persistent inflationary pressures, and evolving regulatory frameworks continue to create uncertainty for businesses and insurers alike. At the same time, technological disruption and sustainability imperatives are accelerating change across multiple sectors.

Predicting the issues that will dominate the market in the coming year remains difficult. However, as our specialists have contributed to this report, several clear trends have emerged. These include the growing complexity of megaprojects, the rapid expansion of data centre developments, and the continued prevalence of remediation claims under the Building Safety Act. Increasing scrutiny from regulators across the professions is placing greater emphasis on robust governance frameworks and clearer accountability for individuals and firms. Workforce shortages and productivity constraints are driving innovation, while digital transformation and AI adoption present both opportunities and new exposures. In parallel, ESG scrutiny and climate-related litigation are intensifying, reshaping governance expectations and liability risk.

The insurance market itself reflects these dynamics. While capacity remains strong and pricing competitive in many classes, underwriting strategies are evolving to address long-tail liabilities, regulatory risk, and technology-driven exposures. Wordings are being refined to capture emerging risks, and insurers are investing in technical expertise to navigate increasingly complex claims environments.

This report provides a comprehensive analysis of these and other developments and their implications for insurers, brokers, and insureds. It is the result of significant effort from our sector experts, and we extend our thanks to all contributors for their insight and commitment in producing this forward-looking review.

INTRODUCTION

Key Themes for 2026

REGULATORY AND LEGISLATIVE PRESSURE

Across multiple sectors, regulation is tightening. The Building Safety Act continues to reshape liability in construction, while new rules on fraud prevention, sustainability disclosures, and anti-greenwashing are increasing compliance burdens for directors and officers. In financial services, the FCA's Consumer Duty and expanded non-financial misconduct rules will demand stronger governance and cultural oversight. These developments are driving demand for broader regulatory cover and more nuanced policy wordings.

TECHNOLOGY AND AI RISKS

AI adoption is accelerating across industries, from construction robotics and modular manufacturing to digital underwriting and automated financial advice. While these innovations promise efficiency and resilience, they introduce new exposures, ranging from data governance failures and algorithmic bias to AI-washing claims and cyber vulnerabilities. Insurers and insureds alike must adapt to manage these risks through robust governance, clear contractual allocation, and updated insurance solutions.

ENVIRONMENTAL AND ESG SCRUTINY

Climate-related litigation and sustainability reporting obligations are moving from emerging to mainstream risk drivers. The UK's Sustainability Disclosure Requirements and anti-greenwashing rules, combined with CMA enforcement powers, are increasing liability for inaccurate or misleading ESG claims. In construction, net-zero targets and whole-life carbon assessments are influencing tender outcomes and project viability. Boards must embed ESG into core strategy to avoid regulatory and reputational fallout.

MARKET CONDITIONS AND CAPACITY

The insurance market remains soft across many classes, with abundant capacity and competitive pricing. Whilst favourable for consumers, the current environment brings its own challenges for the market: pressure on underwriting discipline, concerns over long-term sustainability, and heightened exposure to large correlated losses in sectors such as construction and financial lines. Insurers are responding by refining wordings, investing in technical expertise, and adopting more data-driven approaches to risk selection.

Peter Sewell

Peter Sewell,
Partner

EXECUTIVE SUMMARY

Here's a summary of our key insurance trends and predictions across the sectors for the next 12 months.

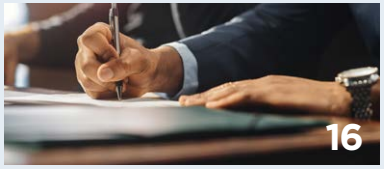
Click on a market area to read our full analysis.

CONSTRUCTION

- Megaprojects are growing, along with their risk.
- The data centre boom is redefining infrastructure demand, and its pressures need to be alleviated in 2026.
- Remediation claims are expected to remain prevalent.
- The Building Safety Regulator and the Gateway Process remain a work in progress.
- Workforce and productivity limitations are hitting the industry, but in turn are fuelling innovation.
- Digital transformation is shaping the industry.

SURVEYORS

- Extended limitation periods under the Building Safety Act 2022, and the Supreme Court ruling in URS Corporation Ltd v BDW Trading Ltd increase the risk for surveyors.
- Bratt v Jones puts the spotlight on the legal basis and justification for the margin of error in surveyor valuations. The margin of error may very well come under attack in the future.
- RICS launched a public consultation in August 2025 on proposed updates to its Home Survey Standard.
- New statutory regimes - including the Renters' Rights Act, Awaab's Law, Martyn's Law and tightening energy performance standards - expand advisory obligations and risk.
- Minimum Energy Efficiency Standard and wider energy-performance reforms point to tighter expectations for non-residential properties.
- Increased reliance on AI brings risks of technical errors and cybersecurity vulnerabilities, with new RICS' standards taking effect in March 2026.



SOLICITORS

- The solicitors' PI market is expected to remain soft for the first part of 2026.
- Expect tighter SRA controls in respect of high-volume claims.
- There will be greater pressure to evidence substantive supervision of unqualified legal staff following the judgment in *Mazur v Charles Russell Speechlys.*
- Reports to the SRA about solicitor misconduct have increased significantly. The SRA will continue to clamp down on persistent weaknesses in AML compliance.
- AI risks include error in the form of AI 'hallucinations', cyber-crime, and data breaches.
- In cases such as *Ayinde v London Borough of Haringey,* the Courts have made it clear that AI should not be used by lawyers in court cases without thorough verification with potential serious consequences if they fail to do so.

ACCOUNTANTS & AUDITORS

- More audit-related claims likely due to economic pressures and increased corporate insolvencies.
- The Financial Reporting Counsel released its proposals for its accelerated procedure to resolve breaches of auditing standards.
- Growing liability from AI-washing, misuse of AI tools, and cyber breaches, with regulators demanding greater scepticism, documentation, and understanding of AI in audit and accounting work. Cybercrime drives demand for cyber insurance.
- Valuation errors in deals remain a key exposure for auditors and accountants, while growing consolidation among firms is increasing conflicts of interest and limiting work opportunities.
- With expanded responsibilities resulting from the Economic Crime and Corporate Transparency Act 2023, it is prudent to tighten engagement terms and verification procedures.
- Claims over inadequate or inaccurate advice on Research and Development Relief are not abating.

EXECUTIVE SUMMARY

INSURANCE BROKERS

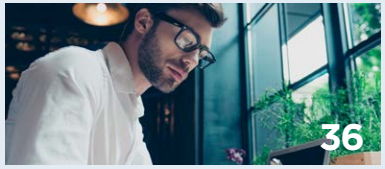
- Broker remuneration is emerging as probably the most significant risk, driven by the FCA's Consumer Duty.
- Detailed record-keeping is needed to demonstrate that the advice provided was suitable for the client's specific demands and needs.
- Rapid growth in MGAs may be creating instability. Delegated authority reviews are uncovering widespread breaches.
- With the Economic Crime and Corporate Transparency Act 2023's 'failure to prevent fraud' offence now in play brokers need to provide clear advice on fraud and D&O cover.
- As personal engagement decreases and reliance on AI grows, brokers need to ensure robust human verification processes remain in place, especially at policy renewal.

DIRECTORS & OFFICERS

- The Economic Crime and Corporate Transparency Act 2023's new "failure to prevent fraud" offence sharply increase corporate exposure, driving heightened insurer scrutiny of fraud controls, identity-verification compliance and director transparency obligations.
- Regulators are escalating action on greenwashing, ESG misstatements and workplace-culture failings.
- AI-related mismanagement, biased outputs, data breaches and "AI-washing" claims are emerging as key D&O risks amid tightening cyber-oversight expectations.
- Persistently high insolvency levels are fuelling more wrongful trading, misfeasance and preference claims— these are often litigation-funded.
- The Building Safety Act's expanded director duties, BLOs/RCOs, long limitation periods and intensified scrutiny of construction practices create significant personal exposure for directors, with building safety likely to remain major driver of 2026 D&O claims.

INDEPENDENT FINANCIAL ADVISORS

- Rising FOS award caps increase insurers' exposure, but new fees for claims management companies are reducing low-value claims, shifting the landscape toward fewer but potentially higher-severity cases into 2026.
- Pension complaints remain high, driven by service-quality issues, misaligned advice, and ongoing Defined Benefit Pension Transfers/ British Steel Pension Scheme activity.
- The Consumer Duty and Advice Guidance Boundary Review will intensify FCA scrutiny on suitability, fair value and record-keeping, increasing liability risks for IFAs unable to evidence tailored, outcome-focused client support.
- A selective but soft PII market will reward proactive risk management, with heightened attention on pensions/complex investments and the adequacy of policy limits for clustered claim exposures.



FINANCIAL INSTITUTIONS

- Financial Institutions face heightened cyber and AI-related exposures, requiring strengthened resilience, integrated governance, and robust controls.
- The growth of AI washing and weaknesses in AI governance frameworks are creating increasing regulatory, litigation and disclosure risks.
- Rapid technological and digital innovation is accelerating competitive pressure, exposing incumbent institutions to strategic and operational risks if they fail to adapt at sufficient speed.
- Financial Institutions must enhance risk management and regulatory engagement to withstand greater supervisory intervention and increased personal accountability for senior leaders.
- The Financial Institutions insurance market is stabilising into 2026, with increased competition and falling premiums, requiring insurers to stay alert to evolving exposures to maintain balanced portfolios.

EDUCATION

- Funding and resource pressures heighten operational strain and increase the risk of complaints and claims.
- Special Educational Needs and Disabilities continue to represent a major concern and a key area for potential claims.
- Schools' disciplinary procedures before the High Court in 2025.
- Education institutions are increasingly attractive targets for cyber-attacks.
- AI presents benefits and risks.
- Student welfare and mental health remain in focus. There is a clear direction of travel towards institutional accountability for protecting students' wellbeing.

EXECUTIVE SUMMARY

ENVIRONMENTAL

- Environmental and green-claims scrutiny intensifies, with greenwashing, and water-sector enforcement driving higher liability exposure, tighter policy wording, and increased D&O/PII risk for regulated sectors.
- Mandatory sustainability reporting is expanding, increasing directors' liability, regulatory enforcement, and reputational risk for inaccurate or incomplete environmental disclosures.
- PFAS has become a major insurability challenge, as global litigation, UK regulatory attention, and high remediation costs shift exposures from emerging to material risk.
- Lithium-battery lifecycle risks grow, with contamination, fire/explosion hazards, and recycling failures creating the potential for new environmental liabilities and tighter regulation.

HEALTH & SAFETY

- In 2024/25, 40.1 million working days were lost due to work-related ill health or injury, with mental health and musculoskeletal disorders being the leading causes.
- The HSE will conduct 14,000 proactive inspections in 2025–2026, focusing on occupational health risks and using AI to target interventions, with construction under increased scrutiny.
- Updated sentencing guidelines for Very Large Organisations allow courts to impose fines outside standard ranges, reinforcing accountability for health and safety breaches.
- The Building Safety Act 2022 and the Building Safety Regulator are driving stricter compliance for high-risk buildings, while off-site construction introduces new safety challenges.
- Technology such as wearables, AI monitoring, and predictive analytics is becoming integral to compliance, with regulators and insurers increasingly expecting adoption.

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE

- Regulatory scrutiny on ESG is intensifying, with new UK rules (Corporate Governance Code, SDR/SRS, FCA anti-greenwashing, CMA fining powers, PRA expectations) requiring stronger controls, evidence-based claims, and more robust climate-related reporting.
- The Procurement Act 2023, which came into force in 2025, requires businesses bidding for public contracts to demonstrate strong ESG credentials to be successful.
- Economic strain and structural challenges hinder ESG progress in construction.
- ESG capability gaps are constraining governance quality, with SMEs particularly struggling to resource ESG demands across supply chains.
- Boards must embed ESG into core strategy and risk management, treating climate, sustainability and social data with the rigour of financial reporting, strengthening internal controls, and pre-clearing high-risk disclosures to avoid regulatory and reputational exposure.

WARRANTIES AND INDEMNITIES

- The increase in M&A activity around the world means that this is a product which is increasing in popularity and uptake.
- This has brought about new entrants into the market and increased capacity which means that insurers have had to react accordingly in relation to pricing structure, premiums and the scope of cover available.
- As with other classes cybersecurity, regulatory scrutiny and ESG are all areas from which claims are likely to emerge against W&I policies.

CYBER

- The cyber threat landscape is continuously evolving, with new vulnerabilities and attack methods emerging regularly.
- We expect an increase in cyber-crime as the use of AI lowers the barrier of entry to novice cyber criminals.
- Unauthorised use of AI in the workplace significantly increases potential exposure.
- Robust third-party risk management is imperative as cyber-criminals are increasingly targeting third-party suppliers because they often have weaker security defences than the large companies they serve.
- We anticipate a large-scale review of cyber cover for losses, and an increase in demand for cyber insurance cover, following some high-profile and very costly cyber-attacks in 2025.
- The higher levels of ICO fines compared to previous years is signalling a firmer stance on UK GDPR security failings.

EXECUTIVE SUMMARY

POLITICAL VIOLENCE

- More businesses are aware of the existence of PV policies and are actively looking to have cover in place in the event of an incident of civil unrest.
- The market is expanding, as is the scope of cover insurers are willing to offer.
- Geopolitical issues such as the rise of populist regimes, increases to the cost of living, the wealth gaps and a growing and deep anxiety about the climate and environmental crisis are contributing factors to the number of incidents seen around the world which might trigger a PV policy.
- Businesses need to work with their brokers to consider the risks which might arise, plan contingencies where possible and try to ensure sufficient cover is in place should the policy need to be called upon.
- Whilst traditionally this was a product which was sought only by global, multi-national companies, more and more SMEs are seeking PV policies to guard against the risks posed.

REGIONAL TRENDS: SCOTLAND

- Expected increase in claims defended on prescription (time-bar) grounds.
- Recent Court of Session rulings clarify Section 6(4).
- Prescription likely to remain a key battleground with early debates expected to save costs.
- Anticipated rise in historic cladding claims with challenges in sourcing evidence and witnesses.

REGIONAL TRENDS: IRELAND

- **Law Society Regulatory Authority's ("LSRA") Annual Report 2024:** Complaints up 14%, signalling potential Professional Indemnity claim increase against solicitors; early insurer intervention can prevent escalation.
- **Kirwan v Connors [2025]:** Clear timelines for inactivity improve strike-out certainty and reduce costs but may trigger claims against plaintiff solicitors.
- **Cyber Insurance:** Rising cyber-attacks and evolving regulation create strong growth opportunity amid low SME uptake.
- **Data Centres:** Rapid expansion and complex risks drive premium growth, specialist underwriting needs, and innovation opportunities.
- **Health & Safety:** New regulations and stricter standards increase liability exposure and demand for proactive risk engineering.

REGIONAL TRENDS: MIDDLE EAST

- Cyber threats in the GCC are rising sharply so demand is increasing although the market is quite saturated and soft.
- In the GCC, there has been increased claims activity for D&O stemming from distressed companies, investor claims, regulatory investigations and shareholder suits.
- The engineering sector in the GCC is under significant pressure (cost-inflation, supply-chain delays, project delays) which increases design/schedule risk and thus PI exposure.
- Regulatory challenges remain an important consideration, especially with regulators such as the DFSA keen to show its teeth and beginning to issue significant fines against both entities and individuals for non-compliance with regulations, particularly in the banking and insurance sectors.
- The downward pressure on rates in 2025 for financial & professional lines indicates improved capacity and underwriting conditions.

REGIONAL TRENDS: CANADA

- Canadian exposures are being reshaped by increased litigation activity, particularly securities and class actions.
- Regulatory and AML expectations are tightening, raising compliance and enforcement risks for financial institutions.
- The Office of the Superintendent Financial Institutions ("OFSI") is driving heightened operational-resilience requirements across banks, insurers, and other financial entities.
- Persistent cyber-related operational losses continue to compound risk profiles for Canadian financial lines.
- There is potential for more complex multi-forum claims, higher defence costs, and deeper regulatory-remediation engagement.

CONSTRUCTION

Last year we discussed widespread economic difficulties and the high level of insolvencies in the construction industry. This year, there is only likely to be a marginal improvement, despite the government's focus on housebuilding and infrastructure. Such insolvencies continue to cause project disruption, leading parties to seek to review, suspend or terminate contracts, or withhold payments – a big driver of disputes. This is leading to a growing use of Building Liability Orders (BLOs) under the Building Safety Act 2022 and an increase in claims under the Third Parties (Rights Against Insurers) Act 2010.

The year ahead will continue to be challenging for the construction industry as it grapples with the issues discussed below, against a background of a soft PII market.

MEGAPROJECTS ARE GROWING

Project size in terms of value is on the rise. Since 2010, the number of 'megaprojects', defined as projects costing USD 1 billion or more, has increased by 280% (200% in the UK). At their core, megaprojects are large-scale, transformative undertakings marked by high complexity and the need for extensive coordination. They demand substantial time and financial investment - often spanning more than five years - and rely on the need for precise, multidisciplinary collaboration.

Policy-driven spend on infrastructure, energy transition and advanced manufacturing is a big driver: grid modernisation, semiconductor fabs, battery plants, offshore wind, etc.

Done well, megaprojects can be profitable, long-duration business that also aligns with insurers' commercial strategies. Done badly, they become a source of large correlated losses, costly protracted multi-party disputes, and capital strain.

Megaprojects are notoriously challenging to execute successfully.

Estimates suggest that nine out of ten megaprojects exceed their budgets, often by more than 50% in real terms, and completion for most is significantly late. Moreover, these cost overruns are frequently accompanied by substantial shortfalls in expected benefits, leaving projects far from meeting their original goals.

Megaprojects are notoriously challenging to execute successfully. The cross-industry nature of these projects means they operate within a complex ecosystem of interconnected organisations, suppliers and policy makers. Political (elections, policy reversals), social, technical, environmental regulation and organisational factors play a significant role in their success or failure. There is heavy dependence on technology (digital controls, operational technology, information technology (IT), modular methods, new materials etc.). Some of the 'on-the-ground' root causes of poor outcomes include the following: contractual misunderstandings, insufficient risk and performance management, optimism bias, supply-chain and execution issues, lack of sufficient skilled workers and decision-making, and procurement processes not having the speed and scale required.

The urgent need for industry transformation in megaprojects

is driven by chronic issues of cost overruns, delays, and poor productivity, coupled with modern demands for sustainability, climate resilience, and technological integration.

These projects require a much more data-driven, engineering-led, partnership-oriented underwriting approach than in 'traditional' construction. It may therefore be prudent for insurers involved in these projects to invest in technical and analytical capability - build in-house, or partner with, expertise in areas such as engineering, delay analysis, climate science and cyber-physical risk.

DATA CENTRE DEVELOPMENTS

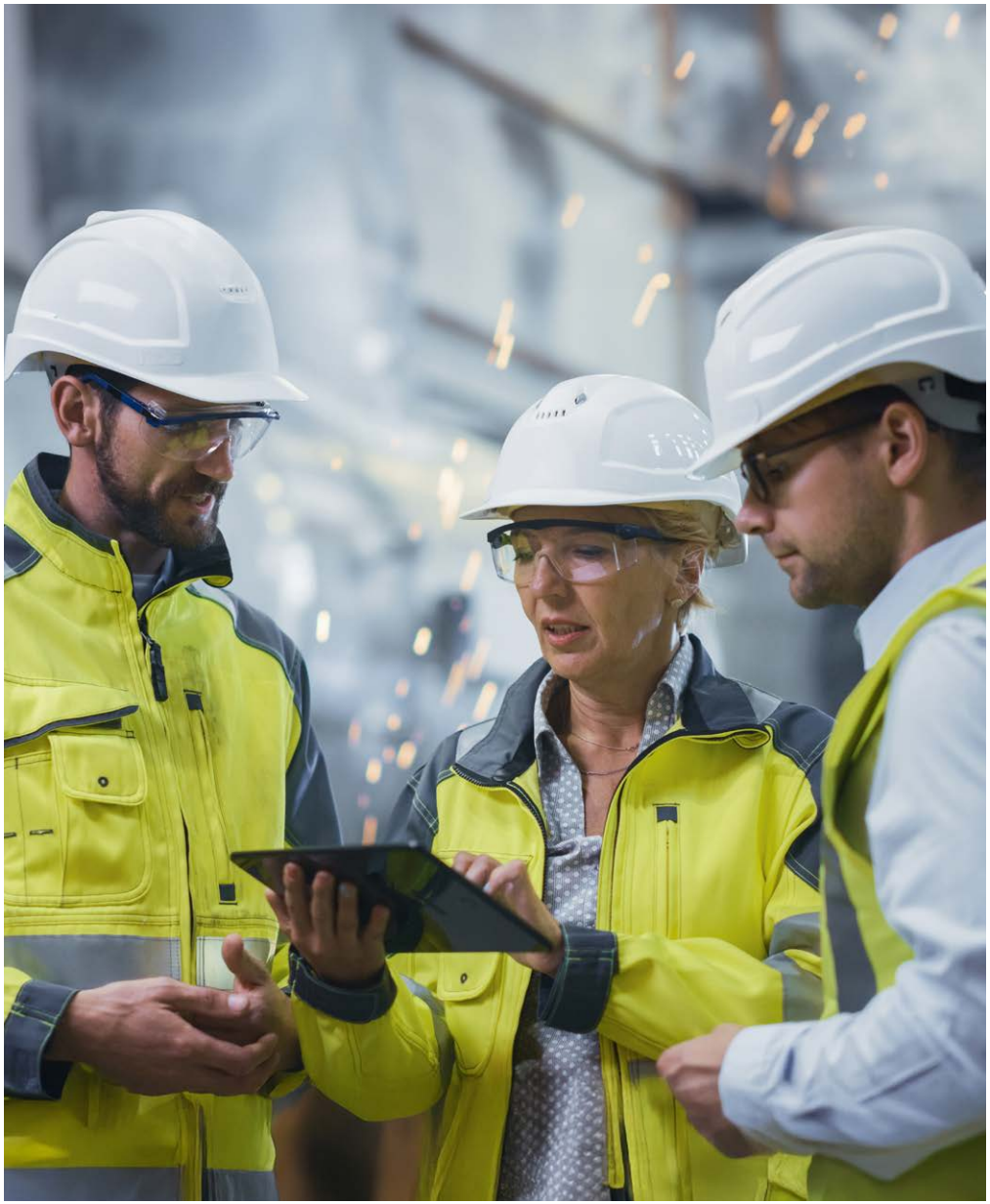
UK data centre development is in a steep growth phase, driven by cloud, AI and financial-services demand. London is still the dominant hub.

The UK data centre sector is set to grow to £13.69 billion in 2026. The growth of 'edge computing' and low-latency applications (those that require micro-minimal delays and therefore need centres that are close) are boosting a demand for smaller, well-distributed, data centres.

A series of obstacles across the construction lifecycle of a data centre are causing design and delay issues. The power-supply bottleneck is driving contractors to work with systems they are not experienced with (complex power backups and generator systems) and whose operations are largely out of their control; delays in power connections and a reliance on temporary solutions are fertile ground for claims. Studies suggest UK data centre power demand could double or more by 2030, outpacing new power generation and creating planning flashpoints over land, energy requirements and potential infringement on sustainability commitments. Data centre servers are high-performance machines that produce a great deal of heat, which in turn requires substantial energy for cooling to prevent overheating, downtime, and potential data loss.

