Winter 2025

W B Baxter
Insurance since 1911

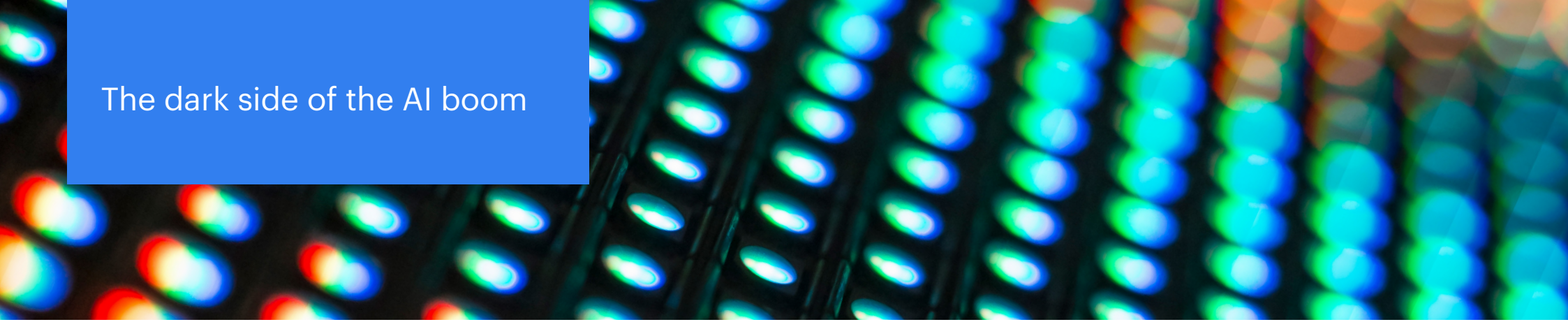
Covernotes

Explaining issues that affect insurance

In this issue

- The dark side of the AI boom
- The perils of social media posting
- Avoid a christmas party liability disaster
- Do not let blackouts cause a business black spot

The dark side of the AI boom



Artificial intelligence has quickly been abbreviated to AI in day-to-day conversation, signalling a growth in awareness of its role in our lives, jobs and futures. However, a more sinister dark side sits alongside the boom in AI-driven technology and the advantages widespread AI adoption can bring. When AI powers cybercrime strategies, there is often a greater threat to challenge our computer systems, banking security and personal information safeguards.

AI-enhanced attacks are rapidly becoming the norm and those most at risk are SMEs. Almost half (46%) of cyberattacks target smaller and medium-sized businesses.[1] Notably, a quarter of the SMEs attacked in 2024 believed AI had been involved.[2] Against this backdrop, nearly nine-in-ten (86%) of SMEs feel "unprepared" to spot AI threats. 64% say AI threats are outpacing their organisation's ability to protect against them.[3]

AI is a valuable tool for cybercriminals, who can earn substantial amounts out of phishing attacks and ransom payments. Phishing emails, until recently, were fairly easy to spot, with cybercriminals deploying poor English, making obvious spelling mistakes and using amateur copies of company logos. AI adds a vastly enhanced level of sophistication. The language is more polished and correspondence more context-aware. Attacks are increasingly tailored to an individual business and information about key personnel and businesses is quickly scraped from online sources. Details, which it could have taken a cybercriminal months to collate previously, are pulled together in seconds.

Due diligence, in checking people are who they say they are, own the bank accounts they claim to operate and are legitimately seeking engagement, should become a habitual action. Unfortunately, deep-fake attacks are on the rise. Impersonation of real company directors and other managers and decision-makers is now a factor in one-in-seven targeted scams.

Phishing and the internal threat

Phishing thrives on the use of AI. The Cyber Security Breaches Survey 2025, by the Department for Science, Innovation and Technology (DSIT) and the Home Office, found 85% of businesses and 86% of charities attacked by cybercriminals in the past 12 months were phishing victims.[4] The survey noted that sophisticated methods, such as AI impersonation, are now becoming "mainstream". The survey also estimated UK businesses experienced 8.58M cybercrimes, of all types, within the year. Ransomware's role had increased significantly, as cybercriminals sought to force businesses to pay for their systems' restoration.

