

Spring 2026

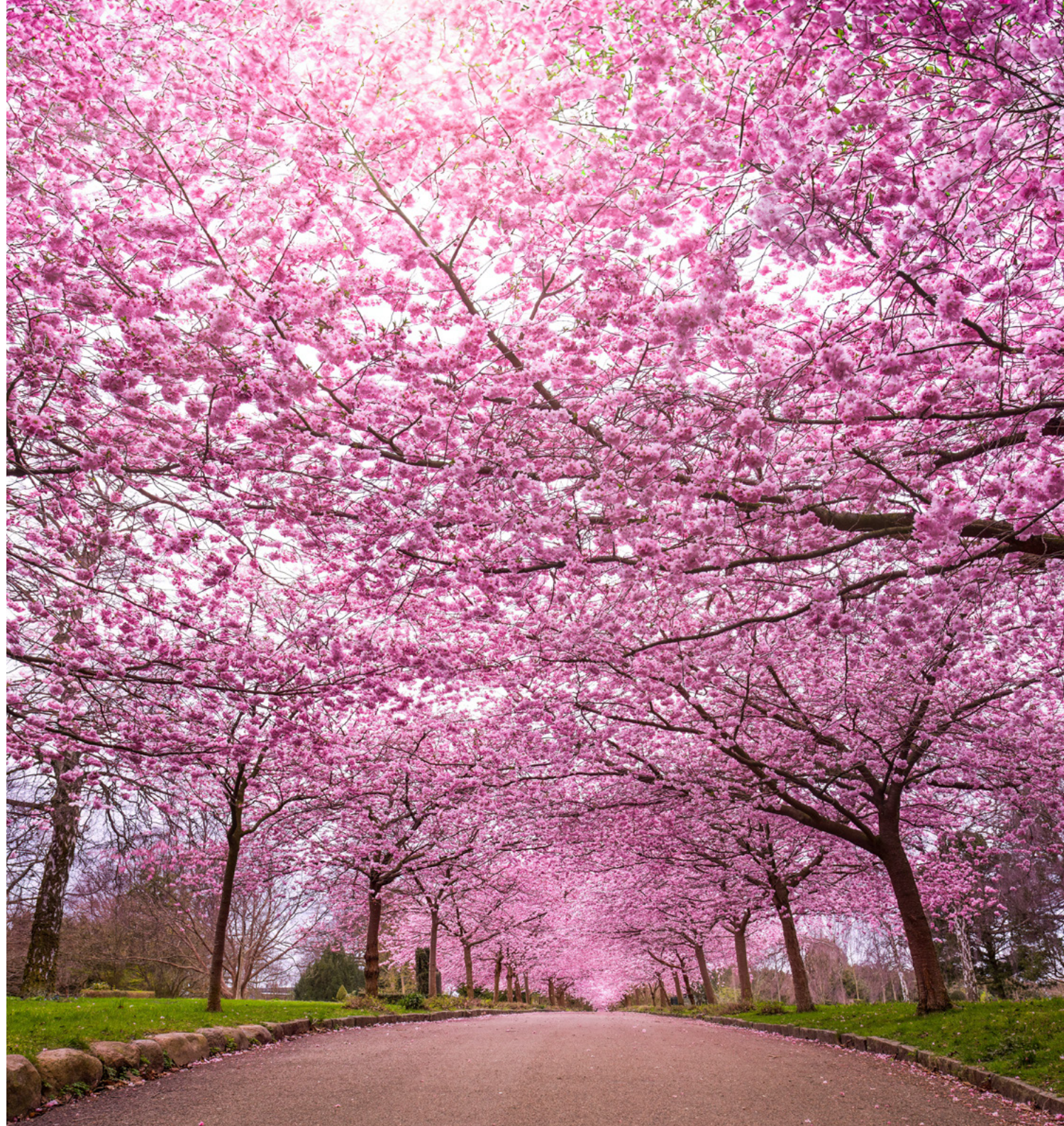


Covernotes

Explaining issues that
affect insurance

In this issue

- The autonomous vehicle revolution: Are your fleets ready for 2026?
- From bananas to business: Why marine cargo insurance matters more than you think
- Cybercrime: The silent threat to UK SMEs — and how to fight back
- Heading to the World Cup? Why standard travel cover might not be enough



The autonomous vehicle revolution: Are your fleets ready for 2026?



