Winter 2026

DAINES KAPP
insurance brokers ltd

Covernotes

Explaining issues that affect insurance

In this issue

- Cyber crime, holiday scams and AI fraud: A growing threat to business resilience
- Winter weather: Is your business ready for disruption?
- Winter driving risks: Could fleet disruption impact your business?
- Water leaks: The winter risk many businesses underestimate



Cyber crime, holiday scams and AI fraud: A growing threat to business resilience



As businesses approach the festive season, attention often turns to year-end targets, customer demand, supplier commitments and workforce planning. However, winter also brings an increase in cyber-related threats, with criminals seeking to exploit busy teams, reduced staffing levels and changes in normal business routines.

While cyber crime is not a seasonal phenomenon, the combination of increased online activity and year-end operational pressures can create opportunities for fraudsters. This challenge is becoming more significant as artificial intelligence (AI) enables criminals to create more convincing and sophisticated attacks than ever before.

For business leaders, the conversation is no longer solely about data security. Increasingly, it is about operational resilience and the potential consequences when a cyber incident disrupts day-to-day business activities.

Why the festive period can increase risk

Many organisations experience operational changes over the winter months. Employees may be working remotely, annual leave can create gaps in approval processes and finance teams are often managing high transaction volumes before year-end.

Criminals understand these pressures. UK Government research highlights that fraud is increasingly technology-enabled, with organised criminal groups continually adapting their methods and using new tools to target both individuals and businesses.[1]

Common seasonal tactics include:

- Fake supplier payment requests
- Delivery and courier impersonation scams
- Executive impersonation fraud
- Phishing emails linked to invoices or seasonal offers
- Fraudulent websites designed to capture credentials

What makes many of these attacks effective is not advanced technology, but their ability to exploit trust, urgency and routine business processes.

1. https://www.gov.uk/government/publications/national-assessment-centre-fraud-assessment-2025/national-assessment-centre-fraud-assessment-2025

How AI is changing the fraud landscape

Artificial intelligence has transformed the scale and sophistication of cyber-enabled fraud.

Criminals are increasingly using AI to create voice clones, generate convincing phishing emails, produce deepfake videos and develop synthetic identities capable of bypassing traditional verification processes.[2]

Unlike many traditional scams, AI-generated communications are often polished, persuasive and free from the spelling mistakes or obvious warning signs that employees have been trained to identify.

Social engineering attacks are becoming increasingly sophisticated, with deepfakes and automated phishing campaigns helping criminals bypass traditional defences and target businesses at scale.[3]

The result is a rapidly evolving threat environment where even experienced employees can find it difficult to distinguish genuine communications from fraudulent ones.