Worryingly, businesses do not just face cybercrime villains from without, but sometimes from the enemy within. An insider threat has been exposed by one BBC reporter, approached by cybercriminals using an encrypted App.[5] They offered a share of the ransom to be demanded of the corporation to restore its systems — a payment that would enable him to "never work again" in their words. In return, they sought his log-in and password or for him to run computer code on his work computer and report back on the result.

In this instance, the reporter reported the contact. Not all employees may be able to resist such an offer.

1. https://www.itbuilder.co.uk/blog/ai-powered-cybercrime-is-here
2. https://datacentrereview.com/2024/10/how-uk-smes-can-balance-ai-adoption-and-security/
3. https://datacentrereview.com/2024/10/how-uk-smes-can-balance-ai-adoption-and-security/ (Section 4)
4. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
5. https://www.bbc.co.uk/news/articles/c3w5n903447o

Protecting against a cyberattack

Businesses have to control risks both in their main workplace and in the homes of remote workers. Some are trying. The Cyber Security Breaches Survey noted an elevated adoption of some cybercrime prevention methods, but there is worrying detail within the figures.

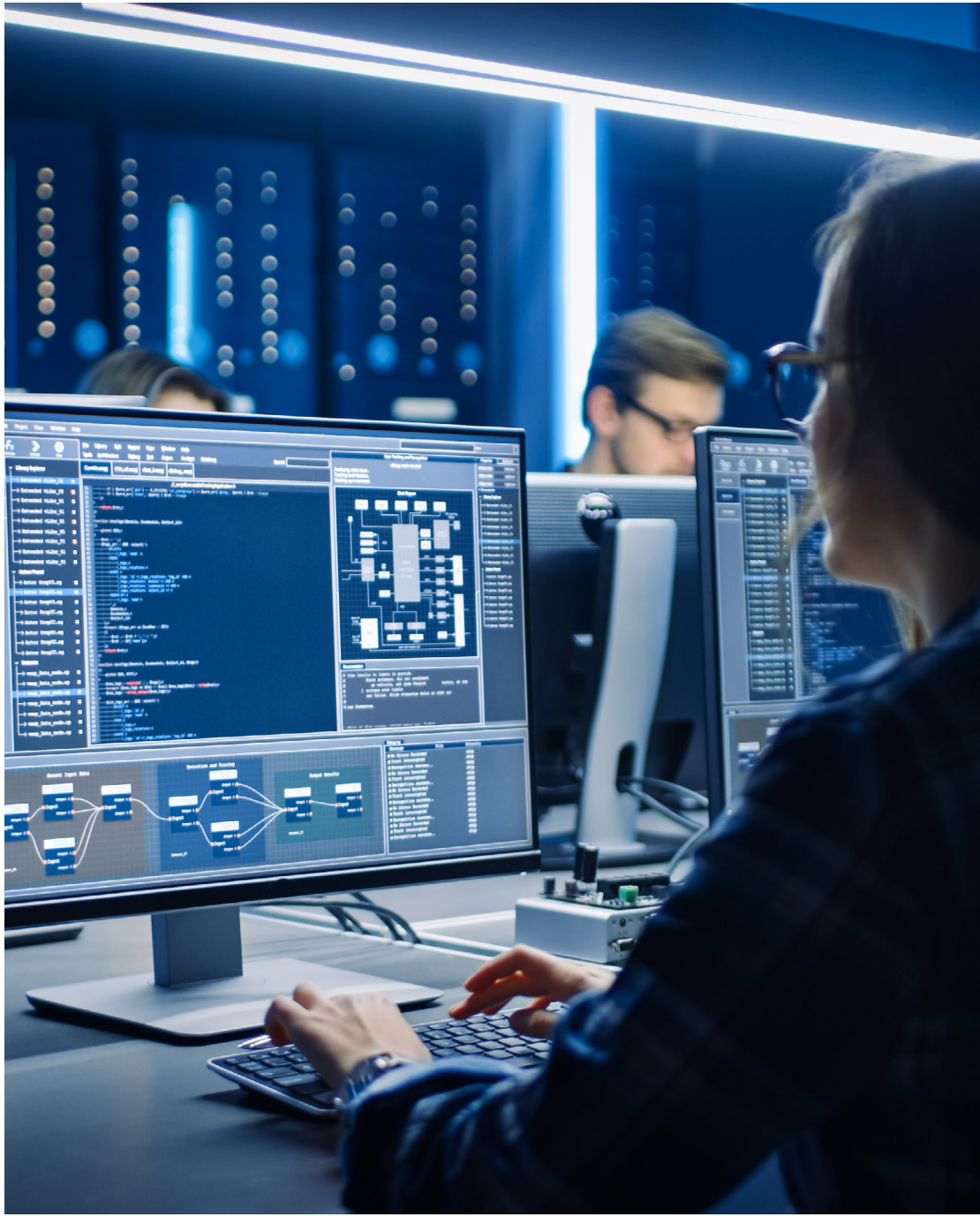
Only 19% of businesses train employees in cyber prevention. Less than a third (31%) use a VPN through which remote staff can connect. 41% of businesses have no formal cyber procedures. Around half (47%) have not drawn up a cyber business continuity plan. This is despite a notable increase in temporary loss of access to business files and third-party services, as reported by those businesses attacked in the past year.