UK data centre development is in a steep growth phase, driven by cloud, AI and financial-services demand.

There are also ongoing concerns with the water consumption of these mega facilities. A UK government report suggests that a 100MW hyperscale facility can consume around 2.5 billion litres of water a year (the same as around 80,000) people. Recycled water systems and efficient liquid cooling technologies are being pushed to reduce consumption and emissions. These innovations generally



lead to higher initial costs, increased design complexity, and longer project timelines, but offer substantial long-term operational and sustainability benefits.

JCT Design & Build (D&B) and FIDIC Yellow remain popular contracting options. However, they are often insufficient for data centre construction because they struggle to adequately address these projects' complex, technology-driven requirements, particularly around performance metrics, risk allocation, and intellectual property (IP).

The UK construction sector continues to grapple with its most severe labour shortage in decades

REMEDIAL AND DEFECTS CLAIMS ARE STILL PREVALENT

Remediation of life-critical fire safety defects continue to dominate the agenda across the UK's built environment. Current government data estimates that 1,844 residential buildings still contain such defects, with an anticipated £3.9 billion required to bring them up to standard. Despite sustained regulatory and political pressure, only around 22% of affected buildings have completed remedial works and achieved building control sign-off. There remains a large backlog of Gateway 2 applications. These delays are impacting project viability, financing and start dates. At the same time, many insurers are once again offering full fire safety cover, signalling a measure of restored confidence in the post-Grenfell risk landscape. However, the shift presents its own underwriting challenge: insurers must now assess layered and often uncertain exposures associated with historic defects, complex contractual webs, and evolving statutory liabilities.

In the remediation context, the Supreme Court's recent decision in **URS Corporation Ltd v BDW [2025] UKSC 21** is expected to prompt more proactive remedial works by contractors and developers as they have the comfort of knowing that they can then recover losses from those further "downstream". This may also encourage earlier settlement, potentially reducing the volume of protracted defects litigation. Insurers will be watching closely to understand how these recovery actions translate into future claims dynamics.

Insurers writing UK construction risks must continue to anticipate a complex, evolving liability environment.

THE WORKFORCE CRISIS

The UK construction sector continues to grapple with its most severe labour shortage in decades. In addition, apprenticeship uptake and young entrants were both down in 2025. The issue is compounded by a reduction in foreign labour. It is anticipated that 251,500 additional workers are required by 2028 to meet the government's infrastructure commitments and house building targets.

The impact of the UK construction labour shortage includes increased costs, project delays with cost overruns, hindered housing and infrastructure targets, heightened competition for talent, and risks to safety and quality. These are classic precursors to PI claims.

INNOVATION

Workforce and productivity limitations are also fuelling innovation.

Construction robotics, automation, and off-site digital manufacturing are transforming the industry by moving repetitive and dangerous tasks to controlled factory settings, which allows for higher quality, faster assembly, and improved safety. Key technologies include off-site prefabrication, modular construction, and 3D printing in factories. Production in a controlled environment allows for higher precision and less waste.

The time and resource efficiency of modular construction is seen as a leading way to combat the skills and labour shortage. The modular market is expected to grow by 5.8% in 2026 and these construction methods are becoming more mainstream in the housing, healthcare and education sectors.

DIGITAL TRANSFORMATION AND AI ARE SHAPING THE INDUSTRY BUT COME WITH RISKS

Most major construction insureds are now integrating connected devices, robotics, BIM-enabled collaboration, and cloud-based project management platforms to improve efficiency, reduce errors, and enhance real-time visibility across supply chains. This shift is creating richer operational data, enabling more accurate risk profiling and early identification of project stressors such as delays, design clashes, and cost overruns.

Machine-learning tools are being deployed to predict equipment failures, assess structural performance, and analyse project documentation for compliance gaps. On-site, computer-vision systems are monitoring worker behaviour, safety compliance, and quality of work, generating audit trails that can assist in claims defence and subrogation. In underwriting, AI-driven assessment of digital project data can support more granular pricing and bespoke policy structures.

However, the increasing reliance on interconnected systems also introduces new exposures. Data quality, contractual allocation of digital responsibilities, and AI-related transparency issues may create uncertainty in liability disputes. Compliance with confidentiality, data protection and contractual obligations is paramount when using AI.

For insurers, the sector's digital evolution offers both enhanced risk insight and emerging categories of loss. Understanding how their construction insureds capture, govern, and share digital information will be central to future underwriting strategies, policy wording, and claims handling.

CONCLUSION

The construction sector faces another pivotal year. Persistent economic pressure, expanding megaproject complexity, rapid data-centre growth, regulatory bottlenecks and workforce shortages are reshaping risk across the market. At the same time, digital transformation and AI offer powerful opportunities - tempered by new technical and cyber exposures. Insurers that deepen technical capability, embrace data-driven insight and adapt to evolving liabilities will be best positioned to navigate volatility and support a more resilient built environment.

To discuss how any of these issues might affect you, please contact

Ian Masser
Partner
+44 (0)20 7469 0439
i.masser@beale-law.com

Peter Sewell
Partner
+44 (0)20 7469 0484
p.sewell@beale-law.com

SURVEYORS

There was a continuation of the softer Professional Indemnity Insurance ("PII") market in 2025 due to increasing capacity, more MGAs and competitive rate reductions. We expect favourable conditions to persist into early 2026, though not uniformly for all surveying activities and not necessarily for long-tail risks linked to building safety.

Underwriters are differentiating more sharply by discipline, claim type and project profile. Property valuation for mortgage purposes with clear processes is likely to remain readily insurable; complex fire-safety advice, external wall system sign-off or high-rise work will continue to attract closer scrutiny, even where cover is available. This is because of longer limitation periods due to the Building Safety Act 2022 ("BSA").

These changes are reflected in the RICS' updated PII Minimum Policy Wording which came into effect on 1 July 2025. Please see our article here for more detail.

Below we discuss other key 2025 developments and claims trends.

THE BSA AND LIMITATION "LONG TAIL"

The BSA significantly (and retrospectively) extends limitation periods for claims related to building defects, allowing claims to be brought for up to 30 years in respect of work carried out before 28 June 2022 (the date the BSA came into force), and up to 15 years for work done after that date (section 135 of the BSA). This is a significant change from the former six years from the completion of a dwelling under section 15 of the Defective Premises Act 1972 ("DPA").

In 2025 the Supreme Court in **URS Corporation Ltd v BDW Trading Ltd UKSC/2023/0110** confirmed how these extended periods enable recovery paths (including contribution) that previously would have been time-barred, underscoring insurers' and professionals' long-tail exposure. We expect these dynamics to remain central in 2026. For surveyors, the key takeaway for 2026 is that claims latency is longer, record-keeping must be 'for decades not years', and scoping letters, reliance wording and duty delineation matter more than ever.

With anticipated reforms and evolving case law, the building and fire safety arena will continue to become a more regulated and complex environment for advisors such as surveyors. Longer limitation periods for DPA claims and the Building Liability Order regime (piercing corporate group structures) broaden who can be liable and for how long. We foresee more claims against construction professionals, including surveyors. Ongoing remediation programmes and persistent numbers of buildings with critical fire-safety defects sustain demand for advice/certification with consequent associated potential liability.

...claims latency is longer, record-keeping must be 'for decades not years', and scoping letters, reliance wording and duty delineation matter more than ever.

UK housebuilding is stymied by planning and Building Safety Regulator ("BSR") delays. These delays suppress project flow and create potentially complex advisory exposures. With bottlenecks common, clients lean on surveyors for strategies around compliance, sequencing and cost

impact. That advisory role creates duty of care debates and potential contribution claims alongside designers and project managers.

The BSA's competency emphasis and "golden thread" documentation raise the bar on evidence of skill, supervision and record-keeping across surveying disciplines. Regulators and tribunals are increasingly focusing on whether professionals were competent and documented advice properly.

We may see more regulatory actions by the BSR. Fur future proofing, as part of an adequate management liability programme, it may be prudent to seek "criminal and regulatory prosecutions" extension under PII.

CLAIMS AGAINST SURVEYORS

THE IMPACT OF BRATT V JONES [2025] EWCA CIV 562

The 2025 Court of Appeal case of **Bratt v Jones** was significant in questioning whether it was right that a valuer should avoid liability where, though their valuation fell within the appropriate margin of error, the methodology adopted to reach that figure may in some respects have nevertheless been negligent. Please see our article here for more detail.

The obiter comments made by the Court of Appeal suggest the orthodox approach may be revisited if an appropriate case reaches the Supreme Court. Should it do so, much will turn on the Supreme Court's view as to the scope of the valuer's duty. For now, at least, the Court of Appeal has reaffirmed the orthodox position, clarifying also that the burden of proof remains at all times on the claimant to demonstrate a breach of duty in respect of the valuation process.

CONSULTATION ON CHANGES TO THE RICS HOMES SURVEY STANDARD

On 19 August 2025, the RICS announced a consultation on its proposed updates to the RICS Homes Survey Standard (the "Standard"). Please see our article here for more detail. The Standard sets out a framework for RICS surveyors to follow when carrying out residential property surveys.

Some of the key proposed changes include new minimum report requirements such as appropriate desktop research, physical inspection of the property by a suitably qualified RICS member, and consideration of relevant information obtained from third parties and other publicly available information.

The proposed changes will assist surveyors in minimising their risks and providing clarity to clients as to the terms of their engagement and applicable inspection and reporting requirements. RICS members will need to undertake adequate training to ensure any new requirements are met.

THE RENTERS' RIGHTS ACT 2025 (THE "ACT")

The Act received Royal Assent on 27 October 2025. The Act's aim is to reform the private rented sector by providing greater security and stability for tenants. Key changes include abolishing 'no-fault' section 21 evictions, replacing fixed-term tenancies with periodic tenancies, introducing a new Decent Homes Standard for private rentals, and applying 'Awaab's Law (considered below) to private landlords regarding issues like damp and mould.

Valuers/surveyors will need to ensure that the new minimum safety and maintenance standards are considered, evidenced and incorporated into their opinion and valuations. It is these standards that will dictate the value and whether a property can be used for letting purposes.

While the Act has received Royal Assent, its provisions will be implemented in phases through further regulations. The timeline for these regulations has not yet been confirmed. The government has stated it will outline its implementation plans as soon as possible. It is important to prepare for the new regime ahead of time, given the significant changes it introduces.

AWAAB'S LAW

The Hazards in Social Housing (Prescribed Requirements) (England) Regulations 2025, commonly referred to as 'Awaab's Law' (following the death of two-year-old Awaab Ishak due to prolonged exposure to damp and mould), came into force in part on 27 October 2025. The regulations impose obligations on social housing landlords to act promptly to address health hazards for tenants.

The evolving regulatory, legal and technological landscape will continue to reshape professional risk for surveyors, valuers and property professionals

Phase 1, already in force, concerns damp, mould and fungal growth, and other 'emergency hazards' (those posing immediate and significant risk to tenants' health and safety). Phase 2, to come into effect in 2026, will focus on wider housing hazards, including excessive cold and heat, risk of falls, structural collapse and explosions, fire and electrical hazards. Phase 3 is expected to come into force in 2027 in respect of remaining hazards.

Awaab's Law imposes significant responsibilities on social housing landlords who will look to their managing agents to ensure those obligations are met by ensuring that hazards are promptly investigated (and such investigations diligently documented) and remediated. It will also require regular inspection of properties, particularly older buildings.

MARTYN'S LAW

The Terrorism (Protection of Premises) Act 2025 (known as Martyn's Law, in remembrance of Martyn Hett, a victim of the Manchester Arena attack in 2017), will impose duties on those with control of predominantly commercial premises to reduce their vulnerability and the risk of harm in the event of a terrorist attack. Martyn's Law took effect on 3 April 2025, initiating a 24-month implementation period to prepare for compliance.

The law primarily concerns public venues with significant capacity (hospitality, retail, entertainment, sports, education, healthcare estates etc.). With the risk of significant civil and criminal penalties for non-compliance, action is essential to meet these new statutory requirements. Documented adequate training in situational awareness, lockdown and evacuation procedures, crowd management, and access control are no longer optional but a legal requirement. Property managers will play a significant role in ensuring compliance, whilst the obligations imposed by the legislation

are likely to be relevant considerations for professionals engaged to survey and value premises impacted by these changes, particularly where compliance may require improvements to infrastructure.

ENERGY PERFORMANCE AND ESG ADVICE: TIGHTENING STANDARDS DRIVE ADVISORY RISK

Minimum Energy Efficiency Standard ("MEES") and wider energy-performance reforms (including the government's ongoing reform of the Energy Performance of Buildings framework) point to tighter expectations for non-residential properties. Industry analysis suggests a likely trajectory toward EPC B by 2030–2035 for commercial properties. The precise timetable is still evolving, but the direction is clear: owners will need upgrades, and surveyors who advise on feasibility, cost and programme will see advice-driven exposure where outputs are used for lending, transactions or lease planning. Expect 2026 to bring more mandates into project briefs - and more claims risk where advice proves materially wrong and contributes to financial loss.

For residential PRS, EPC E remains the level required for letting out a property; although plans to push to C were scaled back, the regulatory environment continues to change - another reason to state assumptions, data sources and uncertainty clearly in reports that clients may rely on for investment decisions.

ARTIFICIAL INTELLIGENCE ("AI")

The increased use of AI brings risks of technical errors and claims.

In September 2025, RICS launched a global professional standard on the responsible use of AI in surveying. Set to take effect on 9 March 2026, the new standard *"sets out mandatory requirements and best practice expectations for RICS members and regulated firms worldwide"*. The standard will require firms using AI to maintain policies, governance, risk registers and review cycles to ensure tools are appropriate for their tasks. For 2026, that may mean:

- Process-based duties: if a firm uses AI to screen defects, triage surveys, draft outputs or assist in valuations, claimants may argue that failures in tool governance or oversight constitute negligence.
- Disclosure and scoping: clients may need to be told when AI is used; disclaimers will not rescue poor oversight.
- Professional indemnity underwriters are likely to ask about AI policies, training data, human controls and audit trails.

Pragmatically, surveyors should treat AI governance like any other critical system or tool - documented, tested and periodically reviewed - with explicit signoffs when AI outputs inform advice or valuation judgments.

The increased use of AI also increases cyber security vulnerabilities – in this regard we refer to the Cyber section of this report.

CONCLUSION

The evolving regulatory, legal and technological landscape will continue to reshape professional risk for surveyors, valuers and property professionals (and construction advisors) throughout 2026 and beyond. Extended limitation periods under the BSA have redefined long-tail exposure, requiring professionals to preserve records and maintain competence documentation for decades. Case law developments, such as Bratt v Jones, signal closer scrutiny of valuation methodologies and potential erosion of traditional liability protections in the future. Simultaneously, new statutory regimes - including the Renters' Rights Act, Awaab's Law, Martyn's Law and tightening energy performance standards - expand advisory obligations and risk. The growing integration of AI introduces fresh governance and oversight duties. Overall, property professionals face a future of heightened accountability, evidential rigour and the need for robust professional indemnity and compliance frameworks.

To discuss how any of these issues might affect you, please contact

Martin Jensen
Partner
+44 (0)20 7469 0505
m.jensen@beale-law.com

Joanna Lewis
Partner
+44 (0)20 7469 0444
j.lewis@beale-law.com

SOLICITORS

2024 renewals saw rate reductions which accelerated through the year. That momentum continued in 2025 as insurer capacity increased and competition intensified. Many firms achieved lower primary and excess-layer rates, although outcomes were still varied based on profile.

Large firms with high fee income benefited the most, often seeing reductions of 5 – 10% in their primary layer rates. Smaller firms, particularly those with fee incomes below £500,000, faced a mixed picture. As did firms exposed to higher-risk practice areas, such as those with heavy property exposure or those involved in financial mis-selling. Most insurers were offering longer policy periods (typically 18 months) with good uptake by firms. Co-insurance on primary layers is becoming increasingly popular to insurers, especially when dealing with larger firms, to spread their risk.

The downward movement in rates and strong capacity are expected to continue into 2026 as more capacity continues to flood into the UK market. Notifications are rising but negligence claims appear to be declining slightly in overall frequency. That said, we are seeing an increase in severity of claims.

We are also seeing a growing trend of claimants notifying the SRA, alleging breaches of regulatory duties, and even the Legal Ombudsman, when pursuing negligence claims. This is typically done by litigants in person, who are apparently relying on ChatGPT/AI generated information. Several insurers are now offering regulatory defence cover as a way of differentiating their offer.

HIGH-VOLUME CLAIMS

The SRA's 2025 thematic review highlighted systemic weaknesses in volume consumer claims citing poor transparency, client-care shortcomings and consumer detriment.

An independent review of the SRA's regulation of the now defunct law firm, SSB Group Limited ("SSB"), was conducted for the Legal Services Board by the law firm Carson McDowell ("CM"). CM's report highlights significant failings on the part of the SRA. In respect of high-volume claims, the CM's report states: *"The lack of a 'joined-up' approach in assessing the reports about SSB's handling of CWI [cavity wall insulation] claims is particularly surprising in light of the SRA's general awareness of the potential risks to consumers arising from the bulk litigation of CWI claims."*

After having dropped the ball very badly in respect of the Axiom Ince and SSB debacles, the SRA is no doubt desperate to not get any more egg on its face. An email circulated by the SRA on 2 October 2025 is self-explanatory regarding the seriousness with which it is treating high-value claims: *"The high-volume claims sector continues to be a big focus for us. When done well, it can help many people access justice, but we are seeing significant issues in this area"*. We expect to see tighter controls on this issue.

If expected reforms bite in 2026 - mandating clearer cost disclosures, tighter client-care, and possibly curbs on certain marketing practices - expect a significant reduction in mis-sold or poorly explained fee arrangements, but also a wave of retrospective complaints/claims about past practices. Firms in high-volume claims will need

to audit historical files for disclosure/consent risk and be ready for block notifications. Firms that invest in personalised on-boarding, transparent costs communications (including success fees/ATE) and robust case selection should find PI underwriters more accommodating, particularly if paired with strong outcomes data.

LITIGATION WORK BY NON-QUALIFIED STAFF

The High Court judgment in **Mazur v Charles Russell Speechlys [2025] EWHC 2341** reverberated through the legal profession. By the time this report is published, or relatively shortly thereafter, we may look back at this as having been the proverbial storm in a teacup. This is because several steps have already been taken, and guidance issued, that will see most practitioners overcome the obstacles that the Mazur ruling seemed to have put in the way. For example, in early November 2025, the Legal Services approved, with immediate effect, a fast-track application from CILEX Regulation to allow legal executives to obtain standalone practice rights.

The Mazur ruling states that only an 'authorised person (as defined in section 18 of the Legal Services Act 2007 ("LSA")) can conduct "reserved legal activities" (section 12 of the LSA), such as litigation, even if they are employees of an authorised firm. Under sections 14 to 16 of the LSA, an employer who is authorised to perform a reserved legal activity may commit a criminal offence if an unauthorised employee carries out that activity. This makes it clear that, within the LSA framework, an employer and their employee are not treated as functionally one and the same for the purpose of authorisation. Mere supervision is not a substitute for proper authorisation. This judgment therefore reinforces that only authorised persons can carry out activities such as issuing proceedings, signing statements of truth and corresponding with the court on behalf of a client. This may continue to present a significant headache in some practice areas, especially those that responded to the challenge of fixed or reduced costs by having used staff without practice rights to conduct litigation. Going forward, there will be greater pressure to evidence substantive supervision of unqualified staff.

FINANCE AND ENFORCEMENT

As above, the SRA has had a difficult year. Further developments include:

- The SRA's annual Business Plan and Budget, published on 31 October 2025, which highlights a significant and sustained increase in the number of reports it is receiving about solicitor misconduct. The number of cases is 46% higher when compared to the same period the previous year.
- For the 2025/26 practising year, increases to the Compensation Fund are modest. However, the SRA is considering the long-term future of the Fund, including whether the current flat-fee apportionment system is fair to all sizes of firms.
- In September 2025 it was reported that the SRA had confirmed that it had, at least for the immediate future, shelved plans to proceed with sweeping changes to prevent solicitors from holding client money in favour of it being held by a third-party. SRA Chair, Anna Bradley, reportedly said that *"there is a strong case to properly explore the long-term transformation of the model of holding client money and how the compensation fund is funded"* but that their immediate focus was on making changes to better protect and safeguard client money under the current system.

- We expect the SRA to keep a close eye on reconciliations, segregation of duties, and payment-change verification, alongside faster interventions when red flags appear. That regulatory posture intersects with the Fund's solvency model: swift interventions limit Fund outflows and reputational damage but can crystallise firm failures and increase notifications to PI insurers.

Notifications are rising but negligence claims appear to be declining slightly in overall frequency

Anti-Money Laundering ("AML") enforcement remains intense.

2025 has seen significant activity in this area:

- Fines more than doubled year-on-year to £1.3 million across 173 fines in the year to 31 October 2024, with subsequent months in 2025 bringing further significant sanctions, including six-figure fines for larger firms.
- The number of AML 'proactive engagements' conducted by the SRA soared by 72% in 2024. Almost a third of inspected firms were non-compliant. Conveyancing, in particular residential conveyancing, remains the area of greatest risk.
- In **SRA v Dentons UK & Middle East LLP [2025] EWHC 353 (Admin)** the High Court recognised a form of "strict liability offence" meaning that Dentons' inadvertent or good faith breach did not justify the dismissal of the allegations that it had breached money laundering regulations. The case has been sent back to the Solicitors Disciplinary Tribunal for determination.
- Responsibility for AML is set to pass to the FCA, which will undoubtedly cause confusion (and potential regulatory risk) for the profession whilst adapting to the behaviours of yet another new regulator.

ARTIFICIAL INTELLIGENCE ("AI")

By 2026, many firms will have embedded AI-assisted drafting, search and workflow tools. From a liability perspective, some of the biggest risks are: (i) automation bias; (ii) failing to verify the accuracy of AI-generated content, consequently running the risk of relying on hallucinogenic AI outputs and deepfakes; and (iii) confidentiality and data breaches.

In **Ayinde v London Borough of Haringey [2025] EWHC 1383 (Admin)** and **Hamad Al-Haroun v Qatar National Bank QPSC and QNB Capital LLC** (heard together) involved the use, or suspected use, of generative AI resulting in fictitious case law, fake

citations, and misstatements of law in litigation. The result was wasted court and practitioner time, the submission of false information that risked interfering with the administration of justice, and conduct that the court considered improper, unreasonable, and negligent. In both cases, the practitioners were found to have either knowingly

Generative AI should not be used without thorough verification, and the full weight of professional regulation applies to any material a lawyer endorses

or recklessly misled the court (or attempted to do so) in breach of their professional regulatory obligations. The consequences included wasted costs orders, referrals to professional regulators and public judicial criticism.

