

**Baker
McKenzie.**

Global Disputes Forecast 2025



Introduction

The landscape for disputes in 2025 looks as complex as it has ever been. Businesses are wrestling with numerous external forces that increase the chance of disputes.

Against this backdrop, we surveyed 600 senior decision-makers with responsibility for litigation at large organizations (annual revenue greater than USD 500 million). Respondents were based in the US, the UK, Germany, Singapore, Hong Kong and Brazil. We asked them to give us their views on the world of disputes for 2025.

We also drew on insight from our clients and our own network of lawyers, comprising over 1,000 practitioners across 74 offices.

We are pleased to present our 2025 Global Disputes Forecast. We hope our analysis helps you to prepare for the year ahead.



Index

Key Dispute Trends

- Cybersecurity and data privacy heighten disputes risk 4
 - Data, ethical and IP concerns are top risk factors for AI disputes 5
 - New legislation fuels employment disputes risk 7
 - Mobility concerns drive tax disputes risk 9
 - Environmental slant to key ESG disputes risk 11
 - Tax issues trigger post-M&A disputes 13
-

Sector Insights

- Consumer Goods and Retail 17
 - Energy and Infrastructure 18
 - Financial Institutions 21
 - Healthcare and Life Sciences 23
 - Industrials, Manufacturing and Transport 25
 - Technology 27
-

The Wider Picture

- Organizations face barriers to litigation preparedness 31
 - Class action concerns growing worldwide 32
 - External factors driving investigations risk 34
-

Contacts

38

Key Dispute Trends





Key Disputes Trends

Cybersecurity and data privacy heighten disputes risk

Cybersecurity and data privacy remain at the forefront of organizational concerns, with respondents identifying this topic as the top risk for both disputes and investigations. The increasing frequency and sophistication of cyberattacks, stringent regulatory requirements and changes to operations are driving this trend.

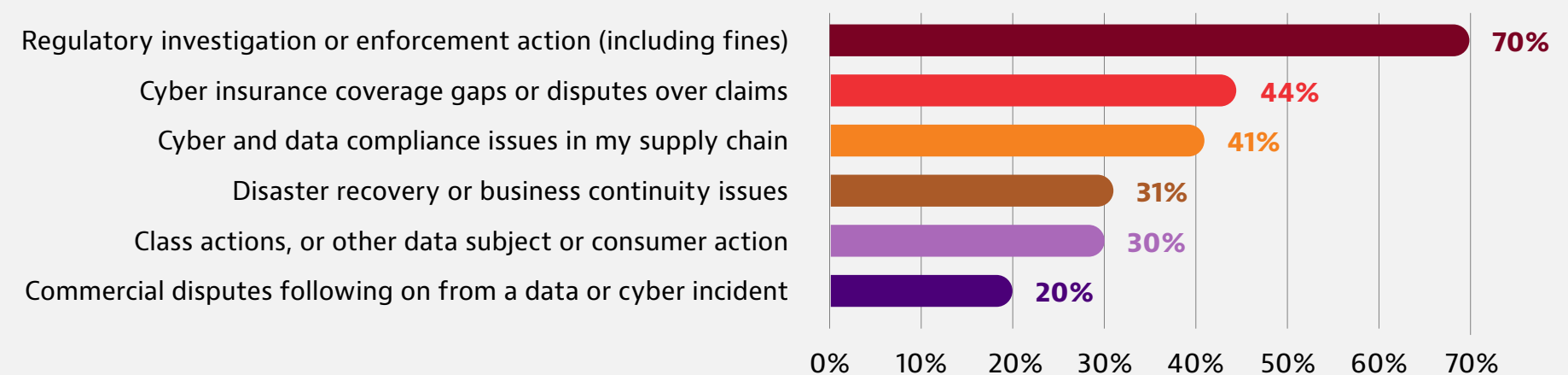
“We are at an inflection point where cyber risk is concerned. With technological advancement — such as AI and other drivers for digital transformation — as well as the increased global geopolitical threat, it’s not hard to see why we are witnessing a rapid increase in cyber attacks right across the eco-system,” says Vinod Bange, partner, London.

“A target can be disrupted by attacks being focused upstream or downstream, so the threat plane is broader than ever before, and this presents a big challenge for securing critical infrastructure, which now more than ever relies heavily on globally distributed private enterprise,” Bange continues.

“The disputes risk and indeed the risk of investigation and enforcement action does not dampen that increasing threat landscape, new regulation, and laws to force higher benchmarks of cyber security readiness and reporting compliance can also increase the risk of disputes across the supply chain.”

How concerned are you about the following potential impacts of a cybersecurity or data breach to your organization? (Ranked top two)

*Base: survey respondents citing cybersecurity/data privacy as a risk



Regulatory scrutiny

Organizations are facing heightened scrutiny from regulators, and the potential for significant financial and reputational damage from data breaches is a major concern.

Recent developments in cybersecurity regulations have further intensified these concerns and exacerbated fears of investigations. In 2024, major economies such as the European Union, the United States and Singapore enacted new laws to bolster cybersecurity resilience.

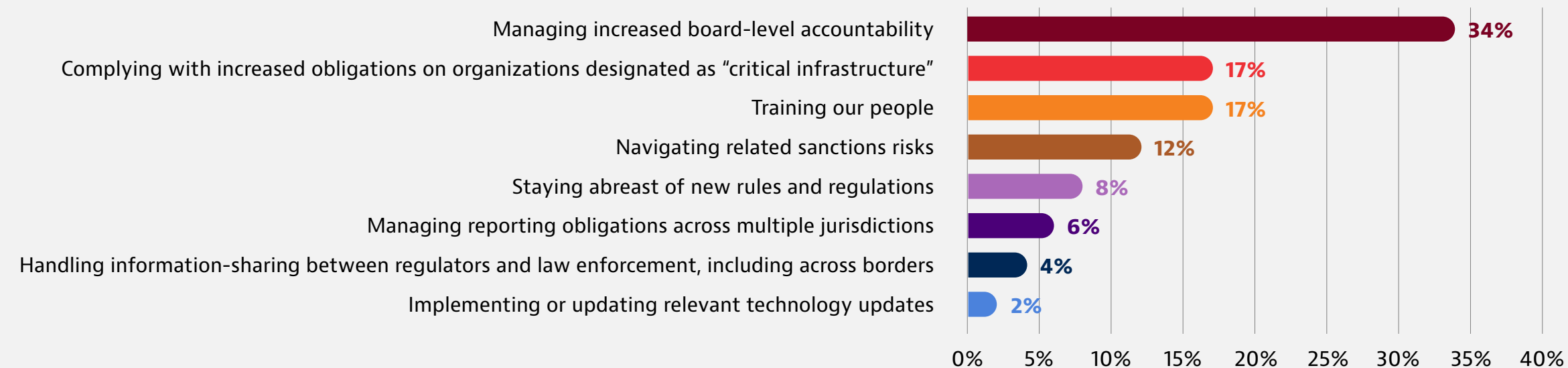
Operational changes

The rise of remote work and the growing use of cloud services and third-party vendors have introduced new vulnerabilities. Meanwhile, cyber and data compliance issues in the supply chain are also an issue. The interconnected nature of modern supply chains means that a breach in one organization can have cascading effects on others. Ensuring compliance across the entire supply chain is crucial.



What are the top five challenges for your organization in managing cybersecurity risk?

*Base: survey respondents citing cybersecurity/data privacy as a risk



Insurance coverage gaps

As cyber threats become more sophisticated, insurance policies may not fully cover the damages or may lead to disputes over claims. Cyber insurance coverage gaps or disputes over claims are a concern for many respondents. This highlights the importance of organizations thoroughly understanding their cyber insurance policies and ensuring that they have comprehensive coverage.

Vinod Bange, partner, London, notes that due diligence levels will inevitably increase in response to this environment but urges organizations to think carefully about their approach: "Efforts need to be focused on the risk rather than simply defaulting to a disruptive papering exercise that fails to mitigate the cyber threat or indeed the dispute risk. A sophisticated threat such as cyber needs an equally sophisticated plan of action that never drops its guard."

"Cybersecurity is not just a technology risk; there are people, process and infrastructure measures that need to be taken to reduce cyber threats and prepare for when they materialize. This naturally requires a center of cyber excellence but that cannot work in isolation. Board-level accountability is essential for resources and establishing a mandate to make change across a whole organization — especially when managing people and supply chain culture," says Bange.

"Board level training should be kept refreshed so that addressing cyber risk is meaningful, effective and positively impactful to a cyber readiness eco-system that is fit for purpose. This is not a one-off exercise for the board as that level of accountability has to be every bit as sophisticated and up-to-date as the threat actors are."

Key Disputes Trends

Data, ethical and IP concerns are top risk factors for AI disputes

AI presents a diverse landscape of disputes risks for organizations in 2025. Primary concerns revolve around data privacy and security, which we have explored above, as well as ethical disputes.

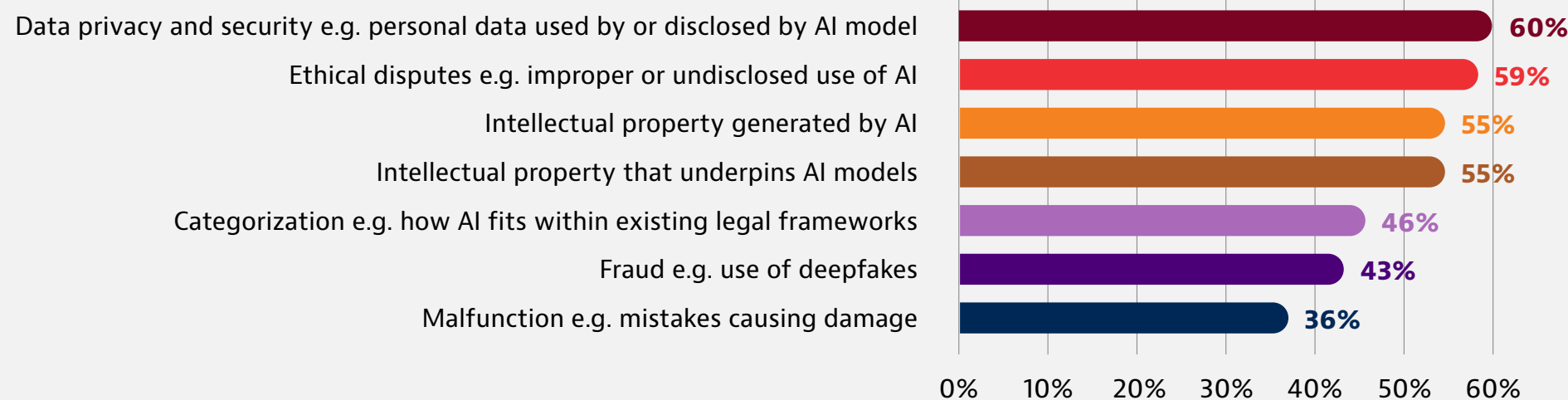
The so-called “soft law” on AI ethics has been around for some time. The OECD principles on AI, ratified by member countries in 2019, call for AI that advances inclusive growth, environmental sustainability, and overall benefits for society. These principles demand that AI systems adhere to legal statutes, human rights, and democratic values and include mechanisms for human intervention. They also advocate for a high level of transparency and responsible disclosure to empower individuals to understand and challenge AI-driven outcomes. Many jurisdictions around the world have introduced AI guidelines which touch on similar areas. However, legal teams continue to wrestle with ethical issues such as unintended bias in recruitment algorithms, customer chatbots or facial recognition technology.

Intellectual property disputes are also prominent, reflecting the complexities of integrating AI into existing legal frameworks and the potential for misuse or misappropriation of AI technologies. IP and AI are inextricably linked: AI tools are typically built on huge data pools containing IP-protected material and can be used to generate valuable content that companies will wish to protect and exploit.

When it comes to IP-related disputes, there are issues to consider throughout the AI lifecycle, from the training data used to the output generated. Businesses are concerned about AI-underpinned output being at risk of IP infringement, alongside other IP risks such as inadvertently infringing a third-party trademark or infringing the personality rights of individuals. Additionally, questions

What type of AI disputes present a risk to your organization in 2025?

*Base: survey respondents citing AI as a risk



around ownership and protectability of content produced by or with assistance from AI can also invoke issues of IP ownership, enforcement and management.

Consideration of the nature and source of data used to train AI, as well as where and how this training takes place, is also key to understanding the scale and type of risks. This includes whether the data is proprietary, the conditions or restrictions placed on its use by the owner, and the applicability of local exceptions to IP infringement.