The need for the right cyber insurance

Whilst cyber insurance policies are now more commonly purchased, businesses may not necessarily bought the right cover for their business recovery needs. Some cyber insurance policies merely offer compensation for losses. The most useful cyber insurance policies, on the other hand, offer immediate access to cyber-focused IT experts, able to quickly launch a forensic examination of the attacked IT system. Speed is of the essence. Having a pro-active policy that can also identify areas of IT weakness before an attack occurs, is another advantage. Using AI, criminals can quickly identify businesses with easy-to-exploit system loopholes, making these prime targets.

Cyber security has moved way beyond installing anti-virus software or updating software. The capacity for human vulnerability is greater than ever in the AI-driven cybercrime world. Genuine errors regularly occur. Staff may be tempted to become the insider threat. Having a contingency plan in place, to cope with an attack's impacts is vital, as is access to professional cyber-expert help. Sit these core elements alongside enhanced staff training in today's sophisticated phishing tactics, deep fakes and impersonation and back this with the use of VPNs for remote workers and the limiting of access to company passwords and the AI-backed cyber threat has a much better chance of being repelled.

To discuss a cyber insurance policy that will provide the right level of assistance before and in the event of an attack and to access help in preparing a cyber business continuity plan, speak to one of our brokers today.



The perils of social media posting

Is your business active on social media? Well, beware two major risks, often going under the radar. The first is that of being sued having infringed the copyright of an original creator of a particular 'work' or material. The second relates to facing costly legal battles if your own original materials are lifted and used by third parties or if negative, reputation-damaging content emerges online.

There is a general lack of awareness as to how copyright works. In 2024, the Intellectual Property Office (IPO)[1] found many SME businesses do not have an understanding of Intellectual Property beyond the "topline terminology", meaning the term itself.[2]

Original photos, videos, written and musical works and much more are protected by the Copyright, Designs and Patents Act 1988.[3] This law prevents copying or republishing content without permission. This differs from trademark law, which protects distinctive names, logos, slogans and elements of brand identity. However, infringing another company's rights in this regard can be equally costly.

Getting caught out by social media posting

There are definite legal pitfalls to consider with social media. The very fact that the social media channels encourage 'sharing' of pieces of content it could be at odds with the principles of copyright law, which protect the author or creator's original rights.[4] Many social media users believe crediting the originator of the work is sufficient, failing to realise this does not eliminate the risk of being sued by an originator who did not give permission to have their material used.[5]