In a subsequent case, an immigration barrister was found to have used AI to do his work for a tribunal hearing after citing cases that were *"entirely fictitious"* or *"wholly irrelevant"*. He has been referred to the Bar Standards Board.

The judiciary's message to the legal profession is clear. Generative AI should not be used without thorough verification, and the full weight of professional regulation applies to any material a lawyer endorses, whether it was created by a human or by an AI system.

It can only be a matter of time before thoughtless or unsupervised use of AI gives rise to negligence liability. Firms should carry out proper risk assessments to manage potential liabilities in relation to AI and have clear training and governance in place.

CYBER RISKS

2025 brought a vivid reminder that legal sector infrastructure is on threat actors' radar, with a major cyber-attack on the Legal Aid Agency resulting in system shutdowns and the exposure of personal data of millions of people. With the help of AI, cyber-attacks are becoming more sophisticated and targeted.

Missed deadlines due to outages may lead to claims. Misconfigured cloud storage remains a common cause of data breaches and notification to insurers. Often breaches occur because of weaknesses at third-party providers. It is therefore imperative to conduct due diligence on all third-party providers (e.g., cloud services, case management software) to ensure they meet appropriate security standards. Security requirements should be formalised in contracts.

The SRA's Minimum Terms and Conditions cover third-party claims in the event of a cyber-attack, but do not cover losses suffered by the firm itself, such as incident response, data restoration, business interruption and ransom payments. The uptake of standalone cyber insurance among firms (28%) remains low relative to the risk.

WORKPLACE CULTURE

The SRA remains focused on workplace culture and wellbeing. The issue has received heightened attention in light of the current US administration's prohibition of EDI initiatives, and the knock-on impact on firms in the UK who have a US presence. Expect the tension between the US and UK approach to continue into 2026 and beyond.

CONCLUSION

Overall, 2026 will demand tighter controls, stronger governance, and clearer accountability across the profession. Heightened scrutiny of high-volume claims, litigation by unqualified staff, client-money safeguards, AML compliance, AI use and cyber resilience will continue to shape risk. Firms that invest in robust systems, credible supervision, transparent client-care and a healthy workplace culture will be better placed to avoid regulatory exposure and maintain insurer confidence.

To discuss how any of these issues might affect you, please contact

Joe Bryant
Partner
+44 (0)7786 679 602
j.bryant@beale-law.com

Claire Revell
Partner
+44 (0)117 428 9296
claire.revell@beale-law.com

ACCOUNTANTS & AUDITORS

The pricing and capacity of professional indemnity insurance for auditors and accountants improved through 2025, largely due to new MGAs entering the market. If the loss experience stays benign, we may continue to see competitive terms in 2026.

The year ahead is likely to bring its own set of challenges. The professional risks facing auditors and accountants continue to expand amid regulatory reform, economic pressure, and rapid technological change. Heightened scrutiny - driven by high-profile audit failures, evolving artificial intelligence ("AI") and cyber-related expectations, and increasing enforcement activity - means firms face growing exposure across audit quality, valuations, governance and financial crime compliance.

AUDIT

Accountants dealing with financially distressed businesses can expect heightened scrutiny. Auditors in particular may face claims for failing to identify going concern issues or material misstatements in financial reports.

A high-profile example is the ongoing case of **NMC Health Plc (In Administration) v. Ernst & Young LLP**, a £2.7 billion negligence claim in which NMC's administrators allege that EY, the company's former auditor, failed to detect a massive fraud, leading to the company's collapse. It is alleged that EY's audits between 2012 – 2018 failed to uncover significant unreported borrowings and missed critical "red flags", failing to get full access to essential financial data (such as the complete general ledger), and having deficient internal controls and supervision of the EY Middle East auditors. EY denies all allegations of negligence, arguing that it was a victim of a "complex, co-ordinated and sophisticated fraud" orchestrated by NMC's senior management and principal shareholders that was deliberately concealed to circumvent the audit process.

AUDIT QUALITY, REFORMS AND ENFORCEMENT

The Financial Reporting Council ("FRC") published its Annual Review of Audit Quality in July 2025 (the "Review"). The Review addressed the inspection and supervision results of audit firms across the UK Public Interest Entity ("PIE") market. The results were published alongside reports for Tier 1 audit firms. The latest inspection results show continued improvement in audit quality, primarily among Tier 1 firms. The Review suggests that the gap is widening between audit quality delivered by Tier 1 firms and other firms in the PIE market. The Review found that many non-Tier 1 firms still struggle to consistently meet adequate standards and maintain robust quality management systems. This may signal closer examination and potential enforcement.

The evolving regulatory, technological and economic landscape is amplifying scrutiny on auditors and accountants

One of the proposals in the current iteration of the Audit and Reform and Corporate Governance Bill (on hold at present) is to dilute the Big Four's dominance by mandating FTSE 350 companies to use challenger audit firms for a portion of their audit. In 2023 it

was found that Deloitte, EY, KPMG, and PwC audited 98% of the FTSE 100, a dominance that has prompted scrutiny over conflicts of interest. This proposed requirement is aimed at, amongst others, fostering competition within the audit market and to improve overall quality and transparency. In our view, these ambitions cannot be reconciled with the Review's findings about the audit quality of smaller firms.

On 1 October 2025, the FRC launched a public consultation on proposed updates to its Audit Enforcement Procedure. The consultation, which closes on 9 January 2026, aims to expand the FRC's toolkit with three new resolution routes - Published Constructive Engagement, an Accelerated Procedure and an Early Admissions Process. The objective is to allow for more targeted and timely regulatory responses to breaches of auditing standards.

The above-mentioned consultation follows alongside the FRC's formal engagement on its Future of Audit Supervision Strategy (FASS) launched in August 2025. The FRC plans to refine its supervisory approach by placing greater emphasis on the effectiveness of audit firms' Systems of Quality Management (SoQM).

The FRC continues to view non-financial sanctions as a key tool for driving improvements and innovation in firms' systems and practices, however, substantial financial penalties continue to be imposed and in 2025, BDO was fined £5.85M and PwC was fined £2.88M.

Recurring issues identified in concluded investigations include a lack of professional scepticism, failure to obtain sufficient appropriate audit evidence, non-compliance with ethical requirements (e.g., independence) and inadequate governance in areas like provisions and asset impairment.

AUDIT REFORM DELAYED AGAIN

The UK legislation intended to create the Audit, Reporting and Governance Authority ("ARGA") is the Audit, Reporting and Governance Bill. 2025 saw the government announcing a further delay to the long-anticipated ARGA.

The Financial Conduct Authority ("FCA") will now oversee the anti-money laundering (AML) activities of accountants (and lawyers), and this shift may require careful coordination with some of the ARGA proposals. Expect more disciplinary cases for poor AML controls and negligence allegations when clients suffer loss tied to financial-crime failures or sanctions breaches.

AI AND CYBER RISKS

AI and cyber risks will continue to pose increasing risks to auditors and accountants. These risks are numerous.

UK regulators can pursue organisations for AI-washing (overstating of AI capabilities or use under consumer protection and advertising laws). Sanctions can include regulatory action, civil claims and criminal penalties.

AI-washing also introduces challenges in relation to the work auditors and accountants do for other businesses. For example, AI-washing can distort valuations, operational assessments and investor expectations. Auditors should therefore scrutinise management assertions more carefully, increasing the need for technical understanding of what constitutes genuine AI capabilities. AI-washing may lead to misstated intangible assets or inappropriate capitalisation of research

& development costs (which remains a ripe source for claims). If a product is marketed as advanced AI but lacks substantive technological innovation, recognition of related assets or revenue may not meet UK accounting standards. Companies in the AI-sector are highly volatile, and this makes accurate valuations much more challenging.

The FRC published its first guidance (in June 2025) and emphasised that auditors and accountants must demonstrate professional scepticism and robust documentation to avoid regulatory criticism or liability.

Accountants and auditors face significant liability from cyber and data protection failures including non-compliance with data protection legislation (such as GDPR), legal action from clients for damages caused by breaches as well as disciplinary action by professional bodies. Cybercrime remains a key concern, increasing demand for cyber-specific insurance cover.

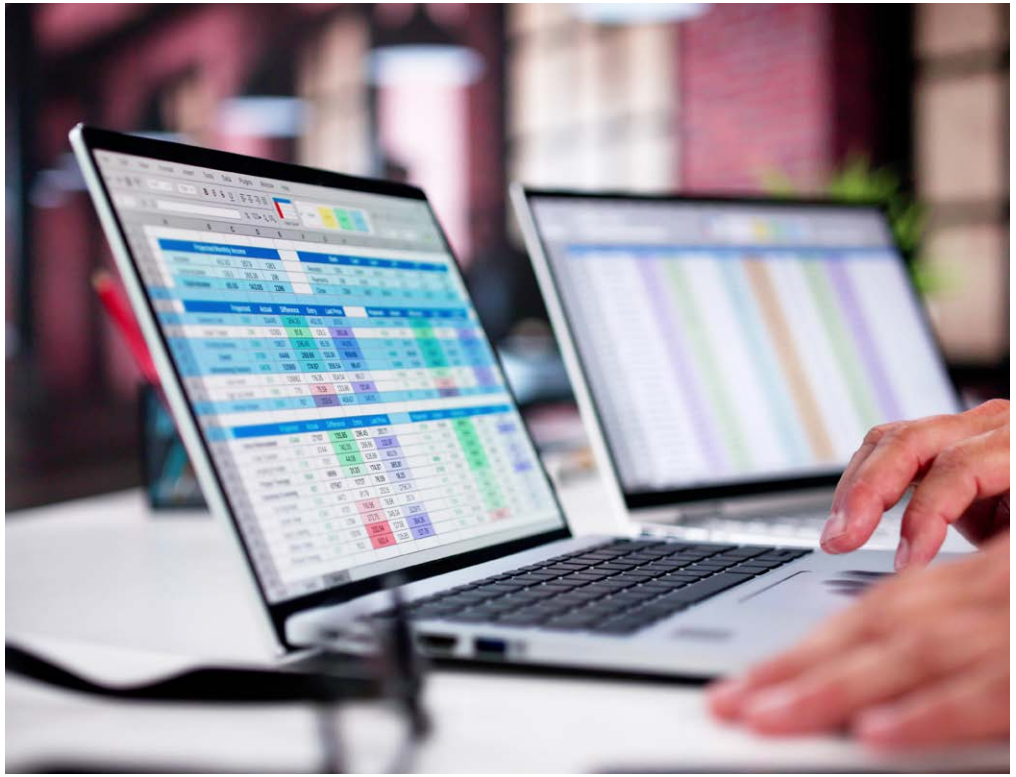
M&A TRANSACTIONS

Errors in advising on valuations of businesses, goodwill, or assets in mergers, acquisitions or disposals remain a perennial exposure for auditors and accountants. Their work in these transactions directly influences deal pricing, investor decisions, and post-acquisition accounting.

Another emerging issue within the UK accountancy profession itself is the growing risk of conflicts of interest, driven by smaller accountant firms being acquired by larger ones. More complex conflict-management procedures are required, and often lucrative work needs to be declined. For example, a firm's protocol may be such that longstanding audit team takes precedence when there is a conflict at the expense of higher value consultancy work.

COMPANIES HOUSE & ECONOMIC CRIME REFORMS MEAN NEW EXPOSURES

The Economic Crime and Corporate Transparency Act 2023 ("ECCTA") is designed to combat economic crime and improve corporate transparency. The "failure to prevent fraud" offence under the Act came into force on 1 September 2025 and makes large organisations criminally liable if an "associated person" (like an employee or agent) commits a fraud intending to benefit the organisation, and the organisation did not have reasonable fraud prevention procedures in place. Accountants advising on systems, filings and governance could be drawn into disputes if clients face enforcement.



The ECCTA has made identity verification mandatory for company directors and persons with significant control ("PSCs") through Companies House. This means that accountants and auditors are required to verify the identities of directors and PSCs of their own practice if they are a limited company or limited liability partnership.

ECCTA has also introduced a new process whereby third parties, including accountants, who want to provide identity verification services for their clients, or file at Companies' House on behalf of clients, will have to register as an Authorised Corporate Service Provider (ACSP). There is a 12-month transition period for compliance (i.e. until mid-November 2026). Errors, failures to verify or reliance on weak processes will create professional negligence and regulatory risks. With these expanded responsibilities it will be prudent to tighten engagement terms and verification procedures.

ENVIRONMENTAL, SOCIAL AND GOVERNANCE

The UK Sustainability Reporting Standards and related consultations point to 2026 activity to enhance integrity and trust in sustainability-related financial information. The FCA's anti-greenwashing rule already applies to all FCA-authorised firms who make sustainability-related claims about financial products and services. The rule is to ensure claims are fair, clear and not misleading. By 2026, those rules will be embedded in marketing and disclosures, and any sustainability narratives accountants touch (advisory, reporting support, or assurance) carry misrepresentation risk.

This rule places indirect pressure on auditors and accountants to ensure sustainability claims are accurate, verifiable and consistently reported. The FCA has made it clear that it will use the rule to challenge and sanction misleading sustainability claims. Auditors and accountants may be called upon as key gatekeepers to prevent misstatements.

RESEARCH AND DEVELOPMENT ("R&D") RELIEF

HMRC's continued crackdown on fraud and errors in R&D tax credits means that negligence claims over alleged inadequate or inaccurate advice on R&D relief are not abating. Client losses on rejected or clawed-back claims will continue to feed negligence allegations in 2026.

Recent HMRC reforms have improved the integrity and transparency of the R&D tax credit scheme. These measures are said to have helped spot weak claims more easily, prevent the submission of fraudulent ones, hold advisors to account and ensure strong oversight. It has been reported that, in some cases, genuine claimants have been opting out of the scheme altogether or even looking beyond the UK. The reasons cited are the time and resources now required, the complexity of the process, and the fear of an enquiry outweighing the potential monetary gain.

CONCLUSION

The evolving regulatory, technological and economic landscape is amplifying scrutiny on auditors and accountants. Heightened enforcement, expanding duties, and greater expectations around governance, AI, cyber risk, ESG and transactional work mean professional exposure is increasing across multiple fronts. As reforms progress, firms must strengthen quality management, scepticism, documentation and conflict controls. Those which adapt proactively will be best placed to mitigate rising risks and maintain trust in an increasingly complex environment.

To discuss how any of these issues might affect you, please contact

Joe Eizenberg
Partner
+44 (0)117 428 9303
j.eizenberg@beale-law.com

Ross Baker
Partner
+44 (0)20 7469 0509
r.baker@beale-law.com

INSURANCE BROKERS

By mid-2025 the UK Professional Indemnity market had clearly softened, with more capacity, broader appetites and falling rates across many professions. This is largely due to an increasing number of managing general agents ("MGAs") having entered the market with renewed capacity from insurers eager to continue their growth after the hard market cycle. Soft markets tend to produce E&O claims, as insurers tighten their belts and review coverage more strenuously; policyholders also tend to face more claims in times of economic uncertainty, so the number of declinatures also rises and, with it, the number of broker E&Os.

REGULATORY

We see broker remuneration as the biggest issue on the horizon.

The FCA's Consumer Duty, which came into force in 2023, has widened expectations on advice, fair value and support. The Duty requires brokers to actively monitor outcomes, assess fair value, and be entirely transparent about their remuneration arrangements.

Detailed record-keeping is imperative to be able to demonstrate that the advice provided was suitable for the client's specific demands and needs

Findings published by the FCA in 2024 revealed that many insurance distributors (typically insurance brokers, MGAs, or insurers acting as distributors) were failing to meet key expectations around fair value, particularly regarding their own remuneration. Most distributors were charging what they had always charged, without analysing whether it was justified, fair, or if it aligned with the value customers receive. They often did not realise they were required to make this assessment and could not demonstrate how their remuneration affected overall value.

The issue of broker remuneration (including commissions, fees, and other forms of remuneration) has become a more pressing issue in light of the recently concluded litigation relating to undisclosed motor finance commission. As such, in 2026 we can expect the Duty to be the central lens through which client disputes around suitability, value, communications clarity, vulnerability handling, or claims outcomes is viewed. Claimants and litigators will continue to use the Duty's outcomes to frame alleged breaches of a broker's duty of care. Cases that show poor documentation of value assessments, lack of a clear rationale for product selection or a failure to detect/triage appropriate products could be fertile ground for consumers disappointed in their insurance outcomes.

For more information on the FCA's stance on transparency relating to broker remuneration, please see our article **here**.

UNDERINSURANCE AND COVERAGE GAPS

Continuing economic headwinds and high insolvency rates in some sectors, supply-chain volatility and lingering construction defect disputes are all examples of current and expected professional liability exposure. In 2026, that translates to more client scrutiny of brokers' advice on issues such as sums insured, business interruption and market wordings/exclusions. Claims

will continue to increase in size and complexity in such a climate.

Issues with underinsurance (and the application of average) will always increase in an inflationary environment, and these will often morph into allegations against the broker. Brokers will need to be on top of their game to guard against these risks and ensure their communications are crystal clear.

Detailed record-keeping is imperative to be able to demonstrate that the advice provided was suitable for the client's specific demands and needs at that time, based on a proper "fact-find". Documented warnings where clients choose to ignore advice are also an essential part of a broker's risk management.

UNSTABLE MARKETPLACE

Commentators have expressed concern that the increase in MGAs is contributing to a distorted and increasingly unstable downward-spiralling marketplace where long-term sustainability is compromised. Brokers who prioritise the lowest-priced carriers risk placing business with insurers that may no longer be solvent when a claim is made.

With an increase in MGAs and competition, it is unsurprising that the insurance sector is seeing greater concern surrounding potential claims against MGAs themselves. Insurers are increasingly scrutinising the performance of their MGA networks and there have been several instances where MGAs have acted beyond their delegated underwriting or claims authority. Some of the resulting claims are extremely large. Brokers with affiliated MGAs should ensure that their own E&O coverage is sufficient to address potential future claims of this kind. Particular attention should be paid to the aggregating provisions within policies, as the claims we are seeing often involve large volumes of alleged individual errors, which can easily give rise to coverage disputes.

Insurance brokers pursuing an "aggregator" strategy typically grow by acquiring smaller brokerages and bolting them onto a centralised platform. In the past decade, private equity ("PE") firms have been the dominant funding source. They supply large amounts of capital upfront, enabling rapid acquisition-led growth. In return, PE firms expect a liquidity event - typically a sale or refinancing - within a predictable time horizon, usually 3-7 years, so they can realise returns for their own investors. Several macro-economic factors have now created headwinds. This makes future PE backing less abundant. Investors are now more sceptical of roll-up strategies that rely heavily on debt, integration

execution, and perpetual access to buyers at ever-higher valuations. The combination of high leverage, reduced PE appetite, and slower exits make it plausible that one or more aggregators could face financial distress or even failure in the near term, with the inevitable claims activity that would follow.

SPECIALIST KNOWLEDGE REQUIRED

Amid growing regulation, rapid technological advances, and the rise of AI, the insurance landscape is becoming more complex. Products (and carriers) are changing all the time. Brokers are now expected to possess a strong grasp of a wide range of policy types to ensure they are offering clients the most suitable and/or favourable terms.

Examples here are major construction and infrastructure projects, some of which are fairly novel, such as Modern Methods of Construction (MMCs) and data centres powered by nuclear energy. Modular builds, innovative materials, off-site manufacturing, and intricate supply chains can alter risk profiles significantly. Issues such as fire behaviour, durability, warranties, design responsibility and contractor interdependencies often fall outside the expertise of generalist brokers. Clients increasingly expect brokers to interpret these technical nuances and connect them with suitable insurance markets. This means that brokers must develop deeper sector-specific knowledge, collaborate more closely with technical experts and continuously upskill. Proper advice now depends on understanding not only the rapidly-changing insurance market conditions, but also emerging technologies and risks, evolving regulations and matters such as specialised construction methods – to ensure clients receive accurate risk assessments and well-structured, future-proof insurance solutions. A failure to do so presents significant risk for complex, expensive and protracted multi-party disputes.

FRAUD

In recent years, UK insurance brokers have reported a noticeable rise in direct fraud committed against them, particularly involving appointed representatives (“ARs”) and consultants who trade heavily in cash-intensive environments such as markets, trade fairs, and pop-up commercial events. When ARs collect premiums in cash, there is greater opportunity for misappropriation before funds reach the broker or insurer. Fraudsters may under-declare premium amounts, delay remittance, or fabricate policy documents entirely, knowing oversight is harder when transactions are not

electronically recorded. 'Teeming and lading' incidents are on the increase.

Technology has made it easier to falsify documents. Fraudsters can produce convincing certificates of insurance, invoices, or receipts to reassure customers or confuse auditors. When combined with cash dealings, discrepancies may go undetected for long periods.

Strengthening due diligence, ongoing monitoring, digital payment adoption, and data reconciliation can help brokers reduce exposure to these evolving fraud risks.

The Economic Crime and Corporate Transparency Act 2023 ("ECCTA") has introduced, with effect from 1 September 2025, a new "failure to prevent fraud" offence. ECCTA applies to large organisations and creates potential criminal liability where an associated person (employee, agent, etc.) commits fraud to benefit the organisation, and "reasonable fraud prevention procedures" were not in place. It is imperative that brokers advise on suitable fraud cover, including commercial crime insurance and Directors & Officers liability insurance. Clients should be clearly informed about the scope of coverage under the policy, including any exclusions, and advised that fines or penalties are generally unlikely to be reimbursed under the policy's terms and conditions.

AI

The insurance industry is already seeing significant advantages from AI, particularly through streamlined underwriting and automated claims handling. However, because insurance has traditionally relied on personal relationships, increased automation - and the resulting reduction in client contact - marks a major shift. While AI can offer benefits such as improved documentation of the advice given, brokers must remain cautious. Gathering disclosure information at renewal is crucial for fully understanding a client's business and recommending appropriate types and levels of cover. In person contact means brokers can recognise nuances that may give rise to insurance requirements that are not standard. As personal engagement decreases and reliance on AI grows, especially during renewals, the risk of claims issues will rise. Brokers will therefore need to ensure robust human verification processes remain in place.

CYBER

Cyber risk is an increasingly significant issue. Having the right protection against cyber incidents - such as unauthorised access, data breaches, or ransomware - is essential. Although some Professional Indemnity policies may include incidental or "silent" cyber cover, clients should be made aware of the potential limitations and ambiguity of these provisions. Where appropriate, they should be encouraged to obtain standalone cyber insurance to ensure they have the necessary level of protection. Doing so can also help mitigate the risk of allegations of insufficient advice.

CONCLUSION

A capacity-driven market offers opportunities for growth and competitive pricing, but it also requires a keen understanding of risk management. Brokers must balance the desire to get a slice of the pie with being prudent, and ensure that all of their dealings (and the basis for their advice) are recorded.

