Summer 2026

tmd insurance group

nlig insurance group

Covernotes

Explaining issues that affect insurance

In this issue

Business Interruption: Why it's worth a fresh look

Business Interruption (BI) insurance cover is often misunderstood. While many assume it covers any form of disruption, policies generally follow insured property risk losses, with some additional coverages for non-damage interruptions. There is therefore a requirement for the property loss to be insured.

Property damage insurance for items such as buildings, plant and machinery and stock indemnify for loss of or damage to physical assets whereas BI helps to compensate for impacts on the profitability of the business through the recovery period.

What BI actually covers

There are a variety of BI covers available, for Revenue, Gross Profit (both of which would normally include increased cost of working cover) and Additional Increased Cost of Working, with actual coverage available depending on the specific policy wording.

Assuming the appropriate cover has been chosen, the underlying aim of the cover is to compensate for lost net profit when you can't trade normally due to an insured event.

In addition to the basic cover, many policies give the option of extensions to cover impacts on the business from causes outside of the insured premises. Typically, these could include damage at suppliers' premises or customers' premises, loss of utilities, denial or restriction of access and impact of diseases.

Why revisit BI now? Three practical reasons:

1. **Fragile supply chains**: A single supplier issue can halt operations.[1]
2. **Tighter cashflow**: Disruption bites harder when payments are delayed and margins are tight.[2]
3. **Policy clarity matters**: BI claims rely on exact policy wording and strong evidence.

Everyday causes of BI

Not all BI claims come from major disasters. Small incidents can still close your premises long enough to impact trading, especially if you can't switch to a back-up plan quickly.

If a small incident occurs at a critical time for the business, particularly where there is a highly seasonal trade, then the profit impact can be much greater than the physical one. Similarly, if there is a process flow in a business and the first part of the process is damaged, then the entire business can be brought to a halt.

How BI links to continuity planning

Choosing the appropriate BI cover in terms of the type and length of indemnity period works best when aligned with a clear business continuity plan, following a detailed business impact analysis. GOV.UK templates help map critical functions, recovery times, suppliers and emergency contacts.[3]

1. https://www.gov.uk/government/publications/uk-critical-imports-and-supply-chains-strategy
2. https://www.gov.uk/government/news/time-to-pay-up-toughest-crackdown-on-late-payments-in-a-generation-unveiled-in-plan-to-back-small-businesses
3. https://assets.publishing.service.gov.uk/media/5f6337fdd3bf7f723c19cb71/Business_continuity_plan_template_and_checklist.docx

Common BI issues for SMEs

- **Indemnity period too short**: It should cover the full recovery time, not just reopening
- **Misunderstood gross profit**: Insurance definitions differ from accounting definitions
- **Incorrect turnover/profit declarations**: These can reduce claim payments
- **Single points of failure**: One supplier, utility or site can create disproportionate risk
- **Poor records**: Claim processes often require detailed evidence of accounting data, trends and extra costs

Why BI matters in today's economy

With rising insolvencies, late payments and more frequent disruptions (including extreme weather events), even short interruptions can quickly become cashflow problems. BI is increasingly central to resilience planning.[4]

A simple BI figure: A worked example

A business turning over £100,000 per month with £40,000 variable costs (materials and direct costs) could lose £180,000 of gross profit (£60,000 per month, depending on policy definition) during a three-month shutdown leaving fixed costs (rent, salaries, utilities, finance payments) to continue and net profit lost without appropriate cover.

Key questions for your next insurance review

If you want your BI cover to work when you need it, ask these questions:

- What events trigger BI cover on our policy? Is it only physical damage or do we have non-damage extensions?
- What is our indemnity period and is it long enough for a realistic return to normal after replacing all damaged assets?
- Do we have cover for additional increased costs of working if we must spend money in recovering un-economically (and what are the limits)?
- What records would we need to evidence a claim and where are they stored if premises or systems are unavailable?
- Separate to the property damage business interruption, if we rely on IT systems and cloud platforms, do we have a plan for cyber-related downtime (and do we have separate cover for that)?

Quick actions to take

Review your business continuity plans, identify single points of failure, stress-test cashflow for a short interruption and make sure essential records are backed up.

Ensure that the maximum indemnity periods are long enough for recovery of the business and seasonal businesses should also ensure their sums insured reflect peak periods.

BI isn't just about the immediate impact whilst replacing damaged property; it's about safeguarding your ability to survive and recover. In a climate of tighter cashflow and greater disruption, reviewing your BI cover is a practical step toward long-term resilience.