The business interruption impact

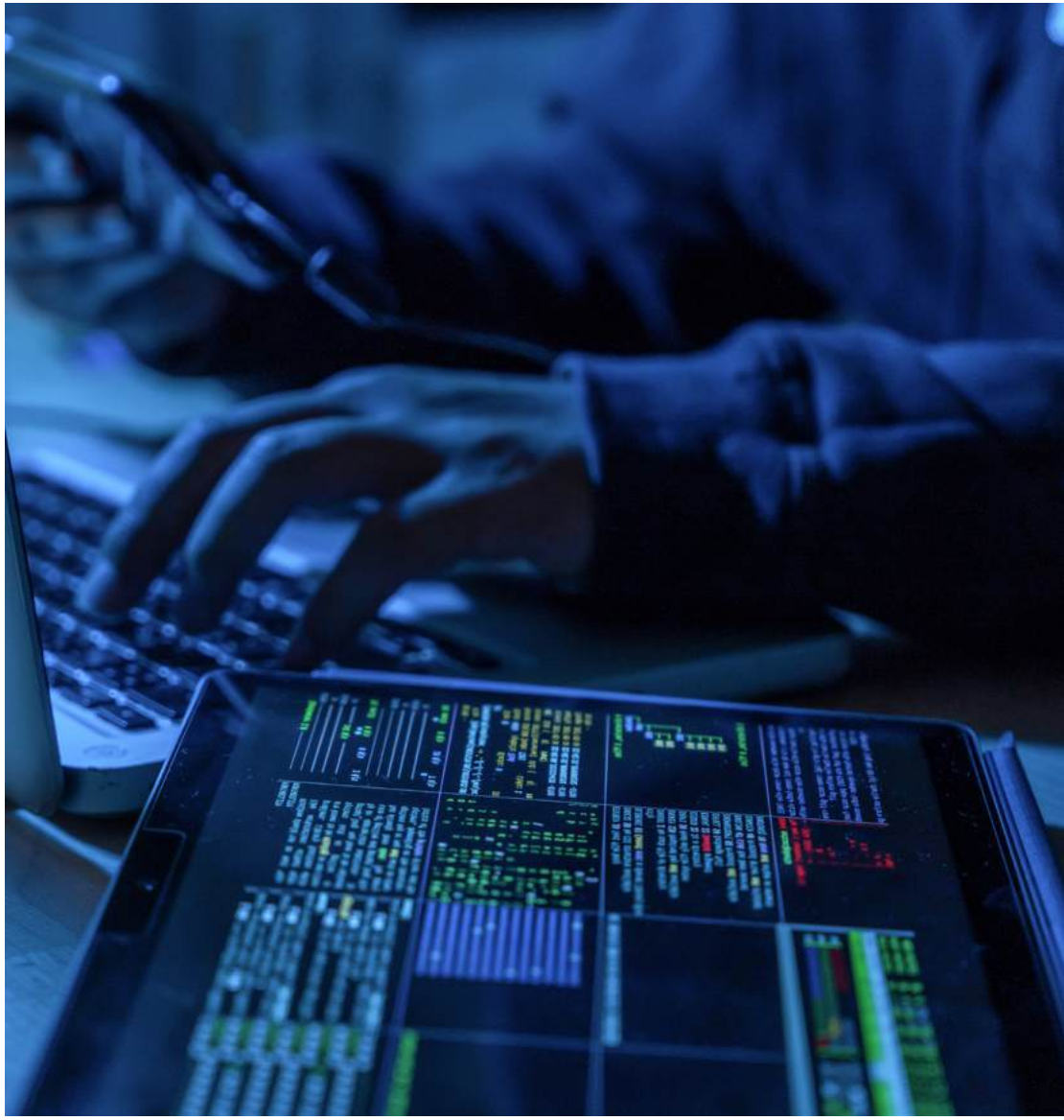
When organisations think about cyber crime, the focus often falls on stolen funds or compromised data. In reality, the operational consequences can be equally significant.

A successful cyber incident may result in:

- Temporary loss of access to critical systems
- Delays in processing customer orders
- Disruption to supplier relationships
- Reduced productivity during recovery efforts
- Reputational challenges with customers and stakeholders

For businesses operating during one of the busiest periods of the year, even short-term disruption can have wider consequences for revenue generation, customer service and strategic objectives.

This is one reason why business resilience continues to be a board-level discussion. An organisation's ability to continue operating when faced with unexpected disruption can be just as important as preventing incidents from occurring in the first place.



2. https://www.wtwco.com/en-us/insights/2026/02/ai-driven-fraud-and-corporate-crime-risks-controls-and-insurance-implications
3. https://www.wtwco.com/en-gb/insights/2025/10/how-artificial-intelligence-ai-is-shaping-the-cybersecurity-battlefield-in-2025-and-beyond



Questions business leaders may wish to consider

Rather than focusing solely on technology, organisations may benefit from reviewing the wider processes that support resilience:

- Are payment instructions independently verified?
- Would employees recognise an AI-generated scam?
- Are escalation procedures clear when staff members are absent?
- Have supplier verification processes been reviewed?
- Is cyber awareness training updated to reflect emerging threats?
- Have business continuity plans been tested recently?
- Would key operations continue if critical systems became unavailable?

These are not simply cyber-security questions. They are broader resilience considerations that can help organisations understand potential vulnerabilities before disruption occurs.

Looking ahead

Government assessments indicate that fraud against UK businesses continues to evolve, with criminals increasingly leveraging technology, social engineering techniques and AI-powered tools to improve the scale and effectiveness of their attacks.[4]

As businesses move through the winter period, maintaining awareness of these risks can help strengthen decision-making, safeguard operations and support wider resilience planning.

While no organisation can eliminate every threat, understanding how cyber crime, AI-enabled fraud and operational disruption intersect is an increasingly important part of risk management.