In 2026, brokers face mounting regulatory scrutiny, complex claims conditions and rising operational risks. Robust value assessments, clearer remuneration oversight, stronger technical expertise and enhanced fraud and cyber controls will be critical. As AI accelerates change and market capacity expands, brokers must document advice meticulously, understand emerging risks and maintain human oversight. Those who adapt proactively will be best placed to navigate disputes, protect clients and preserve long-term resilience.v

To discuss how any of these issues might affect you, please contact

Joe Bryant
Partner
+44 (0)7786 679 602
j.bryant@beale-law.com

DIRECTORS & OFFICERS

The market remains soft, favouring buyers, with premiums staying the same or seeing 5% - 10% reductions. However, the percentage decrease is levelling off compared with recent years. Companies in riskier emerging sectors (such as AI) face increased premiums. There is abundant capacity and significant competition between carriers with some MGAs offering significant value for buyers that traditional carriers cannot compete with.

Key risks are regulatory and litigation risks, including ESG and Health & Safety, "failure to prevent" offences, insolvencies (driven by ongoing economic uncertainty) and AI and cyber exposures.

FRAUD

The UK's Economic Crime and Corporate Transparency Act 2023 ("ECCTA") came into force on 26 October 2023, but its provisions are being implemented in phases over several years. The ECCTA has brought substantial reforms that greatly heighten the risk of corporate criminal liability.

The ECCTA has brought substantial reforms that greatly heighten the risk of corporate criminal liability.

One of the most important additions is the new 'failure to prevent fraud offence' (section 199 of ECCTA), which came into force on 1 September 2025. It requires large organisations worldwide to evaluate and manage the risk that employees, agents, or subsidiaries might commit fraud for the benefit of the business. To use the 'reasonable procedures' statutory defence, companies must pinpoint fraud risks, review existing controls, and enhance them where necessary. The ECCTA also broadens the scope of corporate liability through a "senior manager" - defined as an individual with substantial managerial or decision-making authority. The ECCTA will accelerate investigations and derivative or follow-on claims after any fraud event anywhere in the group or supply chain - especially if risk assessments and training are thin or poorly documented. We also expect these investigations to involve multiple calls on the D&O policy through different layers of management, including middle management employees.

Companies House identity verification became a legal requirement on 18 November 2025, with a 12-month transition period for companies to comply. All new and existing company directors and "people with significant control" ("PSCs") must verify their identity to improve transparency and prevent fraud.

According to the UK Finance's Fraud Report 2025, the total cost of fraud in 2024 was £1.177 billion stolen from individuals and businesses (with remote purchase fraud the largest share and authorised push payment fraud accounting for £450.7 million).

Saxon Woods Investments Ltd v Costa 2025] EWCA Civ 708 established that directors could breach their fiduciary duty under section 172 of the Companies Act 2006 (which ECCTA modifies) by not providing full transparency and information to the board. A subjective belief of a better future outcome is not a valid defence against breaches of shareholder agreements.

In 2026, expect a noticeable increase in disputes about conduct exclusions (intent, knowledge), closer underwriting scrutiny of anti-fraud frameworks, and renewed negotiation on "failure to prevent" clauses.

ESG

The FCA's anti-greenwashing rule has been in force since 31 May 2024. Its sustainability labelling & disclosure regime began on 31 July 2024, with phase-ins running through 2025–26. For 2026, the risks are twofold: (i) enforcement of public claims over "greenwashing" (statements by listed companies, funds or portfolio-managed products), and (ii) shareholder actions where ESG claims prove misleading. The Competition & Markets Authority ("CMA") also has a Green Claims Code which sets out 6 principles to help businesses comply with the law. From 6 April 2025, the CMA can now directly enforce this with fines of up to 10% of global annual turnover.

Shareholder activism around climate issues is shifting rather than disappearing. Scrutiny of boards' climate strategy, transition plans, and statements persists. This presents potential D&O exposures for missteps or misstatements. Company statements about sustainability (and AI use), typically contained in the strategic report, are now very vulnerable to regulator action if unsupported by clear evidence. Ofgem fined Drax £25 million for an absence of adequate data supporting environmental claims (despite confirming that there was no evidence of deliberate misreporting). The risk of offences of false representation, false accounting and fraudulent trading are all tied to any potential misstatements made by the company and senior directors.

Climate and other ESG-related litigation remains a potential pressure point, even after **ClientEarth v Shell**. The UK courts did not provide permission for that derivative action to proceed, mainly due to ClientEarth's very small shareholding having a bearing on the application of section 172 of the Companies Act 2006. Having said that, in circumstances where shareholders with a greater overall stake in companies look to bring a claim, one could see the UK Courts being more amenable to allowing a derivative action to continue. This might involve climate change pledges, but it could also involve claims arising from the S pillar of ESG such as claims challenging claims about board diversity or the use of AI to filter through applications for jobs. Activist scrutiny and "green-washing" allegations are rising globally.

In 2025, the FCA announced plans to expand the scope of its non-financial misconduct rules - encompassing

behaviours such as bullying and harassment - to tens of thousands of firms governed by the Senior Managers and Certification Regime ("SM&CR"). SM&CR aims to hold senior leaders accountable for misconduct within their organisations. The strengthened rules, which will also cover racism, sexual harassment, violence, and intimidation, are scheduled to come into force on 1 September 2026. Directors will therefore need to ensure that adequate policies, training and compliance are in place, particularly regarding the monitoring and reporting of breaches of internal policies.

Looking ahead, we expect more insurer focus on ESG compliance and disclosure controls and how boards oversee climate transition narratives.

CYBER & ARTIFICIAL INTELLIGENCE ("AI")

AI presents significant legal, ethical and reputational risks to businesses if not managed properly. AI tools trained on copyrighted material without permission could lead to intellectual property infringement claims. Mishandling personal data can result in breaches of data protection legislation. Employees using free generative AI tools could compromise confidential business information, especially when using third-party services without clear safeguards. AI models can hallucinate or intentionally discriminate by relying on biased data, leading to unfair or unethical outcomes.

There are also increased risks of AI washing claims becoming more common. There has been a number of lawsuits launched in the USA against boards for perceived exaggerations and misrepresentations as the use of AI which allegedly induced investors to purchase shares in the company, only for the use of AI to be very limited. Whilst currently these claims are largely in the US and other more legally volatile countries, there is a risk of claims of this nature reaching UK shores over the course of the next 12-18 months.

AI presents significant legal, ethical and reputational risks to businesses if not managed properly.

From the perspective of insurers, AI introduces a range of coverage considerations. Directors could face claims from third parties - such as employees, customers, or shareholders - alleging that they failed to exercise proper judgment in their use of AI in decision-making, amounting to breaches of duty or mismanagement. Claims may also arise concerning the accountability of senior managers for how junior staff deploy AI within the business. While standalone AI-specific

policies are increasingly available, many directors are likely to rely on their existing D&O insurance, arguing that it implicitly provides "silent" AI cover. Insurers will therefore need to determine whether, and to what extent, they are willing to underwrite AI-related risks, at what cost, or whether exclusions should apply.

Government proposals aired in 2025 contemplate mandatory incident reporting and restrictions on ransom payments for public bodies, with knock-on expectations for private firms (especially critical infrastructure and regulated sectors). The National Cyber Security Centre continues to warn on ransomware and AI-boosted phishing, while DSIT's Cyber Security Breaches Survey 2025 highlights persistent attack prevalence. For 2026 boards, this all means faster notification obligations and higher regulatory expectations of board cyber oversight, and potential personal exposure where governance is deficient.

INSOLVENCIES REMAIN HIGH

Allianz Trade research suggests 27,650 firms will go bust in 2025. This is around 30% above pre-pandemic levels. The official UK government figures come out around 21 January 2026. The corporate insolvencies sustain the risk of wrongful trading, misfeasance and preference claims against directors. These types of claims are often pursued by liquidators, creditors or litigation funders. We are seeing an increase of liquidators using litigation funders to

finance claims against former directors (and accountants).

We expect continued notifications tied to insolvency office-holder investigations. Underwriters will examine refinancing risk, covenant headroom, and board decision making around dividends and buybacks in the run-up to distress.

ONGOING BUILDING SAFETY CONCERNS

Health and Safety has long been a significant source of claims against company directors. Allegations under the Health and Safety at Work Act 1974 are expected to continue, alongside prosecutions for corporate manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007. In addition, routine investigations by the Health and Safety Executive will remain a feature. We also anticipate a growing number of claims linked to workplace culture, with accusations likely to focus on failures to address employee concerns such as stress, burnout, and hostile working environments. The HSE recently reported on 20 Nov 2025 that the estimated cost of injury and ill health from working conditions is £22.9B.

In 2026, building safety will remain one of the most pressing Health and Safety concerns. The Building Safety Act 2023 ("BSA") has introduced wide-ranging reforms, placing significantly greater personal responsibility and liability on company directors. Central to this is the Principal Accountable Person role under section 161 of the BSA - an onerous duty requiring individuals to assess and manage structural and fire safety risks in occupied higher-risk buildings ("HRBs"), with criminal sanctions applying for non-compliance.

In addition, the provisions on Building Liability Orders ("BLOs") under section 130 and Remediation Contribution Orders ("RCOs") under section 123 are drafted in very broad terms. BLOs allow "relevant liabilities" to be extended to "associated entities," enabling claimants to pursue recovery even where the original company, such as a special purpose vehicle (SPV), has no assets. The definition of "associated" is similarly expansive. Meanwhile, RCOs can be issued against former landlords, developers, and other companies - or their directors - connected with those landlords or developers. Together, these measures create fertile ground for D&O claims.

Looking ahead, directors' actions in relation to building construction are likely to face significantly greater scrutiny. This will extend to both directors' and officers' direct involvement in the construction practices used on HRBs, as well as their diligence in selecting contractors - areas expected to undergo close examination. Recent amendments to the Defective Premises Act 1972, which have extended the limitation period for claims involving defective construction products to 30 years, are also highly significant.

CONCLUSION

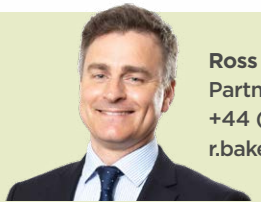
We expect increased risks of regulatory actions against companies and their directors especially rising out of ECCTA, but more generally with newer statutes making it easier to prosecute directors for consent, connivance or neglect (especially where there is a risk of harm to others).

Expect many more small-scale fines and penalties next year from Companies House as it takes proactive steps to clean up the register and identity verify directors and "people of significant control".

We are seeing a rise of liquidators using litigation funders to finance claims against former directors (and accountants).

Greenwashing and AI washing are driving class actions in the USA and we can expect to see that in the UK.

To discuss how any of these issues might affect you, please contact



Ross Baker
Partner
+44 (0)20 7469 0509
r.baker@beale-law.com

Nathan Penny-Larter
Partner
+44 (0)20 7469 0498
n.penny-larter@beale-law.com

INDEPENDENT FINANCIAL ADVISORS

There has been a continuation of the soft market generally across most professions in the Professional Indemnity Insurance market.

However, in recent years, there has been a marked increase in claims against IFAs, driven by the growing complexity of financial products, rising consumer expectations, and a more assertive approach from claims management firms. Both the Financial Ombudsman Service ("FOS") and the Financial Services Compensation Scheme have reported a rise in complaints related to unsuitable advice, mis-selling, and failures to act in clients' best interests. In parallel, the Financial Conduct Authority ("FCA") continues to strengthen its focus on consumer protection, with particular emphasis on ensuring the suitability of advice provided by IFAs. This contributes to increased risk exposure within the sector. Consequently, insurers are incurring higher costs when underwriting IFA policies, resulting in rising premiums across the sector.

Raising the FOS award cap increases insurers' potential exposure, which can push up professional indemnity premiums and tighten policy terms.

Those insurers still offering cover are applying tighter underwriting standards and more restrictive policy terms.

Advice relating to defined benefit ("DB") pension transfers and some SIPP / SIPP-operator exposures still attracts tighter terms or exclusions on many wordings. Several market notes for IFAs continue to flag this as a persistent sensitivity, even as the broader PII market eases.

FOS AWARD CAP INCREASES BUT FEWER SPECULATIVE CASES

FOS award limits have increased. For complaints referred on or after 1 April 2025, the cap is £445,000 (lower caps apply to earlier years).

Raising the FOS award cap increases insurers' potential exposure, which can push up professional indemnity premiums and tighten policy terms.

In Q2 2025, overall FOS complaints fell year-on-year. This is linked to new fees for claims management firms/ representatives per case after the first ten – this is encouraging greater selectivity. If sustained, this could ease nuisance frequency into 2026, though complex investment/pension cases will still progress.

For 2026, expect a lower volume of low-value claims but unchanged or higher tail severity, reinforcing the case for reviewing policy limits, excess layers and any inner sub-limits for pension investment disputes.

PENSIONS ARE REMAINING A SOURCE OF COMPLAINTS

Pensions have consistently ranked among the most complained-about products and 2025 was no different. Several factors have driven the rise in pension-related complaints.

The quality of service provided, along with the reported absence of annual reviews, has been a major source of complaints in recent times - particularly from claims management companies, which are focusing on the FCA's emphasis on value for money and Consumer Duty (the "Duty") requirements. Although these issues may not result in substantial financial losses, firms are still required to

address them through their complaints procedures, leading to additional time and cost burdens. They can also lead to reputational damage and disproportionate operational costs due to the time involved in resolving disputes.

Consumer frustration when their pension funds failed to deliver the expected returns is not new. Financial advisers continue to face criticism for recommending investment strategies that did not align with clients' financial objectives or risk tolerance, especially in light of the benefits they forfeited.

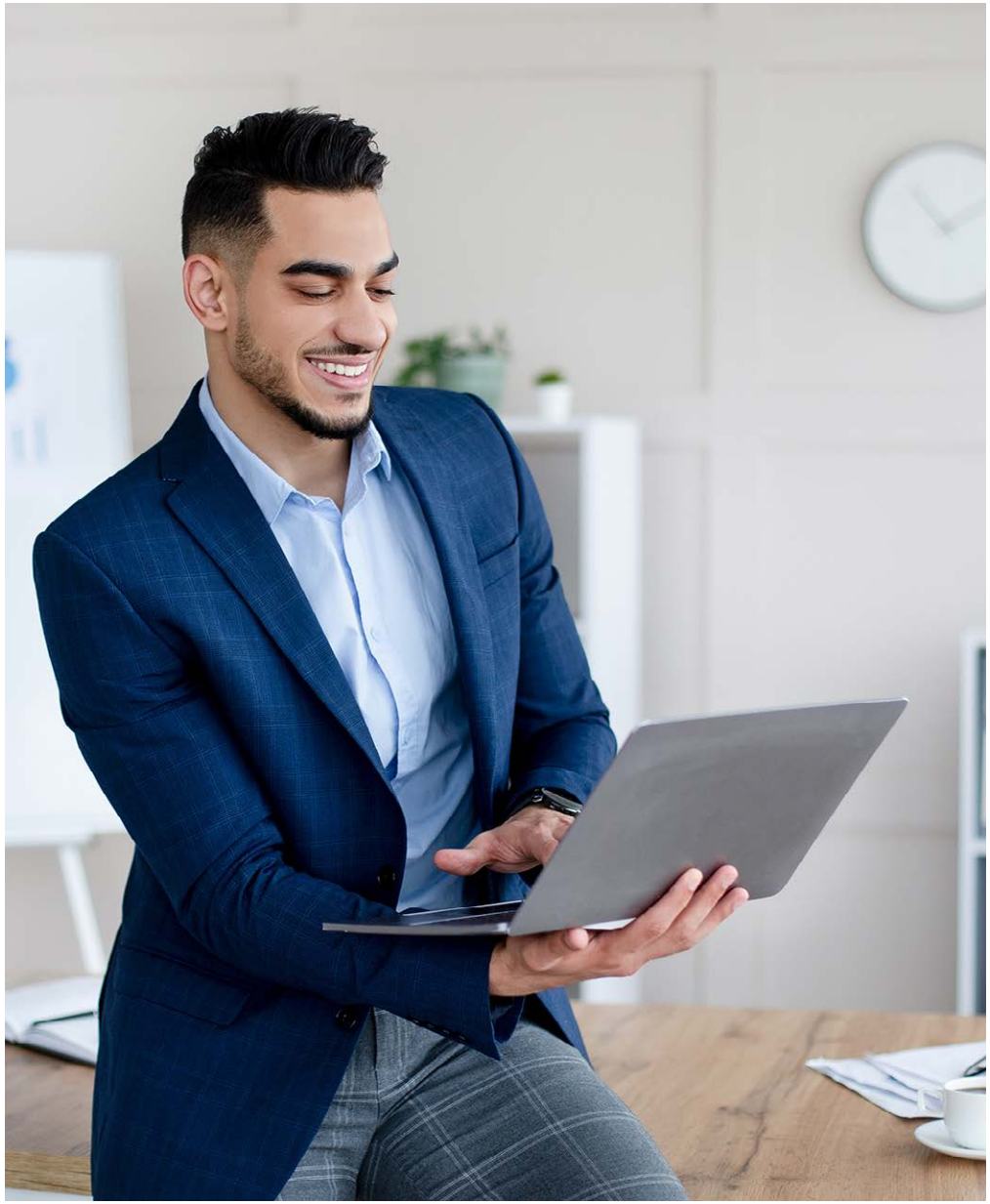
The FCA's British Steel Pension Scheme ("BSPS") redress programme continues to run its course. Notably, the FCA withdrew its redress calculator from 1 April 2025 due to the number of cases no longer requiring a bespoke calculation. Transitional arrangements are in place for ongoing cases. Firms still handling historic defined benefit ("DB") transfer complaints should assume continuing activity into 2026, but the overall number of cases is gradually finite.

For 2026, expect underwriters to keep asking about BSPS/DB transfer exposure. Strong documentation and proactive risk management strategies and actions should convert into better policy terms.

REGULATORY FOCUS IS LIKELY TO SHAPE 2026

The Duty (defined above) is a regulatory regime aimed at raising the standard of care firms must apply to retail financial consumers. The Duty introduced a new "consumer principle" under the FCA's rules: firms must act to deliver good outcomes for retail customers. It applies to authorised firms offering products or services to retail customers. The aim is to move beyond "tick-box" compliance and push firms to think about how consumers fare – in value, transparency, support, and suitability.

The FCA's 2025–26 Duty focus areas are explicit. Some priority themes include: (a) embedding the Duty and sharing good practice; (b) price and value outcome scrutiny; and (c) vulnerability and data protection. The first of these will entail multi-firm reviews on how the Duty is embedded across sectors, product governance, monitoring and customer journeys. In terms of price and value outcome scrutiny, firms will be particularly scrutinised for how they assess "fair value" and demonstrate value for customers. In terms of vulnerability and data protection, the FCA will work with the Information Commissioner's Office to issue joint guidance in early 2026 on the interplay of vulnerability, data-sharing and the Duty.



IFAs should assume continued scrutiny of suitability, vulnerable customer support, and fair value. The FCA has recently stated that it sees *"the greatest need to address actual or potential harm."*

The Advice Guidance Boundary Review ("AGBR") is a response to a growing concern that most consumers in the UK are not getting the financial help they need. The review is a joint initiative between His Majesty's Treasury ("Treasury") and the FCA, to examine the regulatory boundary between financial advice and other forms of support. The AGBR timetable signposts a policy statement on *"targeted support"* by December 2025 and a consultation on *"simplified advice"* in January 2026. If implemented (via proposed amendments to the Financial Services and Markets Act 2000), 2026 could see new, clearer pathways for lower-cost help - reducing "advice gap" friction but introducing fresh operational and liability questions around scope, disclosures, and triage. Making financial advice more accessible to a larger portion of the population should, in theory, lead to improved financial outcomes. However, providing advice to customers who may be relatively inexperienced or less financially sophisticated inevitably increases the risk of complaints and claims - particularly where the advice was not fully understood or was based on incomplete information about the customer's financial situation. Expect ongoing FCA scrutiny and potential FOS sympathy where firms cannot evidence tailored support to vulnerable customers; this directly affects causation and quantum in professional negligence claims.

Documentation and file quality will be an IFA's best defence (and best premium lever). It is imperative that files demonstrate customer understanding and fair value, not just technical suitability.

The FCA's supervisory stance in 2026 will raise the bar for IFAs' files and proper record-keeping. We expect miscommunication and fees/value disputes to remain a fertile area for complaints. Documentation and file quality will be an IFA's best defence (and best premium lever). It is imperative that files demonstrate customer understanding and fair value, not just technical suitability. Evidence Duty outcomes: keep a concise pack - product governance, value assessments, vulnerable customer framework etc. In terms of legacy pension exposures, maintain a live register of BSPS/DB cases, redress status, and reserves. IFAs should also be ready to show lessons learned from errors and remedial actions.

AI & TECHNOLOGY (INCLUDING CYBER RISKS)

The FCA's 2025–2030 strategy places innovation, economic growth and responsible AI at the centre of UK financial regulation. Aimed at becoming a smarter, more tech-driven regulator, the FCA plans to streamline supervision, digitise authorisations and reduce unnecessary reporting. Its four priorities are: improving regulatory efficiency, supporting sustained economic growth, helping consumers make informed decisions, and strengthening the fight against financial crime. A major shift is the FCA's focus on responsible AI deployment, supported by tools such as the Regulatory Sandbox, AI Lab, and new AI Live Testing. These initiatives encourage firms to innovate confidently while protecting consumers and markets. These pro-technology and agile initiatives are a clear sign that the FCA recognises AI's potential to transform financial services. Firms that

invest early in responsible AI, better data management and strengthened controls will be best positioned to grow under the new regime.

The emergence of digital advice platforms and robo-advisers - offering algorithm-based investment recommendations tailored to clients' risk profiles and financial objectives - has redefined the traditional IFA role. While these technologies make financial advice more affordable and accessible, they also bring new risks such as algorithmic mistakes, technical malfunctions, or unsuitable advice generated by automated systems.

As these digital solutions continue to gain traction, the nature of claims against IFAs is likely to evolve, potentially focusing on issues like inaccurate recommendations or system breakdowns. Consequently, PII policies will need to adapt to address these emerging risks, prompting insurers to evaluate the exposures associated with digital advisory tools. It remains essential for IFAs to maintain robust human oversight and verification processes to help prevent errors.

Another technology-driven factor influencing the PII market is the growing significance of cybersecurity and data protection. Financial advisers handle highly confidential client information, and any data breach - whether from hacking, phishing, or internal mismanagement - can result in severe reputational and financial consequences.

Insurers are increasingly prioritising cybersecurity when assessing PII applications. IFAs are expected to demonstrate strong data protection measures, including encryption, secure data storage, and regular security assessments.

UNDERWRITING BEHAVIOUR TO EXPECT IN 2026

With the PII market soft but selective, expect underwriters to reward IFAs undertaking proactive risk management. Proactive risk management is a key aspect underwriters look for when selecting risks. Carriers will continue to differentiate strongly between firms with similar revenue but different work-mix and legacy exposure.

There will continue to be persistent scrutiny of pensions and complex investments. DB transfers remain an underwriting red flag; even where exclusions soften (especially for vulnerable clients and retirement income advice).

IFA firms should review whether their level of cover still fits their case-mix. They should check that policy limits and aggregates properly cover a cluster of medium-to-large claims.