Isabella Liu, partner, Hong Kong, shares, “Companies should remain savvy in monitoring AI developments across legal

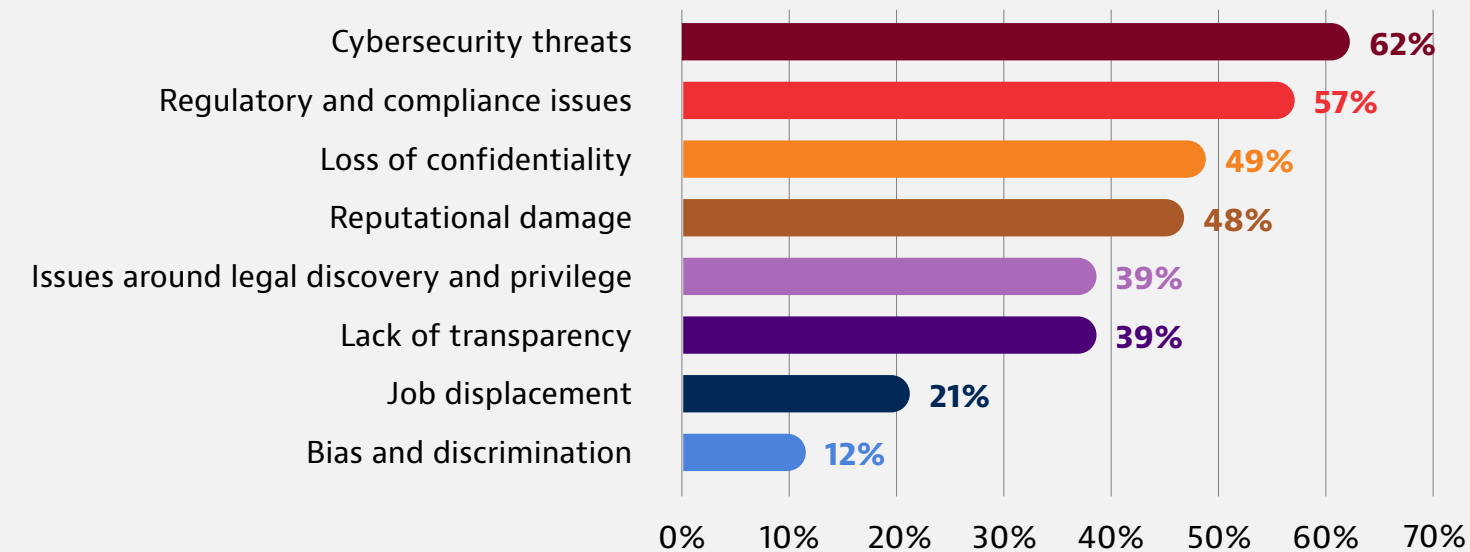
disciplines — not just IP-related case law and legislative developments but also existing privacy and sector-specific regulation, and emerging AI regulation — to develop a strategy to manage legal risk and maximize opportunities.”

For example, in Singapore and Japan, there are specific exemptions provided for access to data in training AI tools. However, such exemptions, where and when they do exist, are not yet standard across other jurisdictions. We expect to see major developments in the coming year as courts, legislators and regulators grapple with the application of existing IP law to the questions raised by AI, and consider whether new guidance or amendments to existing legislation are required.



How much consideration have you given to the following risks of using AI in your business? (Ranked top two)

*Base: survey respondents citing AI as a risk



“AI regulation remains very much driven by jurisdictional nuances, including the patchwork of existing IP laws and the specific policies put in place or under consultation by regulators and legislators. Ultimately, court decisions are likely to look very different across jurisdictions, due to the nature of how local law views and/or defines the concepts of IP ownership, validity and infringement, and the specific nature and use of the AI tools at issue in each case,” shares Liu.

Nevertheless, even where AI is highlighted as an area of concern, organizations are leveraging the technology in dispute management, particularly in analysis (73%), decision-making (70%) and research (69%). The use of AI elsewhere is less prevalent: Only 34% are using the technology for prediction, 32% for discovery/disclosure and 24% for drafting — suggesting that organizations are still exploring the full potential of AI in these areas.

Businesses are alert to some of the risks posed by AI adoption, particularly cybersecurity threats, as well as regulatory and compliance issues. Ultimately, regulation around the use of AI, particularly when it concerns IP is still rapidly developing. Companies must pay close attention to potential liabilities and contractual protections in the purchase, training, use and reporting of AI tools.

It is striking that only 12% of respondents cite bias and discrimination as a potential AI disputes risk, and only 21% of respondents have considered issues of job displacement arising from the use of AI, which indicates a potential risk gap.

“AI regulation remains very much driven by jurisdictional nuances, including the patchwork of existing IP laws and the specific policies put in place or under consultation by regulators and legislators.”

Isabella Liu
Partner | Hong Kong



Key Disputes Trends

New legislation fuels employment disputes risk

Competition scrutiny has become the leading concern for employment disputes. In 2024, the US Federal Trade Commission took steps (which face ongoing legal challenges) to impose a nationwide, nearly complete ban on worker non-compete agreements. This aligns with the broader trend of global antitrust regulators closely monitoring HR practices — specifically, looking at competition between employers as they vie to attract and retain employees. The increased scrutiny means that companies that agree not to poach employees from other firms or engage in wage-fixing face significant financial and even criminal risks.

Celeste Ang, principal, Singapore, shares that Singapore has seen “a number of relatively high-profile cases involving the enforcement of restrictive covenants in the Singapore Courts and there is increased public interest. The Ministry of Manpower indicated early 2024 that it was working with the other tripartite partners to develop a set of guidelines to shape norms and provide guidance on the inclusion of restrictive clauses in employment contracts.”

In Australia, a public consultation on restrictive covenants was launched in 2024 (and now concluded). Notwithstanding differing laws, multinationals generally want to take a consistent approach across all markets in which they operate. Ang shares that if multinationals “update their practices in response to developments in the US, for example, then typically, they will want to evaluate that approach across their global network.”

Equal pay considerations are another key concern, prompted by pay transparency regulations that have swept the globe in a bid to close gender gaps in the workplace. The EU Pay

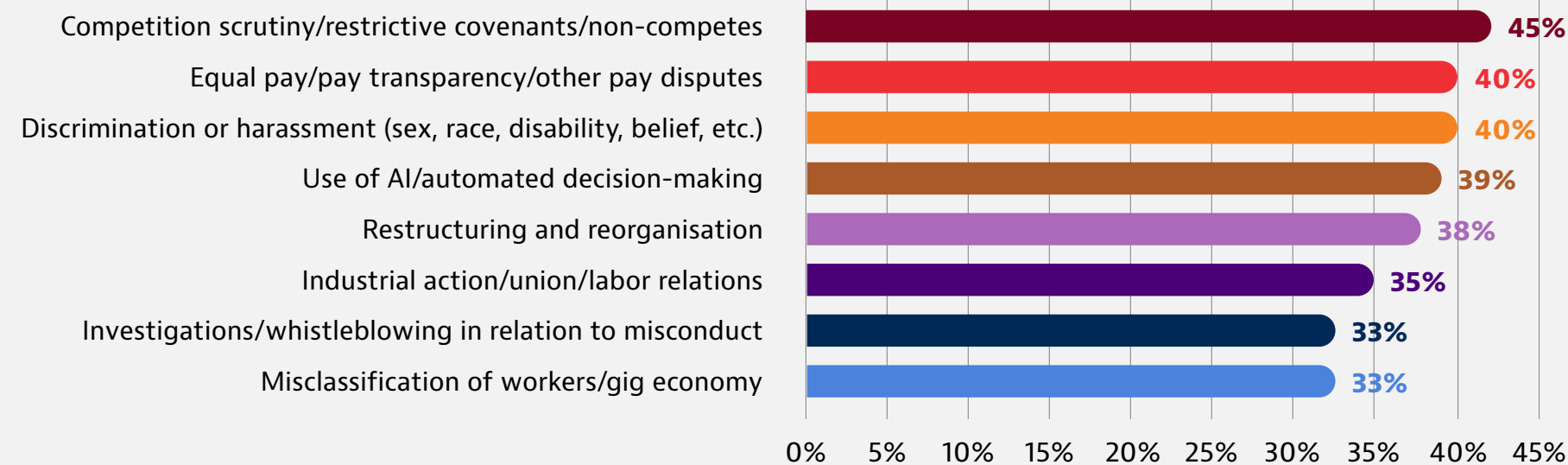
Transparency Directive has sought to solidify the principle of equal pay for equal work through enhanced transparency and enforcement. In the US, New York and California have introduced legislation requiring employers to post pay scales in job postings, while larger employers in the UK must report on their gender pay gap.

Workplace investigations are another contentious area, with 40% of respondents concerned about discrimination or harassment disputes. Stronger protection for whistleblowers has prompted a rise in reporting.

“We see a lot more investigations relating to discrimination, bullying, abuses of power and harassment. This is driven partly by changing legislation but also a shift in attitudes. There’s more awareness of bad behavior — which is a positive step — and more companies are undertaking training to ensure a safe and healthy work environment and mitigate risks,” shares Ang.

What type of employment disputes present the greatest risk to your organization in 2025? (Ranked top three)

*Base: survey respondents citing employment as a risk





“Multinationals generally want to take a consistent approach across all markets in which they operate. If they update their practices in response to developments in the US, for example, then typically, they will want to evaluate that approach across their global network.”

Celeste Ang
Principal | Singapore

Baker McKenzie's **Workforce Redesign** hub explores the biggest factors shaping the workforce so that business leaders can confidently build their flexible futures.

Baker McKenzie's **Contingent Worker Misclassification Tool** provides high-level information about pensions, wage tax, employment law and employee benefits risks of engaging contingent workers across 29 jurisdictions.





Key Disputes Trends

Mobility concerns drive tax disputes risk

What type of tax disputes present a risk to your organization in 2025?

*Base: survey respondents citing tax as a risk



Global employee mobility is the chief driver of tax dispute risk for 62% of respondents.

“Enhanced technological platforms, digital nomadism, the easing of COVID-19 restrictions, job relocation and increasing demand for remote work opportunities have all triggered an increase in global mobility. This has led to an increase in focus for tax authorities on cross-border employment arrangements for tax compliance,” shares Jorge Narváez-Hasfura, partner, Mexico City.

Restructuring, acquisitions and changes to operational structures can also trigger complex tax dispute risks in relation to labor and compensation. To tackle this, companies should

conduct thorough reviews of their current global mobility tax policies to identify any potential gaps or weaknesses.

Maria Antonia Azpeitia, partner, Madrid, notes that, “It’s crucial to stay updated with the constantly changing tax regulations in different jurisdictions. Implementing robust tracking systems for employee movements, clearly communicating the rules and ensuring proper documentation and reporting are essential steps. Additionally, seeking advice from tax professionals and leveraging technology to manage compliance can significantly help in mitigating risks.”

For multinationals, managing the layers of industrial, local, regional, and global tax legislation is complex, particularly with

varying adoption and implementation of Pillars One and Two, which regulate the tax affairs of multinational companies. Over half of respondents also cite indirect tax, industry-specific tax and transfer pricing as key tax dispute areas.

Indirect tax disputes arise from the dynamic nature of VAT and GST regulations and the attempts of tax authorities to try to adapt to a fast-changing economy. “The current trend of introducing new indirect taxes to target specific industries that are perceived as performing particularly well or that can provide very useful information to the tax authorities to control third parties’ tax compliance is also a contributing factor. Organizations need to invest in systems and processes that ensure accurate registries and timely filings to avoid these disputes,” says Azpeitia.



Transfer pricing disputes continue to be one of the main focuses of tax authorities, and they represent a challenge for multinational companies since they involve a thorough analysis of their business model and value chain. This analysis can be very disruptive and usually includes a tremendous amount of information requests that goes beyond how multinationals organize their reporting lines, as well as interviews with non-tax employees and the need to provide appropriate background to third-party information that the company does not control and can be misleading.

"All of this analysis must be done with a clear strategy and consistency from the beginning of the audit, being conscious that different tax authorities with different interests can arrive at different conclusions," says Azpeitia.

When it comes to managing tax disputes, litigation remains the resolution mechanism of choice, with more than 90% of respondents citing litigation as a preferred mechanism and 72% citing arbitration. The high percentage of respondents citing litigation as the most effective mechanism reflects the significant stakes involved in tax disputes. Tax disputes often involve substantial financial implications and can affect an organization's reputation. Litigation provides a structured and formal process for resolving such disputes, without losing control of the proceedings or being impacted by third-party interests.

"Multinational organizations are more likely to resort to litigation to resolve tax disputes because it can set legal precedents that may benefit the organization in future disputes. Even when tax litigation requires an important investment of time and economic resources, when tax assessments are high, multinational organizations feel more comfortable litigating as they will have a space in which to challenge interpretations made by tax authorities in complex tax cases. In some cases, litigation can provide an advantage in negotiations with tax authorities. In short, perhaps the most attractive feature of litigation is that it allows for the judicial review of positions put forward by the tax authorities," says Narváez-Hasfura.

However, organizations should also explore alternative dispute resolution mechanisms. Only 21% of respondents named Advance Pricing Arrangement (APA) and 15% cited Mutual Agreement Procedure (MAP) as preferred tax dispute resolution mechanisms. It is important for organizations to explore alternative dispute resolution mechanisms, such as MAP or arbitration, which depending on the nature of the dispute and the countries affected, can be also a good or even better alternative. Choosing the right path is a relevant part of the defense strategy.

“It’s crucial to stay updated with the constantly changing tax regulations in different jurisdictions. Implementing robust tracking systems for employee movements, clearly communicating the rules and ensuring proper documentation and reporting are essential steps.”