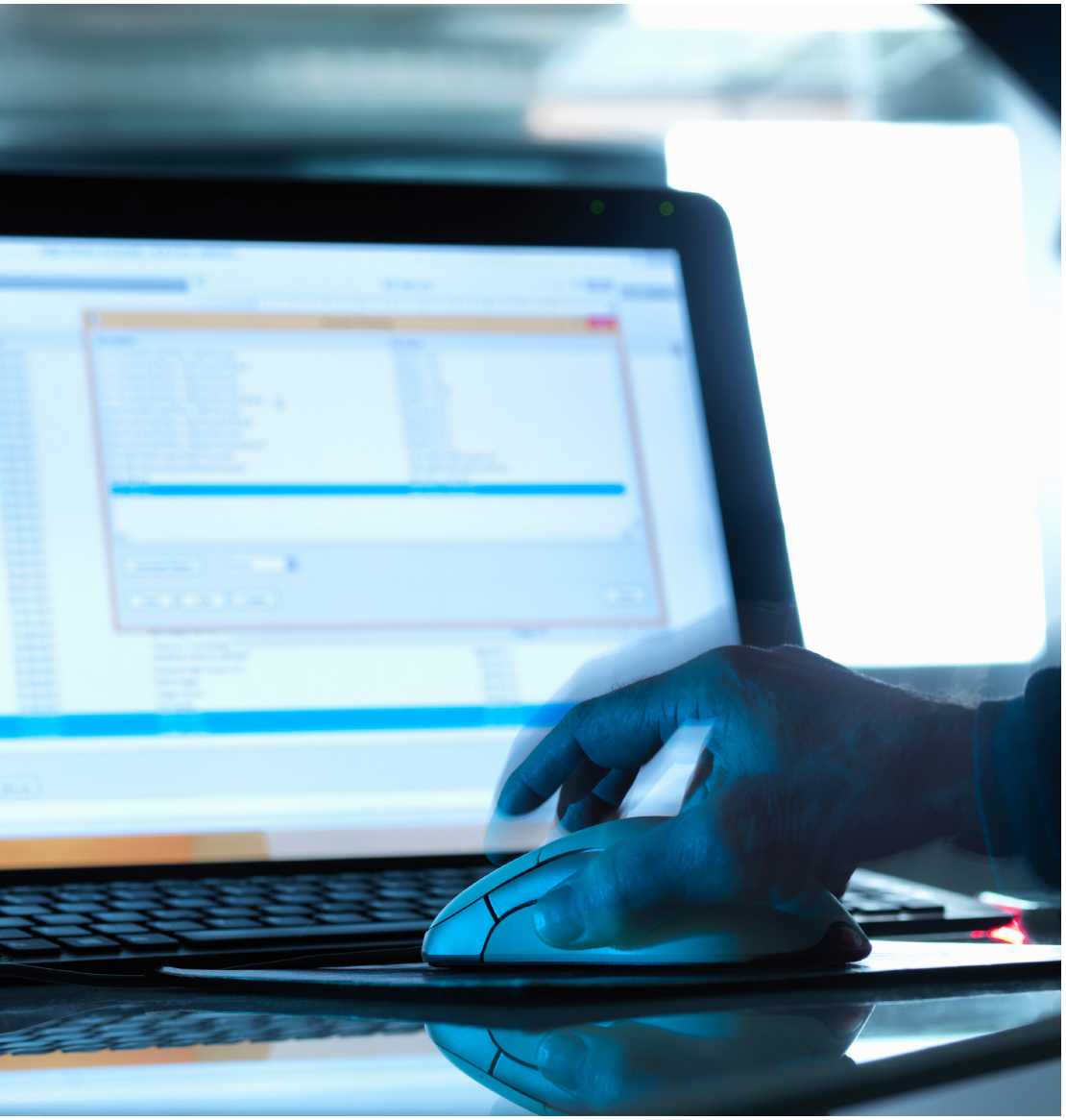
A surge in IP infringement cases suggests many business are getting it wrong. Just because somebody posts a picture on to the internet or onto a social media channel does not mean the image has entered the public domain and is available for use.[6]

Some of the popular image libraries are strongly protective of their copyright, as are many photographers. Any business could easily find themselves faced with a very worrying lawyer's letter. Similar issues occur when using GIFs or memes. Unless permission has been granted and the material used precisely as intended, the end-user can be in hot water.

Failing to understand that personal use and commercial use are two different matters is another problem. Royalty-free music libraries often place a ban on 'commercial use' of tracks, whilst allowing individuals to utilise their materials.

'Fair use' is a further grey area. Under UK copyright law, fair dealing permits use of copyrighted material without permission, but only for specific purposes such as criticism, review, news, reporting, research and private study. Commercial use is not automatically excluded, but the fairness of the use is judged on factors like the amount used, the purpose and the potential impact on the market for the original work which could lead to legal challenges.[7]

1. https://www.gov.uk/government/organisations/intellectual-property-office
2. https://www.gov.uk/government/publications/ip-awareness-and-understanding-among-uk-smes/ip-awareness-and-understanding-among-uk-smes
3. https://www.legislation.gov.uk/ukpga/1988/48/contents
4. https://journals.sagepub.com/doi/10.3233/ISU-240006
5. https://axaxl.com/fast-fast-forward/articles/navigating-social-medias-copyright-and-liability-risks?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase
6. https://ipwatchdog.com/2024/04/25/rise-ip-lawsuits-posting-images-navigate-avoid-copyright-infringement-issues/id=175810/
7. https://www.gov.uk/guidance/exceptions-to-copyright