FINAL THOUGHTS

The trends in IFA professional indemnity insurance mirror the evolving landscape of financial advice - shaped by shifting regulatory requirements, technological advancements, and the growing complexity of financial products. Increasing premiums, heightened scrutiny of advice, the influence of claims management firms, and emerging risks such as cybersecurity threats and digital platform-related claims are transforming the PII market. For IFAs, keeping pace with these developments and adjusting their business models will be crucial to maintaining sufficient protection against potential liabilities and ensuring appropriate PII coverage.

To minimise these risks, financial advisers should take a proactive approach - providing clear and transparent advice, maintaining strong communication with clients, keeping up to date with regulatory developments and maintaining good record-keeping. This approach should enable them to better manage potential complaints and preserve a strong, trusted relationship with their clients.

To discuss how any of these issues might affect you, please contact

Martin Jensen
Partner
+44 (0)20 7469 0505
m.jensen@beale-law.com

FINANCIAL INSTITUTIONS

Financial institutions ("FIs") function within one of the most complex and rapidly changing risk landscapes. Below we briefly touch on just a few (of many) of these risks going into 2026 and beyond.

The past year has presented yet another challenging period for FIs. Ongoing conflicts in Ukraine and the Middle East, tariff/trade wars and the UK's domestic cost of living crisis have all contributed to an unstable geopolitical and economic environment. Regulatory, shareholder and customer expectations are increasing. Cyber risk is escalating, and fraud risk remains a persistent challenge.

The UK's economic outlook for 2026 is one of modest, below-trend growth. This growth is expected to be supported by falling inflation and potentially lower interest rates but constrained by global trade uncertainty, elevated labour costs and possible reduced public spending.

The full impact of tariffs is still unfolding and may turn the outlook more negative if there is further trade dampening in 2026 and beyond. Businesses may face challenges in adapting due to lengthy processes of supply chain reconfiguration and the uncertainty of changing trade policies which necessitate increased investment in technology and more flexible sourcing strategies.

Adopting a holistic approach to cyber risk management is essential.

Overall, it remains a period marked by uncertainty and pressure, with ongoing challenges for both FIs and their insurers.

CYBER AND AI

FIs, in common with other large organisations, must continuously evaluate and enhance their cyber security measures to reduce the risk of attacks. This involves maintaining robust security systems, conducting regular data breach assessments, and providing comprehensive staff training on how to recognise and respond to ransomware threats.

Adopting a holistic approach to cyber risk management is essential. This should encompass preventative measures, a well-defined incident response plan, and cyber insurance coverage. Implement robust cyber resilience, incident response plans, third-party oversight, penetration testing, and continuous monitoring. Fostering a 'no-blame' culture is essential, as it motivates employees to report incidents promptly, even when they may have accidentally caused, or contributed to, a breach. Together, these elements help organisations effectively manage breaches, reduce the likelihood of attacks, maintain regulatory compliance, and ensure financial resilience. 2025 saw several major cyberattacks on a number of UK businesses (see the Cyber section of this report) causing operations to be scaled back significantly or halted completely with significant financial, reputational and potential legal consequences.

Against a backdrop of heightened geopolitical tensions, the increasing interconnectedness and digitalisation of FIs is raising concerns around systemic cyber risk caused by malicious attacks. With policy makers and regulators pushing for enhanced cyber resilience frameworks that mitigate this risk and protect the stability of the wider financial system, FIs must ensure that

cyber risk management is integrated into their broader governance and operational risk structures so they can deliver against evolving regulatory expectations.

While AI delivers significant advantages - such as enhanced operational efficiency, improved regulatory compliance, personalised financial services, and sophisticated data analytics - it can also exacerbate certain vulnerabilities within the financial sector. These systems depend on large volumes of sensitive data which, if inadequately protected, may expose an organisation to cyberattacks, data breaches, or misuse. Additionally, AI can unintentionally reinforce existing biases, resulting in potentially discriminatory outcomes in areas such as lending, credit assessment, or recruitment.

A growing trend is the practice of making exaggerated or misleading statements about their use of artificial intelligence – this is known as "AI washing." This occurs when businesses overstate or fabricate their use of AI in order to attract investors or customers. AI washing can take several forms: claiming to use AI when none is actually involved, overstating an AI system's capabilities, or misrepresenting how AI is applied within the business.

The potential consequences of AI washing include regulatory enforcement (for example, under the Consumer Protection Regulations 2008) and possible legal claims from investors or shareholders over misleading representations about a company's AI use.

Some key AI risk management steps include carefully assessing risks across data, models, operations, and ethics, taking time to understand how each area may introduce vulnerabilities. It is important to ensure strong data integrity throughout the entire lifecycle of the system. FIs should implement safeguards like regular audits and structured human oversight, while also staying updated on relevant regulation to maintain compliance. Establishing proper governance frameworks and maintaining clear explainability documentation are also essential, ensuring that AI and algorithmic systems are both understood and explainable to stakeholders.

INNOVATION RISKS (GETTING LEFT BEHIND)

Fintechs, embedded finance, open banking, digital platforms and rapid technological advancement are reshaping the competitive landscape, elevating customer expectations and introducing new, more complex risk exposures. These forces are accelerating change across the sector and redefining how financial services are delivered,

accessed and integrated into everyday digital experiences.

Incumbent institutions may misjudge the scale or speed of these shifts, or underinvest in the innovation required to keep pace, leaving them increasingly outmatched by more agile players and vulnerable to strategic, operational and technological disruption.

Incumbent institutions may misjudge the scale or speed of these shifts, or underinvest in the innovation required to keep pace

INCREASING SCRUTINY (CONSUMER, ESG / REGULATORY, AND LEGAL)

The Consumer Duty remains a top FCA priority. Insurers of FIs anticipate more supervisory challenges around price and value assessments, as well as their treatment of vulnerable customers. This heightened scrutiny raises the likelihood of PI and D&O claims where FIs mishandle remediation or deliver redress that falls short of regulatory expectations.

The "failure to prevent fraud" element of the Economic Crime and Corporate Transparency Act 2023 ("ECCTA"), which came into force on 1 September 2025, makes large organisations criminally liable for fraud committed by associated

persons without reasonable prevention procedures. Other changes under the ECCTA, such as new responsibilities for the Registrar of Companies and identity verification rules for directors, have also been implemented.

There are increased expectations from shareholders, customers and society for ESG (covered elsewhere in this report), climate resilience, ethical AI and fairness in financial services. The FCA's anti-greenwashing rule took effect on 31 May 2024. This fuels mis-selling/ greenwashing exposures. FIs should exercise caution to avoid failing to disclose or misrepresenting ESG-related risks. There has been growing attention on ESG issues such as diversity and inclusion, social value, and employment practices.

In 2025 the FCA confirmed plans to extend non-financial-misconduct rules (bullying and harassment etc.) across tens of thousands of firms that are bound by the so-called senior managers and certification regime ("SM&CR") that is meant to hold senior bosses accountable for wrongdoing at their firms. While these are HR/culture rules, failures can spill into regulatory findings that aggravate PI exposure (e.g., systems and controls weaknesses). In terms of these plans *"serious, substantiated cases of poor personal behaviour"* by senior managers at a range of firms will have to be reported to the FCA, as well as future employers who are assessing whether new hires are fit and proper for the job. Previously, only banks were required to report bad behaviour to the watchdog. The expanded rules on non-financial misconduct, which also cover racism, sexual harassment and violence and intimidation, will come into force on 1 September 2026. Expect governance and HR investigations to feature more in due diligence and claims arguments.

The FCA has remarked that behaviour like bullying or harassment going unchallenged is one of the reddest flags – a culture where this occurs can raise questions about a firm's decision-making and risk management.

With the expanded SM&CR expectation around non-financial misconduct, FIs should ensure that incident reporting, speak-up channels, HR investigations, and regulatory references are handled in a manner fully aligned with their policies. Any regulatory findings of inconsistency or weakness in these processes can materially undermine a FI's ability to defend itself.

Cross-border legal risk stems from inconsistent rules across countries. For FIs, differing standards on product liability, insurance contracts, capital requirements, and data/privacy laws can create compliance gaps, raise legal exposure, and complicate operations when a product or practice acceptable in one jurisdiction violates another's regulations.

Social media, faster information flows and heightened brand risk now amplify the consequences of failures or

scandals. FIs are increasingly exposed to "narrative risk" - where perception, misinformation or rapidly spreading online commentary can distort reality or escalate negative sentiment.

Regulators are pushing for stronger governance, more rigorous stress testing, enhanced climate-risk disclosures and greater operational resilience. As a result, non-compliance risk is rising, with fines, enforcement action, and legal challenges becoming more frequent as regulators take a more proactive and interventionist stance. FIs are facing increased customer actions and board members and senior leaders are facing heightened personal accountability and liability exposure.

RISK MANAGEMENT STEPS

There are a number of risk management steps FIs (and insurers) can adopt, such as the following:

- Integrated risk management: Adopt holistic, enterprise-wide stress testing and forward-looking scenario analysis that brings together climate, credit, cyber, market, regulatory, operational and other emerging risks.
- Operational resilience and business continuity: Develop robust scenario planning for major outages and extreme but plausible disruptions. Diversify vendor and third-party dependencies, particularly across IT, cloud and data infrastructure to avoid concentration risk and single points of failure. Strengthen continuity playbooks, recovery protocols and testing cycles, aligned with UK operational resilience expectations.
- Regulatory engagement, transparency and compliance: Proactively stay ahead of evolving UK and international regulatory standards. Enhance transparency through clearer disclosures, stronger reporting and improved auditability of risk frameworks. Build reinforced governance structures, with active board oversight and integrated risk committees that maintain continuous dialogue with regulators.
- Culture, talent and adaptability: Cultivate a risk-aware culture that encourages accountability, foresight and agility in responding to new and evolving threats. Invest in talent with cross-disciplinary capabilities - spanning risk management, data science, climate risk, technology literacy and cyber resilience - to ensure the organisation can adapt quickly and confidently to future challenges.

Insurers offering D&O and FI policies will need to carefully assess the questions posed to prospective insureds to ensure they have adequate policies capable of withstanding regulatory scrutiny. Likewise, brokers may need to take a more detailed look into their clients' operations to confirm that coverage is sufficient - particularly regarding extensions for regulatory investigations, which are gaining increasing significance and complexity.

THE FI INSURANCE MARKET

As we move into 2026, it appears that the FI insurance market is beginning to stabilise, marked by increased competition among insurers and a decline in premiums. In this soft market, insurers are likely to keep a close eye on both existing and emerging trends to ensure they assume appropriate levels of risk, knowing that the tide can quickly turn against them.

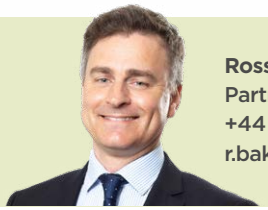
CONCLUSION

In common with many other lines of business, FIs face risks relating to AI and cyber, increased regulatory scrutiny and the potential for claims arising out of the three pillars of ESG.

There is some stability in the market after a few years of volatility, and this has seen an increase in capacity and a lowering of premiums.

With the economy in the UK in a state of flux, lenders could look closely at investments to determine whether funds are being used appropriately and in line with facility agreements - this could lead to claims against a range of different institutions.

To discuss how any of these issues might affect you, please contact



Ross Baker
Partner
+44 (0)20 7469 0509
r.baker@beale-law.com

Nathan Penny-Larter
Partner
+44 (0)20 7469 0498
n.penny-larter@beale-law.com

EDUCATION

The education sector in the UK continues to face an evolving landscape of legal, regulatory, and operational challenges.

It is now trite to say that the sector is in the midst of a funding crisis. Combine this with increasing expectations from parents and students, and it is easy to see a basis for increasing dissatisfaction among stakeholders and, in turn, an increase in the risk of complaints and claims. Problems of funding and resources are a common thread linking the topics addressed in this year's update.

SPECIAL EDUCATIONAL NEEDS AND DISABILITY ("SEND")

The Institute for Fiscal Studies (IFS') has warned that, without reform, supporting children with SEND in England could cost the government an additional £3 billion per year by 2029. The government is already spending c.£12 billion on SEND support in 2025 - an increase of 66% over the past decade, and according to projections from the IFS this will rise by a further £3 billion by 2029. It is widely acknowledged that the present system is not working, with substantial impacts on affected pupils. The Government has recently announced a delay, until 2026, of its much-anticipated white paper, citing the need for a further period of engagement.

Schools must monitor sanctions, consider their impact, ensure the cumulative effect of sanctions was not disproportionate, and apply discretion

In the meantime, children, parents, and schools, will have to continue to navigate the difficulties of the current system, and levels of disputes ending up before the overburdened SEND Tribunal will remain high. The impact on Schools (and their insurers) is not limited to defence costs in responding to SEND claims, but includes substantial time being spent by staff and senior leadership on such matters, with potentially adverse effects on all other pupils in the classroom and the corresponding risk of complaints from others. This is not an area that affects only those with SEND.

Whilst SEND Tribunal claims cannot themselves result in awards of compensation or costs to complainant parents, we are seeing an increase in parents and their solicitors seeking to use other means to try to persuade Schools to provide compensation, including parents bringing civil claims for damages following a successful SEND Tribunal claim. We have also seen parents seeking to amend the standard direction that proceedings (including the judgment) are to remain anonymous, with the obvious threat of adverse publicity thereafter. We understand that the Upper Tribunal is currently in the process of considering the basis for anonymity orders and the circumstances in which they may be lifted.

SCHOOL DISCIPLINARY POLICIES

The case of **EBB & Others v Gorse Academies Trust [2025] EWHC 1983 (Admin)** has gained wider attention as a test of disciplinary sanctions in schools.

The parents of three children brought claims for judicial review, having spent a total of 154 days in isolation during the 2023–24 academic year. Whilst the parents did not dispute the school's right to use isolation as a disciplinary measure, they argued

that its repeated use was so excessive as to be unlawful. It was argued that the school had failed to consider the negative impact of repeated isolation on the pupils' education, self-esteem, and socialisation. The High Court ruled that there was no legal basis for it to intervene. It found that each instance of isolation was consistent with the school's policy, noting that ongoing misconduct should be met with *"persistent, and indeed escalating, sanctioning"*. The Court emphasised that Schools must monitor sanctions, consider their impact, ensure the cumulative effect of sanctions was not disproportionate, and apply discretion (even a rigorous policy *"must be applied with an open mind"*).

We noted in last year's report that a 'hot topic' in the sector was the use of mobile phones, and that issue reached the High Court in 2025. In **R (SAG) v Governing Body of Winchmore School [2025] EWCA Civ 1335**, SAG was permanently excluded after being found to have had a mobile phone in her possession whilst on a school trip, and then, after the phone was confiscated, she (with the assistance of others) obtained the key and went into a teacher's room to retrieve it. The High Court and (via a 2:1 majority) the Court of Appeal found that the School had acted lawfully on the grounds that SAG's misconduct satisfied the threshold of 'serious breach', notwithstanding several references to the potential for the punishment to be deemed harsh. In a lesson for those drawing up such policies, a key reason for the dispute reaching the High Court (and for the dissenting judgment in the Court of Appeal) was inconsistent wording between the School's Behaviour Policy and its Exclusion Policy, which on the face of it contained different thresholds for misconduct warranting exclusion.

CYBER, PRIVACY AND DATA GOVERNANCE

The UK Government's 2025 *'Cyber Security Breaches Survey'* showed education institutions are a prime target for cyber security attacks. Among primary schools, 44% reported being the target of either breaches or attacks, close to the average UK business figure of 43%, but the percentages for secondary schools (60%), further education colleges (85%), and HEIs (at a staggering 91%) show them to be particularly attractive targets. The cause is perhaps not hard to identify; increasingly commercial institutions which hold substantial personal and sensitive data), but without the budget for (or perhaps focus on) the most rigorous cyber security measures.

In the latter part of 2025, the Information Commissioner's Office

("ICO") published a report which found that students were the primary source of the increase in cyber-attacks, many as a result of flawed practices such as the use of weak passwords. Students are unlikely to feel the same obligation to protect their university's cyber security as employees in a commercial business who may face disciplinary action for failures in that regard.

At the other end of the age spectrum, hackers attempted to extort the Kido nursery chain by stealing (and then later posting on a darknet site) images of children, and parents' data. Unusually, the hackers then blurred the images (and, they later said, deleted the data) because of a backlash against the nature of the target. The attack highlighted the need for greater focus on cyber security across the range of institutions in the sector. There are a number of 'no win no fee' solicitors seeking to bring claims against universities for data breaches.

The risks of claims from cyber-attacks are not limited to claims by those whose data may have been breached, since cyber-attacks have the potential to cause widespread disruption and loss of access to learning.

ARTIFICIAL INTELLIGENCE ('AI')

In June 2025, an article published by the OfS recognised the risks of the use of AI in the sector, whilst at the same time acknowledging the vast potential benefits of the use of AI by students and in the sector as a whole.

The government's White Paper on further and higher education stated that the Government would support the OfS *"to assess the impact of artificial intelligence, including how students are using it in assessments, to ensure the integrity of higher education assessment and qualifications are not compromised"*. Much work in this area is needed, and progress will need to be made at pace; a survey by the Higher Education Policy Institute ("HEPI") in February 2025 noted that the proportion of students using generative AI tools such as ChatGPT for assessments had jumped from 53% to 88% in the previous year, and that the proportion of students reporting using any AI tool has jumped from 66% to 92%. Of those who use AI, 50% said it was to improve the quality of their work. It is of course difficult for universities and regulators to keep up with the pace of change, and the exponentially increasing abilities of generative AI will only make the sector's position more difficult. Interestingly, 59% of AI users agreed with the statement that the way they are assessed has changed 'a lot' in response to generative AI, and 76% believed that their institution would spot the use of AI in assessments, so plainly measures are being taken to deal with the potential threat.

Generative AI is not going away and simple bans are unlikely to be effective or practical at least in the medium to long term.

We are yet to see a claim relating to the use of AI, but there are undoubtedly risks not only from the use of AI but also the ways in which institutions adapt to the risks of AI being used. The HEPI survey noted students' concern at the lack of certainty being provided by universities as to if, when, and how, AI can be used. Uncertainty in policies and practises around the use of AI presents obvious risks of claims and will affect the extent to which universities will be able to effectively respond to such claims. Generative AI is not going away and simple bans are unlikely to be effective or practical at least in the medium to long term.

STUDENT WELFARE

In May 2025, the National Confidential Inquiry into Suicide and Safety in Mental Health ("NCISH") published its *'National review of higher education student suicide deaths'*, relating to academic

year 2023-24. NCISH was informed of 169 incidents; 107 suspected suicide deaths and 62 incidents of non-fatal self-harm. Of the 169 incidents, serious incident reports were submitted for 104 (62%) of these.

Of the incident reports of suspected suicides, 70% were for students who were already known to university support services, including in relation to mental ill-health (almost half of them), financial problems, and harassment.

The report makes a number of recommendations, including mandatory mental health awareness and suicide prevention training for all staff; increased input from students' families; and the introduction of a 'duty of candour' to be open and transparent with families. HEIs should provide earlier and more integrated support, especially at transition points (first year, exam periods), and more actively monitor disengagement. The report suggests that universities, rather than external agencies alone, need to view student mental health and suicide prevention as integral to institutional governance and student safety - not just a pastoral add-on.

Again, the implementation of recommendations will be subject to universities' conducting an increasingly difficult financial balancing act, with around four in 10 universities in financial deficit.

The legal context for this issue remains the High Court decision in **Abrahart v University of Bristol [2024] EWHC 299 (KB)[WM2.1]**, in which the High Court declined to decide the question of whether a duty of care was owed by HEIs to their students in this regard. Campaigners, including Ms Abrahart's parents, have long called for the statutory introduction of such a duty, and although the Government's is reported as saying there are "legal challenges" to the introduction of such a duty, it has not been ruled out.

CONCLUSION

The year ahead presents increasing challenges for educational institutions to strengthen compliance, improve student welfare protection, and pro-actively manage a number of increasingly uncertain risks, in order to avoid legal, regulatory and reputational repercussions, whilst battling a funding crisis which shows no signs of abating.

To discuss how any of these issues might affect you, please contact

Nathan Penny-Larter
Partner
+44 (0)20 7469 0498
n.penny-larter@beale-law.com

Martin Jensen
Partner
+44 (0)20 7469 0505
m.jensen@beale-law.com

ENVIRONMENTAL

Environmental issues continue to be a major concern for both businesses and governments in the UK and around the world. Key focus areas include the impact of the fossil fuel sector, the expansion of the renewable energy industry, challenges related to air quality, biodiversity, waste management, and water quality.

Environmental reporting in the UK is becoming increasingly mandatory and wide-ranging. Businesses are facing stronger expectations to be more transparent and accountable for their environmental impact.

In July 2025, the International Court of Justice issued a unanimous advisory opinion stating that states have stringent obligations to prevent and reduce greenhouse gas emissions to protect against climate change. This ruling is not binding but can have wide-ranging consequences by providing legal backing for countries to take action against each other.

These are all issues that are of significance for insurers, both within the specialist environmental sector and the broader insurance market.

POTENTIAL LIABILITY EXPOSURE PRESSURE POINTS IN 2026 AND BEYOND

UK-specific scrutiny and early litigation signals relating to per- and polyfluoroalkyl substances ("PFAS") are growing.

The FCA's anti-greenwashing rule (effective 31 May 2024) applies to all FCA-authorised firms' communications. In 2026, expect more scrutiny of sustainability claims. In parallel, the Digital Markets, Competition and Consumers Act 2024 ("DMCC") grants the Competition and Markets Authority ("CMA") direct fining powers (effective from 6 April 2025), raising green claims exposure (including for insureds, with implications for PII/D&O). Insurers will keep tightening wording around "sustainability" claims and exclusions/conditions for marketing-related misstatements.

PFAS pose one of the most complex and urgent environmental challenges currently confronting the UK

Recent developments suggest that scrutiny and action against the water sector continues to increase. This presents elevated liability risk for utilities and their contractors in 2026. Examples of recent developments in this arena are:

- In May 2025, Thames Water was fined a record £122.7 million for repeated sewage discharges and breaches of rules relating to wastewater operations and dividend payments.
- Government information released on 20 May 2025 states that a record 81 criminal investigations into water companies had been launched in England since the election, as part of the government's crackdown on sewage dumping. The number of inspections carried out by authorities into sewage pollution has increased by nearly 400% since last July 2024.
- The Water (Special Measures) Act 2025 (the "Act"), in force from 24 February 2025, strengthens the powers of water sector regulators to address pollution and underperformance in water companies. Notably, these rules require water companies to stop performance-related pay for senior executives when the company fails to meet specified performance

standards. In Q2 2025, Ofwat exercised its new statutory powers to issue bonus prohibition orders against six major water companies, including Thames Water, United Utilities, and Southern Water.

With effect from 24 April 2025, the Act also provides for criminal sanctions. The Act increases the maximum punishment for water executives, where they impede an environmental investigation through consent, connivance or neglect, or fail to assist a drinking water inspector's investigation without reasonable excuse, to 2 years' imprisonment.

Under the Companies Act 2006, directors are required to act in the company's best interests (s.172) and to exercise appropriate care, skill, and diligence (s.174). The Act effectively elevates expectations by recognising that environmental non-compliance can amount to a breach of these statutory duties, especially where directors disregard regulatory warnings or fail to respond to issues identified in internal audits.