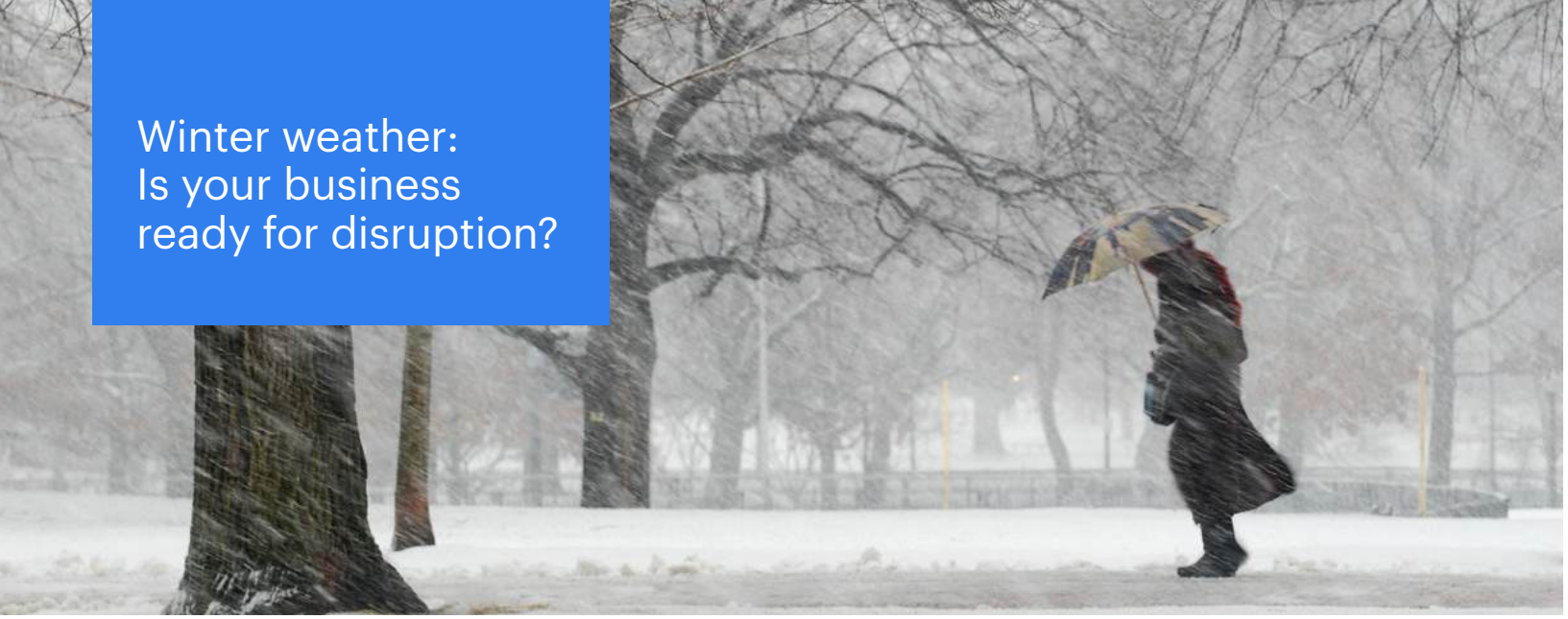
Speak to your broker

Every organisation faces different operational and cyber-related exposures. If you would like to discuss business resilience, cyber risk considerations or wider continuity planning, speak to your insurance broker, who can help you explore issues relevant to your business and circumstances.

Note: This article is intended as thought leadership and general information only. It does not constitute insurance, legal or risk management advice and should not be relied upon as such.

4. https://www.gov.uk/government/publications/fraud-strategy-2026-to-2029

Winter weather: Is your business ready for disruption?



Winter can bring more than difficult commuting conditions. Severe weather, flooding, power outages and supply chain disruption can all affect a business's ability to operate, sometimes long after the immediate event has passed.

Recent UK resilience and climate assessments highlight the growing importance of preparing for operational disruption, particularly as businesses become increasingly dependent on interconnected infrastructure, technology and suppliers.[1]

For many organisations, the biggest challenge is not physical damage to premises but loss of a service they rely on. Power, telecommunications, cloud services, transport networks and key suppliers all play a critical role in day-to-day operations. When one link in the chain fails, the impact can quickly spread.[2]

A temporary loss of power, inaccessible premises or disruption to a key supplier may not sound significant, but even short interruptions can affect customer service, revenue, contractual obligations and business reputation.