If you'd like help reviewing your BI cover or understanding your exposure, speak to your broker, they can clarify your policy and highlight any gaps and help ensure your business is properly protected.

4. https://www.wtwco.com/en-gb/insights/2025/10/when-the-furnaces-go-cold-what-recent-industrial-losses-teach-us-about-business-interruption

Trade credit insurance: Why it matters now

For many UK businesses, the biggest day-to-day risk isn't fire, flood or cyber attack — it's a customer who pays late or not at all. When cashflow is tight, a single unpaid invoice can quickly lead to missed payroll, delayed supplier payments and stalled growth.[1]

Even where cashflow is currently stable, the cost of acquiring new customers is high. Time spent prospecting, onboarding and extending credit increases exposure, particularly when trading with new or unfamiliar counterparties.

Why this is on the radar now

Economic uncertainty remains elevated due to fluctuating oil prices, geopolitical tensions and the ongoing energy transition.

In January 2026 alone, 1,744 companies in England and Wales entered insolvency — a 4% increase on December 2025.[2] Notably, the largest increase in failures has been among larger companies. This is a concern as the failure of a large buyer often has a ripple effect across suppliers, potentially triggering further insolvencies.[3]

What is trade credit insurance?

When you supply goods or services on deferred payment terms, you are extending trade credit and creating an unsecured receivable.

Trade credit insurance (TCI) protects businesses against non-payment of those commercial trade debts. It may also be referred to as credit insurance, accounts receivable insurance or receivables insurance.

What is typically covered?

Trade credit insurance commonly covers:

- **Insolvency** — where the buyer becomes insolvent, enters administration or is legally unable to pay
- **Protracted default (slow payment)** — failure to pay an undisputed invoice within an agreed period
- **Political risk (for exporters)** — including currency transfer restrictions, import/export restrictions and certain government actions, subject to insurer and structure

Beyond claims protection, TCI supports credit management by helping assess new and existing customers, identify early warning signs and support controlled growth. Insurers can also provide supply-chain insights, assist with cash collection and help mitigate fraud risk.

Common exclusions

Typical exclusions include:

1. Disputed or queried invoices
2. Sales to connected companies (e.g., subsidiaries of the policyholder)
3. Taxes such as VAT
4. Public sector buyers

Solutions may be available for some of these exposures, so it is always worth discussing with your broker.

Why it matters

Trade receivables are often one of the largest assets on a balance sheet — and one you have limited control over once goods or services are delivered. A single unexpected customer failure can quickly become a cash-flow issue.

1. https://www.gov.uk/government/consultations/late-payments-tackling-poor-payment-practices/late-payments-consultation-tackling-poor-payment-practices
2. https://www.gov.uk/government/statistics/company-insolvencies-january-2026
3. Insolvency Service, Company insolvency statistics releases, GOV.UK (April 2026)

The domino effect

A common bad-debt scenario is contagion: A key customer experiences financial stress, delays payment and the impact ripples through suppliers and the wider supply chain.

Typical triggers for loss

- Buyer insolvency or restructuring
- Concentration on a small number of key accounts
- Prolonged late payment
- Cross-border disruption (political events, payment restrictions, sanctions or transport disruption)

Using credit insurance to support finance

Trade credit insurance is frequently used alongside receivables finance, including invoice discounting, factoring, Asset-Based Lending (ABL) and structured receivables programmes.

Key considerations include:

- Whether the policy wording meets lender requirements (e.g., loss payee, step-in rights, reporting)
- Insurer counterparty requirements driven by lender policy (rating, jurisdiction)
- Operational alignment, including limit management, eligible receivables and dispute handling
- Alignment between finance documentation and insurance policy terms

Common structures include:

- Invoice discounting supported by loss payee or assignment endorsements
- Single-buyer cover aligned to large contracts or key account exposures, including (where appropriate) protection against contract frustration to support bank financing

Getting started

To assess market appetite and obtain indicative insurer terms, you will typically need to provide:

1. An overview of your business model, trading terms and geographies
2. Top buyers and peak exposures (including seasonality)
3. Your credit management process
4. Insurable turnover by country or region
5. Aged debt and historic bad debt or claims experience (if any)
6. Details of any receivables-backed financing and lender requirements

In today's environment, late payment and customer insolvency are board-level risks — not just finance issues. Trade credit insurance is most effective when combined with strong credit control and clear contractual processes.