Maria Antonia Azpeitia
Partner | Madrid



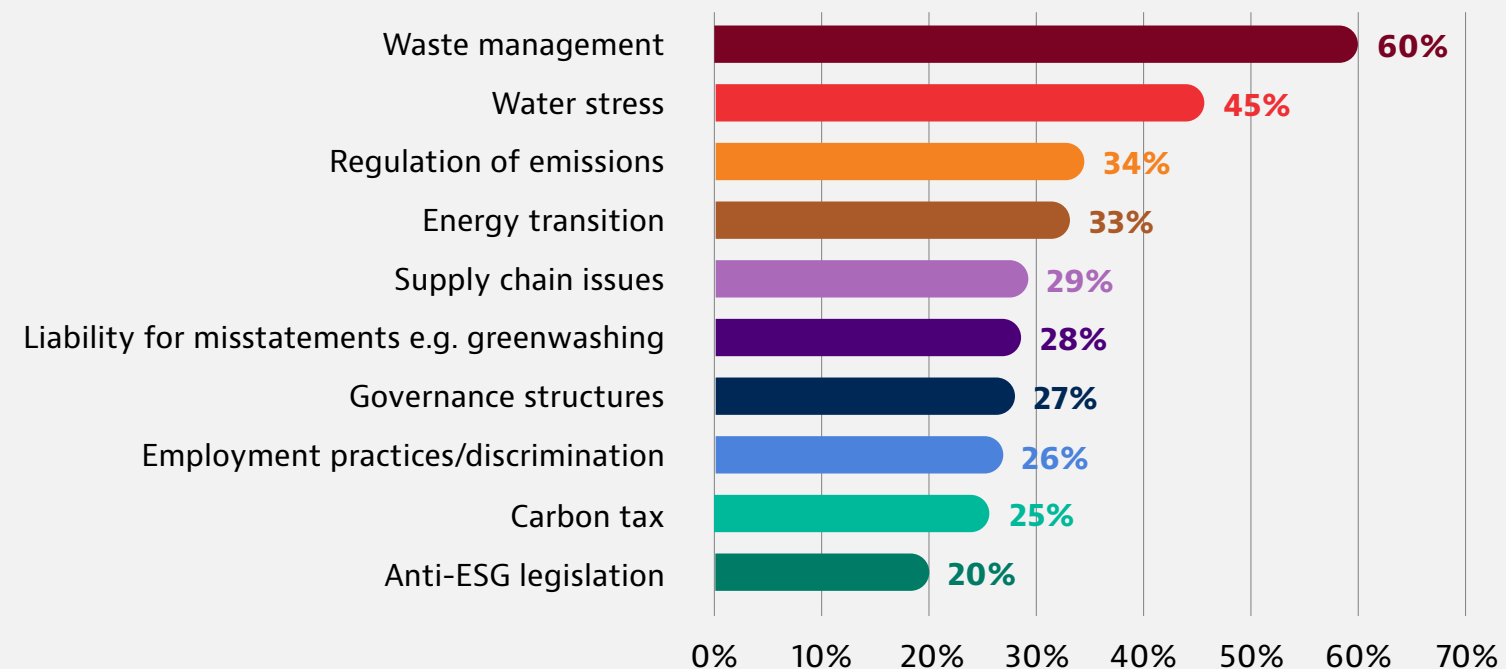


Key Disputes Trends

Environmental slant to key ESG disputes risk

What type of ESG disputes present a risk to your organization in 2025? (Top ten)

*Base: survey respondents citing ESG as a risk



ESG disputes remain a concern for organizations, with 40% of respondents highlighting them as a significant risk.

The most prominent ESG dispute risk is waste management, as reported by 60% of respondents, while almost half (45%) cite water stress as a prominent risk. Legislation is compelling companies to adopt (and report on) more sustainable practices. The EU's Waste Framework Directive sets stringent requirements

for waste management, while the United Nations' Sustainable Development Goal 6 aims to ensure the availability and sustainable management of water and sanitation for all, in the face of increasing scarcity of water resources. The EU's Corporate Sustainability Reporting Directive (CSRD) requires large and listed companies to report on ESG risks and how their activities affect people and the environment.

“ ESG litigation risk is now an important factor in strategic business planning. Organizations may be less inclined to invest in more challenged businesses.”

Peter Tomczak
Partner | Chicago

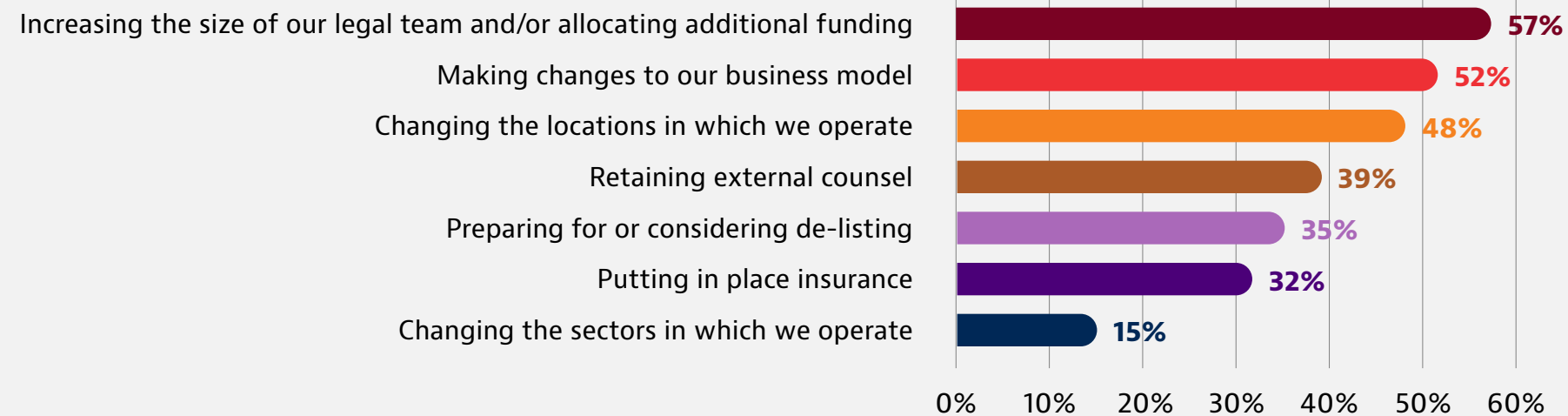
The regulation of emissions (34%) and energy transition (33%) are also significant concerns. The transition to a low-carbon economy and the need to comply with emissions regulations, such as the EU's Emissions Trading System, pose challenges for organizations. Failure to meet these regulations can result in substantial fines and reputational damage. The Paris Agreement further emphasizes the need for organizations to reduce their carbon footprint and transition to renewable energy sources.

Climate change cases will continue to develop at pace. A decision of the European Court of Human Rights against Switzerland in April 2024 found a violation of Convention rights and outlined positive obligations on states within its jurisdiction to mitigate climate change. Similar cases will follow.



Which of the following steps are you taking to prepare for ESG disputes?

*Base: survey respondents citing ESG as a risk



The threat of ESG disputes is driving strong operational action. More than half of respondents (57%) say they are increasing the size of their legal team and/or allocating additional funding in the year ahead.

Significantly, 52% of respondents are making changes to their business model, while 48% are considering a change in their operating locations in response to, and anticipation of, ESG disputes.

“ESG litigation risk is now an important factor in strategic business planning. Organizations may be less inclined to invest in more challenged businesses,” says Peter Tomczak, partner, Chicago. “Companies are also making changes to their business models or considering de-listing to avoid some of the regulations and disclosures required by authorities, such as the US Securities and Exchange Commission.”

For the first time we are also seeing respondents alert to disputes arising from the “Anti-ESG” movement.

“There is now anti-ESG legislation in several US states as well as the Middle East, China, and parts of Europe. ESG initiatives have a cost and it is incumbent upon governments and organizations to make sure it is quantified and considered,” says Tomczak.

In terms of geographical risk, Canada (44%), the UK (35%) and Australia (34%) are the top regions where organizations anticipate ESG disputes. These regions have robust regulatory frameworks and actively enforce ESG regulations, making compliance critical. The EU (23%) and Germany (23%) also present significant risks.

David Gadsden, partner, Toronto, notes that in Canada, “recent amendments to the Competition Act have explicitly prohibited, and imposed significant penalties for, deceptive marketing practices relating to environmental claims, or ‘greenwashing’”. This increased focus on greenwashing has no doubt pushed ESG concerns up the agenda for businesses operating in Canada.”

Baker McKenzie is a participant of the **UN Global Compact**. View our **progress**, and see our commitment to **inclusion, diversity and equity**.



Key Disputes Trends

Tax issues trigger post-M&A disputes

The most common triggers for post-M&A disputes include tax indemnities or other tax-related topics, as well as general contract claims, each cited by 56% of respondents. Transactions often trigger an audit by the tax authorities which can then lead to taxes relating to the time period before the closing of the transaction. Purchase price or valuation questions (46%) are also a major trigger.

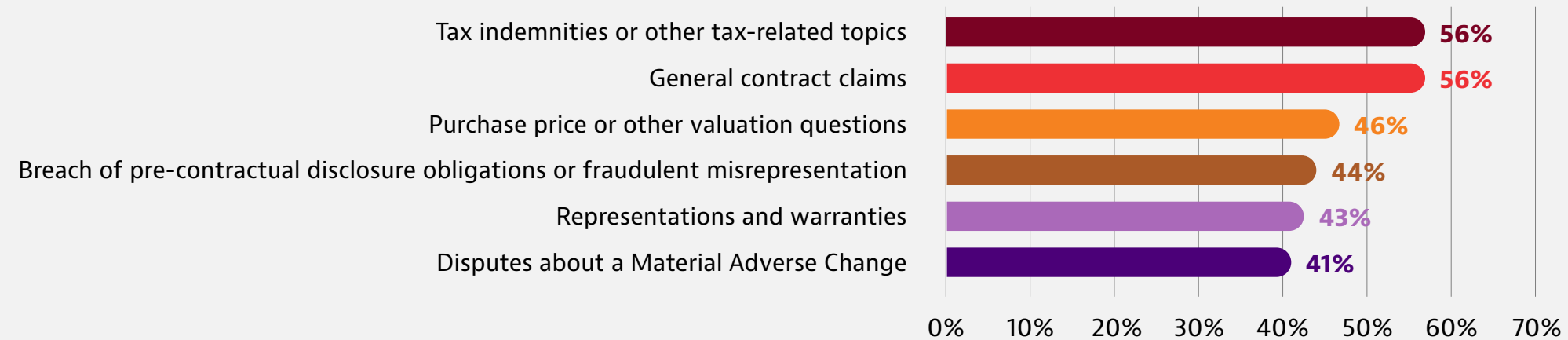
Organizations are most likely to consider legal claims against the other party in an M&A transaction due to third parties asserting claims (72%), earnings problems or operative liquidity issues in the acquired company (66%), and problems identified during the preparation and audit of annual financial statements (62%).

Markus Altenkirch, Counsel, London, who focuses on post-M&A disputes, observes: "One of the most common reasons for post-M&A disputes initiated by purchasers is that the purchaser discovers after the closing of the transaction that the target company's financial performance is worse than expected. In most cases, purchasers then bring a claim based on the financial statements warranty — the warranty that is triggered more often than any other."

These issues often arise from discrepancies discovered post-transaction, which can significantly impact the financial health and operational stability of the acquired company. Ad hoc reviews before the end of warranty periods under the purchase agreement (53%) and financing problems (47%) are additional factors that can prompt legal claims.

Which of the following may be triggers for post-M&A disputes involving your organization?

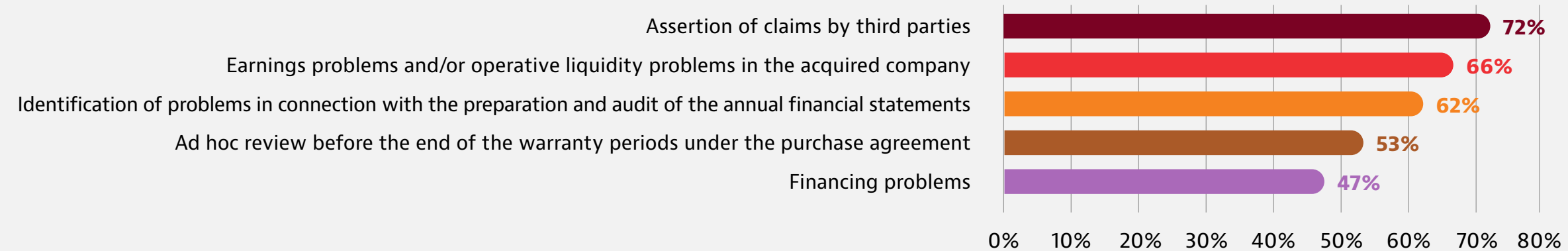
*Base: survey respondents citing corporate/securities/post-M&A risk





Which of the following are most likely to prompt you to consider legal claims against the other party in an M&A? (Ranked one two three)

*Base: survey respondents citing corporate/securities/post-M&A risk



To minimize or prevent post-M&A disputes, organizations are taking several steps. These include implementing a better understanding and assessment of technology (47%), which can help identify potential issues early and ensure that the technology integration process runs smoothly. Including dispute resolution mechanisms such as arbitration and mediation clauses in contracts (41%) is another strategy, providing a structured approach to resolving conflicts without resorting to litigation.

Conducting more due diligence (41%) and implementing detailed integration plans (40%) are also crucial steps to ensure that potential risks are identified and managed effectively.

"In-depth due diligence offers value for money as it prevents surprises after the closing. Moreover, in-depth due diligence often leads to specific indemnities for issues that were spotted during the due diligence. If the risk that was identified during the due diligence materializes, this often leads to an out-of-court settlement of the respective losses," says Altenkirch.

“In-depth due diligence offers value for money as it prevents surprises after the closing.”

Markus Altenkirch
Counsel | London

Baker McKenzie's **Disputes Clause Finder** provides users with individually tailored choice-of-court or arbitration clauses in just a few steps.