The question for business leaders is simple: how long could your organisation continue operating if a critical dependency became unavailable?

Severe weather can affect both business premises and the utility networks they depend on, potentially extending downtime and increasing business interruption losses.[3]

As winter approaches, organisations may wish to consider:

- Which activities are most critical to the business?
- What services and suppliers do those activities depend upon?
- Are continuity plans still fit for purpose?
- How quickly could alternative arrangements be implemented?
- Have recovery assumptions been tested recently?

While no organisation can eliminate every source of disruption, understanding operational dependencies and recovery requirements can help reduce the impact when issues arise.

Winter provides a useful opportunity to review resilience planning and ensure the business is prepared for the unexpected.

Speak to your broker

Every business faces different interruption risks. If you would like to discuss resilience planning, operational dependencies or wider risk considerations, speak to your broker for guidance tailored to your organisation's circumstances.

Note: This article is provided for general information only and does not constitute insurance, legal or risk management advice. Readers should seek guidance based on their individual circumstances.

1. https://www.gov.uk/government/publications/uk-government-resilience-action-plan/uk-government-resilience-action-plan-html
2. https://www.wtwco.com/en-cm/insights/2025/09/making-insurance-work-for-operational-resilience
3. https://www.wtwco.com/en-gb/insights/2026/07/how-to-manage-natural-hazards-and-climate-risks-to-your-operations-and-the-utilities-they-depend-on

Winter driving risks: Could fleet disruption impact your business?

For many businesses, winter brings a familiar set of challenges. Ice, heavy rain, fog and shorter daylight hours can all increase the risks associated with driving for work. Yet the greatest impact is often not the incident itself, but the disruption that follows.[1]

Whether managing a fleet of vans, HGVs or company cars, organisations depend on vehicles to support customer service, deliveries, site visits and day-to-day operations. When vehicles are unavailable, routes are delayed or drivers are unable to travel safely, the knock-on effects can quickly extend across the business.

The Health and Safety Executive note that driving for work is one of the most significant risks many employees face, with factors such as weather conditions, fatigue, vehicle condition and journey planning all requiring careful consideration.[2]

Winter can also expose wider operational vulnerabilities. A single vehicle incident, fuel supply issue or transport disruption may affect customer commitments, project timelines and workforce productivity. This highlights the importance of understanding fleet dependencies and building resilience into operational planning before disruption occurs.[3]

Business leaders may wish to consider:

- How dependent are critical operations on vehicle availability?
- Are winter driving risks reflected in journey planning processes?
- Do drivers receive seasonal safety guidance and support?
- Could alternative transport arrangements be implemented if disruption occurs?
- Are fleet risks reviewed as part of wider business continuity planning?



Recent government resilience assessments continue to emphasise the importance of preparedness and adaptability in the face of increasingly complex and interconnected risks.

For organisations that rely on vehicles to serve customers, transport goods or support field-based employees, winter can provide a timely opportunity to review fleet resilience arrangements and reduce the potential impact of disruption.

Speak to your broker

If you would like to discuss fleet-related risks, operational resilience or broader business continuity considerations, speak to your broker for guidance tailored to your organisation's circumstances.

Note: This article is provided for general information and thought-leadership purposes only. It does not constitute insurance, legal, health and safety or risk management advice and should not be relied upon as such.

1. https://www.hse.gov.uk/roadsafety/employer/plan-manage-journeys.htm
2. https://www.hse.gov.uk/roadsafety/employer/index.htm
3. https://www.wtwco.com/en-gb/insights/2026/05/building-fleet-resilience-practical-steps-to-protect-against-fuel-disruption



Water leaks: The winter risk many businesses underestimate

When business leaders think about winter risks, attention often turns to severe weather, travel disruption and cyber threats. Yet one of the most common causes of business disruption can start with something far less dramatic: a water leak.

Freezing temperatures, burst pipes, heating failures and periods of low building occupancy can all increase the likelihood of water-related incidents during the winter months. While often viewed as a maintenance issue, the impact can extend far beyond the initial damage.