If you would like help reviewing your credit exposures or exploring trade credit insurance options, speak to your broker. They can explain what's available and help you identify the right level of protection for your business.

Cyber crime: What it is, what it isn't and why cyber liability matters

Cyber is often talked about like it is a technical issue. For most SMEs, it is simpler: Cyber crime is theft and disruption carried out using digital tools. The impacts are very real — lost money, downtime, reputational damage and regulatory headaches.

The scale of the issue for UK organisations

The UK Government's Cyber Security Breaches Survey is one of the most useful benchmarks because it is based on a large, structured survey of UK organisations. In the 2025 release, just over four in ten businesses (43%) reported experiencing a cyber security breach or attack in the last 12 months — and the rate was higher for medium and large organisations.[1]

Cyber breaches, cyber attacks and cyber crime: What is the difference?

Even official reports make a clear distinction:

- A cyber security breach or attack is a broad category — for example phishing emails, malware infections or attempts to gain unauthorised access
- Cyber crime is a subset of that broader picture and is defined with reference to criminal offences (for example under the Computer Misuse Act 1990)[1] and Home Office counting rules
- In plain terms: Not every suspicious email is a crime that results in loss, but it may still be an attack attempt — and it can still disrupt operations

Malware, ransomware and "why it escalates fast"

The National Cyber Security Centre (NCSC)[1a] explains malware as malicious software that can steal, delete or encrypt data, lock devices or take control of systems. Ransomware is a type of malware that prevents you accessing computers or data, usually accompanied by a demand for payment. The NCSC warns that even if you pay, there is no guarantee you will regain access and paying can increase the likelihood of being targeted again.[2]

Common SME cyber crime scenarios

Most SME cyber incidents fall into a few patterns:

- **Phishing and impersonation**: An email or text that looks like a supplier, HMRC or your own CEO — prompting a payment or password reset
- **Business Email Compromise (BEC)**: Criminals trick staff into transferring funds, often using targeted phishing that looks plausible and urgent
- **Ransomware**: Systems are locked and business stops until recovery steps are taken
- **Data theft or accidental leak**: Customer or employee data is accessed or shared incorrectly
- **Supplier compromise**: An IT provider or platform is breached and you are impacted as a downstream customer

Cyber crime versus cyber liability: Why the second one surprises owners

Cyber crime is what criminals do to you. Cyber liability is what you may owe to others because of a cyber incident.

1. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
1a. https://www.ncsc.gov.uk/
2. https://www.gov.uk/government/publications/financial-sanctions-guidance-for-ransomware/financial-sanctions-guidance-for-ransomware

Examples of cyber liability include:

- **Data protection obligations**: If personal data is affected, you may need to assess and potentially notify the Information Commissioner's Office (ICO)[2a]
- **Customer or supplier claims**: If you cause them loss (for example by leaking data or disrupting a service), you could face legal claims
- **Regulatory and communications costs**: Investigations, specialist advice and customer notifications can follow a serious incident

The ICO's guidance for organisations is explicit: you must report certain personal data breaches to the ICO within 72 hours of becoming aware of them (where feasible) and in high-risk cases you must also inform affected individuals without undue delay. The ICO also provides simple steps for small organisations to follow in the first 72 hours after discovering a breach.[3]

The basics that prevent a large share of incidents

You do not need a big IT department to reduce risk materially. The NCSC's Small Business Guide[3a] sets out practical steps that cost little to implement but significantly reduce exposure to common attacks. The NCSC also provides detailed principles for ransomware-resistant backups, because attackers increasingly try to encrypt or delete backups.

- Back up important data and practise restoring it. Keep at least one backup protected from ransomware
- Use multi-factor authentication (MFA), especially for email and remote access
- Keep devices and software updated (patching)
- Use strong passwords and a password manager where possible.
- Train staff to spot phishing and to report suspicious messages quickly

Your response plan

The NCSC's Small Business Guide to Response and Recovery[4] recommends preparing for incidents in advance and then moving quickly through identification, resolution, reporting and learning. For most SMEs, a basic plan looks like this:

1. **Immediate actions**: Contain (disconnect affected devices, change passwords where safe to do so), contact IT support, start an incident log and decide who will communicate internally and externally.
2. **Follow on actions**: Confirm what systems and data are affected, restore from backups if appropriate, consider whether you need to report to Action Fraud or the NCSC and assess whether personal data is involved (ICO threshold).