Sector Insights

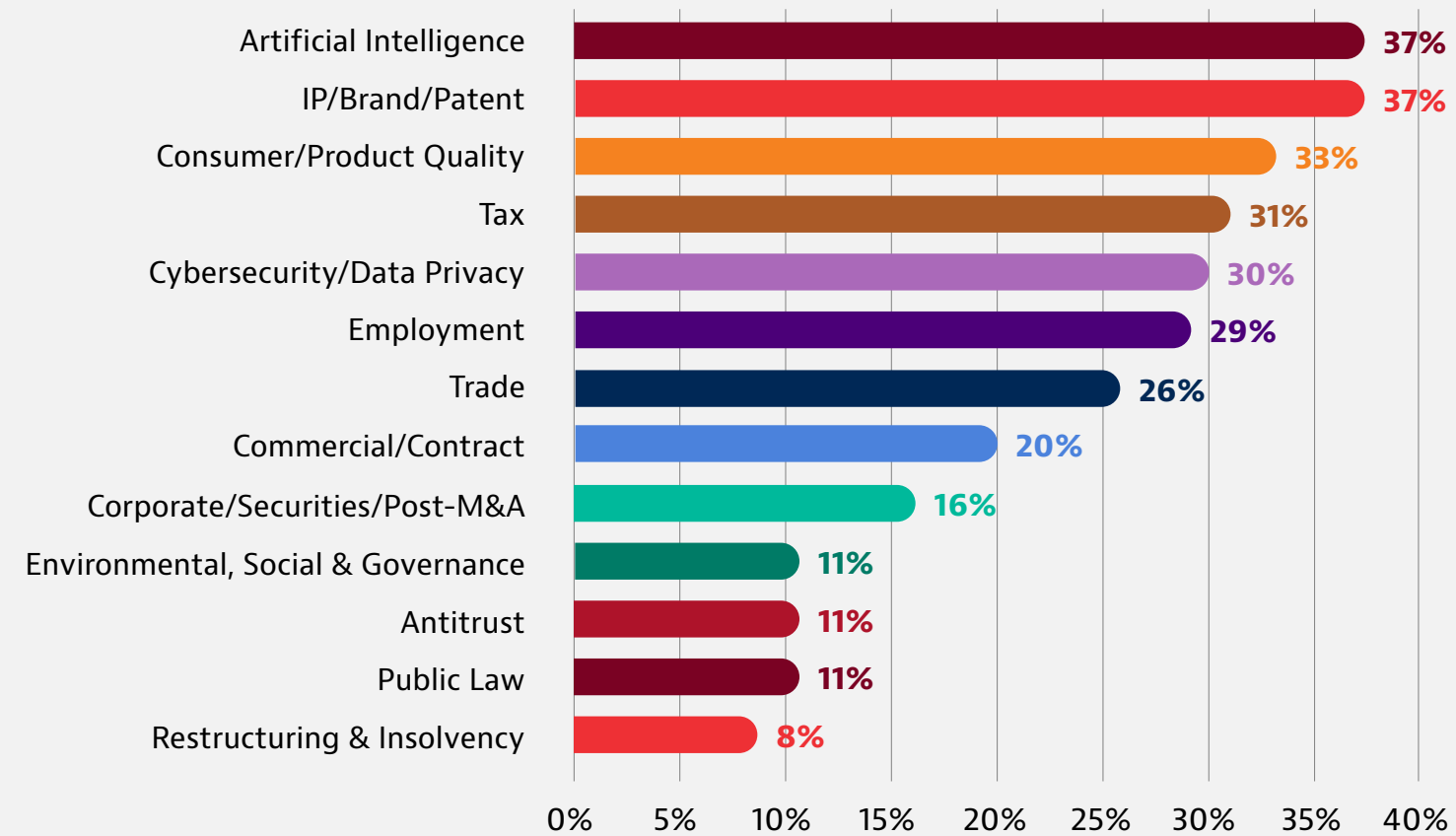




Sector Insights

Consumer Goods and Retail (CGR)

What type of disputes present the greatest risk to your organization in 2025?
(Ranked top three)





AI has received a lot of interest from CGR clients and the sector has been enthusiastic in embracing opportunities made available by the developments in AI technology, including generative AI. CGR businesses are seeking legal advice on how to deal with AI internally and incorporate governance into existing policies — for example around recruitment, marketing, third party contracting, social media engagement, as well as monitoring new legislation.

IP and AI issues have overlapped in recent high-profile litigation related to the unauthorized use of material in training generative AI. There is also a growing threat of litigation from “AI washing” whereby companies may (deliberately or inadvertently) make false and misleading statements about their use of AI. The US Securities and Exchange Commission was particularly active in 2024 in bringing charges in this area, and this trend looks set to continue into 2025.

IP, brand, and patent disputes are prominent risk areas for respondents from this sector. As counterfeits get more sophisticated, brands have to keep improving their technology and detection methods, particularly as e-commerce has provided a wide variety of selling methods to those peddling counterfeit goods.

“The rise in ‘dupes’ is a major concern for many brands. Social media is full of advertisements and posts around dupe products, openly comparing themselves to more expensive and luxurious goods. Dupes do not try to confuse consumers but instead compete against the brands as cheaper versions. This makes traditional trademark infringement challenging and provides new problems for brands to address,” says Katia Boneva-Desmicht, partner, Paris.

For CGR companies, some of the most important IP considerations are centered on ownership and infringement risk in consumer-facing content, such as promotional advertising, logos, images and so on. For other sectors, where AI may be incorporated into end products or used in research and development, key IP issues are around the protectability of AI

technologies themselves and AI-generated or enhanced output. Businesses across sectors will be concerned to understand how their own valuable content can be leveraged by AI tools and how to manage the risks associated with the use of AI by their employees and for internal operational purposes.

“Consumer and product quality disputes are always a concern for consumer goods and retail brands. Disputes around ESG and product ingredients and provenance are of particular interest. Class actions are also a concern, particularly in the US,” says Boneva-Desmicht.

“The rise in ‘dupes’ is a major concern for many brands. Social media is full of advertisements and posts around dupe products, openly comparing themselves to more expensive and luxurious goods.”

Katia Boneva-Desmicht
Partner | Paris



Our **360° IP Solution** has been developed for complex, diverse and global IP portfolios



Brands with high profiles have always been attractive targets for cybersecurity and data attackers, but the increasing digitalization of organizations and their supply chains has created new vulnerabilities, and cyber resilience is now a key focus of governments and regulators, as well as brands themselves.

The Digital Markets Act, Digital Services Act, Data Act and Data Governance Act have all had a significant impact on this sector, and the new EU AI Act will require close consideration (particularly relating to consent for using consumers' personal data to train AI).

Cybersecurity/data privacy has replaced supply chain issues as the leading external risk for CGR companies. Respondents point to internal challenges, particularly with training their people and implementing relevant tech updates. 67% of respondents also cite a lack of budget within the organization as a barrier to finding the right litigation/arbitration support.

"The risk of a cyberattack can be devastating if not handled quickly and effectively by both the internal team and external advisers. This is one of the reasons why we advocate training sessions that simulate a real cyber event to ensure that all members of the internal response team are aware of their roles and responsibilities if the worst does happen. Addressing budget constraints can be managed by prioritizing initiatives that offer the highest mitigation risk and exploring cost-effective solutions. It is hard for clients to anticipate disputes and budget accordingly for them. It is vital for the external adviser to understand the brand's objectives and non-negotiables at the outset so that the litigation strategy is bespoke and meets the brand's needs," says Boneva-Desmicht.



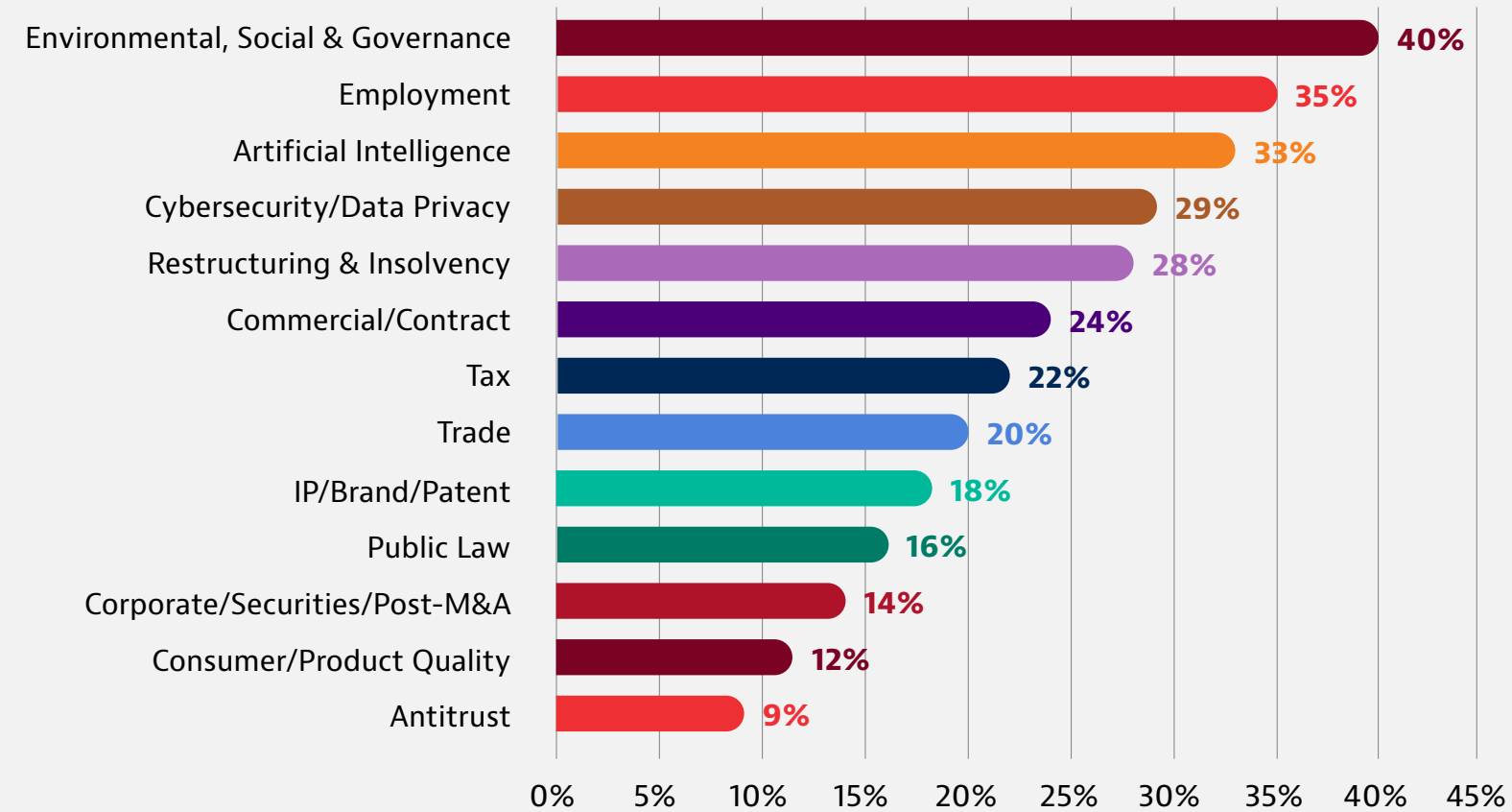
For more on the Luxury sector, read about the future of sustainability legislation in **Positive Luxury: ESG Policy Guide**

For a deep dive into disputes within the CGR sector, contact us **here**.

Sector Insights

Energy and Infrastructure (E&I)

What type of disputes present the greatest risk to your organization in 2025?
(Ranked top three)





Respondents in this sector were more concerned about ESG disputes than in any other industry. E&I respondents are also most worried about an ESG investigation (either internal or external) in 2025. The conflicting demands of climate change mitigation and rising energy costs create the potential for legal disputes.

Companies in this sector have vastly increased the resources they are putting into ESG in recognition of the increased focus on both regulatory compliance and media and public scrutiny. This investment may be starting to ease concerns: Although 40% of respondents anticipate ESG disputes, the figure is significantly lower than last year.

Michelle Porter-Wright, partner, Johannesburg, states, "Disputes and investigations risks are tied to energy transition for E&I businesses. They face challenges like balancing climate commitments against energy poverty concerns, while also considering the environmental impacts of critical mineral extraction for battery material. Additionally, disputes and investigation risks extend to social issues and stakeholder management as they relate to local community rights and benefits, as well as complex and nuanced ESG compliance standards."

Respondents in E&I were twice as likely as those in other sectors to predict a dispute in response to restructuring and insolvency.

"This increase is likely due to changes in the business environment, including the shift from fossil fuels to renewables, resource nationalism trends and volatile commodity prices, which are affecting product viability. Macroeconomic trends, such as currency fluctuations, foreign exchange control issues and challenges in accessing international financing for projects, are also driving structural changes," says Porter-Wright.

We also asked respondents how they are using AI in the context of dispute management. E&I respondents have embraced technology and are ahead of other sectors in using AI for decision-making and research. This is unsurprising given that disputes are common in these sectors, and many organizations have experienced disputes teams. It is likely that multinationals are driving this push, while many players in the industry try to keep pace, amid policy and regulation lag.

The top external risk for disputes is the challenge of doing business in emerging markets. The geopolitical climate remains uncertain in several key regions for this sector, but there are also challenges faced by global companies establishing projects in new regions that might have new ESG regimes. Indeed, the previous year has seen a large number of company-versus-emerging-state arbitrations, particularly in the mining industry.

“ Disputes and investigations risks are tied to energy transition for E&I businesses. They face challenges like balancing climate commitments against energy poverty concerns, whilst also considering the environmental impacts of critical mineral extraction for battery material. Additionally, disputes and investigation risks extend to social issues and stakeholder management as they relate to local community rights and benefits, as well as complex and nuanced ESG compliance standards.”