The UK is standing on the brink of a transport revolution. By 2026, fully autonomous vehicles (AVs) will begin appearing on British roads, following the landmark Automated Vehicles Act 2024.¹ This legislation sets out a clear framework for safety, liability and operational standards, positioning the UK as a global leader in self-driving technology.

The fundamental question for businesses — particularly those managing fleets, logistics and commercial transport — is how insurance will adapt to this new reality.

What are autonomous vehicles?

Autonomous vehicles use advanced sensors, cameras, radar and AI systems to navigate without human input. The UK industry follows the SAE scale of automation, from level zero (no automation) to level five (full automation). The UK rollout will initially focus on level four vehicles, which can operate without a driver in defined conditions.

Why 2026 is a pivotal year

The UK government has significantly accelerated trials. Commercial pilots of self-driving taxis and buses are now scheduled for spring 2026. These new services will operate via app-based booking systems, similar to existing ride-hailing platforms before a potential wider rollout when the full Automated Vehicles Act becomes law from the second half of 2027.²

The adoption of AVs is projected to have a major economic and safety impact:

- **Economic projection:** The industry is projected to be worth £42 billion by 2035²
- **Job creation:** This sector is expected to create 38,000 new jobs²
- **Safety promise:** The technology is expected to reduce road collisions caused by human error, which is currently responsible for 88% of all accidents²

1. <https://www.legislation.gov.uk/ukpga/2024/10/contents>

2. <https://www.gov.uk/government/news/driving-innovation-38000-jobs-on-the-horizon-as-pilots-of-self-driving-vehicles-fast-tracked>

Opportunities and challenges for businesses

Autonomous vehicles bring efficiency, cost savings and sustainability benefits through optimised routing and reduced downtime. However, challenges remain — public trust, infrastructure readiness and cybersecurity risks will all need attention.

Insurance implications: The liability shift

The biggest change for insurers is the move from driver liability to product liability. Under the Automated and Electric Vehicles Act 2018,³ insurers will compensate victims first⁴ and then recover costs from manufacturers if a system failure caused the accident.⁵ Policies are available to cover risks such as motor liability, cyber threats and trial interruptions.⁶

Preparing your business

For UK businesses, the time to plan is now, as the driverless future is arriving in 2026. Preparation involves three critical steps:

- 1. Review fleet strategy:** Assess how and when AVs will integrate into your existing operations
- 2. Update risk management:** Implement new protocols for technology-based risks
- 3. Engage your broker:** Contact us about your plans so that your commercial insurance policies can be reviewed and necessary covers put in place to cover the risks faced

Autonomous vehicles hold the promise of safer roads, greener transportation and greater operational efficiency — but they also bring new risks and responsibilities that must be carefully managed. To ensure you're prepared, get in touch with us today to discuss how we can support you.



3. <https://www.legislation.gov.uk/ukpga/2018/18/contents>

4. [https://www.legislation.gov.uk/ukpga/2018/18/contents/text=2-Liability%20of%20insurers%20etc%20where%20accident%20caused%20by%20automated%20vehicle,-\(1\)](https://www.legislation.gov.uk/ukpga/2018/18/contents/text=2-Liability%20of%20insurers%20etc%20where%20accident%20caused%20by%20automated%20vehicle,-(1))

5. https://www.legislation.gov.uk/ukpga/2018/18/pdfs/ukpgaen_20180018_en.pdf (page 5)

6. <https://axaxl.com/press-releases/axa-xl-launches-single-customisable-policy-for-autonomous-vehicles>



Picture this: a shipment of bananas — perfectly packed, temperature-controlled — leaves Central America bound for the UK. It's a routine journey, but global supply chains can be fragile. If the vessel hits severe weather, containers shift or refrigeration fails, the cargo spoils. Suddenly, the crucial question becomes: who pays for the loss?