Good practice on social media

If using social media, always check you have ownership of materials being posted or are properly licensed to use the content. Keep evidence of the licence or permission granted and ensure permission is in writing. UK courts can award significant financial compensation depending on the nature and impact of the infringement.[8]

Finding your business on the other end of copyright infringement, can be equally challenging and costly. Nevertheless, it can be absolutely crucial to assert rights over a piece of work, image or material. Similarly, should you be defamed, suffer fake reviews, see a copycat account established or be misrepresented online, it can be imperative to act decisively and quickly. Having access to the right specialists is almost always necessary and that comes at a cost. IP litigation costs are typically higher than the final settlement costs.

Protecting your business against IP risks

There are steps to take, to try to safeguard against the continual risks. Make employees aware that actions taken on social media can create liability issues and train them in good practice when posting and sharing content.

Beyond that, consider stand-alone Intellectual Property insurance or a cyber or technology Errors & Omissions (E&O) policy with media liability coverage.

An IP policy will protect you from the penalties applying to infringements of copyright, trademarks and patents, as well as any breaches of Non-disclosure Agreements. It can provide access to experienced claims handlers and a network of panel lawyers worldwide, highly experienced in resolving disputes swiftly.

Defence costs are covered, along with damages payments for infringements. The policy also allows for the pursuit of claims against third parties. There is, in addition, some directors and officers cover, to help protect a director held personally liable for an IP infringement.[9]

To discover the options available to you, if using social media as a marketing tool, talk to one of our brokers today and allow us to get you protected.

8. https://sprintlaw.co.uk/articles/photo-copyright-infringement-penalties-in-the-uk-what-businesses-need-to-know/#What_Are_the_Penalties_for_Photo_Copyright_Infringement_in_the_UK
9. https://www.wtwco.com/en-gb/solutions/services/intellectual-property-insurance-and-risk-management

Avoid a Christmas party liability disaster

Party season is almost here, which should give both hospitality businesses and businesses organising Christmas shindigs much food for thought beyond the turkey, tinsel and mince pies.

Those opening up their premises to revellers should check all liability covers are in place. Employer liability insurance is a legal requirement, protecting the business should an employee suffer injury or illness due to work-related activities. If your cover has expired, you can be fined up to £2500 per day.[1] Do check the documentation.

Welcoming members of the public onto the premises, makes public liability insurance another key cover. If you injure a guest or customer or damage their property, whether by leaving a wet floor unguarded or spilling gravy onto their designer clothing, the policy will protect you.

Christmas is a key income-boosting time for many businesses, so safeguard against any unanticipated closure caused by something like fire or flooding. Business interruption insurance can be a lifeline, covering the income you would have earned under normal circumstances.

You may also need product liability insurance, if serving your own food and drink fayre to revellers. Maybe professional indemnity insurance is required, to prevent your business being sued if you plan an event that goes horribly wrong? Also remember that cyber criminals will know you are busy over the festive period and paying less attention to that phishing email or deep fake impersonation scam. Consider arranging your cyber liability insurance before opening the first door of your advent calendar — it's a smart way to stay protected during the busy season.

The risks posed by vicarious liability

But if organising a staff works 'do', reflect on vicarious liability. Are you aware employers can be held responsible for employees' actions and wrongful acts "closely connected" to their employment?[2]

Often, these are fuelled by alcohol consumption, high jinks or a combination of the two. Anything, from personal injury to another person to sexual harassment, could occur.

Even at work Christmas parties, 'off duty' is not really 'off duty', if the event is laid on by the employer. It is seen as an extension of the workplace. The law's view is that "employers are held vicariously liable for any wrongful acts committed by their employees "in the course of their employment".[3]

The common duty of care is an extremely flexible concept and it is something party organising employers must consider. Robust risk assessments must examine a venue and event's risks and how alcohol consumption might amplify those.