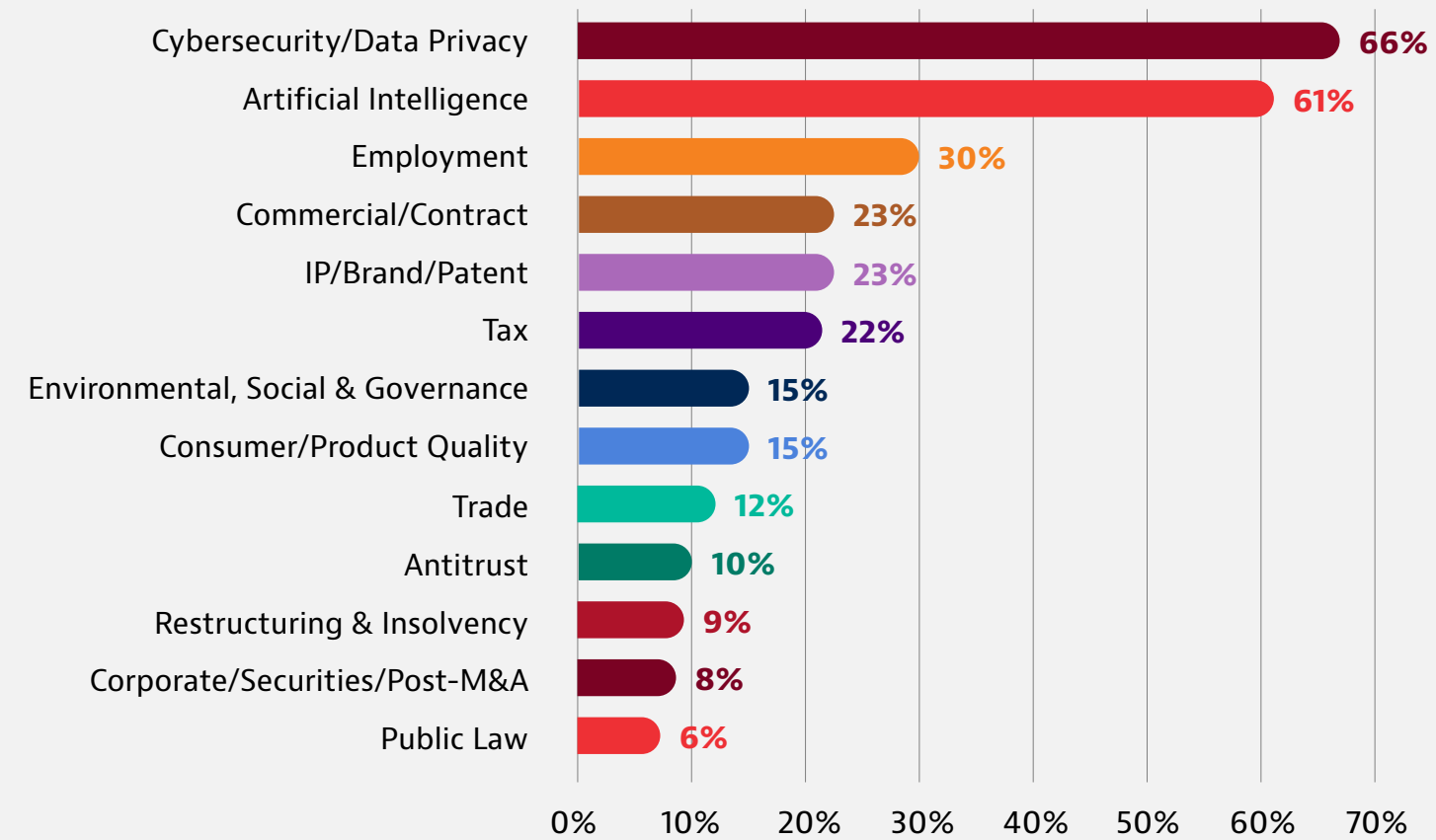
Michelle Porter-Wright
Partner | Johannesburg

For a deep dive into disputes within the E&I sector, contact us [here](#).

Sector Insights

Financial Institutions (FI)

What type of disputes present the greatest risk to your organization in 2025?
(Ranked top three)





Respondents from financial institutions were more optimistic in their disputes outlook than respondents in other sectors. More than a fifth of respondents predicted that their disputes spend would decrease in 2025 (the highest proportion of any sector group).

“Financial institutions have strong systems in place due to strict regulations, which help them manage disputes effectively. They also invest in advanced technologies like AI and machine learning to detect and prevent disputes early. Experienced legal and compliance teams contribute to efficient dispute handling. A stable financial environment reduces the likelihood of disputes, and efforts to improve customer relations and satisfaction help prevent issues from arising.

However, despite this optimism, there are continued risks. For example, in Europe there could be a growth in consumer finance disputes driven by factors like increased consumer awareness, evolving financial products and economic pressures on individuals,” says Łukasz Hejmej, partner, Warsaw.

When we asked FI respondents where they see the greatest risk of disputes, cybersecurity/data privacy and AI were the clear front-runners.

Perrie Weiner, partner, Los Angeles, notes that when it comes to a cybersecurity and data breach, “it’s not a question of if there will be a data breach but when. As for publicly held financial institutions, especially after the *Solar Winds* matter in the US, there are fairly immediate SEC reporting requirements when there is a data breach. Those disclosures frequently result in an immediate and precipitous drop in a public company’s stock prices. And, whenever this is a stock drop of more than 15%, both civil class actions (concerning the data breach) and an SEC investigation (to see if the public company’s prior disclosures were accurate, among other things) usually follow. Companies must remain prepared; a data breach is not only a very expensive matter to address mechanically, but the cost of litigation is significant.”

The financial industry is the custodian of vast amounts of customer personal data that can (with appropriate consent) be used to train and maintain AI systems (either proprietary or third-party systems). With increasing competition from start-ups and market disruptors, financial institutions want innovative solutions to keep existing customers and attract new ones. And while AI systems provide huge opportunities for innovation, efficiency savings and potential benefits to customers, they may also create more opportunities for cybercrime, data breaches and allegations of mishandling personal data.

“AI is a wild card, depending on what a company’s public disclosures say about it. To protect themselves, many companies are having their law firm’s cybersecurity compliance teams come in to evaluate the strength and integrity of their cybersecurity measures and to beef them up where necessary. They are also having their securities lawyers examine their public disclosures in that regard, to see what they say about their cyber risk and compliance. Financial institutions are also meeting with their insurance brokers to make sure they are adequately insured given the increased risk,” notes Weiner.

Although AI is perceived as a higher area of risk for FI respondents, the sector is using AI proactively in dispute management, particularly in analysis and decision-making.

“AI automates routine tasks, detects fraud in real time and assigns risk scores to prioritize cases. It also integrates data for better decision-making and uses predictive analytics to foresee potential disputes and/or their potential outcome. These AI-driven solutions help financial institutions manage disputes more efficiently, for instance by enabling them to assess which cases are worth pursuing and/or defending and which should be settled, and hence reduce costs,” says Hejmej.

Weiner notes the role of AI in driving down the price of discovery — perhaps the most expensive part of litigation.

“At the same time, AI is still in the relatively incipient stage, and there are cracks in the technology. Most financial institutions utilizing AI are encouraged to proceed with caution and avoid complete reliance on AI, especially in high-risk, high-exposure areas of their business,” Weiner says.

“Regarding cybersecurity and data breach, it’s not a question of if there will be a data breach, but rather when.”

Perrie Weiner
Partner | Los Angeles

For a deep dive into disputes within the FI sector, contact us [here](#).

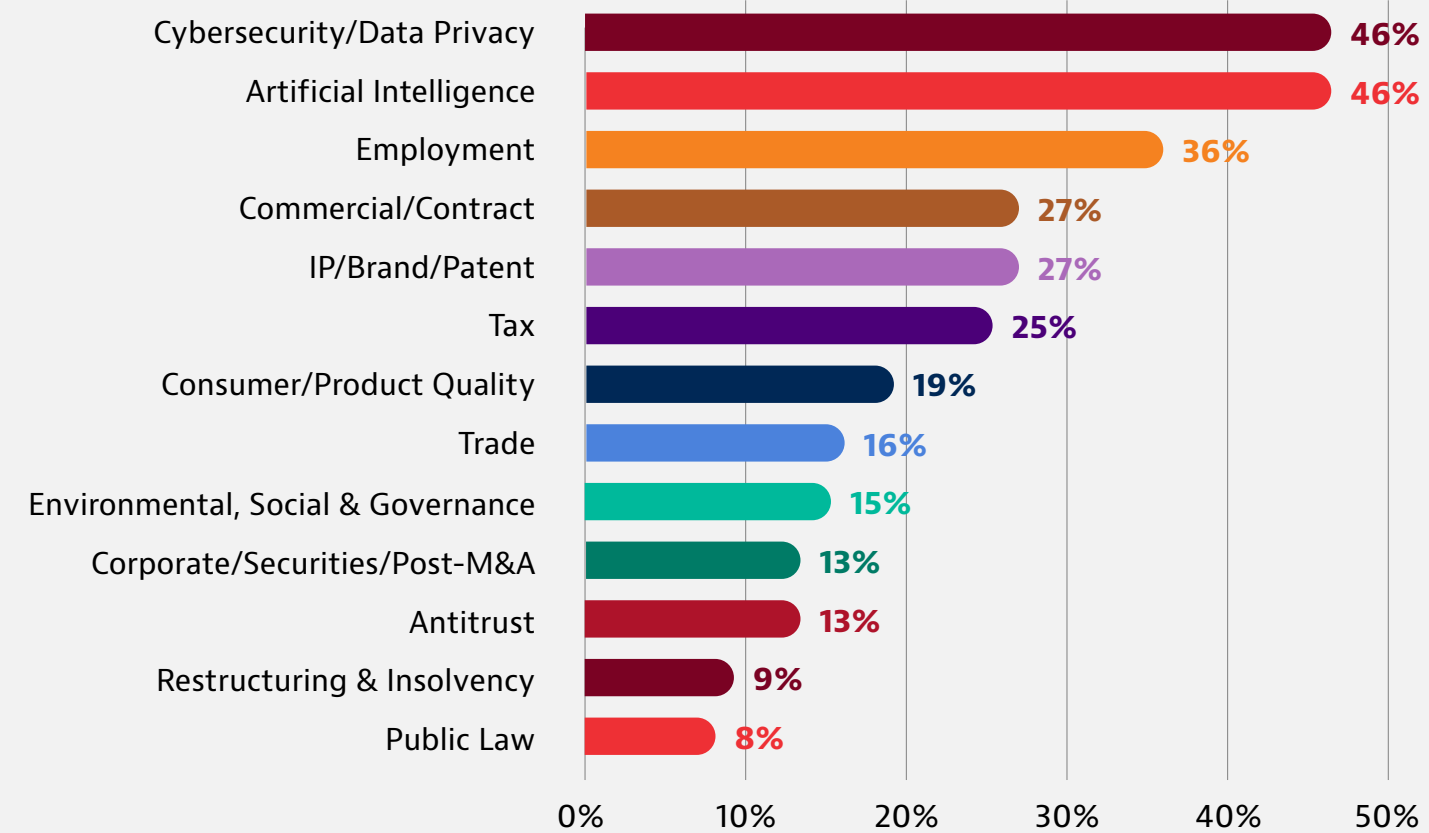
Explore how technology will transform the financial sector with our series: **Next Decade in FinTech**.

Read more about the impact of digital assets on the investment management landscape: **Tokenization & Blockchain in Asset Management**.

Sector Insights

Healthcare and Life Sciences (HLS)

What type of disputes present the greatest risk to your organization in 2025?
(Ranked top three)





Cybersecurity/data privacy and AI were the top disputes concerns for companies in this sector. Among those concerned about a cyber or data incident, 83% fear regulatory investigation or enforcement action, including fines.

Yindi Gesinde, partner, London, says that “it can be difficult to know how some AI makes its decisions: the quality of the outputs very much depends on the quality of the inputs. At the same time, there’s a lot of pressure on organizations to use AI and stay ahead of competitors, so that pressure brings with it considerable risk. For a healthcare company, if aspects of your research and development are reliant on AI, you have to be confident that the information on which your decisions are made is reliable.”

The use of AI also goes hand-in-hand with increased cyber threats, a particular consideration for HLS companies that handle so much sensitive information, such as patients’ personal and medical data. Clinical trials, research and testing also involve copious amounts of data that must remain secure, adding to the burden of responsibility for companies in this industry. Additionally, the use of AI in products and services, particularly in predictive health, telemedicine/remote medicine and remote patient care further increases risk.

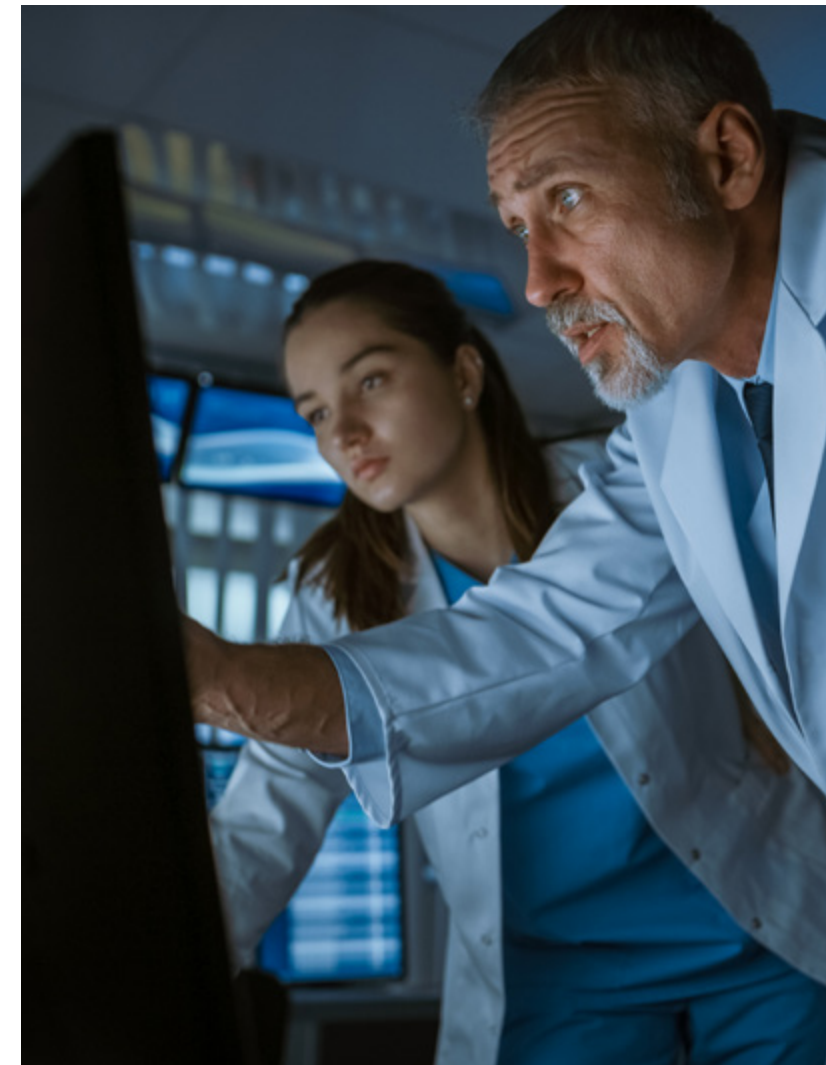
The EU AI Act only applies directly to systems used in the EU, but global manufacturers of medical products and services that use AI would be wise to utilize guidance and compliance standards under the act, even if they do not initially plan to deploy their AI systems in the EU. In particular, companies in this sector can get specialist advice to determine the type of AI they are using and the level of risk that their AI systems would fall under in the EU AI Act. From this information, the level of testing, registration and risk management required for it to be used in the EU can also be assessed. As a way to further mitigate the risk of continuing digital transformation and the evolution of AI, companies in this sector can use new regulatory sandboxes being created to facilitate safe development of AI systems.