This is why marine cargo insurance isn't a luxury — it's an essential safeguard for any business moving goods internationally.

The risks in transit

Every international shipment exposes a business to potential financial loss. The journey from origin to destination is fraught with risk events such as physical damage from mishandling, opportunistic theft during transit or storage, delays caused by strikes or port closures and deterioration — especially for temperature-sensitive goods like fresh produce.

The sheer volume of international trade highlights this exposure. According to the Office for National Statistics (ONS),¹ the UK imports hundreds of billions of pounds worth of goods annually, meaning every shipment represents a potential financial risk.

What marine cargo insurance covers

Marine cargo insurance exists to protect the financial value of goods from the moment they leave the seller until they reach the buyer. The broadest form of protection is all risks cover, which safeguards against physical loss or damage. Policies are typically structured using the Institute Cargo Clauses (A: provides the widest "all risks" cover, B: offers a more limited set of named perils such as fire, explosion and loss overboard and C: clause C provides the most restricted cover, applying only to major incidents like collision, fire or vessel capsizing).²

Additional extensions can be added, such as war and strikes, which protects against losses from conflict or civil commotion and delay, which addresses unforeseen disruptions in transit.

For SMEs, insurers offer tailored solutions like Stock Throughput Policies, covering goods from raw material stage through processing, storage and final transit.

Specialised cover for temperature-controlled cargo is also vital for perishable goods — just like those bananas.

Every shipment is a link in your supply chain — and if that link breaks, the impact can ripple across your entire business. Marine cargo insurance is not just about replacing goods; it's about business continuity. A single uninsured loss can halt production, delay customer deliveries and damage your reputation. Having the right cover ensures your operations keep moving, even when the unexpected happens.

The simple banana shipment illustrates a complex truth: every movement of goods is a risk event waiting to happen. Marine cargo insurance is critical for business continuity and financial stability. Without it, a single incident could disrupt operations and damage your bottom line.

Ready to protect your goods and your bottom line?

Don't leave your shipments to chance. Marine cargo insurance can be tailored to your business — whether you move goods occasionally or every day. Speak to an independent insurance broker today for advice and options that keep your supply chain secure.

1. <https://www.ons.gov.uk/businessindustryandtrade/internationaltrade/bulletins/internationaltradeinuknationsregionsandcities/2023>

2. <https://www.wtwco.com/en-gb/solutions/services/shipping-and-maritime-industries>

Cybercrime: The silent threat to UK SMEs — and how to fight back

Cybercrime is a pervasive and growing threat that affects businesses of all sizes. UK Government data shows that 43% of businesses¹ faced a cyber breach last year, demonstrating that small and medium-sized enterprises (SMEs) are not too small to be targets. Ransomware pressure is also rising, placing boards on notice.

The state of UK cyber risk

Prevalence and attack vectors

- **Reported breaches:** 43% of businesses reported a cyber breach or attack in the last year
- **Phishing dominance:** Among those businesses hit, 85% cite phishing as the primary cause. Phishing remains the number one route in for attackers²
- **Ransomware:** Ransomware attempts increased, equating to roughly 19,000 companies³

Five technical controls that reduce risk

The good news is that a handful of controls can reduce cyber risk. Implementing these controls can help turn cyber from a critical business risk into a manageable risk, which Insurers will expect you to have in place. These five essential controls are:⁴

1. **Multi-factor authentication (MFA)**
2. **Patching** (ensuring a regular patching cadence)
3. **Tested backups** (including secure backups)
4. **Endpoint detection and response** (EDR)/email and endpoint protection
5. **Access hygiene** (e.g., implementing least privilege)



1. [https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025#:~:text=breaches%20and%20attacks-,Just%20over%20four%20in%20ten%20businesses%20\(43%25\),-and%20three%20in](https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025#:~:text=breaches%20and%20attacks-,Just%20over%20four%20in%20ten%20businesses%20(43%25),-and%20three%20in)
2. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025#:~:text=Phishing%20attacks%20remained,breach%20of%20attack>
3. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025#:~:text=increased%20between%202024%20and%202025-,The%20estimated%20percentage%20of%20all%20businesses%20who%20experienced%20a%20ransomware%20crime%20in%20the%20last%2012%20months%20increased%20from%20less%20than%200.5%25%20in%202024%20to%201%25%20in%202025%2C%20which%20equates%20to%20an%20estimated%2019%20C000%20businesses%20in%202025,-Phishing%20cyber%20crime%20remained%20by>
4. <https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf>

The role of cyber insurance

Cyber insurance is essential for fighting back against modern threats. It provides a comprehensive safety net that extends beyond mere financial reimbursement.