Insurance implications: What cyber cover typically relates to

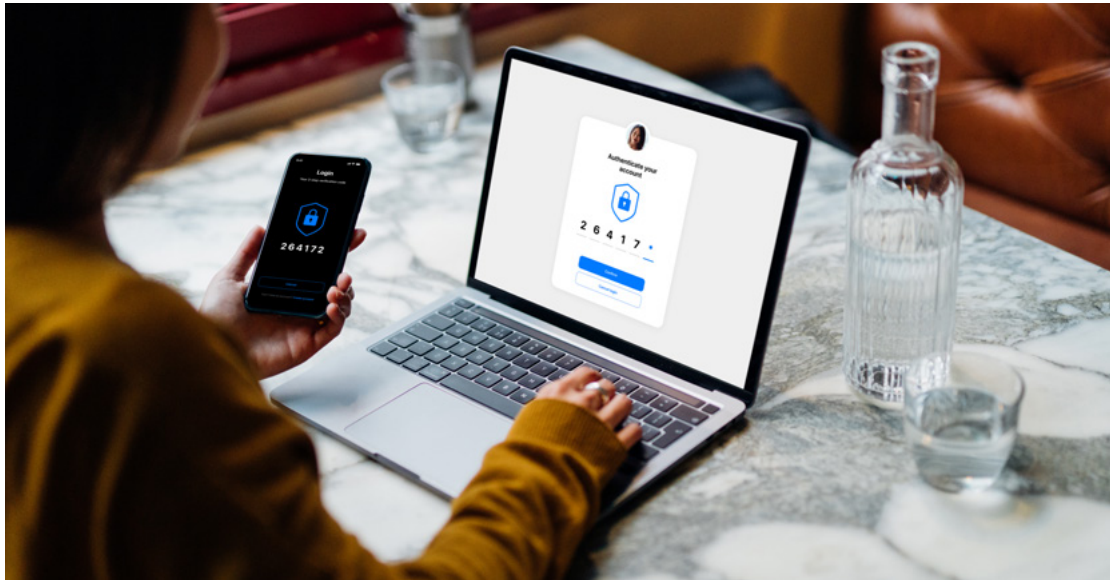
Cyber insurance is designed to help businesses respond to a cyber incident and may include some combination of:

- Incident response support (IT, legal, communications)
- Costs of investigating and restoring systems and data
- Business interruption costs linked to a covered cyber event
- Liability cover for third-party claims arising from the incident
- Support with notifications and data breach response (depending on wording)

Cyber policies vary significantly and many require certain security controls to be in place. The practical takeaway is to treat cyber insurance as part of resilience planning, not a substitute for basic controls.

Cyber risk is now a normal cost of doing business — like theft, fraud and health and safety. The difference is speed: cyber incidents can escalate in hours. If you understand the basics, build a response plan and put simple controls in place, you can reduce both the chance and the impact of an incident.

Cyber attacks move fast — your protection should too. If you want to check whether your business could withstand a cyber incident or compare cyber insurance options that fit your risks, speak to us today.



2a. https://ico.org.uk/
3. https://ico.org.uk/for-organisations/advice-for-small-organisations/personal-data-breaches/72-hours-how-to-respond-to-a-personal-data-breach/
3a. https://www.ncsc.gov.uk/collection/small-business-guide
4. https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

Summer workplace guide for SMEs: Keeping teams safe, healthy and productive

Summer can be one of the most productive times of year — longer daylight, stronger customer demand in some sectors and more outdoor activity. But it also brings predictable workplace risks: Heat stress, dehydration, sun exposure, fatigue and seasonal travel hazards.

Start with the basics: Temperature is a workplace hazard

HSE's guidance is clear on two points that surprise many employers:

- There is no legal maximum workplace temperature, because "too hot" depends on the type of work and conditions[1]
- Employers still have legal duties: heat is a hazard and must be assessed and controlled like any other workplace risk[2]

HSE also explains what heat stress is, typical symptoms (such as dizziness, cramps, fainting and heat exhaustion) and how risk rises with heavy work, humidity and restrictive clothing or Personal Protective Equipment (PPE).[3]

A practical summer checklist

Use this as a short seasonal add-on to your normal risk assessment:

- **Hydration**: Make cold drinking water easy to access; encourage regular drinking (water is better than caffeine or fizzy drinks)
- **Ventilation and shading**: Fans, blinds, reflective film, moving workstations away from direct sun; consider earlier starts where possible
- **Breaks and pacing**: Extra rest breaks in hot conditions; rotate physically demanding tasks
- **Dress codes and PPE**: Relax formal dress codes where safe; ensure PPE is still used and suitable
- **First aid readiness**: Remind teams of heat exhaustion signs and when to get help
- **Lone workers**: Check welfare and ensure someone knows where they are
- **Driving for work**: Plan safer journeys, avoid time pressures and build in breaks
- **Outdoor work**: Manage UV exposure with clothing, shade and sunscreen