Employment disputes have risen up the list significantly this year as an area of concern for all respondents. In this sector, respondents cited employment dispute concerns relating to (i) investigations/whistleblowing in relation to misconduct and (ii) equal pay/pay transparency/other pay disputes.

“Companies are being held to account for their commitment to their people and the need to provide safe spaces in the workplace. The EU Whistleblowing Directive has brought greater protection for whistleblowers, while a generational shift in attitudes has seen employees empowered to critique certain behaviors in the workplace, leading to a proliferation of workplace investigations,” says Gesinde. “This has created a huge challenge for organizations being hit with wave after wave of complaints. In addition to the legal and reputational considerations, there are also significant operational and governance concerns: cases must be investigated properly, but sometimes this takes bandwidth from other areas of risk. Businesses must find a sustainable model to investigate concerns on an ongoing basis.”

“If aspects of your research and development are reliant on AI, you have to be confident that the information on which your decisions are made is reliable.”

Yindi Gesinde
Partner | London

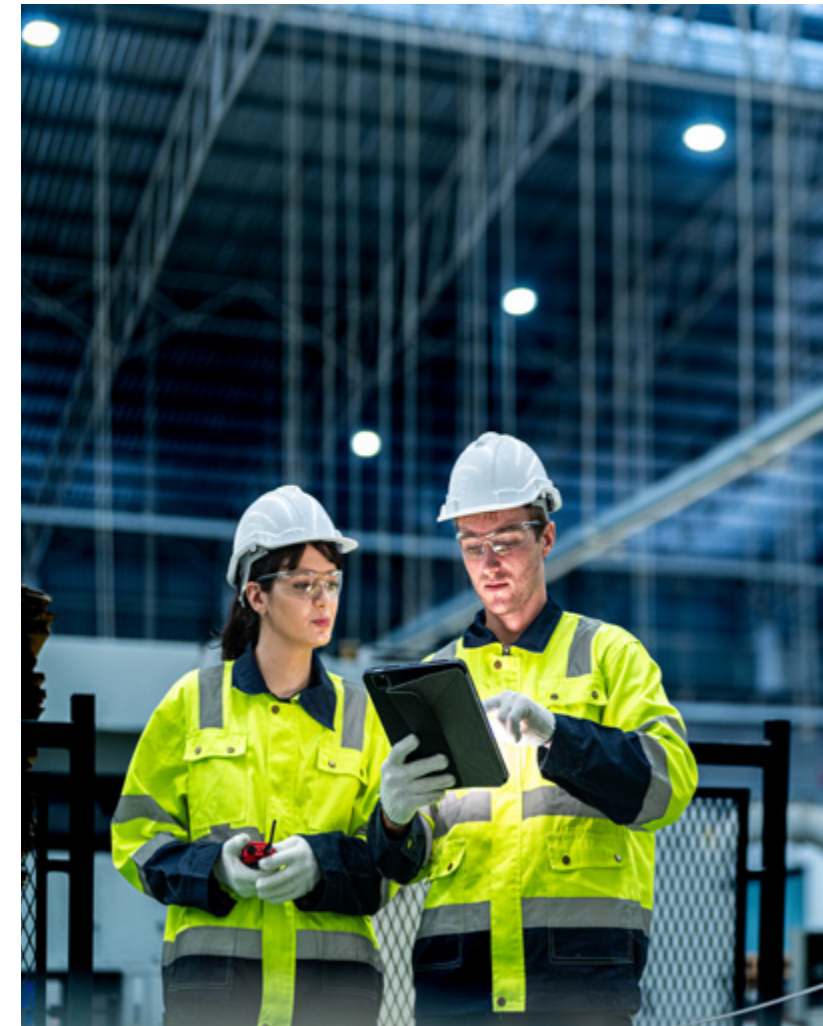
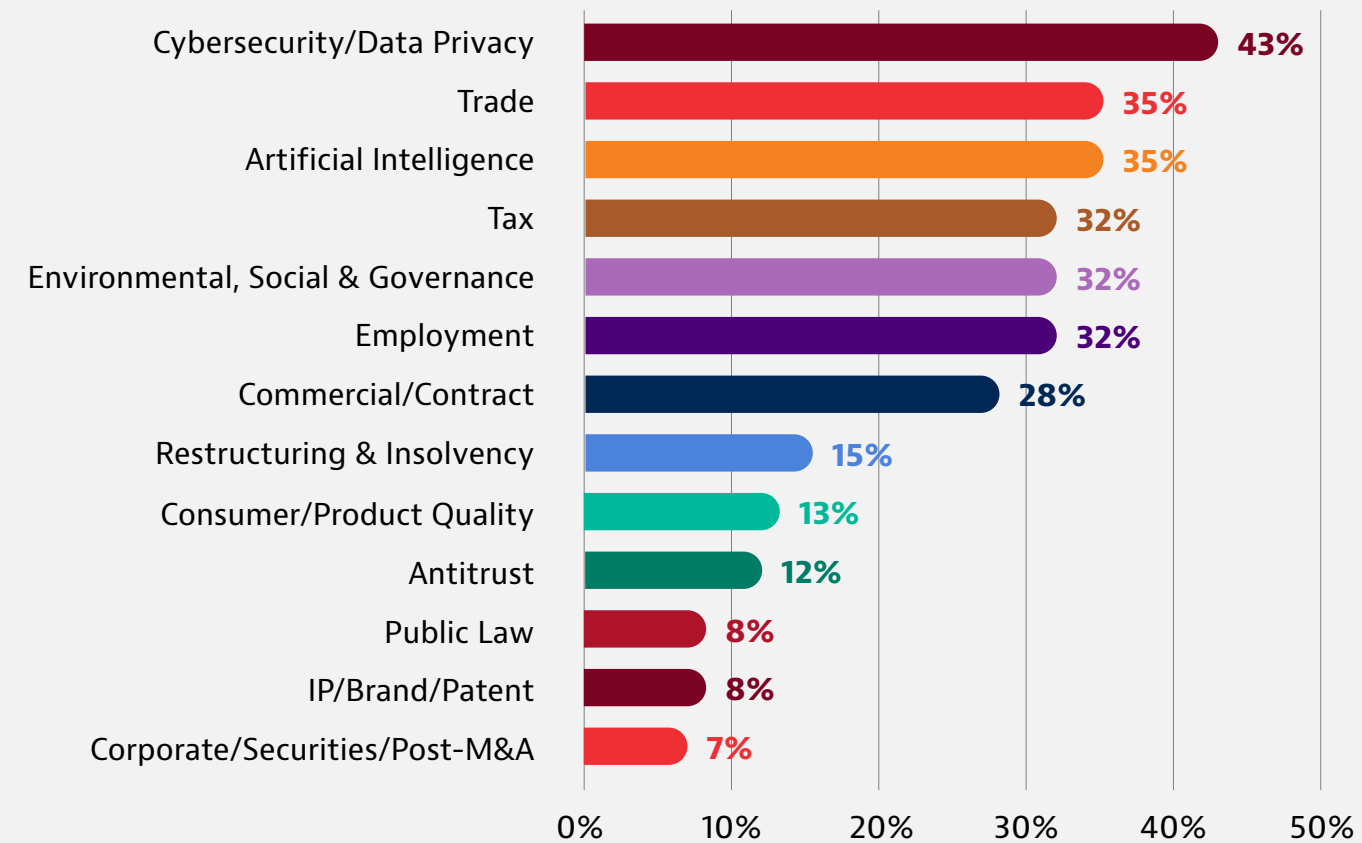


For a deep dive into disputes within the HLS sector, contact us [here](#).

Sector Insights

Industrials, Manufacturing and Transportation (IMT)

What type of disputes present the greatest risk to your organization in 2025?
(Ranked top three)





Almost half of IMT sector respondents anticipate an increase in disputes spending in 2025, compared to an average of 33% across all sectors.

Cybersecurity/data privacy and AI were the top expected dispute types, related to issues such as the development of automated machinery and transportation systems using AI systems. Increasingly, companies in this sector must consider contractual clauses that explicitly deal with potential failures, injury and resulting liability related to the AI systems they create, maintain or even just use.

Richard Allen, local principal, Singapore, shares “within the IMT sector, there is a particular concern regarding potential legal exposure for improper use of AI, which suggests that AI is being more widely adopted as part of the R&D process in this sector. The best way to mitigate these risks is to formulate clear policies on acceptable use of AI and to undertake proper due diligence on which data sets are being used to train any relevant AI tools.”

Digital regulation in this sector is increasing but not at the same pace as the technology, which means companies face the challenge of not only demonstrating compliance with existing regulations but also needing to consider what future regulations will demand. Therefore, IMT companies may need to look to other industries as they consider best practices for testing the AI with which they interact.

When asked about litigation preparedness, 60% of IMT respondents cited the inability to keep pace with regulation as a chief barrier to them feeling prepared to deal with litigation.

“Supply chain vulnerabilities are cited as one of the key barriers to litigation preparedness in the IMT sector, which reflects the particularly complex and interdependent nature of supply chains in this sector. With the growing regulatory trend toward supply chain transparency and the imposition

of liability for ESG-related harms down the supply chain, we regularly advise clients on the policies and contractual protections that should be put in place to prepare for the worst-case scenario,” says Allen.

“ Supply chain vulnerabilities are cited as one of the key barriers to litigation preparedness in the IMT sector, which reflects the particularly complex and interdependent nature of supply chains in this sector.”

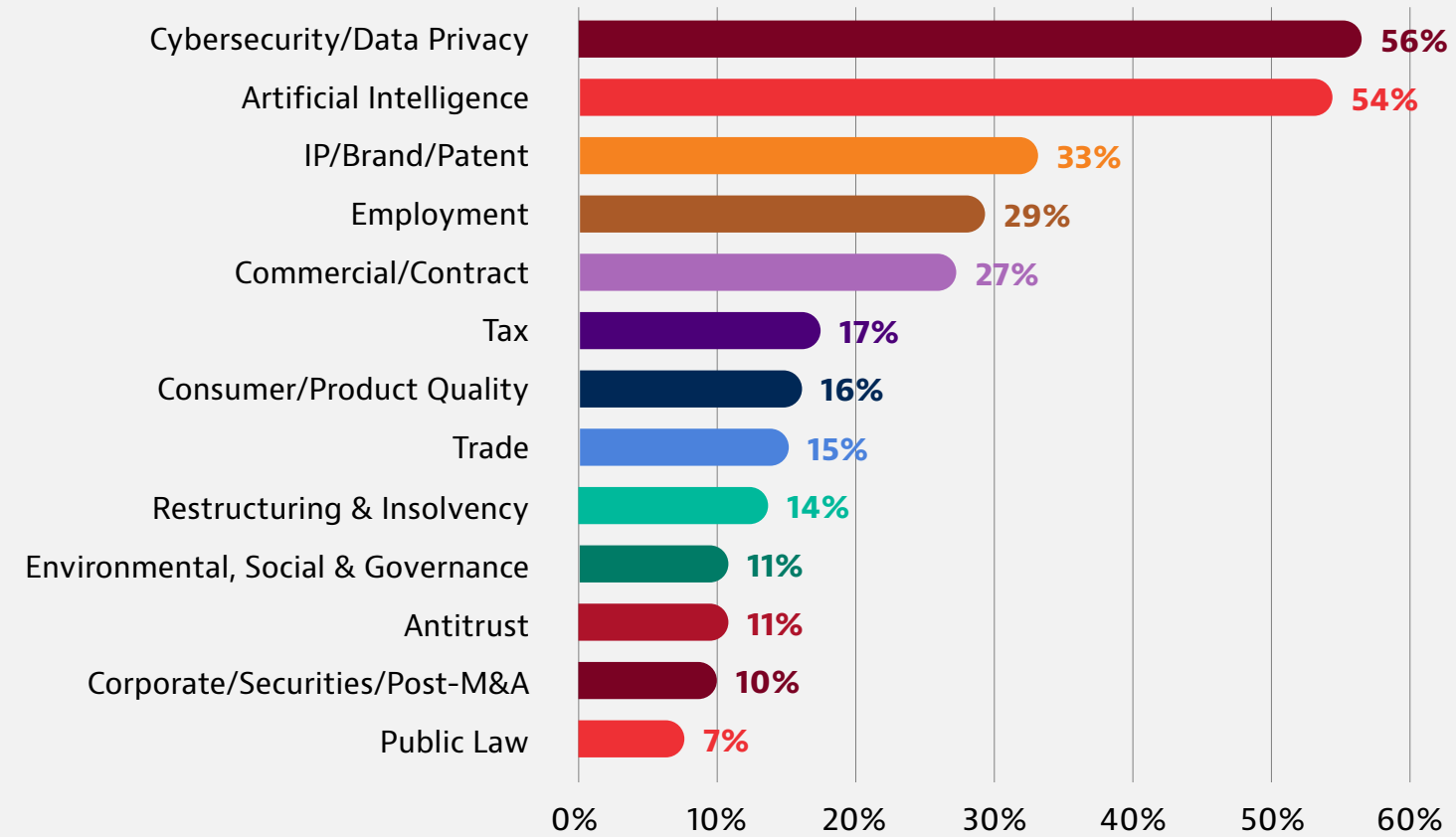
Richard Allen
Local Principal | Singapore



For a deep dive into disputes within the IMT sector, contact us [here](#).