Key coverages can include:

- **Incident response:** Provides 24/7 access to experts, including forensic investigators and legal counsel
- **Business interruption:** Covers lost revenue due to a covered cyber event
- **Liability cover:** Protects the business from claims arising from a breach, such as regulatory fines or third-party lawsuits
- **Crime protection:** Covers financial losses from crime events like funds transfer fraud

Conclusion: a manageable risk

The path to turning cyber risk into manageable risk involves three clear steps:

Step one:

Foundation: Start with the five core controls: Multi-Factor Authentication (MFA), regular patching, secure backups, Endpoint Detection and Response (EDR) and least privilege access.

Step two:

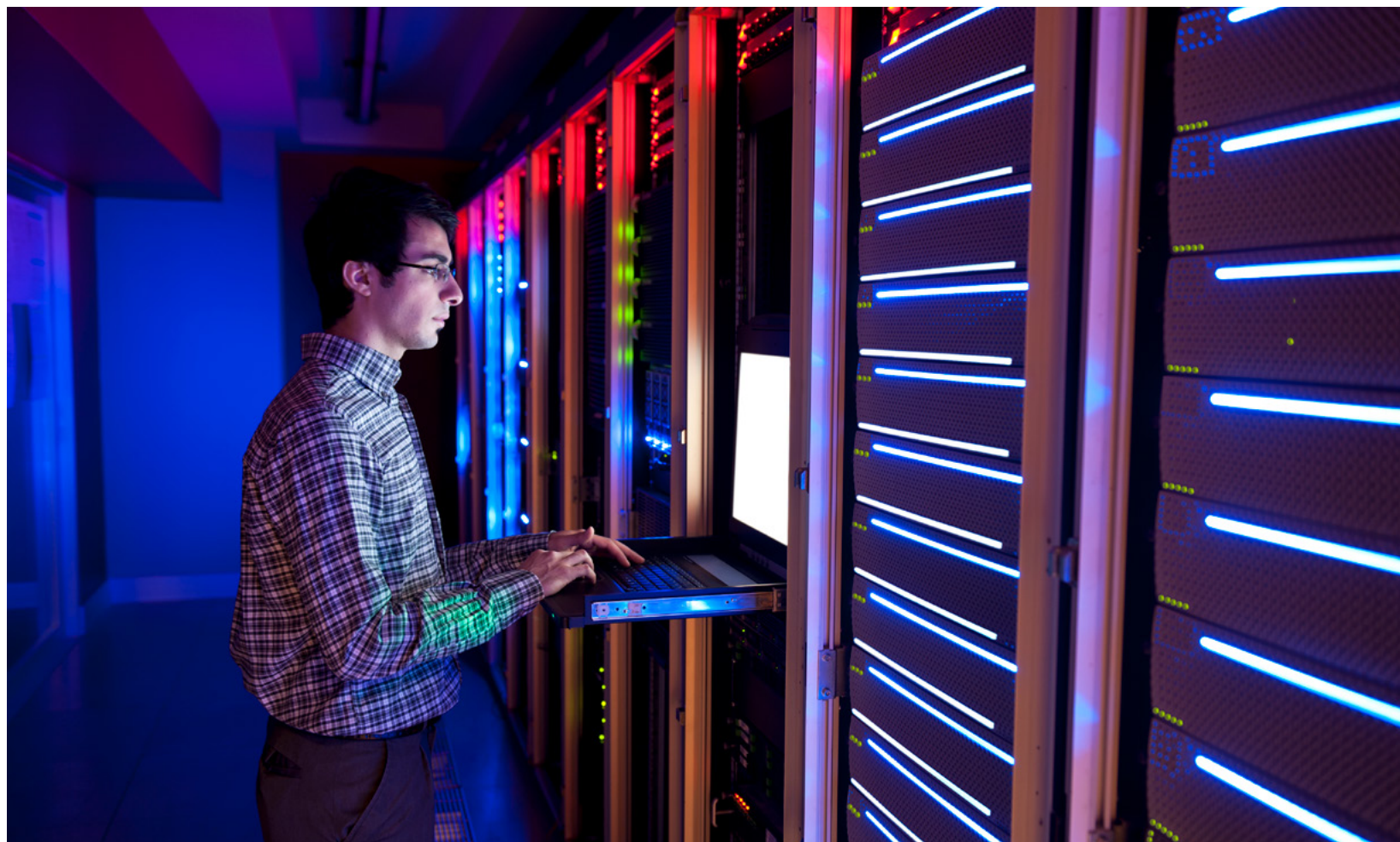
Validation: Prove these controls are in place by achieving certification such as cyber essentials, which demonstrates your commitment to security.