Although the Act's provisions currently apply only to the water industry, they signal stricter regulatory oversight of environmental liabilities across various sectors. The provisions of the Act may serve as a model for future sector-specific measures, reinforcing the idea that those who exercise operational control and profit financially should also carry legal responsibility for environmental damage.

In October 2025, the UK government launched a public consultation on strengthening the Environment Agency's ("EA") enforcement powers against water companies, following the abovementioned Act. The proposals include allowing the EA to impose variable monetary penalties to the civil standard of proof (i.e. "on the balance of probabilities" rather than the stricter criminal standard of "beyond reasonable doubt") for a range of permit and licence breaches, as well as other permitting, abstraction, impounding and drought offences. It also proposes automatic fixed penalties that can be applied more swiftly and proportionately to minor and moderate environmental offences without the need for lengthy criminal proceedings.

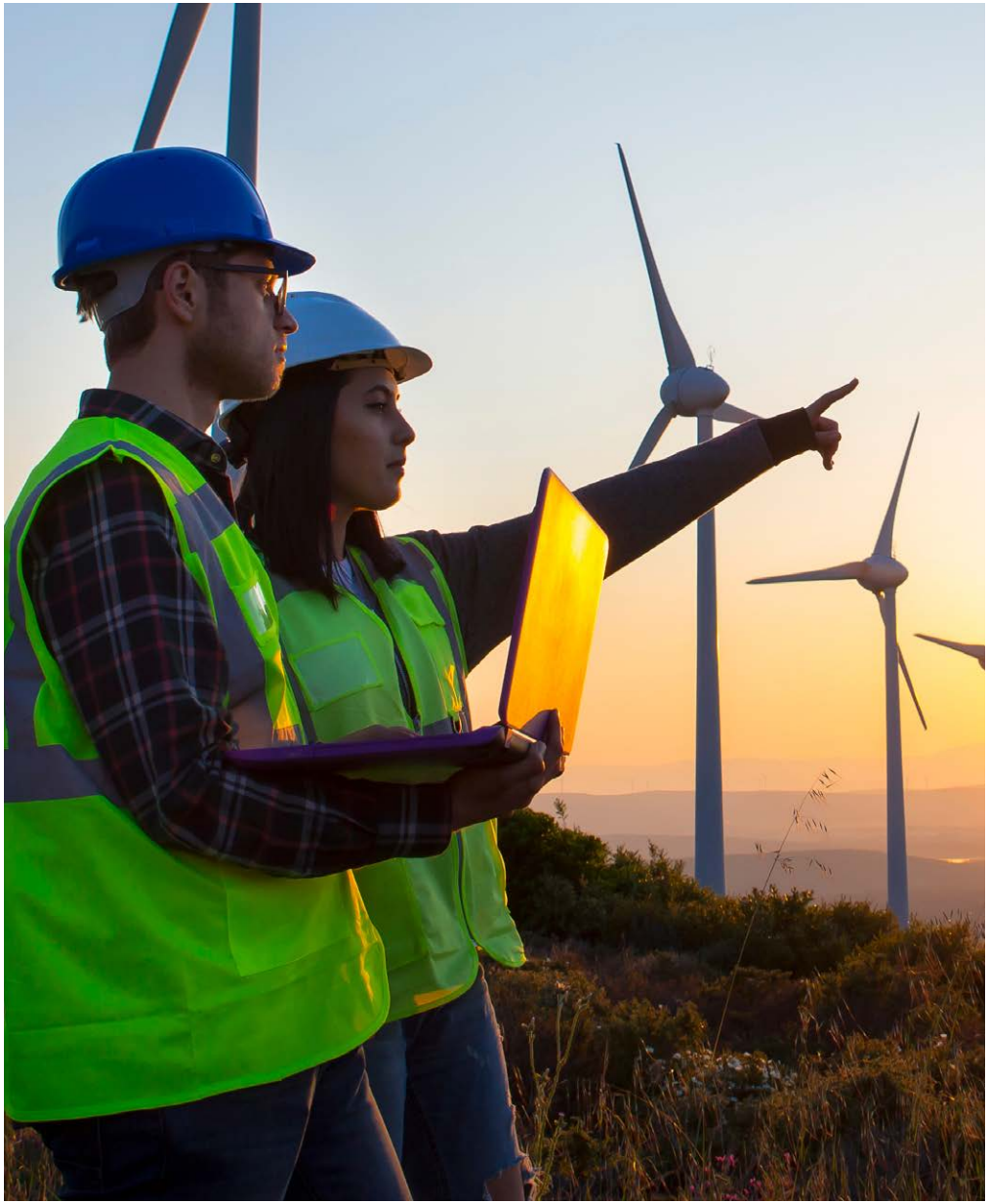
ENVIRONMENTAL REPORTING

UK environmental reporting is becoming more mandatory and comprehensive, driven by increasing scrutiny from stakeholders and government. There is a growing demand for more transparency and accountability from businesses regarding their environmental impact.

Key obligations relating to environmental reporting include mandatory Streamlined Energy and Carbon Reporting ("SECR") and the implementation of new Sustainability Disclosure Requirements ("SDRs"). The government is also monitoring progress against environmental targets, adding pressure for effective implementation and reporting across all sectors.

SECR is a mandatory regulation for large companies meeting at least two of three criteria: £36 million turnover, £18 million balance sheet, or 250 employees. SECR requires reporting on energy use and carbon emissions in the UK. In terms of SDRs, the UK is expected to adopt the International Sustainability Standards Board's (ISSB) standards in 2026. This will require UK-listed companies to report on sustainability-related risks and opportunities in a standardised way. As part of the SDRs, companies will need to include climate-related financial disclosures in their strategic reports, focusing on governance, strategy, risk management, and metrics and targets.

Ensuring accurate and transparent reporting is both a legal requirement and a key part of modern corporate governance. There are several potential consequences in the event of non-compliance. A failure to ensure accurate reporting may breach directors' duties under the Companies Act and lead to directors' and officers' liability. Non-compliance can damage reputation, affect investment decisions and increase scrutiny from lenders and



shareholders. Non-compliance may also signal potential operational risks such as the masking of climate-related risks, exposing the organisation to financial and strategic harm.

PFAS LIABILITY RISKS ACCELERATE FROM EMERGING TO MATERIAL

Also known as 'forever chemicals' due to their very strong chemical bonds, PFAS do not break down easily in the environment, can build up in living organisms, and are linked to serious illnesses. These synthetic chemicals are found in many consumer products like non-stick cookware, stain-resistant fabrics, cosmetics, firefighting foam, and food packaging. PFAS pollution is so widespread that the chemicals are thought to be in the blood of almost every human on the planet.

An EA-commissioned report (July 2023) estimated the cleanup of high-risk PFAS sites in England could cost £31 billion to £121 billion, potentially making development projects unviable. The report identified up to 10,200 high-risk sites, including landfills, wastewater treatment works, and industrial areas. The high cost stems from the persistence of PFAS and the specialised equipment needed to remove them from water and soil.

Businesses using, or having used, 'forever chemicals' in their manufacturing processes, or supplying products containing such substances, are facing increasing risks of legal claims in the UK as regulatory standards governing their use come under greater scrutiny.

Leading experts in PFAS have criticised the UK government for failing to take stronger action to tackle PFAS pollution and refusing to match the impetus in the EU to ban non-essential uses of the substances. For example, currently, there are no legally binding limits on PFAS levels in drinking water in England - only guidance from the Drinking Water Inspectorate. In contrast, Scotland has adopted more stringent standards, aligning more closely with EU proposals.

There have been claims and class actions across various other jurisdictions, raising liability and coverage concerns for UK insurers:

- In 2024, 3M announced settlements for $10.3 billion with certain US public water systems/municipalities (responsible for drinking water supply) because of alleged PFAS contamination in drinking water. 3M have said it plans to exit PFAS manufacturing by the end of 2025.
- In a class action filed in the US in January 2025, Apple are facing

allegations that certain Apple Watch bands contain harmful levels of PFAS. It is claimed that Apple knowingly sold smartwatch bands that may contain potentially harmful PFAS, while marketing its product as health-conscious and environmentally sustainable.

- In a landmark ruling in June 2025 an Italian court sentenced 11 former executives of the Miteni chemical company to up to 17 years in prison for polluting water and soil in the Veneto region with PFAS. The company was also ordered to pay €58 million in compensation. This case is significant as it is one of the first times corporate managers have been held criminally liable for PFAS pollution in Europe.

PFAS pose one of the most complex and urgent environmental challenges currently confronting the UK. Intensifying regulatory scrutiny and potential litigation are driving UK insurers to take precautionary measures. They are re-evaluating their exposure to PFAS-related liabilities, especially within sectors such as manufacturing, waste management, and water utilities. Several insurers have already excluded PFAS from general liability and environmental impairment policies, while others are introducing stricter underwriting requirements.

NUISANCE

In June 2025, the Irish High Court passed judgment in the case of **Byrne & Moorhead v ABO Energy Limited & Ors ([2025] IEHC 330)**. Please see our article here for more detail. The case concerns remedies for private nuisance and damages for amenity interference relating to the adverse impact of wind turbine operations on a couple's home. The court ruled in the couple's favour, ordering the permanent shutdown of three out of six turbines, awarding them €360,000 in damages (including €60,000 in aggravated damages). While the judgment refers to UK Supreme Court cases, it diverts from the traditional methods of assessing damages for loss of amenity in England and Wales. The judgment is significant as it may influence how nuisance claims are assessed, especially regarding the measurement of damages for loss of amenity and the appropriateness of injunctive relief, even beyond the Irish legal system.

LITHIUM (BATTERIES): AN EMERGING RISK?

Lithium-ion batteries have become widespread, powering everything from electric vehicles and consumer electronics to renewable energy storage systems. However, as production and disposal volumes increase, a variety of environmental liability and civil liability risks are emerging.

For example, their manufacturing involves toxic chemicals (lithium, cobalt, nickel, manganese) that pose contamination risks. Mining lithium and cobalt can lead to groundwater depletion and contamination. Even though these batteries enable decarbonisation, their supply chains can be energy-intensive. Thermal runaway incidents can cause air pollution (toxic fluorine compounds) and property loss. Fires or leaks may release heavy metals and electrolytes, leading to soil or water contamination. Improperly disposed batteries can leach toxic materials in landfills or explode. Incomplete recycling or informal recycling operations pose environmental and worker safety hazards.

Regulations emerging abroad (e.g., EU New Battery Regulation 2023/1542) may encourage UK-specific legislation and/or create new liabilities.

CONCLUSION

Environmental regulatory action continues to increase as authorities intensify enforcement to address pollution, climate risks, and corporate non-compliance.

Perhaps unsurprisingly, within the insurance industry there is an increasing trend of more and wider exclusions in environmental impairment liability and standard liability policies. This is driven by the growing awareness of environmental risks, mounting liabilities, and evolving regulation.

To discuss how any of these issues might affect you, please contact

Michael Salau
Partner
+44 (0)20 7469 0448
m.salau@beale-law.com

HEALTH & SAFETY

In 2025, several key developments and trends have emerged of which every UK employer should be aware, no matter their industry or size. As legislation and steps being taken by the HSE evolve, staying ahead of the curve is not just smart - it is essential. It is about safeguarding your people, your business, and your reputation.

RECENT HSE STATISTICS

On 20 November 2025, the Health and Safety Executive ("HSE") published its statistics on work related ill-health and workplace injuries for 2024/25. Although Great Britain is one of the safest places in the world to work today, the HSE has stressed that there remains room for further improvement with an estimated 40.1 million working days lost in 2024/25 due to self-reported work-related ill health or workplace injury. The HSE reported 1.9million workers suffering from work-related illness, 964,000 of which were owing to mental health and 511,000 as a result of musculoskeletal disorder.

The construction industry recorded the highest number of deaths, with 35 fatalities, equating to c. 28% of all fatalities

The HSE's annual fatality statistics published on 2 July 2025, show that 124 workers were killed in work-related accidents in Great Britain in the period from April 2024 to March 2025. While this marks a reduction of 14 fatalities from 2023/24, the figure remains broadly consistent with levels observed prior to the COVID-19 pandemic, indicating a return to the long-term average rather than a significant shift in safety outcomes. This may suggest that overall progress in reducing workplace fatalities has plateaued.

These figures do not include: (a) a total of 92 members of the public who were in a workplace but were not working themselves; or (b) deaths arising from occupational diseases or diseases arising from certain occupational exposures.

The construction industry recorded the highest number of deaths, with 35 fatalities, equating to c. 28% of all fatalities. This is owing to its inherently high-risk activities such as working at heights, operating heavy machinery, and exposure to various site hazards.

KEY TRENDS

A CHANGE IN HSE'S INSPECTION APPROACH

The HSE is preparing for a major change in its inspection approach for 2025 - 2026, placing a stronger focus on occupational health and hygiene. The aim is to allocate more resources towards proactive health initiatives to better manage risks and enhance worker protection. The HSE aims to deliver 14,000 of these proactive inspections.

Unlike safety compliance, tackling health risks requires a more complex evaluation of long-term management and control strategies. For this reason, the HSE plans to direct its inspection efforts toward areas where there is the greatest potential to improve worker well-being and reduce work-related ill health. These targeted inspections will focus on managing risks from asbestos, noise, musculoskeletal disorders, hazardous dust and work-related stress and aggression. As these are all risks that can be found in the construction industry, coupled with its inherent high-risk nature, the construction sector is

likely to come under more intense HSE scrutiny.

The inspections will check dutyholder compliance where health surveillance is legally required, including the quality of consultancy and occupational health services being provided.

According to the HSE, its use of artificial intelligence ("AI") to analyse vast quantities of data (including inspection reports) is unlocking valuable insights to improve safety for workers across construction and other industries. The HSE has stated that in 2025 to 2026, this will identify further interventions.

SENTENCING GUIDELINES TIGHTENED FOR VERY LARGE ORGANISATIONS (VLOS)

In June 2025, the Sentencing Council announced amendments to the sentencing guidelines, specifically targeting organisations with turnovers far exceeding £50 million – 'Very Large Organisations' ("**VLOs**"). These revisions, in force since 1 June 2025, are intended to give the courts clearer guidance, and therefore more consistency, when sentencing VLOs.

The amendments specify that courts *should* consider imposing fines outside the range set for large companies, ensuring that penalties appropriately reflect both the organisation's financial position and the gravity of the offence - replacing the previous guidance that they may do so. The revised wording relating to VLOs does not introduce any threshold, fixed mathematical formula, or additional guidance on determining the starting point or range of fines for such organisations. The Sentencing Council has confirmed that it would be inappropriate to define VLOs by reference to a specific turnover threshold.

The HSE is preparing for a major change in its inspection approach for 2025 - 2026, placing a stronger focus on occupational health and hygiene.

The practical effect of the revised wording is that it could, in theory, lead to higher fines. However, we do not expect a substantial change in practice. This is because even before the amendment, judges were unlikely to begin within the large organisation category when sentencing VLOs. Accordingly, VLOs were already being sentenced outside the large organisation bracket. The updated wording simply codifies existing practice.

The court is advised to take account of any potential reduction for a guilty pleas in accordance with section 144 of the Criminal Justice Act 2003. In practice, companies and individuals

may enter early guilty pleas for health and safety offences to reduce the financial penalties imposed by the court.

ENFORCEMENT AND HEADLINE CASES KEPT PRESSURE HIGH

A number of substantial fines and sentences were handed out for health and safety breaches in 2025. Examples pertaining to the construction industry are as follows: Network Rail was fined £3.75 million for health and safety breaches that led to the death of two track workers in south Wales in 2019; Marlborough Highways Limited was fined £1 million following the death of an employee who was struck by a reversing road sweeper on a resurfacing project.

There has also been a focus on individual liability. A paddleboard business owner, Ms Nerys Lloyd, was sentenced to 10 years and six months in prison for gross negligence manslaughter and a breach of the Health and Safety at Work etc. Act 1974 after the deaths of four people in October 2021. Gross negligence manslaughter may be pursued when a failure to act or improper actions breach a duty of care and create a foreseeable risk of death. Despite severe weather warnings and significant flooding, Ms Lloyd proceeded with a paddleboarding excursion without assessing the dangerous conditions at the weir, conducting a safety briefing, or warning participants about the risks. Ms Lloyd also lacked the proper qualifications to lead the tour. The conviction stands as a clear warning to all organisations about the critical importance of complying with safety regulations and effectively managing risks.

BUILDING SAFETY (INCLUDING CONSTRUCTION)

- As one of the most hazardous industries, the construction sector will remain under scrutiny in 2025 as the government seeks to enhance safety measures within the built environment sector.
- Following the Grenfell Tower Inquiry, the HSE has continues to increase its scrutiny of individual accountability. With increased investigation in about those carrying out dutyholder roles and potential failures to meet their responsibilities under the CDM Regulations 2015. This approach is reflected in the HSE's 2025/26 inspection plan, which, as alluded to above, sets a target of 14,000 proactive and targeted inspections focusing on health priorities and verifying that dutyholders are effectively managing physical health risks in the workplace.

  The Building Safety Act 2022 ("the Act") has significantly increased the responsibility and potential criminal liability for individual site managers and companies for safety failures, particularly in high-rise residential buildings. A key aspect of the Act is the creation of the Building Safety Regulator ("BSR") within the HSE to oversee enforcement and competence. The BSR's strategic plan for 2025 – 2026 focuses on embedding the new regulatory regime, improving competency across the sector, and accelerating remediation for high-risk buildings (HRBs) still affected by unsafe cladding.
- **Off-site construction:** The growing adoption of modular and prefabricated construction is rapidly transforming how buildings are made. By producing components in controlled factory settings and assembling them on-site, offsite construction minimises exposure to hazards like working at heights or in adverse weather conditions. This method not only improves worker safety but also reduces on-site risks such as overcrowding, theft, and vandalism, while boosting efficiency and lowering environmental impact. However, these techniques also bring new safety challenges, particularly related to site assembly and transportation logistics. This may shape future safety standards and guidelines.
- As covered further in this report, **Martyn's Law,** officially the Terrorism (Protection of Premises) Act 2025, is

legislation that requires venues and events to improve security and preparedness for potential terrorist attacks. Martyn's law creates duties for specified public premises and events to take proportionate protective-security steps against terror risks (with thresholds by venue size). This materially affects public-facing insureds (hospitality, retail, entertainment, sports, education, healthcare estates). With both civil and criminal penalties at stake, immediate action is essential. Documented adequate training in situational awareness, lockdown and evacuation procedures, crowd management, and access control is a legal requirement.

Wearables, monitoring tools, and digital compliance platforms are rapidly becoming integral to the health and safety compliance landscape.

INCREASED USE OF TECHNOLOGY

Wearables, monitoring tools, and digital compliance platforms are rapidly becoming integral to the health and safety compliance landscape.

Wearable devices can monitor worker fatigue, heart rate, and exposure to hazards, sending real-time alerts for immediate action. AI-powered cameras and sensors can detect hazards, ensure PPE compliance, and predict equipment failures. AI/predictive analytics can analyse data to identify trends and predict potential hazards or equipment failures before they cause an accident.

Although not yet mandatory, the direction is evident - HSE authorities and insurers increasingly expect businesses to adopt smart, trackable systems.

CONCLUSION

Health and safety legislation is moving towards greater accountability, stronger documentation, and a wider view of workplace risks - from physical to psychological.

We expect continued inspection programmes in high-risk industries such as construction, agriculture, and waste/recycling. Continued attention to high-risk industries and activities is essential. The HSE's increased use of data/AI may lead to more targeted and successful prosecutions.

We expect a potential increase in claims and notifications under professional indemnity policies. It is important that organisations undertaking dutyholder roles ensure that they have a good understanding of their statutory responsibilities. It is also expected that the HSE's focus on individuals will result in an increase in notifications under Directors & Officers policies.

It is important to note that insurance policies do not cover fines arising from health and safety breaches (for public policy reasons). However, in our experience, they do typically cover defence and prosecution costs, including expenses related to preparing for and attending police interviews. Furthermore, given the nature of health and safety investigations, conflicts of interest can occur when both an organisation and its employees are prosecuted in connection with the same incident. In such cases, insurers may need to seek guidance on whether separate legal representation is required for the company and the individuals involved during an HSE investigation

To discuss how any of these issues might affect you, please contact

Joanna Lewis
Partner
+44 (0)20 7469 0444
j.lewis@beale-law.com

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE

Whether it is the cancellation of Diversity, Equity and Inclusion policies and climate change commitments following President Trump's re-election in the US, forthcoming regulations in respect of climate change 'greenwashing', or so-called ESG ratings providers closer to home, ESG issues have continued to make the headlines around the world in the last twelve months. This gives cause for concern for both insurers and insureds in a rapidly changing landscape.

INCREASING (REGULATORY) SCRUTINY

The landscape in the UK is being reshaped by several new and updated regulations:

- The updated Corporate Governance Code mandates boards to report on the effectiveness of all material controls, including those for non-financial issues (which include ESG).
- Providers of ESG ratings will come under the regulatory remit of the Financial Conduct Authority ("FCA"). The new rules are expected to be effective from June 2028. The legislation is aimed at ensuring transparent, reliable, and comparable ESG ratings, requiring both domestic and international ESG ratings providers that serve UK clients to be authorised and supervised by the FCA to increase transparency, reduce conflicts of interest, and address greenwashing in the growing market. The FCA plans to consult on specific rules for the new regime, which will be shaped by international standards, including recommendations from the International Organisation of Securities Commission ("IOSCO") and responses to the consultation are being accepted up to and including 31 March 2026.
- Europe is also tightening oversight of ESG ratings providers. In October 2025, the European Securities and Markets Authority announced that it would begin registering ratings agencies under the new ESG ratings regulation, with effect from 2 July 2026. The framework, to be enforced by the financial markets regulator, sets out how agencies issue ratings that assess companies' financial exposure to ESG-related risks.
- The FCA has been developing the Sustainability Disclosure Requirements ("SDR") regime, which aims to enhance transparency in corporate sustainability practices, standardise sustainability reporting, and combat greenwashing through clear and credible sustainability labels. An "anti-greenwashing" rule for FCA-regulated firms came into effect in 2024. Insurers and intermediaries making sustainability-related claims face the FCA anti-greenwashing rule and SDR-adjacent marketing guardrails.
- From 2026, the UK will begin phasing in mandatory climate-related financial disclosures under the UK Sustainability Reporting Standards ("SRS"). The SRS forms a key part of the SDR framework and is aimed at guiding how organisations assess and disclose information about their sustainability-related risks and opportunities, with an initial focus on climate-related disclosures.
- Beyond the FCA, the Competition and Markets Authority ("CMA") is actively policing environmental claims (e.g., fashion sector undertakings). The CMA now has direct fining powers (up to 10% of global group turnover) under the Digital Markets, Competition and Consumers Act

2024, effective from 6 April 2025. Action taken by the CMA in recent years includes ASOS and George at Asda to ensure the environmental impact of products are "accurate and clear" and to clamp down on "greenwashing". In practice, general-purpose "eco/sustainable" claims without evidence, or weak qualifiers, are high-risk.