Sector Insights Technology

What type of disputes present the greatest risk to your organization in 2025?
(Ranked top three)





“Software supply chains were designed to be interconnected and integrated with multiple systems and businesses, which make it a potential single point of failure and attractive target for malicious cyber actors.”

Justine Phillips
Partner | Los Angeles

For the third year in a row, cybersecurity/data privacy is the top expected dispute for this sector, closely followed in second place by AI. For a sector that is heavily based on the collection, storage, communication and use of data (much of which is personal data), this is unsurprising, particularly given that these issues rank highly on the survey lists for respondents of every other sector.

We expect to see more disputes (and more regulation) around the data generated by IOT devices and the cybersecurity risk that these devices present. The EU Data Act, which imposes new obligations to share data generated by connected devices with users, will take effect in 2025, complementing the Cyber Resilience Act, which creates a new regulatory framework governing the cyber resilience of all products with digital elements. We also expect to see disputes under the Data Act given the significance of the unintended consequences of data disclosure and sharing.

“Cyber laws like the US CIRCIA and the EU’s NIS2 and the Cyber Resilience Act are emerging globally to impose legal obligations on businesses to adopt technical, organizational and administrative cyber controls. These laws affirmatively require businesses to identify and report third-party and supply chain risk and vulnerabilities. Businesses developing and manufacturing software have even greater obligations to implement and document security-by-design into the product lifecycle,” says Justine Phillips, partner, Los Angeles.

Among the technology companies concerned about cyber security and data privacy, 61% were most worried about a regulatory investigation or enforcement action. Almost half of respondents (45%) noted concern around cyber and data compliance issues in their supply chains.

Companies must consider the wider legal risk if a cyberattack in their supply chain shuts down core business operations. For example, a cyber incident in an upstream supply chain that prevents an organization from delivering to downstream customers might bring contractual liability as well as cyber-specific legal risks. Phillips notes that, “these emerging legal risks require legal teams to collaborate enterprise-wide with product development, engineers and security teams to adequately identify and mitigate cyber risk. In addition to proactive cyber governance requirements, businesses must also be prepared to respond to supply chain attacks that may disrupt business operations. Now is the time to identify new laws and reporting obligations, update incident response plans and tabletop those new protocols.”

“Software supply chains were designed to be interconnected and integrated with multiple systems and businesses – which make it a potential single point of failure and attractive target for malicious cyber actors. Lawmakers around the world recognize the disruptive and potentially catastrophic impact of supply chain attacks and have taken action to mitigate this

insecurity by regulating businesses cyber practices. Putting it simply, a weak link in the chain can create unacceptable levels of cyber risk,” notes Phillips.

A new external risk for disputes for this sector is rising environmental regulation. This may be related to the growing environmental impact of data collection, storage and generative AI that powers companies in this sector.

For a deep dive into disputes within the technology sector, contact us [here](#).

The Wider Picture



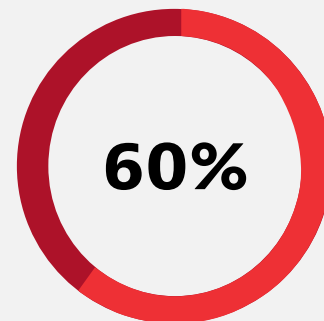


The Wider Picture

Organizations face barriers to litigation preparedness

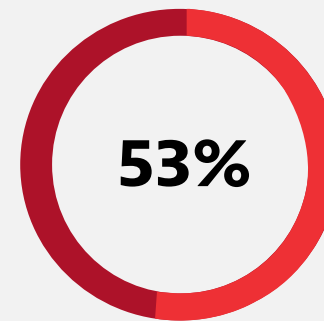
Litigation preparedness remains a critical concern for organizations, with several barriers preventing them from being fully prepared for potential disputes.

Inability to keep pace with regulatory developments



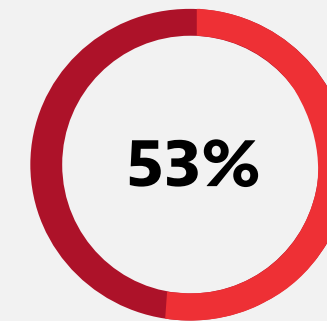
According to our survey, the most significant barrier to litigation preparedness is the **inability to keep pace with regulatory developments**. The complexity and frequency of regulatory changes require organizations to invest in continuous monitoring and updating of their compliance programs, which can be resource intensive.

Difficulty finding the right external advisors



More than half the respondents have **difficulty finding the right external advisors**. Respondents have struggled to find external teams that understand their business and the wider context in which they operate. This lack of sector-specific expertise can hinder effective litigation strategy and increase the risk of unfavorable outcomes.

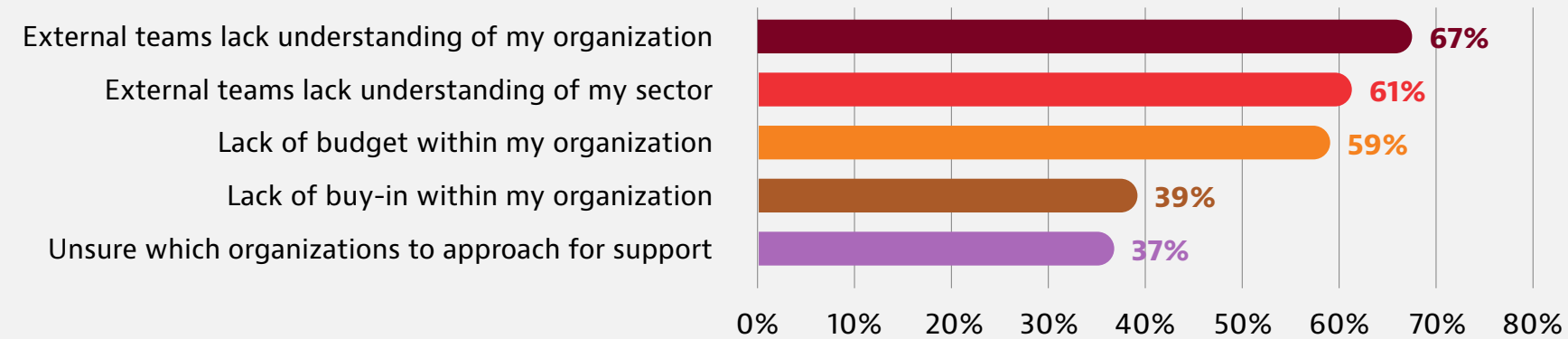
Funding and resourcing challenges



Funding and resourcing challenges are also significant barriers, with 53% of respondents indicating that they face difficulties in allocating sufficient resources for litigation preparation efforts. This can result in inadequate preparation and a reactive approach to litigation.

Elsewhere, supply chain vulnerabilities (50%) and internal organizational structures (45%) also lead to gaps in litigation preparedness.

What are the barriers to finding the right litigation or arbitration support?



“External counsel need to engage deeply with their clients to know their business and spot the underlying issue that could lead to a dispute. For example, as knowledgeable as arbitration counsel may be about different tribunals and arbitrators, they need to be equally well versed in the client’s business. Instead of focusing on broad sector knowledge, clients should seek counsel that are focused on their business imperatives,” shares Andy Moody, partner, London.

Moody also stresses the importance of proactivity: “Some disputes are unavoidable, but the best counsel will invest a lot of time into dispute avoidance. Proactivity is also key to understanding how geopolitical risk, political developments and evolving regulation affect individual businesses and the wider market.”



Contact us for an in-depth conversation on how we might support you in building an effective litigation strategy and decreasing the risk of unfavorable outcomes, through our deep understanding of your specific industry organizational needs.



The Wider Picture

Class action concerns are growing worldwide

Class actions continue to be a significant concern for organizations, with the UK, Germany and Australia identified as the top three countries posing the greatest risk outside the US.

Respondents perceive the greatest risk to be in the UK, following the significant upswing in collective claims filed after the UK Supreme Court's judgment in *Merricks*. The *Merricks* decision — released in December 2020 — established a relatively low bar for antitrust lawsuits being pursued before the UK's Competition Appeals Tribunal (CAT) and has resulted in a steady increase in collective claims filed before the CAT.

David Gadsden, partner, Toronto, notes that "Australia has also become more active in the class action space, while Canada is probably the most litigious jurisdiction outside the United

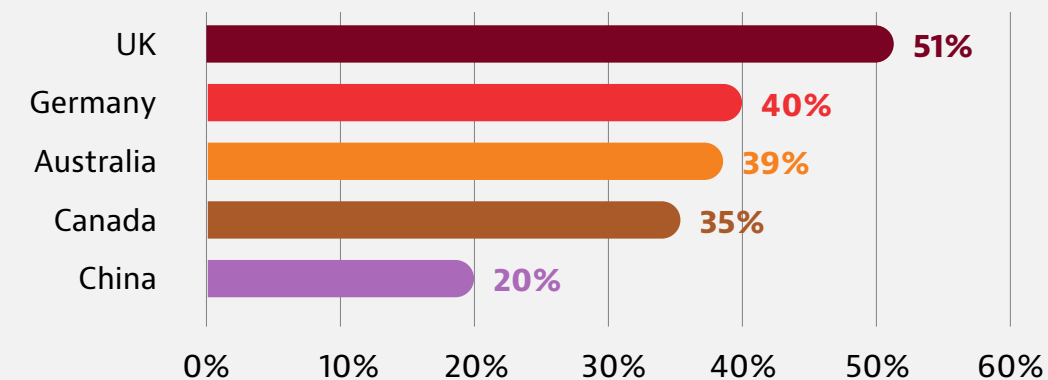
States. US and Canadian businesses have become accustomed to dealing with class actions as part of their litigation risk management strategy. Across Europe and in regimes where class actions are a newer phenomenon, in-house counsel have often had little exposure to class actions and are now taking steps to understand what it means for them and their business."

Even in the US, where class action risk is well known, organizations must remain alive to new threats.

"Perhaps the largest growing area that we are seeing is in the ancillary privacy space, particularly wiretapping claims, as there are hundreds of these cases being filed each year," says Nancy Sims, partner, Los Angeles.

Companies may be liable for wiretapping based on the use of common analytics software. In California, for example, plaintiffs have filed hundreds of lawsuits against businesses in a wide range of sectors, alleging that the use of technology, including chatbots and website cookies, requires express consumer consent. Those operating without that consent would potentially fall foul of unlawful eavesdropping or wiretapping under the California Invasion of Privacy Act.

Which countries outside the US pose the greatest class action risk to your organization?





UK

The rise in collective redress mechanisms and evolving legal frameworks, particularly in data privacy and consumer protection, have made it easier for groups of claimants to bring class actions.



Germany

The introduction of the redress action (Abhilfeklage), alongside the existing Model Declaratory Action, has facilitated more collective actions. Since the introduction of the redress action in October 2023, five cases have been registered, relating to streaming media services, mobile telephone services and energy supply.



Australia

Australia's well-established class action regime is supported by a proactive plaintiff bar and litigation funding, reflected in an ongoing flow of class actions filings across various areas, including consumer protection, employment and financial products.



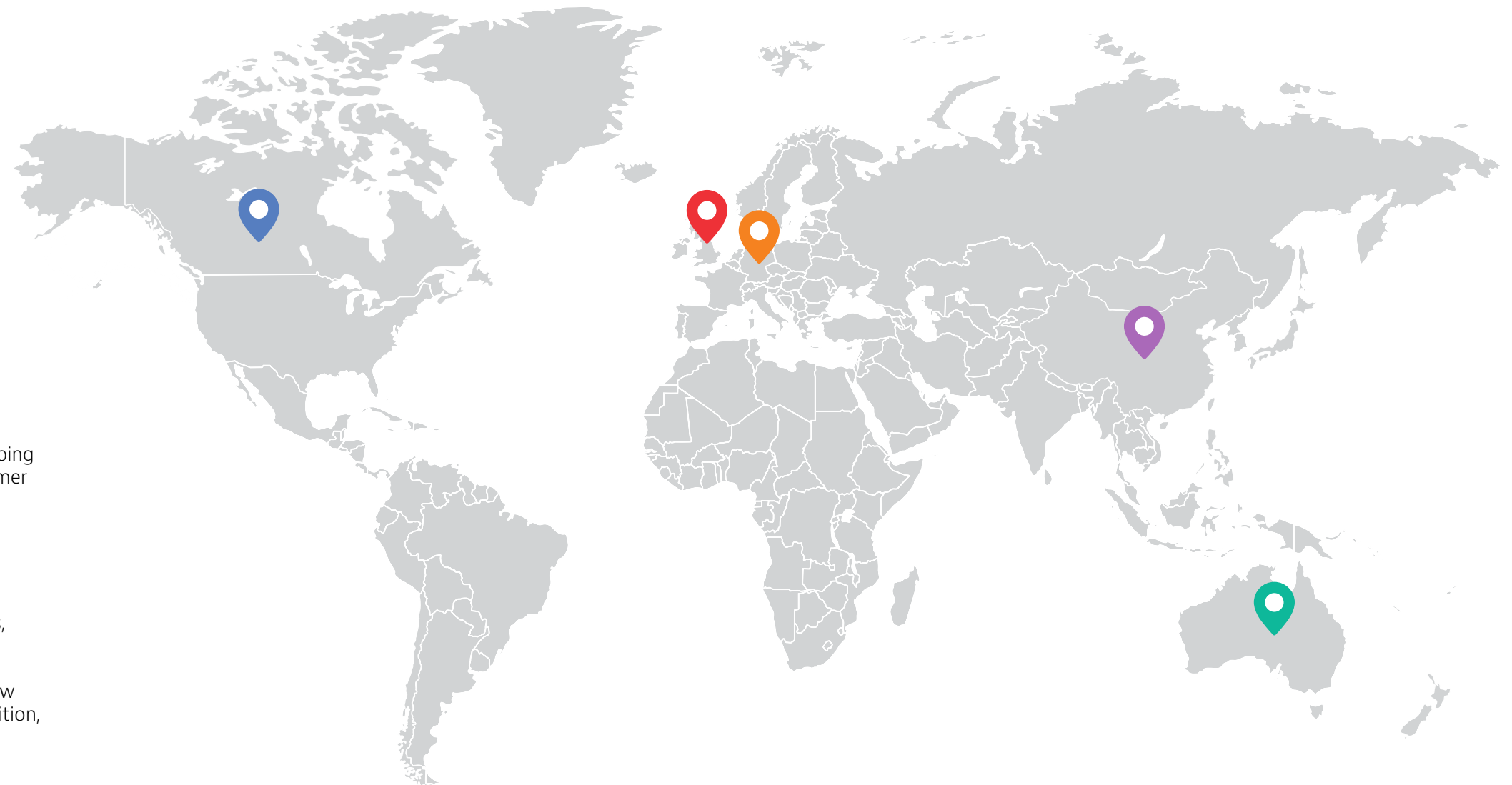
Canada

The legal system allows for class actions in a wide range of areas, with a well-established plaintiff bar and contingency fee and third-party funding arrangements making it easier for claimants to pursue collective redress. Recent developments in Canadian law have expanded the scope of class actions, particularly in competition, privacy and consumer protection cases.