Step three:

Protection: Ensure your cyber insurance coverage aligns with your security controls, so you have financial and expert support when an incident occurs.

By combining strong cyber hygiene, certification and tailored insurance, SMEs can significantly reduce exposure and recover quickly if the worst happens.

Don't wait until it's too late — speak to your independent insurance broker today to review your cyber risk strategy and arrange comprehensive cyber insurance cover that safeguards your business.



Employers also have a legal duty of care to protect employees travelling for work, as outlined in ISO 31030:2021 Travel Risk Management guidelines.¹

Common gaps in standard travel insurance policies

While standard travel insurance covers basics like medical emergencies and trip cancellations, it often excludes critical protections needed for major events, such as:

- **Event cancellation or postponement:** If the World Cup match or conference is cancelled due to political unrest or health concerns, standard cover rarely reimburses associated costs
- **Extended accommodation and travel costs:** Employees stranded by transport strikes or security lockdowns may face significant out-of-pocket expenses
- **Security and emergency evacuation:** Crisis management and evacuation services are typically not included in basic policies
- **High-value equipment and cyber risks:** Employees often carry laptops and sensitive data. Standard policies usually exclude cyber incidents or specialist equipment loss
- **Enhanced medical and repatriation cover:** In countries with limited healthcare infrastructure, standard cover may not provide sufficient support

Heading to the World Cup? Why standard travel cover might not be enough

Sending employees to global sporting events such as the FIFA World Cup or other major event, can be an exciting opportunity for your business — but it also comes with unique risks. Many companies assume their standard corporate travel insurance will provide adequate protection. Unfortunately, that's often not the case.

In this article, we'll explore why standard travel cover falls short, the common gaps in policies and the key exposures businesses face when sending staff to major events. Plus, we'll share practical steps to ensure your organisation is properly protected.

Why major events increase travel risk

Large-scale events attract millions of visitors, creating an environment where risks multiply.

Here are some of the biggest challenges:

- **Heightened security threats:** Terrorism, civil unrest and political demonstrations are more likely during global events
- **Transport disruption:** Strikes, traffic congestion and last-minute cancellations can leave employees stranded
- **Accommodation shortages:** Hotels fill up quickly and prices surge — making last-minute changes costly
- **Cybercrime and theft:** High-profile events are prime targets for cyberattacks and opportunistic theft

1. <https://www.wtwco.com/en-gb/insights/2024/05/iso31030-2021-travel-risk-management>

Key exposures for employers

Financial loss: Unplanned accommodation, transport and security costs can escalate quickly.

Reputational damage: Failure to meet duty of care obligations can harm your brand.

Employee well-being: Stress and safety concerns impact morale and productivity.