- Supervisory expectations keep tightening. The Prudential Regulation Authority ("PRA")'s SS3/19 (updated in November 2024) remains the anchor for climate risk governance, scenario analysis and capital. In 2025, the PRA consulted on clearer expectations for banks/insurers to integrate climate impact across underwriting, reserving, market, credit and operational risk (Consultation Paper 10/25). Firms are expected to evidence board oversight, risk appetite, exposure measurement, and forward-looking scenarios (with less reliance on backward-looking data).

CONSTRUCTION

ESG in the UK construction industry can involve adopting strategies to achieve net-zero, address sustainability, and improve ethical practices, driven by increasing investor and stakeholder interest and a growing need for regulatory compliance. Key aspects include reducing carbon emissions through whole life carbon assessments and sustainable material use, improving worker safety and community engagement, and enhancing governance through transparency and accountability in supply chains. Companies are integrating ESG into project planning to enhance their long-term viability, attract investment, and stay competitive in a rapidly evolving and ESG-aware market.

Supervisory expectations keep tightening.

The construction industry accounts for a substantial share of global emissions. Transforming this sector will play a crucial role in helping the UK achieve its 2050 net-zero targets. However, progress is being hindered by the high cost associated with green innovation. These financial burdens primarily fall on contractors and developers, who are already working with extremely narrow profit margins. The construction industry is under significant pressure, facing continuing inflation and a high level of insolvencies.

A strong ESG strategy should encompass not only the business itself but also its entire supply chain and suppliers. Smaller suppliers (SMEs) may often lack the resources to invest in sustainability on their own. Construction

leaders need to identify effective ways to promote and support sustainability initiatives throughout their supply networks.

ESG is playing an increasingly important role in commercial decisions, including in tenders. We expect that trend to continue. From 24 February 2025, the Procurement Act 2023 places greater weight on social value and environmental factors in public sector contracts. Businesses bidding for public contracts must now demonstrate strong ESG credentials to be successful. The Procurement Act integrates ESG principles more formally into public procurement by expanding the definition of "value" beyond cost to include social and public benefits. Public bodies must now *"have regard to the importance of maximising public benefit,"* moving beyond the previous requirement to "consider" and making ESG a legal obligation when awarding contracts. This shift is supported by changes including replacing 'Most Economically Advantageous Tender' with 'Most Advantageous Tender' and requiring suppliers to demonstrate ESG credentials like carbon reduction plans and fair labour practices.

ESG RISK MANAGEMENT

Climate and ESG-related litigation, including those challenging fossil fuel projects, is more often reaching the highest courts around the world. According to an analysis published in June 2025 (by the Grantham Research Institute on Climate Change and the Environment at the London School of Economics and Political Science), there were over 3,000 climate-related cases globally as of mid-2025. The analysis further revealed that around 20% of climate cases filed in 2024 targeted companies, or their directors and officers. Holding companies directly liable remains difficult in Europe. In our report of two years ago we discussed **ClientEarth v Shell Plc [2023] EWHC 1897 (Ch)** in which ClientEarth failed to make out a prima facie case to enable the grant of permission under section 261(1) of the Companies Act 2006 for it to continue a derivative claim against Shell plc's directors for alleged breaches of their general duties in connection with the company's climate change risk management strategy.

While these sorts of cases have not really gained traction in the UK they may well do in the future. The authors of the abovementioned analysis state that there is a continued maturation of climate-aligned strategic litigation aimed at advancing climate action, but also a growing number of cases challenging such action - creating new difficulties for policymakers, businesses, and climate activists. In the last couple of years, we have also seen a number of significant pronouncements by major European and international courts. In the Environmental section of this report, we briefly mention that, in July 2025, the International Court of Justice issued a non-binding

ESG is playing an increasingly important role in commercial decisions, including in tenders.

advisory opinion that countries can sue each other over climate change, including historic emissions. In **Verein KlimaSeniorinnen Schweiz and Others v Switzerland**, the Grand Chamber of the European Court of Human Rights ("ECHR") found that the European Convention includes a right to effective protection from climate change, though it found the individual applicants did not meet the *"victim status"* criteria. Section 2(1) of the UK's Human Rights

Act 1998 requires the domestic courts to consider judgments of the ECHR and a judgment of the Grand Chamber such as this is likely to be given significant weight. The positive obligations mapped out by the ECHR in the Verein case might be relied upon by those promoting measures to reduce greenhouse gas emissions and to adapt to climate change when dealing with disputes (for example in balancing competing rights for planning permission). In July 2025, an application was lodged at the ECHR arguing the UK's climate adaptation plan (NAP3) fails to meet human rights requirements. This is believed to be the first time the court will directly examine a government's climate adaptation responsibilities as the sole focus of a case.

The broader impacts of climate litigation are becoming increasingly well-documented. It is no longer a niche concern; it is increasingly seen as a financial risk. Boards of directors face increasing demands to demonstrate their competence and accountability on ESG matters. There is an expectation for boards to move beyond superficial statements and fully embed ESG considerations into core business strategy.

There is a recognised need for ESG expertise at board level and for non-executive directors to enhance their ESG knowledge to provide effective oversight. Some companies are creating dedicated sustainability committees to support the board.

FINAL THOUGHTS

Forward-looking companies view sustainability as a driver of resilience and long-term value, not merely a matter of compliance. They understand that embracing sustainability creates opportunities, mitigates risks, and strengthens trust.

Implementing strong corporate governance frameworks and ethical business practices, along with maintaining a clear understanding of the division of responsibilities among senior directors, will be increasingly

vital in the coming years. This is particularly important as regulators continue to focus on assigning personal accountability to individuals - a trend especially evident in the UK (see the D&O section of this report). These responsibilities also extend to ESG initiatives and policies. With businesses placing greater reliance on AI, it has become even more essential for directors to exercise diligent human oversight over decision-making processes, both domestically and internationally.

Companies that view ESG and sustainability as strategic, long-term investments - rather than mere compliance obligations - will be better equipped to adapt, attract skilled talent, and stay competitive.

To discuss how any of these issues might affect you, please contact

Nathan Modell
Partner
+44 (0)20 7469 0442
n.modell@beale-law.com

Nathan Penny-Larter
Partner
+44 (0)20 7469 0498
n.penny-larter@beale-law.com

WARRANTIES AND INDEMNITIES

The W&I market has seen a significant increase in mergers and acquisition ("M&A") activity in 2025. This is expected to continue into 2026 and, perhaps, beyond. There has been a particular growth in technology-driven transactions.

In addition, deal sizes are on the up, which means there has been a surge (and again, this is a trend which is likely to continue into 2026) in the demand for towers of insurance and therefore a greater burden on excess capacity in the market.

With the increase in technology-driven transactions and also growing appetite in other sectors such as IP rights, data privacy and cyber security, the demand for W&I insurance shows no signs of abating. There has also been, and will continue to be, growing interest in infrastructure and property transactions, particularly in jurisdictions with good regulatory and financial incentives and also deals involving an element of green energy or sustainability.

The W&I market is buoyant and growing as appetite for M&A around the world increases.

THE STATE OF THE MARKET

W&I is an insurance product which is gaining increase prominence in various jurisdictions around the world. Parties to transactions increasingly see the policy as a necessity rather than a luxury and this increased awareness also brings about an increased sophistication with regard to what policyholders require from the policies.

POLICIES WHICH ARE SPECIFICALLY TAILORED TO THE DEAL

With an increase in uptake globally (on which, please see more below) the market is becoming increasingly competitive with a number of new entrants. The increasingly sophisticated purchaser is also seeking policies which are suited to the jurisdictions in which the transactions are taking place, the sector and the complexity of the deal. Insurers are therefore having to adapt and become more flexible with regard to the policies they are willing to write.

PRICE WARS

Part of this flexibility, and also a reflection of the competition in the market, is in relation to the pricing structures Insurers are willing to agree. Some premiums are reducing, and this is particularly the case with sectors which might be considered lower risk or transactions which are more straightforward or traditional in nature.

Added to this reduction in premiums is a reduction in the levels of excess which insurers are willing to agree and this all contributes to the wider uptake of the product in general.

WIDER COVERAGE

Insurers have started to look at the scope of coverage they are willing to offer. There has been a general reticence in the past to cover tax risks and contingent liabilities, but there is evidence that some carriers are looking at these areas with increasing interest. As mentioned above, there could be some appetite to cover ESG risks if the due diligence reveals there is scope to do so. As we have examined in more detail elsewhere in this report, awareness of ESG Is becoming more and more commonplace and this is seeping into the world of M&A.

GREATER GLOBAL DEMAND

Traditionally, W&I (or R&W as it is known in the US) has been a class of insurance most widely used in the US, the UK and Australia, where M&A activity has been greatest. However, that pattern is changing. The GCC Countries are increasingly looking to W&I policies as M&A activity rises; and other regions such as Latin America and southeast Asia are also becoming more active in the field, which leads to greater appetite for insurance. This all contributes to the competition and new entrants to the market which we highlight above.

WHAT TYPES OF CLAIMS MIGHT WE SEE IN 2026?

Claims against W&I policies in the UK are becoming more commonplace. The two cases of the last few years, **Finsbury Foods** and **Angel Bidco** have increased awareness and helped educate parties to M&A transactions of the benefits of having a policy in place. With this greater awareness, comes greater scope for claims under the W&I policy.

We consider there are a few areas in which claims might arise over the course of the next year or so (and indeed, have started to emerge in the second half of 2025).

CLAIMS LINKED TO GEOPOLITICAL DISRUPTION

With the continuation of well publicised geopolitical tensions come inevitable issues arising from the supply chain, whether that be directly as a result of goods sourced from countries affected by warfare or sanctions; or whether the tensions lead to logjams in transportation networks. Either way, we consider there is likely to be an increase in claims where supply chain issues and performance problems as a result of the disruptions to the supply chain which are not disclosed to purchasers in the due diligence process.

ESG AND EMPLOYMENT-RELATED CLAIMS

The most likely source of issues in this area arises out of the “S” pillar of ESG and particularly failure to disclose hiring practices and employment policies during the due diligence process which then give rise to claims. This slightly more nuanced type of claim sits alongside the more traditional employment claims and general labour disputes which, if not disclosed to the other party to the transaction, could bring a claim for an indemnity under the W&I policy.

There could also be claims arising from enforcement of clauses in employment contracts, such as non-compete and non-solicitation clauses. This could

also spill over into disputes relating to employee retention following the sale of a company as, with many of these deals, the purchasing company is, more often than not, first and foremost buying the people involved in the business.

There are also concerns of claims emerging from the "E" pillar, particularly in larger deals where companies have obligations to make environmental disclosures such TCFD and have failed to accurately to make those disclosures; or have regulatory issues (for example, ongoing regulatory investigations, either into the entity itself or into the directors and officers of the entity, which might remain undisclosed in the due diligence phase of the transaction.

TECHNOLOGY

As with most lines of business, cyber security and technological risks loom large in W&I. disputes over cybersecurity breaches and data breaches are likely to increase in the coming year, as are disputes over intellectual property, particularly where transactions take place in the technology sector and the ownership of IP is a particular concern.

FINANCIAL REPORTING

This will not come as earth-shattering news to those au fait with W&I risks, but the prevalence of claims arising out of inaccurate financial statements and unreported debts and creditors will continue to be a central pillar of claims under these types of policy. This is also the case for undisclosed contractual breaches in contracts and undeclared contingent liabilities, which have been a mainstay of W&I risks for a number of years and will continue to be so.

CONCLUSIONS

The W&I market is buoyant and growing as appetite for M&A around the world increases. The demand of policies has continued to grow from the traditional markets (UK, US, Australia and Europe) into new regions such as Latin America and Asia.

This has led a number of new entrants which has increased competition and forced insurers to look at wider scope of cover, reduced premiums for lower risk transactions and smaller excesses/ retentions.

As with most lines of business, risks to W&I insurers are posed by cyber threats as well as geopolitical issues; and they are also not immune from ESG claims, particularly those arising from the "E" and "S" pillars.

This is an exciting line of business with lots of opportunity for Insurers. The converse of that argument is that losses tend to large and therefore there are specific underwriting challenges which Insurers face when compared with more traditional classes of business.

To discuss how any of these issues might affect you, please contact

Nathan Penny-Larter
Partner
+44 (0)20 7469 0498
n.penny-larter@beale-law.com

CYBER

2025 carried forward the trends of 2024, only with sharper, more pronounced edges. We have seen a marked increase in both the frequency and sophistication of cyber incidents. Comparitech reported 5,186 ransomware attacks in the first nine months of 2025, a 36% increase compared to the same period in 2024.

The UK cyber insurance market became even more buyer-friendly in 2025, with fierce competition for business and a surplus of capacity ready to be deployed across an ever-expanding range of sectors. Premiums for specialist cyber cover have reduced. Cover remains more readily available, even for industries previously considered high risk.

The cyber threat landscape is in a state of constant evolution, with new vulnerabilities and attack vectors appearing all the time. As we move into 2026, we set out below some of the clear trends that are likely to shape the cyber insurance landscape.

A BRUISING YEAR

There were several high-profile cyber-attacks in 2025. They serve as cautionary tales of the true cost of cyber vulnerability in modern thriving organisations.

A sophisticated intrusion of Marks & Spencer began as early as February 2025 and culminated in a major ransomware incident disclosed in April 2025. The incident caused a more than £500 million drop in the company's stock market value and is estimated to have cost the company around £300 million in lost profits. The Co-operative Group suffered a large-scale attack after a social engineering campaign allowed attackers to reset an employee's password.

Jaguar Land Rover ("JLR") is said to have suffered the costliest cyber-attack in UK history at an estimated cost of £1.9 billion. The attack, affecting several sites, resulted in work stoppages for around 30,000 employees and leaving many of the 100,000 in its supply chain without orders or pay. The company occupies the top of a pyramid of thousands of suppliers, with some warning that they were on the brink of collapse. The government provided a £1.5 billion loan guarantee to support the supply chain and protect jobs.

The cyber threat landscape is in a state of constant evolution, with new vulnerabilities and attack vectors appearing all the time

We anticipate a large-scale review of cover for losses, and an increase in demand for cyber insurance cover, following these very costly high-profile cyber-attacks.

EXPOSURE TRENDS

The following are common cyber exposures leading to claims, regulatory action and reputational damage.

AI driven incidents: We expect an ongoing increase in cyber-crime as the use of AI lowers the barrier of entry to novice cyber criminals. AI-driven cyber threats are also becoming more widespread. This includes deepfakes and AI-powered phishing and impersonation attacks. AI and generative AI technologies can be used to produce highly realistic and sophisticated videos and audio recordings in phishing attacks. In a notable case, a deepfake posing as a company's CFO during a conference call tricked a finance employee in Hong

Kong into transferring $25 million to fraudulent accounts.

Incorporating AI-related processes within an organisation heightens the risk of cyber incidents. For instance, implementing AI often requires the use of multiple interconnected devices and platforms, which can greatly expand the number of potential entry points for a cyber-attack. In May 2025, the National Cyber Security Centre of GCHQ released a report highlighting the escalating risk posed by hackers leveraging AI tools. The report cautioned that within the next two years, *"a widening gap will develop between organisations able to keep up with AI-driven threats and those that cannot - leaving the latter more vulnerable and increasing the overall risk to the UK's digital infrastructure."* As AI-enhanced cyber-attacks can significantly increase the frequency of claims, they may affect numerous losses typically covered by cyber insurance, such as business interruption ("BI"), data breach liability, data restoration, and ransomware-related losses. Although cyber policies generally cover damages from AI-driven cyber incidents, other AI-related risks - like model manipulation, data poisoning, liability from hallucinations or inaccurate outputs, and intellectual property infringement - are often not explicitly addressed in policy wordings.

Unauthorised use of AI in the workplace: An increasing number of people are using AI (in particular large language models such as ChatGPT) in the workplace, often without their employer's or IT department's knowledge or permission. This is fraught with risks. Using AI systems trained on copyrighted materials without authorisation may expose companies to intellectual property infringement claims. Improper handling of personal data can lead to violations of data protection laws. Employees who use free generative AI tools risk disclosing confidential business information, particularly when relying on third-party platforms lacking robust safeguards. Additionally, AI models may produce false information or perpetuate bias, resulting in unfair or unethical outcomes. Without clear governance and policies, organisations face potential penalties, reputational harm, and erosion of client trust.

Attackers are increasingly skilled at evading **multi-factor authentication** ("MFA") measures. Therefore, organisations should consider adopting more advanced MFA solutions that leverage contextual data - such as location, time of access, and user behaviour patterns - to better assess and manage risk.

Cyber-criminals are increasingly targeting **third-party suppliers** because these vendors often have weaker security defences than the large companies they serve. Third parties are often responsible for critical services such as cloud storage and software development. Compromising a smaller supplier offers a much easier entry point than directly attacking a large company's main systems. As a result, organisations must protect not only their own infrastructure but also their entire digital ecosystem. Robust third-party risk management is therefore imperative.

With the expansion and increasing reliance on digital technology, the large amount of **non-malicious outages losses** is not surprising. This occurs when digital systems, cloud services, or networks fail. Such outages can disrupt sales, supply chains, and customer access, leading to lost revenue, reputational harm, and potential legal liabilities. While standard cyber insurance generally covers losses resulting from security, operational, or system failures within an insured organisation's own operations, it often excludes losses caused by non-malicious cyber incidents at third-party network service providers. An example of this is the July 2024 CrowdStrike outage (discussed in last year's report).

Data breaches and theft, including wrongful collection and processing of data, will inevitably continue to be a source of claims and regulatory action.

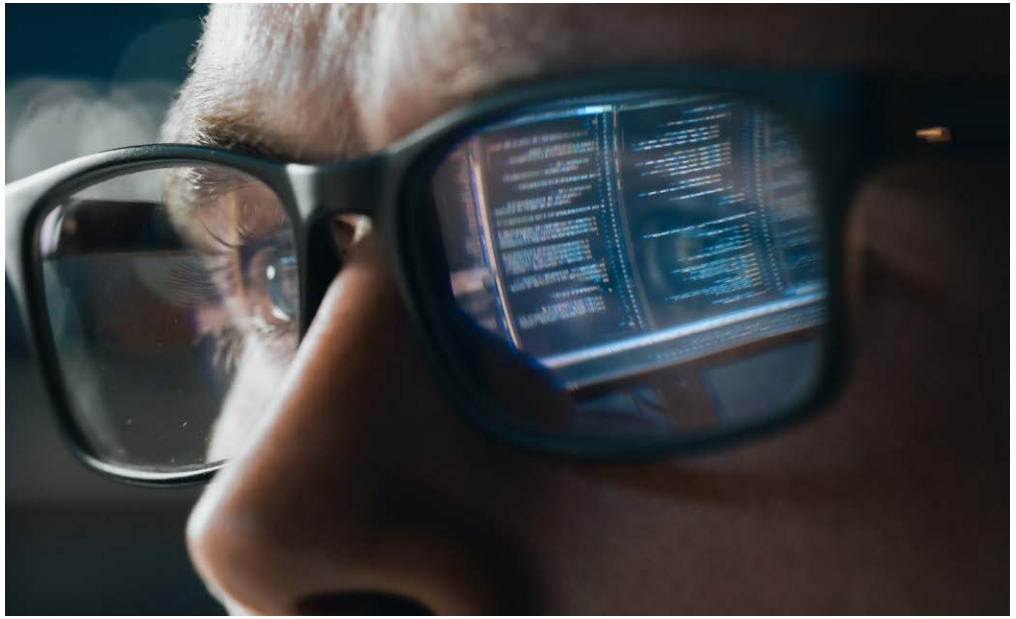
The **geopolitical landscape and cyber risk are deeply intertwined**, with geopolitical tensions amplifying cyber threats and cyber-attacks, acting as tools of geopolitical influence. This connection affects nation-states, businesses, critical infrastructure providers, and individuals alike. It has never been more relevant than the current geopolitical climate.

IT skills shortages are also considered as a key "trendsetter" for cyber (in) security.

UK REGULATION AND ENFORCEMENT

Progress from the UK government in implementing measures relating to cyber security remain slow.

Following consultation, the UK government announced plans in July 2025 to develop legislation banning public sector bodies and operators of critical national infrastructure ("CNI") from paying ransoms to cyber criminals. The plan includes mandatory reporting of incidents and potentially a requirement to consult the government before making a payment. The goal is to make these organisations less attractive



targets and reduce the financial incentive for attackers to target them.

The Cyber Security and Resilience Bill's ("Bill") passage to becoming law has been repeatedly delayed. It is expected to come into law in 2026. The Bill has been proposed to update the 2018 Network and Information Systems Regulations ("Regulations"). One of the main motivations behind the UK Government's proposal is to maintain broad alignment with evolving EU legislation - particularly given the expanded scope of the new EU NIS 2 Directive. The current Regulations apply to a defined set of *"operators of essential services"* and *"relevant digital service providers"* in CNI sectors, including energy, transport, health, water and digital infrastructure. The Bill intends to expand the scope to encompass IT-managed service providers ("MSPs") which are fundamental in managing many of the UK's critical IT systems and networks. MSPs are considered an attractive target for attack given the access they have to clients' IT systems, infrastructure and data. The government expects around 1,000 MSPs to be captured by the Bill. Data centres with 1 megawatt or greater capacity may also be included in the scope of potential inclusion. The Bill further

seeks to impose new requirements on critical infrastructure operators to strengthen security measures, report cyber incidents to regulators more promptly and secure their supply chains (supply-chain oversight).

The Information Commissioner's Office ("ICO") levied notable penalties in 2025, including £3.07m against Advanced Computer Software (stemming from a 2022 ransomware event) and £2.3m against 23andMe (150,000 UK data subjects affected). The ICO fined DPP Law Ltd £60,000 for a breach exposing sensitive client data. Analyses suggest that the higher levels of fines compared to previous years is signalling a firmer stance on UK GDPR security failings.

THE MIDDLE EAST ("ME")

Whilst the ME continues to progress in its digital transformation, it also faces increasing complexities and challenges in cyber security. The region has experienced a growing number of cyber threats, such as ransomware attacks and data breaches.

The 2025 cyber-attack on American Hospital Dubai ("AHD") has highlighted the growing scale and sophistication of cyber threats across the region, where aggressive and increasingly frequent attacks are targeting businesses of all sizes. AHD reportedly suffered the theft of 450 million patient records and personal information. AHD is one of the UAE's most prominent private healthcare providers, yet it still became a target. This underscores the reality that no organisation is immune, regardless of size, sector, or investment in technology. The fallout from an attack of this magnitude is severe. The expenses tied to recovery - including system restoration, legal defence, and rebuilding reputation - can be overwhelming.

Overall, the data protection regulatory landscape in the ME is becoming increasingly comprehensive, signalling a heightened awareness of the importance of cyber security. Simultaneously, enforcement actions by the relevant authorities are expected to become more frequent and robust.

SOME KEY TAKEAWAYS

Businesses can take numerous steps to protect themselves from prolonged disruptions and significant financial losses, while also helping to stabilise the cyber insurance market and keeping insurance premiums at reasonable levels.