1. https://www.gov.uk/employers-liability-insurance
2. https://www.lawrencestephens.com/news/seasonal-parties-and-employer-liability-for-acts-of-misconduct-carried-by-employees/

Consider games, activities — even moves on the dance floor — and what might result. Factor in the need for designated supervisors or security guards. Make sure employees get clear guidance on what you deem acceptable behaviour and mirror this in employment contract wording. Having employees sign and formally accept responsibility for their own actions, is a wise step.

Proactively try to prevent sexual harassment too. Failure to do so is a costly mistake at tribunal with a new duty under the Equality Act 2010 introduced in October 2024 and a potential uplift of 25% on the employee's compensation, if the employer was deemed to have failed in its duty of care to prevent the issue.[4] Christmas parties can sometimes lead to misunderstandings or inappropriate behaviour, so it's important for employers to remain attentive and proactive.

Even if vicarious liability is eventually not proven, the legal costs incurred can be immense. It required two hearings, the second at the High Court, in the case of Shelbourne v Cancer Research, to determine the charity was not responsible for an employee's injuries, after she had been lifted and dropped on the dance floor by a visiting scientist.[5]

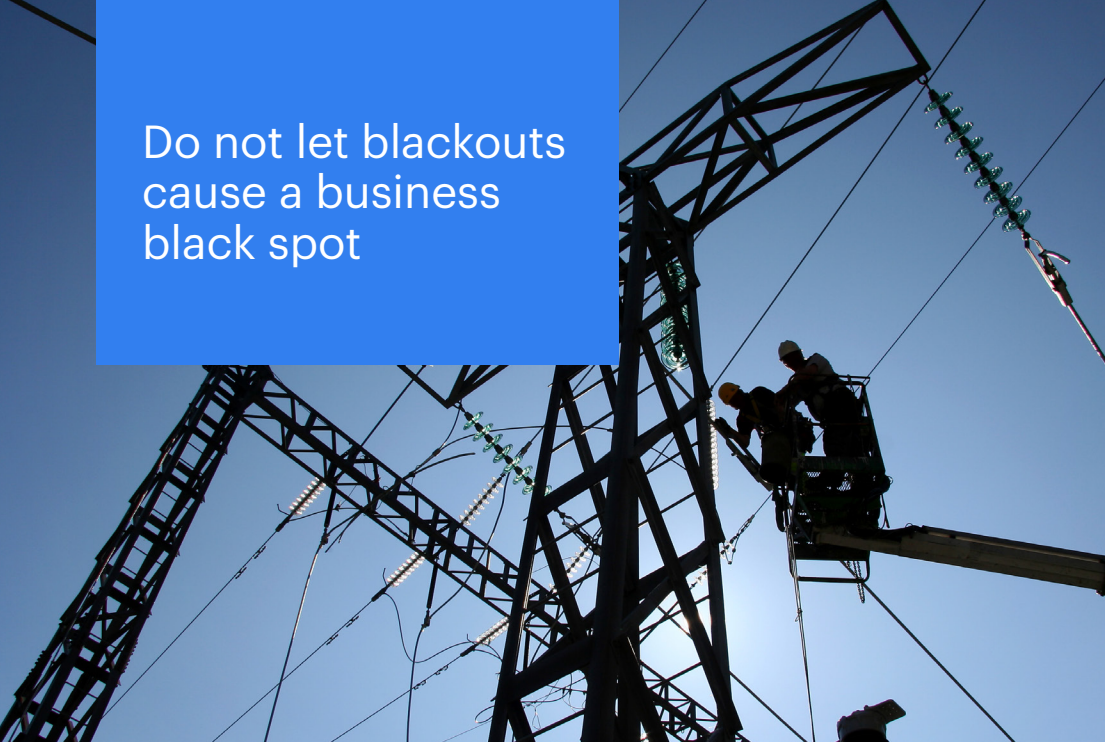
So, carry out the right risk assessments, consider all potential scenarios and mitigate the risks, documenting all actions taken, well ahead of the party. Employers may also be well-advised to protect against vicarious liability claims by taking out Employment Practices Liability Insurance (EPLI).

Keep in mind that employers may still be held liable for an employee's actions if those actions are considered closely connected to their role — even if they occur outside normal working hours or off-site. This highlights the importance of clear behavioural expectations and appropriate supervision at work-related events.

Talk to us about vicarious liability, how it works and the risks to your business and let us help your party pop, rather than implode.