Government guidance stresses the importance of tailored travel insurance for overseas trips, especially for high-risk destinations and events.²

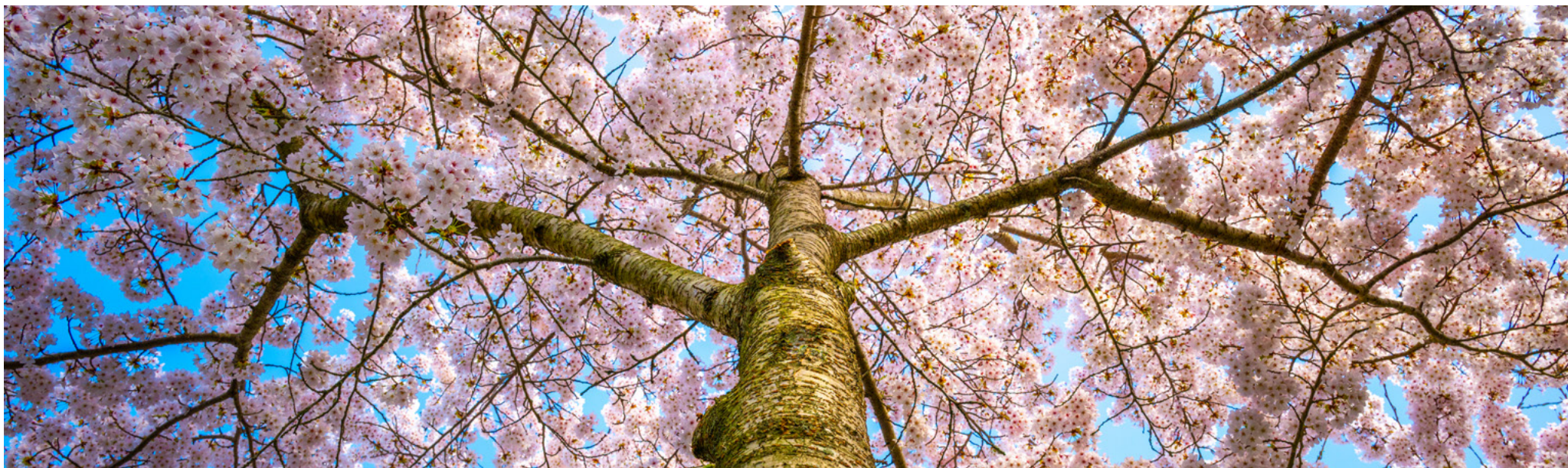
How to protect your business and employees

- 1. Review existing policies:** Check exclusions for event-related disruptions, terrorism and crisis response
- 2. Upgrade to specialist cover:** Look for policies that include political evacuation, security assistance and extended travel disruption benefits
- 3. Implement a travel risk management plan:** Align with **ISO 31030** standards to demonstrate compliance and protect employees

Don't leave your business exposed. If you're planning to send employees to the World Cup or any major event, now is the time to review your travel insurance. Speak to us today about specialist corporate travel cover that protects your people and your organisation — no matter where the game takes them.



2. <https://www.gov.uk/guidance/foreign-travel-insurance>



Tony McDonagh & Co Ltd
Avoca House, The Pavilion Business Centre, 6 Kinetic Crescent
Enfield
Middlesex
EN3 7FJ

Tel: 0199 270 3000

www.mcdonaghs.co.uk
insurance@mcdonaghs.co.uk

Authorised and regulated by the Financial Conduct Authority.

NLIG Ltd T/A North London Insurance Group
Avoca House, The Pavilion Business Centre, 6 Kinetic Crescent
Enfield
Middlesex
EN3 7FJ

Tel: 0199 270 3300

www.nlig.co.uk
insurance@nlig.co.uk



WTW offers insurance-related services through its appropriately licensed and authorised companies in each country in which WTW operates. For further authorisation and regulatory details about our WTW legal entities, operating in your country, please refer to our [WTW webpage](#). It is a regulatory requirement for us to consider our local licensing requirements.

The information given in this publication is believed to be accurate as of February 2026. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date.

This newsletter offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market and we disclaim all liability to the fullest extent permitted by law. It is not intended to be and should not be, used to replace specific advice relating to individual situations and we do not offer and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third-party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of WTW Networks. Copyright WTW 2026. All rights reserved.