Heat-health alerts and weather warnings: What the colours actually mean

Many businesses now use official warnings to trigger practical changes (for example earlier starts, extra welfare checks or pausing outdoor work). The Met Office Heat-health Alert service (run with UKHSA) uses an impact-based colour system in summer. In simple terms:

Green: Summer preparedness (no alert) — keep plans ready.

Yellow: Heat may affect vulnerable people; action is needed in health and social care settings and sensible precautions help workplaces too.

Amber/red: Higher likelihood and/or higher impacts; organisations should take more active protective steps.

Alongside this, the Met Office National Severe Weather Warning Service uses yellow/amber/red warnings for impacts like extreme heat and thunderstorms. Read each warning for the expected impacts and the likelihood, not just the colour.[4]

Outdoor work: Do not ignore sun and UV exposure

HSE warns that too much sunlight is harmful and that a tan is a sign of skin damage caused by ultraviolet (UV) rays. Outdoor workers should keep covered, use at least SPF30 sunscreen on exposed skin, use shade where possible and drink plenty of water. Sun protection is also about eyes, dehydration and overheating — not just skin.[5]

1. https://www.hse.gov.uk/temperature/employer/the-law.htm
2. https://www.hse.gov.uk/temperature/employer/the-law.htm
3. https://www.hse.gov.uk/temperature/employer/managing.htm
4. https://weather.metoffice.gov.uk/warnings-and-advice/seasonal-advice/heat-health-alert-service
5. https://www.hse.gov.uk/skin/sunprotect.htm

Driving for work: A summer risk multiplier

Hot weather can worsen fatigue and discomfort, while summer traffic and roadworks increase journey times. HSE reminds employers that health and safety law applies to work on the road in the same way as it does on a fixed site and that driving for work is one of the most dangerous activities workers do.

A simple "safe journey, safe driver, safe vehicle" approach helps. Planning routes, allowing breaks and avoiding unrealistic schedules reduces risk and often improves morale and efficiency. It also helps if you build weather into journey planning: storms, heat and glare can all raise accident risk.[6]

Premises and equipment: Summer also stresses buildings

Summer disruption is not only about people. Heat can affect equipment performance, increase the chance of spoilage for temperature-sensitive stock and amplify the impacts of storms. Even a short power interruption can have outsized operational impact if it affects refrigeration, IT, alarms or access control. A simple "hot day plan" should include who checks critical systems and what the fallback is if a system fails.

Insurance implications: Where summer risks show up

Even if you never make a claim, understanding where insurers see summer risk can help you prioritise controls:

- **Employers' Liability**: Heat stress or sun exposure claims can be alleged as workplace-related illness, particularly for outdoor workers
- **Public Liability**: Higher footfall, events and outdoor trading can increase third-party injury risk
- **Motor and fleet**: More driving, more miles and more congestion can increase incident frequency
- **Property and interruption**: Thunderstorms and flash flooding can damage premises and disrupt operations
- **Contractors and grey fleet**: If staff use their own vehicles for work, ensure the risk is managed and insurance arrangements are clear

Quick actions to take before summer peaks

1. Update your risk assessments for heat, dehydration and outdoor work.
2. Check welfare arrangements: water, shade, rest areas and suitable facilities.
3. Brief managers on heat stress symptoms and response.
4. Review driving for work policies, including journey planning and fatigue controls.

5. Create a hot day plan (who decides, what changes, how you communicate).
6. Use Met Office alerts and warnings to trigger practical adjustments.
7. Check your emergency contacts and business continuity plan for severe weather disruption.

Summer risks are predictable — and that is good news. With simple planning, most heat, sun and travel-related incidents are preventable. A short seasonal review now can protect your team, avoid downtime and reduce the chance of costly claims.

Need help preparing your business for summer risks?

If you'd like support reviewing your risk assessments, strengthening your hot-weather controls or checking whether your insurance cover is still fit for purpose, we're here to help.

Get in touch with your usual broker contact today to make sure your people, premises and operations are protected before temperatures rise.

6. https://www.hse.gov.uk/roadsafety/employer/index.htm

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 May 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.

FPS1257939 WTW-4442701752-05-2026