Organisations should prioritise implementing robust cyber security measures, supported by effective risk management and crisis response systems. MFA ought to be standard practice. As any organisation is vulnerable to social engineering attacks, it is crucial for all employees (from the CEO to interns), and especially those on the front line of customer interactions, to be trained to recognise and respond to threats. With attacks often coming through third-party connections (such as cloud services and fintech vendors), supply chain management is critical.

BI losses - which typically make up more than 50% of total cyber claim values - are strongly linked to how quickly incidents are detected, contained, and managed.

Policyholders should ensure that their cyber insurance policies are up-to-date and provide adequate coverage for emerging risks. Although cyber insurance cannot stop an attack from occurring, it plays a vital role in assisting with rapid response and minimising damage.

CONCLUSION

The market will be watching closely to see how emerging technologies such as AI influence risk exposure and insurance claims. As cyber-attacks grow increasingly frequent and sophisticated, organisations must move away from reactive measures and adopt a proactive approach to preparedness.

The JLR outage highlighted how rapidly BI and contingent BI losses can escalate within supply chains. If the Cyber Security and Resilience Bill is enacted in 2026, insurers can leverage this to harmonise questionnaires with statutory controls.

To discuss how any of these issues might affect you, please contact

David McArdle
Partner
+44 (0)117 428 9306
d.mcardle@beale-law.com

POLITICAL VIOLENCE

Businesses round the world, particularly those with a footprint in several jurisdictions, are beginning to view political violence as a key consideration. Whilst many may consider this to be a concern of large businesses, in fact, the issues which arise are ones which touch companies of all sizes and all types.

There are a number of ways in which political violence can affect businesses, whether that be safeguarding employees and customers, or fears of business interruption and/or damage to property or other assets if that business operates in an area where there is war or civil unrest, or adjacent to such an area.

The conflicts between Russia and Ukraine and in the Middle East has been a focus of the last few years, but there are also continuing tensions between China and Taiwan and civil unrest in countries such as the UK, France, parts of Latin America and Asia. There has been a particular impact on supply chains over the last few years (and these concerns remain in place for companies) and what makes political violence and civil unrest generally such an unpredictable concept and, therefore line of insurance business, is the complete lack of certainty over how long periods of unrest and conflict might last. It also typically escalates very quickly and in an unpredictable manner, meaning businesses and insurers need constantly to monitor situations to be in the best possible position to react.

Over the last five years, this has led to larger numbers of enquiries as to the availability of PV policies, and an increasing number of policies actually placed throughout the world.

THE STATE OF THE MARKET

The evolving nature of PV risk creates real pressure on policy wordings, particularly those based on traditional Lloyd's or London Market clauses. Definitions such as "riot," "civil commotion," "terrorism," "insurrection," and "war" are being tested in ways that would have seemed academic a decade ago. In reality, the consequences of these interpretations are very real, and they determine whether cover is triggered, whether exclusions apply, and how losses are aggregated.

PV events now escalate faster, last longer and emerge in previously stable regions making the risks increasingly unpredictable and harder to protect against.

The rise of lone-actor violence, hybrid cyber-physical threats and fast-spreading information means past patterns are no longer reliable indicators. PV events now escalate faster, last longer and emerge in previously stable regions making the risks increasingly unpredictable and harder to protect against.

Given the global nature of many PV claims, often involving local policies, facultative placements and treaty reinsurance, there are also layers of governing law, jurisdictional issues, and parallel proceedings to navigate.

WHAT TYPES OF CLAIMS MIGHT WE SEE IN 2026?

Against all of this background, we consider some areas in which claims might emerge against PV policies in the next few months to a year.

GENERAL CIVIL UNREST

With the gap between rich and poor in many western and developing countries becoming ever-wider comes the rise of right wing, populist governments which seemingly come to power on a manifesto of tackling immigration and decreasing the gap between the "haves" and the "have nots" by putting forward short-term solutions to solve a country's economy. When one combines the rising cost of living, citizens anxious about the ongoing environmental crisis and attacks on civil liberties, it is easy to see how civil unrest dominates the thoughts of business worldwide. This convergence of issues sometimes brings to the fore the divides in society and increases incidents of nationalism and xenophobia.

In the UK, there have been incidents of protests which have led to periods of civil unrest as a result of demonstrations against Israel's policies in the war against Palestine and also protests on racial and religious lines. This has led to damage to property and assets in London and other large commercial centres around the UK. Incidents of dissent of this nature are not limited to the UK. There have been similar demonstrations in mainland Europe in countries such as France, Germany and The Netherlands and the spectre of civil unrest seems never to be too far away in the US, particularly given the recent demonstrations against ICE operations in several US states, and Latin America countries such as Argentina and Brazil.

Whilst 2024 was the year of elections, 2026 is likely to see increased civil unrest arising from the election outcomes and this is likely to test the PV policies which companies have in place.

THE CONTINUED RISE OF TECHNOLOGY

Social media has fundamentally changed how PV events unfold. Platforms can instantly mobilise huge crowds, amplify outrage, and coordinate flash protests that can quickly turn violent. Misinformation, such as that seen in the aftermath of the Southport stabbing, can distort public understanding and inflame tensions before authorities can respond.

State-sponsored cyber groups, or Advanced Persistent Threat (APT) actors, are also increasingly active in this space. These actors use cyber disruption and disinformation campaigns to exploit political fault lines, sometimes triggering physical violence.

The hybrid nature of these events raises complex questions around causation, attribution, and the interplay between PV and cyber exclusions.

CLIMATE ACTIVISM

Several countries around the world are backing away from previous pledges made following the Paris Agreement,

leading to protests as a result of broken promises or perceived broken promises.

Protests are becoming more violent in nature, with a large increase in damage done to property, whether that be graffiti on buildings or housing companies which are believed to have investments in the fossil fuel industry, or protesters physically attaching themselves to buildings or other assets.

STATE-SPONSORED EVENTS

There are a number of states now actively working to sabotage other countries. It has been well-documented how Russia has sought to sponsor acts against key infrastructure, and this has only increased since the invasion of Ukraine in early 2022. In 2024 alone, there were more than 40 known Russian linked attacks, and the latter half of 2025 has seen several incidents of Russian submarines in other countries territorial waters, including those of the UK and the Scandinavian countries.

Whilst the cause of the wide-scale power outage in Spain and Portugal earlier this year has not yet been uncovered, it is not difficult to envisage circumstances where that might be an example of state-sponsored sabotage and these attacks can potentially cause physical damage and business disruption to critical infrastructure to the extent that a PV policy might well be engaged.

WHAT DO BUSINESSES NEED TO DO IN THE FACE OF THESE RISKS?

As with any type of risk, forward planning is necessary, as is the ability to anticipate issues which might arise.

Companies will need to look closely at the supply chains and from where they are purchasing goods or having goods manufactured, if they could be affected by civil unrest, or their transit might be affected by it; in those circumstances it is important to source potential alternatives.

This requires engagement across the business and with third parties, but it

is necessary to try and avoid issues arising.

Brokers can be key to assisting with the process and the need to know a client's business to ensure that sufficient PV cover is obtained will be of central importance.

CONCLUSIONS

More companies are recognising the risks they face from civil unrest and other incidents which might engage a PV policy.

This phenomenon is not limited only to global businesses; the SME market is becoming more aware of what is available in this regard. SMEs traditionally lacked the resilience to absorb major business interruption losses, which meant that they were less able to relocate operations and may not have had crisis protocols in place. They were also less likely to have sufficient cover in place, leading to an increase in uninsured losses. The traditional PV market, however, is changing as businesses and their brokers look to ways to protect their position in the event of incidents which might triggger a PV policy.

To discuss how any of these issues might affect you, please contact

Nathan Penny-Larter
Partner
+44 (0)20 7469 0498
n.penny-larter@beale-law.com

REGIONAL TRENDS 2026

SCOTLAND

In Scotland, we expect to see similar trends to other regions in respect of professional indemnity claims. However, Scotland's unique legal framework, particularly its distinct approach to prescription (i.e. time-bar), is likely to shape the way these trends are defended. Insurers and insured parties must pay close attention to the evolving interpretation of key provisions such as Section 6(4), and developments critical for navigating disputes.

THE LAW OF PRESCRIPTION AND THE COURT OF SESSION

The law of prescription is a complex area of law and is ever evolving. The Court of Session recently issued three important decisions in connection with the application of Section 6(4) of the Prescription and Limitation (Scotland) Act 1973. Reference is made to the cases of **Tilbury Douglas v Ove Arup [2024] CSIH 15**, **Greater Glasgow Health Board v Multiplex Construction Europe Limited [2025] CSOH 56** and **Legal and General Assurance v Halliday Fraser Munro [2025] CSIH 24**. Section 6(4) is widely relied upon by Claimants in arguing that the 5-year prescriptive clock should be delayed.

Section 6(4) provides that any period during which the Claimant fails to make a relevant claim by reason of the Defender's fraud, or error induced by the Defender's words or conduct, shall not form part of the prescriptive period. Section 6(4) therefore acts a mechanism by which the prescriptive period is delayed.

The Court of Session has held that it is not enough to show ignorance as to a state of affairs in reliance on Section 6(4) – a Claimant must establish by evidence that somebody was induced by error. For large organisations, it can be difficult to show that a specific person was induced by error. The Inner House has put it beyond doubt that Section 6(4) will not operate in circumstances where a Defender has merely asserted it has performed its contractual obligations or has not been negligent.

IMPLICATIONS FOR INSURERS AND INSUREDS

The recent decisions are certainly helpful from an insurer / insured client perspective when faced with complex professional indemnity claims. Previously, a Claimant did not have to rely on much evidence the establish the test under Section 6(4) but the Courts are clearly now adopting a stricter approach. While the issue of prescription remains a complex area of law in Scotland, it is no longer enough for a Claimant to simply rely on everyday conduct.

As a result of the precedent fixed by the Court of Session, we believe that prescription will remain the battleground for many professional indemnity claims in Scotland. We believe that Defenders in such claims will seek to have early Debates fixed by the Court in relation to the issue of prescription and, in particular, the application of Section 6(4). A Debate would therefore save costs and time as compared to a lengthy and expensive Proof (trial).

IMPACT OF THE BUILDING SAFETY ACT 2022

We will also start to see the effects of the Building Safety Act 2022 in Scotland. While the 2022 Act does not fully apply in Scotland, it has extended the prescriptive periods for defective construction and cladding products by 15 and 30 years. We may start to see an increase in cladding claims from projects which were completed many years ago where it is likely that evidence and witnesses will be difficult to source.

To discuss how any of these issues might affect you, please contact

Lindsay Ogunyemi
Partner
+44 (0)141 674 7051
l.ogunyemi@beale-law.com

Andrew McConnell
Partner
+44 (0)141 674 7052
a.mcconnell@beale-law.com

IRELAND

Ireland's insurance sector is entering a period of significant transformation driven by regulatory developments, evolving risk profiles, and rapid market growth across multiple industries. We have highlighted five key trends that insurers with exposures in Ireland should monitor to effectively navigate this dynamic and evolving market.

LSRA ANNUAL REPORT 2024 – PROFESSIONAL INDEMNITY RISKS

The Legal Services Regulatory Authority (LSRA) reported a 14% increase in complaints during 2024, with a notable rise in cases brought by financial institutions against solicitors for non-compliance with undertakings. This trend signals a potential uptick in Professional Indemnity (PI) claims, which insurers should monitor closely. Importantly, there is an opportunity for early intervention – by supporting solicitors when LSRA complaints arise, insurers can help resolve issues before they escalate, reducing the likelihood of costly PI claims and improving client relationships.

KIRWAN V CONNORS [2025] IESC 21 – LITIGATION TIMELINES

The Supreme Court's decision in Kirwan v Connors introduces structured time limits for inactivity, making strike-out applications more predictable and reducing the need to prove prejudice. Courts are now less tolerant of delays, which should lead to faster resolution of dormant cases, lowering claims handling costs and reserves. However, insurers must remain alert to knock-on risks, as solicitors could face negligence claims if cases are dismissed due to inactivity.

CYBER INSURANCE – A GROWING OPPORTUNITY

Cyber risk continues to escalate, yet fewer than 20% of Irish SMEs currently hold cyber insurance. Rising attack frequency and stricter regulations, including GDPR and the upcoming NIS2 Directive, are reshaping the market. NIS2, due to be transposed into Irish law by late 2025 with penalties from 2026, will require entities to demonstrate resilience against cyber threats. Brokers expect claims to rise by 70% in the next year, creating a major growth opportunity for insurers offering tailored cyber liability solutions.

DATA CENTRES – DRIVING MARKET EXPANSION

Ireland's status as a leading European data centre hub is transforming insurance demand. The sector, valued at $2.15bn in 2025 and projected to double by 2030, presents complex risks, including hyperscale construction challenges, operational hazards such as fire and water usage, and sustainability concerns linked to high energy consumption (21–22% of national electricity). Regulatory pressures, including Digital Operational Resilience Act ("DORA") compliance and climate targets, require specialist underwriting and risk engineering expertise. Premium growth across property, cyber, and environmental liability is expected, alongside opportunities for innovative, sustainability-focused insurance products.

HEALTH & SAFETY – REGULATORY TIGHTENING

New regulations, such as Quarry Safety Rules effective January 2026, stricter electrical inspections, and the Health & Safety Authority's 2025-2027 strategy, will increase compliance demands. Updates to Lifting Operations and Lifting Equipment Regulations ("LOLER")/Provision and Use of Work Equipment Regulations ("PUWER") standards and wider adoption of ISO 45001 heighten liability exposure for non-compliance. Insurers should review policy wording for tech-related risks and expand risk engineering support to help clients meet evolving safety standards.

CONCLUSION

From professional indemnity and cyber liability to environmental and health & safety risks, Ireland's insurance market in 2025 is seeing change across a wide range of financial risks. Specialist expertise, proactive risk management, and innovative solutions will be critical for insurers seeking to mitigate the impact of these emerging claims trends in the Irish market.

To discuss how any of these issues might affect you, please contact

Niamh Loughran
Partner
+353 (0) 1 536 9614
n.loughran@beale-law.com

Sarah Conroy
Partner
+353 (0) 1 536 9613
s.conroy@beale-law.com

MIDDLE EAST

The insurance market in the Middle East remains competitive with a number of insurers either returning to the UAE or considering setting up an office. Dubai is the regional insurance hub and has influence over a number of regions including the GCC countries, Central Asia, North and East Africa and Turkey.

Federal Decree-Law No. 48 of 2023 ("New Insurance Law") came into force 30 Nov 2023, with a compliance grace period to 29 May 2024.

However, this was substantively repealed by Federal Decree-Law 6 of 2025 (known as the "New CBUAE Law") which came into effect in September 2025 although its implementing regulations and circulars continue until replaced.

This clarified non-admitted insurance in that onshore risks must generally be insured with CBUAE-licensed insurers.

It also created "BIDRU" (Banking & Insurance Dispute Resolution Unit) as the mandatory pre-court forum for many insurance disputes.

In addition, it extended regulation to "insurance-related professions" such as brokers, TPAs, consultants and actuaries.

Saudi Arabia is also seeing a similar approach but with hesitancy from some due to the regulatory requirements.

The Insurance Brokers' Regulation 2024 (CBUAE) were issued in the UAE inIN July 2024 and became effective in February 2025.

It applies to all onshore insurance brokers, UAE-incorporated insurers, their UAE branches, and reinsurers (with some carve-outs for pure reinsurance brokers in DIFC/ADGM).

The result of this is brokers cannot collect premiums or claim payments anymore: money must flow directly between insurer and policyholder for primary insurance.

There are explicit data-localisation/ cybersecurity and outsourcing controls and all personal data has to be stored in the UAE, with defined cyber-incident response expectations.

Brokers must hold PI insurance with CBUAE-licensed insurers, on terms approved by CBUAE, with minimum limits (between AED 2m/3m depending on structure).

KEY TRENDS

The increasing growth of data centre construction in the region to advance AI and supplier business practices are now ranked as emerging risks.

Cyber and data protection laws are evolving in Saudi Arabia, the UAE and the region generally so that exposures tied to digital operations and cloud/third-party vendors are increasing.

The Giga Projects in Saudi have seen a recent shift in focus as well as supply-chain disruptions and face possible clams in respect of directors/officers and professional indemnity policies.

In Saudi Arabia and the UAE, the increased regulatory oversight of listed companies, disclosure requirements, class-action regimes (or possible threat of these), Anti Money Laudering and sanction regimes, are elevating risks under Management Liability policies.

On 14 October 2025 the UAE passed the Federal Decree Law No. 10 of 2025 which brings about a significant change to the country's Anti-Money Laundering and Combatting the Finance of terrorism regulations. It introduces new criminal offences for directors and officers, expands the enforcement powers of the regulators and provides for fines of up to AED 100m for infractions of the law. All businesses handling transactions or providing designated services are required to meet far more robust regulatory obligations. This makes it essential for businesses and their directors and officers, to understand the regulations, and implement changes to corporate strategy in order to comply with them.

The appetite for mergers and acquisitions in the region means that the Warranties and Indemnities ("W&I") market is expanding and becoming a more popular product. This is part of a wider global trend of greater interest in, and great uptake of, W&I polices generally.

Overall, the market remains buoyant and competitive and we appear set to see some more new or returning insurers entering the market in 2026, which might prolong the current struggle for rate in the region.

To discuss how any of these issues might affect you, please contact

Lyndon Richards
Partner
+971 (0)4 356 3904
l.richards@beale-law.com

CANADA

CLAIMS ENVIRONMENT

PROFESSIONAL INDEMNITY ("PI") & DIRECTORS' & OFFICERS' LIABILITY ("D&O")

Securities-related and class-action filings increased in 2024 to 14 filings. This reflected pre-pandemic levels and was a significant increase on filings made in 2023 (8). There was a notable rise in secondary-market securities claims and multi-jurisdictional litigation. That trend drives D&O exposures (derivative suits, securities claims, regulatory follow-ons) and PI claims for advisers, auditors and law firms involved in public transactions. This upward trend continued into the first half of 2025, no fewer than 164 proposed class actions filed in the principal jurisdictions, with 78 of those being filed in Quebec and 38 in Ontario. This crystallises the prevailing trend of Quebec being the jurisdiction du jour for class actions. The highest number of class action filings were reported in the consumer sector, with product liability and data privacy following behind.

The trends in securities class actions we are likely to see over the course of the next year include AI-washing claims and claims relating to misrepresentations made in financial and non-financial disclosures. Defence costs and reputational remediation are becoming dominant drivers of insured losses even where ultimate liability is limited. London underwriters should assume more protracted reserving profiles and higher litigation spend per claim.

FINANCIAL INSTITUTIONS (FI) EXPOSURES

OSFI's recent risk workstreams emphasise operational resilience, integrity/security and liquidity/credit risks — signalling regulator expectations that FIs will be held to higher standards on continuity, third-party oversight, and security controls. Failures in operational resilience or AML controls are translating into regulatory enforcement actions and attendant civil claims (including class actions), producing composite loss events that involve fines, remediation costs and third-party PI/D&O claims. Insurers should expect more claims where operational outages, misconduct, or weak AML controls intersect with customer loss or market disruption.

REGULATORY & LEGISLATIVE DRIVERS

Canada's Anti Money Laundering ("ALM") /Anti-Terrorist Funding ("ATF") regime has been actively updated and expanded, increasing compliance obligations for financial services firms and heightening the consequences of control failures. Simultaneously, provincial developments and court decisions have kept class-action practice active and amenable to multi-jurisdictional and intra-provincial filings In addition, legislation passed now means that plaintiffs can choose the best Canadian province in which to bring the class action, which means that plaintiff lawyers are naturally picking the province with the most amenable laws. The combination of tougher regulatory guidance, expanded AML rules, and a busy class-action landscape creates a higher-severity tail for claims that often implicate D&O, PI and FI portfolios together. Underwriters must factor in regulatory enforcement timelines and possible parallel class suits when modelling loss creep.

CYBER (BRIEF)

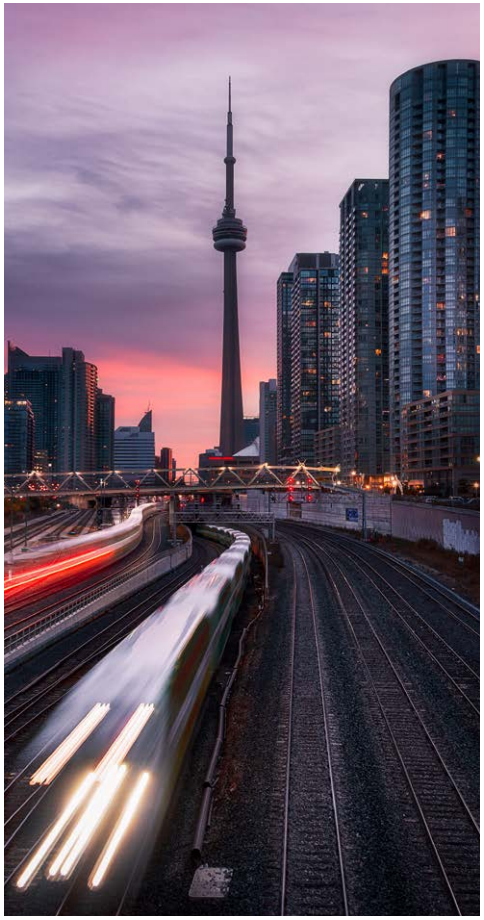
Ransomware, data breaches and supply-chain incidents continue to generate operational outages and contagion losses for financial firms - producing first-party remediation spend and third-party liability (PI) claims. While cyber remains a separate line, its intersection with operational resilience and AML/controls failures amplifies FI and D&O claim scenarios (e.g., board oversight failures, inadequate vendor management). Expect increasing demand for integrated coverage and for clarity on cover interplay (cyber vs. PI vs. D&O).

IMPLICATIONS FOR LONDON MARKET INSURERS

1. **Underwriting diligence:** require deeper controls evidence (operational resilience, third-party/vendor management, AML program strength) and scenario testing for multi-line events.
2. **Claims handling & legal panels:** invest in cross-border litigation and regulatory-response capabilities; early crisis and regulatory counsel will materially reduce loss escalation.
3. **Product design/pricing:** consider layered limits, explicit aggregation language for regulatory remediation, and exclusions/wordings that address cyber-PI overlap and AML-related fines (where permitted).
4. **Reserving & capital models:** stress scenarios for class actions plus regulatory fines and extended defence spend; tail risk modelling should include simultaneous cyber + operational outage + securities suits.

CONCLUSION

Canada's financial lines loss landscape is trending, in common with many jurisdictions around the world, towards higher legal/regulatory complexity and concentration of loss drivers (class/securities actions, regulatory enforcement, operational resilience failures and cyber). London Market insurers that tighten front-end controls, enhance cross-disciplinary claims response, and recalibrate pricing/reserving for multi-headline loss events will be better positioned to manage this evolving risk over the course of the next year or so.



To discuss how any of these issues might affect you, please contact

Andrés Durán
Partner
+1 437 900 7471
a.duran@beale-law.com

Nadir Hasan
Partner
+1 437 900 7472
n.hasan@beale-law.com

BEALE&CO

International Construction and Insurance Law Specialists

www.beale-law.com