3. https://sprintlaw.co.uk/articles/all-about-employers-liability/
4. https://www.gov.uk/government/news/new-protections-from-sexual-harassment-come-into-force
5. https://www.crosslandsolicitors.com/site/cases/Shelbourne-v-Cancer-Research-UK-vicarious-liability-negligence

Do not let blackouts cause a business black spot



How prepared is your business for winter? We are not just talking here about clearing out the guttering, checking the state of the roof and ensuring you are not one of UK businesses that cumulatively loses £1 billion to snow and ice-related events each year.[1] All of those actions are important though.

Nor are we referencing the requirement to ensure security cameras are working, to control theft risks on dark winter nights. We are not even pointing to the ever-present requirement to check pipework is insulated and background heating kept on, to safeguard against burst pipes, which should have received a pre-winter plumbing check.

Instead, we are focusing on the black spot that can relate to blackouts.

We have seen high profile instances of the impacts of blackouts this year. In March, Heathrow Airport shut down for around 16 hours, when a catastrophic failure of equipment caused a fire that led to a power outage.[2] In April, the Iberian peninsula was the location of Europe's biggest blackout for over 20 years.[3] It proved no electricity grid is infallible.

August 2019 saw Britain's biggest blackout in a decade when one million people in England and Wales lost power.[4] Fast-forward to the impacts of Storm Darragh in December 2024 and the "biggest restoration effort ever" was required on the National Grid network.[5]

Some blackouts can be very localised. A sudden power outage hit Lowestoft in June 2024, causing a 40-hour blackout for restaurants, shops and businesses.[6]

In a time of climate change and when we have already seen violent storms hitting the UK this season, no business can be sure that it will not suffer downtime. Such an eventuality can damage reputation, erode customer trust and lead to a distressing loss of income and output.

It could also involve losses emanating from spoiled goods or refrigerated stock, whether that is in a grocery store or supermarket, restaurant or pub or distribution centre.

Electricity outages can result in corrupted data, problems with elevators and lighting systems and heating and ventilation. Workers and employees may struggle to exit a building left with no lighting. In other words, unsafe workplace scenarios can be created during blackouts.

One answer is to consider emergency power generation, if your business could be left particularly vulnerable. The risk of losing power is not necessarily purely the result of poor weather or a localised network issue. System overload could also potentially occur. A blackout 'near miss' is said to have taken place on January 8, 2025, when the National Energy System Operator[7] was forced to issue an Electricity Margin Notice. This indicates that spare capacity within the grid did not cover the contingency deemed necessary.[8]