Water damage can affect premises, stock, equipment and technology, potentially disrupting operations at a time when organisations are already managing year-end deadlines and reduced staffing levels. In some cases, the interruption caused by recovery and remediation activities may create a greater challenge than the original incident.

Periods of closure over Christmas and New Year can add to the risk. Buildings operating with fewer employees or left unoccupied for several days, may be more vulnerable to issues going unnoticed until significant damage has already occurred.

For business leaders, the key consideration is not simply whether a leak could occur, but what effect it might have on business continuity.

As winter approaches, organisations may wish to consider:

- How dependent are critical operations on a single site?
- Could water damage affect customer service, productivity or trading activities?
- Are building maintenance and inspection arrangements up to date?
- Would a problem be identified quickly during periods of reduced occupancy?
- Have recovery and continuity plans been reviewed recently?

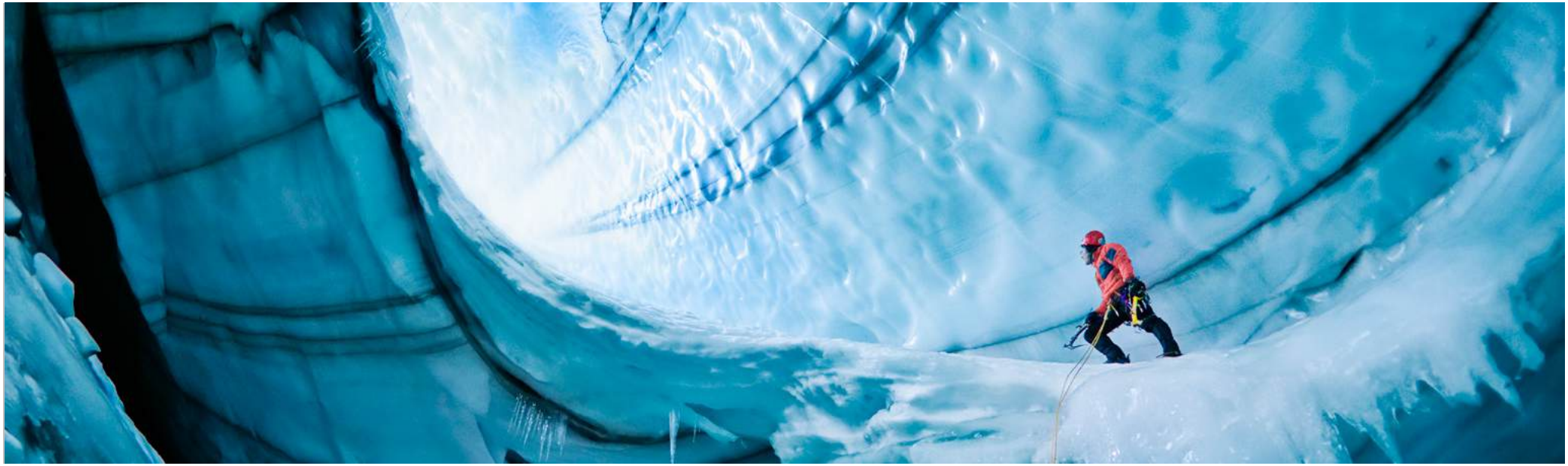
The most resilient organisations recognise that relatively minor incidents can sometimes create disproportionate operational consequences. Understanding key dependencies and recovery priorities can help reduce the impact when unexpected disruption occurs.

Winter provides a timely opportunity to review resilience planning and challenge assumptions about what could interrupt normal business operations.

Speak to your broker

Every organisation faces different operational and property-related risks. If you would like to discuss business continuity, resilience planning or wider risk management considerations, speak to your broker for guidance tailored to your organisation's circumstances.

Note: This article is provided for general information and thought-leadership purposes only. It does not constitute insurance, legal or risk management advice and should not be relied upon as such.



Daines Kapp Insurance Brokers Ltd
Daines Kapp House, 4 Baldock Street
Ware
Herts
SG12 9DZ

Tel: 0192 048 4844

www.daineskapp.co.uk
info@daineskapp.co.uk

Authorised and regulated by the Financial Conduct Authority.

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 November 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 disclaimer 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 Willis Networks. Copyright WTW 2026. All rights reserved.

FPS14940253 WTW-4592420210-11-2026