China

While there is no formal class action mechanism, alternative systems such as joint litigation, representative litigation, and public interest litigation have been developed to address group disputes effectively. Public interest litigation in particular has increased in recent years, driven by government encouragement to address issues such as environmental pollution and product safety.

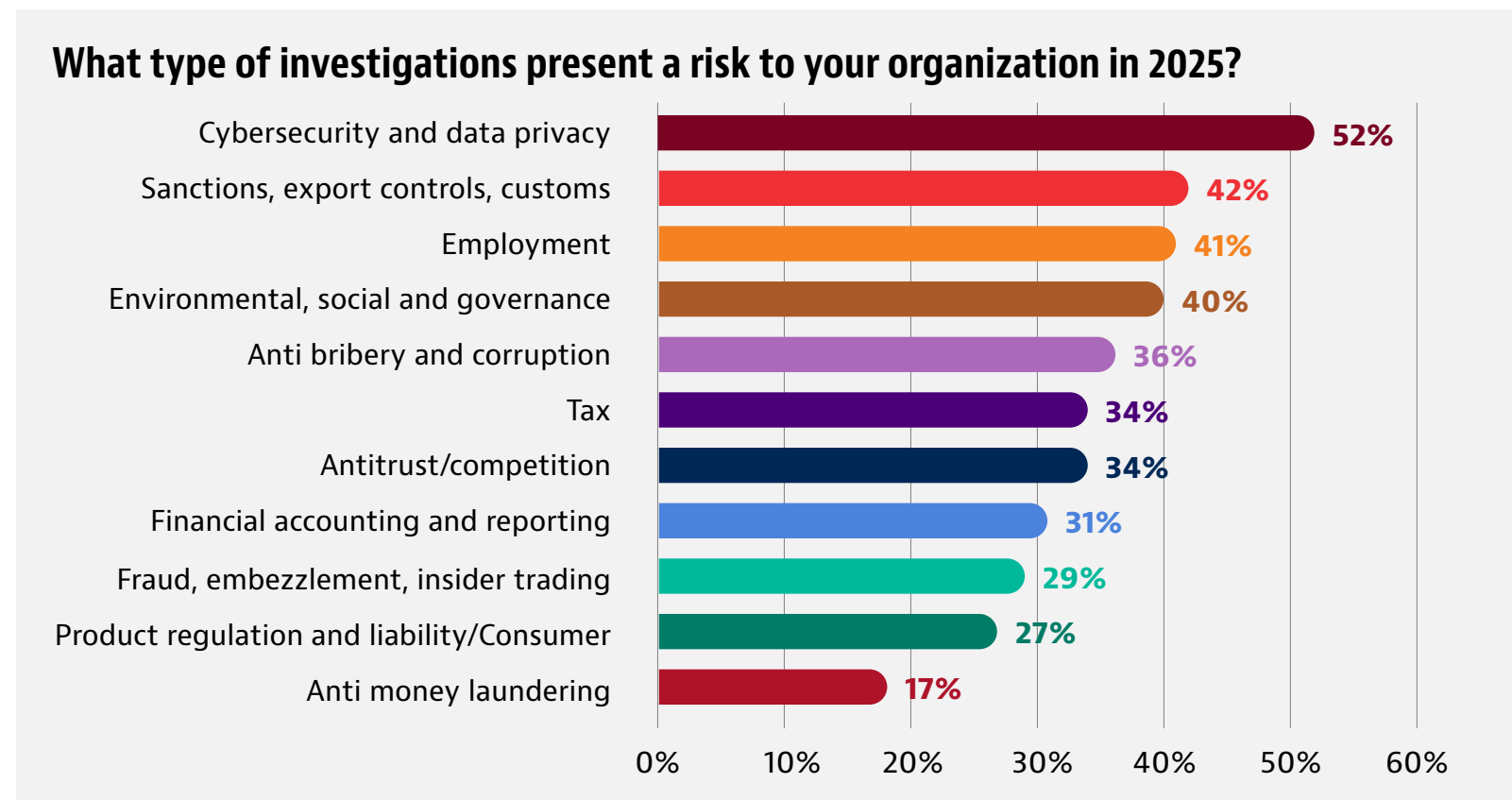


What other countries are on the radar for class action concerns? Contact us [here](#).



The Wider Picture

External factors driving investigations risk



The proliferation of data breaches and new data privacy laws around the world have contributed to cybersecurity and data privacy topping the list for investigation risks in 2025. The rise of remote work and digital technologies has expanded the attack surface, making data security more challenging.

Nic Behr, partner, Munich, says that this trend "reflects the rising complexity of global data protection regulations and the heightened threat landscape driven by cyberattacks and ransomware. Additionally, businesses are increasingly aware of the potential legal and reputational consequences of data breaches and privacy violations. Cybersecurity incidents can disrupt businesses, especially if the attackers manage to block access to their systems or steal customer or other sensitive data."

Trade winds and geopolitical concerns have brought sanctions and export controls front of mind for organizations, which must comply with legislation such as the US Export Administration Regulations and the International Traffic in Arms Regulations. "The type of sanctions and export control investigations has partly changed. Over the past years, sanctions and export control investigations focused on business activities that were not stopped in time when sanctions came into force. Recently, investigations often deal with alleged circumventions of sanctions or export control regulations," says Behr.



Widge Devaney, partner, New York, explains, "The rigor of sanctions enforcement has increased throughout the world, particularly in the US. The Department of Justice (DOJ) has hired over 20 additional prosecutors focused on criminal sanctions enforcement; it created a new position of corporate enforcement director; the deputy attorney general has called sanctions 'the new FCPA'; and BIS, OFAC and DOJ (the three main enforcement agencies) are coordinating more meaningfully than they have before. And we see more rigorous enforcement in the UK and the EU. At the same time, many companies need to consider countersanctions from China and Russia."

Meanwhile, ESG investigations have slipped down the list of concerns this year (after taking the second spot in 2024), becoming the fourth most prevalent concern for respondents in 2025. Nevertheless, ESG remains important due to the continued focus on sustainability and corporate responsibility, with regulations like the EU's Corporate Sustainability Reporting Directive (CSRD) and the Task Force on Climate-Related Financial Disclosures driving compliance efforts.

"In many countries, the ESG enforcement focus has been on human rights and environmental violations. These two sub-risk areas are more specific and manageable than the much broader ESG scope. Moreover, companies are becoming more adept at managing their ESG risks and obligations. Over the past year, many organizations have invested heavily in ESG frameworks, reporting mechanisms and compliance measures, which could explain this increased confidence in avoiding investigations," says Behr.

In our survey, around a quarter (24%) of respondents see rising environmental regulation as an external threat to their organization, while 40% believe ESG investigations more broadly present a risk.

Says Devaney: "ESG may have lost a bit of luster, but the risks remain at the governmental, civil and reputational levels. Enforcement has increased, as have 'greenwashing' and other ESG civil lawsuits."

Anti-bribery and corruption investigations are placed a little higher in priority than last year, perhaps reflecting uncertainty over new governmental objectives following elections in many major economies.

Finally, tax investigations are driven by complex regulations and global business operations, with a focus on transfer pricing and the OECD's Base Erosion and Profit Shifting (BEPS) framework.





Contacts

EUROPE, THE MIDDLE EAST AND AFRICA



Steve Abraham
Partner, London



Andy Moody
Partner, London



Francesca Richmond
Partner, London



Katia Boneva-Desmicht
Partner, Paris



Łukasz Hejmej
Partner, Warsaw



Markus Altenkirch
Counsel, London



Maria Antonia Azpeitia
Partner, Madrid



Michelle Porter-Wright
Partner, Johannesburg



Nic Behr
Partner, Munich



Vinod Bange
Partner, London



Yindi Gesinde
Partner, London

NORTH AMERICA



William Devaney
Partner, New York



Peter Tomczak
Partner, Chicago



David Gadsden
Partner, Toronto



Kelsey Machado
Partner, Houston



Justine Phillips
Partner, Los Angeles



Michael Brewer
Partner, San Francisco



Nancy Sims
Partner, Los Angeles



Perrie Weiner
Partner, Los Angeles

ASIA PACIFIC



Nandakumar Ponniya
Principal, Singapore



Celeste Ang
Principal, Singapore



Isabella Liu
Partner, Hong Kong



Richard Allen
Local Principal,
Singapore

LATIN AMERICA

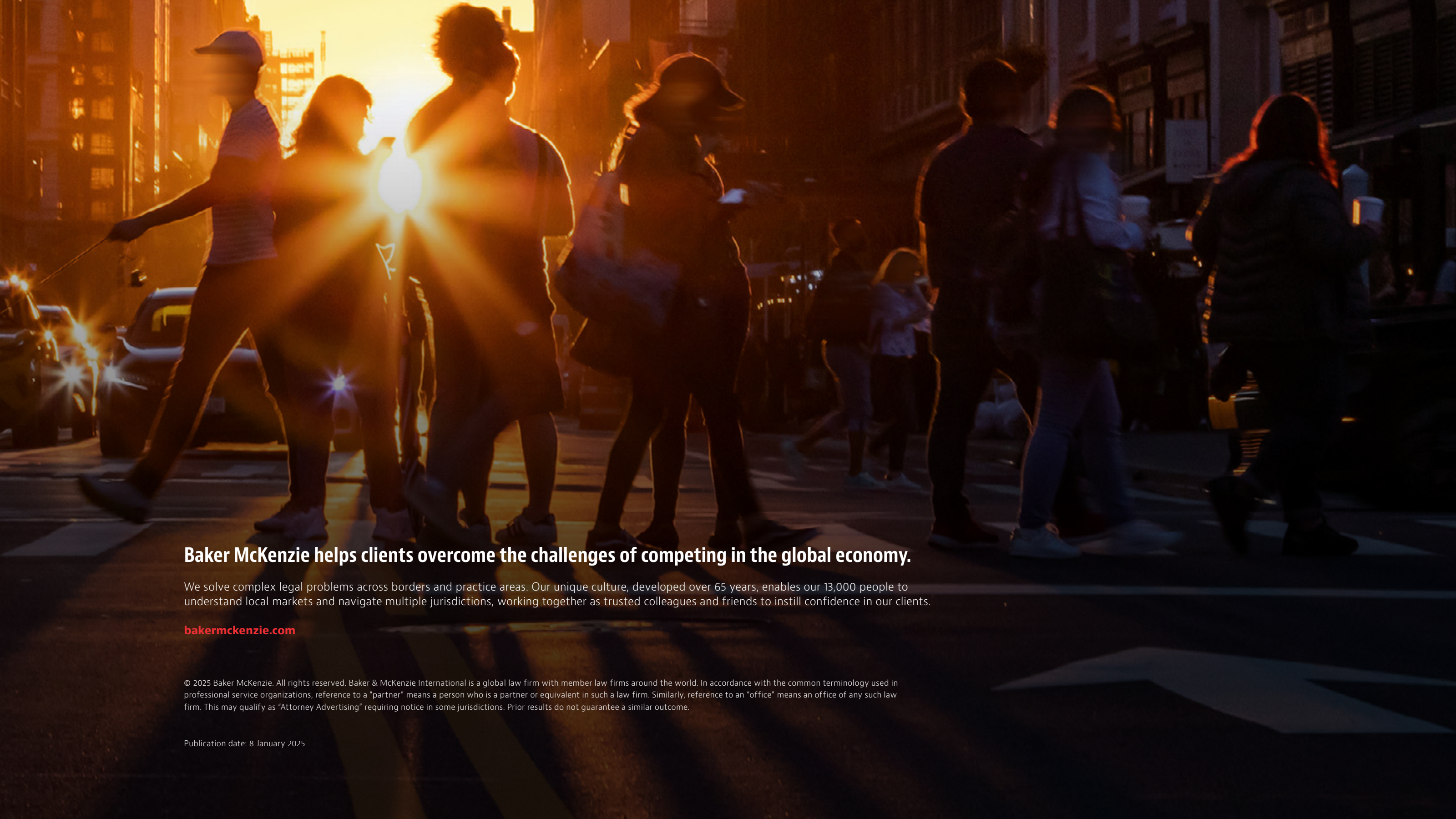


Luis Dates
Partner, Buenos Aires



Jorge Narváez-Hasfura
Partner, Mexico City

Contact us [here](#).



Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

bakermckenzie.com

© 2025 Baker McKenzie. All rights reserved. Baker & McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Publication date: 8 January 2025