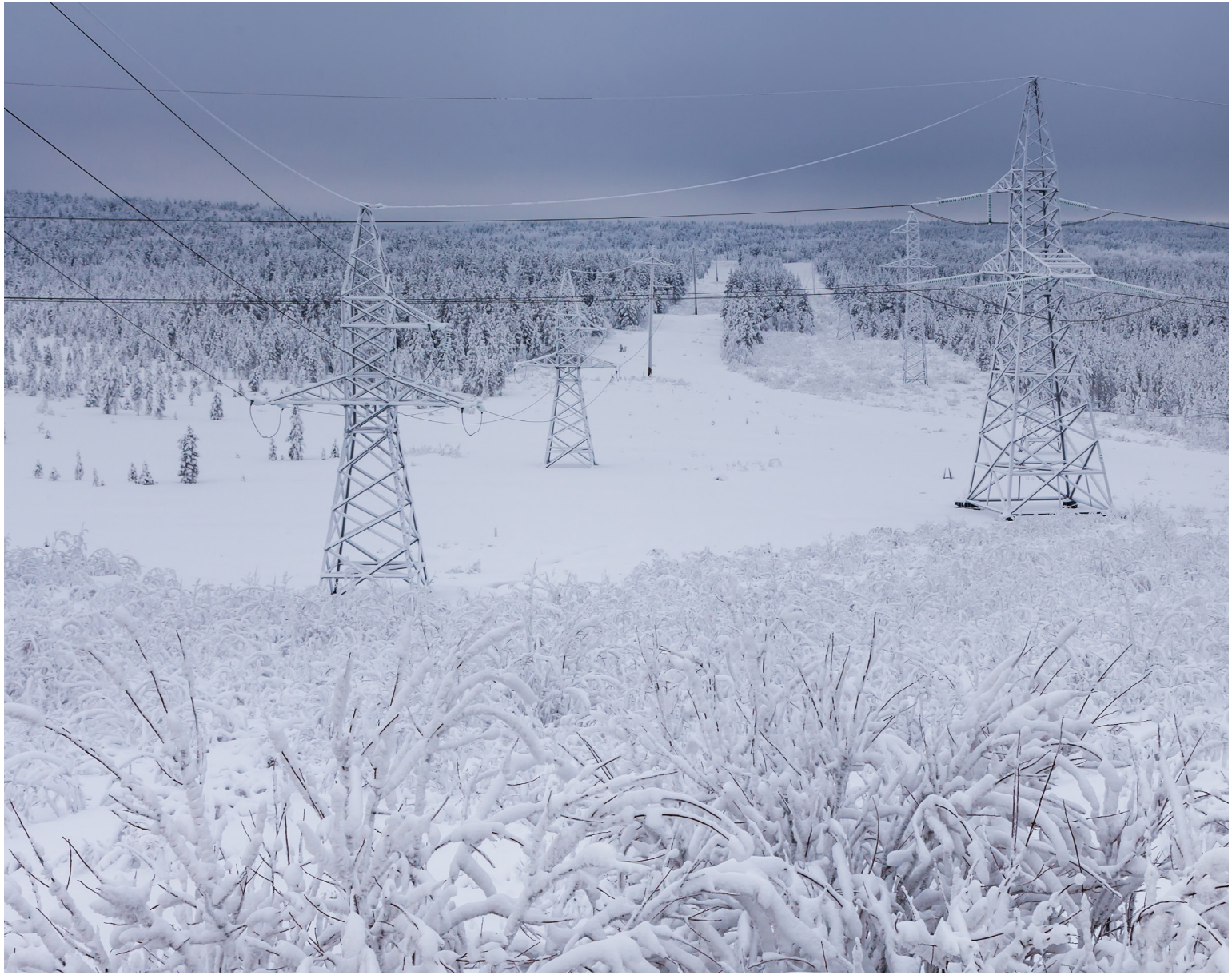
The other thing to do, as a business, is review your emergency, continuity and resilience plans and see how power outages are covered by those. How will critical plant continue to operate? What maintenance checks might be required if a power outage occurs and plant has to be restarted? Which equipment will be most affected? How would you communicate with shift workers, to prevent them coming to site, if power was lost? Would internal communications systems go down, causing an on-site issue?

1. https://www.outco.co.uk/winter-preparation-checklist-for-smes-multi-site-estates/
2. https://www.bbc.co.uk/news/live/
3. https://www.bbc.co.uk/news/articles/cg7d4vjdlrmo
4. https://www.drax.com/opinion/britains-blackout/
5. https://www.bbc.co.uk/news/articles/cm2ek12wje8o
6. https://www.mems.com/hidden-costs-power-outages/
7. https://www.neso.energy
8. https://watt-logic.com/2025/01/09/blackouts-near-miss-in-tighest-day-in-gb-electricity-market-since-2011/

Everyone's role in the event of a power outage needs to be detailed within the planning documents and risk assessment, with training provided to back up the words on file. If an emergency generator will be deployed, employees will require training in how to use that. If it is a case of turning to alternative sources of heating, to keep the workplace operational, consideration must be given to the combustibility of materials that could lie near temporary heaters and the fire hazards that might be created by those.

Ask yourself, 'how would we operate' if a power failure occurred and devise workable solutions, if possible, before that happens.

It is also well worth checking your insurance policy's small print and assessing under what circumstances, if any, your business interruption policy would cover you for losses incurred during a power outage. This is something you should discuss with your broker, particularly if a power outage would be highly detrimental to your business or manufacturing operation. Back this with the right business continuity planning and, hopefully, any winter blackouts will not leave you fumbling around, seeking a way forward.



W B Baxter Ltd
Regus Civic Building, 2nd Floor, 323 High Street
Epping
Essex
CM16 4BZ

Tel: 0208 554 5500

www.wbbaxter.co.uk
contact@wbbaxter.co.uk

Chartered Insurance Brokers

Authorised and regulated by the Financial Conduct Authority.

FPS10608437 WTW-1787650720-11-2025