STEWARTS

The Policyholder Review 2026

Cyber

Cyber

Chloe Derrick and Claudia Seeger

Cyber resilience: A call to action

2025 was an unprecedented year for high-profile cyber incidents, with attacks on several household names hitting headlines nationwide. It has led to continued concern about the UK's ability to withstand increasing cyber threats, and with good reason: the Cyber Security Breaches Survey 2025 reported that in the last year alone, 45% of businesses have experienced a cyber incident.

The wide-ranging financial and operational impact of cyber events means that cyber security is now an enterprise risk, as opposed to an IT risk. Despite this, an overwhelming 57% of businesses are reported to be uninsured for cyber risks[1]. In a recent speech to the Corporation of the City of London, Nikhil Rathi, CEO of the Financial Conduct Authority, voiced his fear that the nation was "massively underinsuring" when it came to cyber risks.

It is unsurprising that against this background, cyber insurance continues its growth trajectory as the fastest-growing global insurance product, with 41% of large enterprises planning to purchase cyber coverage for the first time within the next five years[2]. Cyber coverage, however, remains a relatively new line of business, and the scope of coverage available can vary significantly, particularly on coverage for business interruption, for example. The recent highly publicised attacks on the retail sector have sparked increasing debate around how cyber insurance may respond (if purchased) to cover large-scale business interruption losses. We review some of the developments, with key takeaways for policyholders looking ahead to 2026.

Chloe Derrick
Partner
Policyholder Disputes

Claudia Seeger
Associate
Policyholder Disputes

1 Cyber Security Breaches Survey 2025
2 Cyber Insurance Report 2025, Howden

Recap from 2025

Reflections from the retail frontline

Discussion in 2024 centred on lessons for operational cyber resilience and the need to identify single points of failure following the widespread disruption triggered by the CrowdStrike outage. In our 2025 edition of The Policyholder Review, we discussed the key coverage issues arising post-CrowdStrike and a single point of failure loss event, including coverage for non-malicious events, waiting period conditions and potentially relevant exclusions.

Since then, 2025 was rife with malicious attacks by cyber criminals on the retail sector, with a number of household names including Marks & Spencer, Jaguar Land Rover, Harrods and the Co-op on the front line.

In April 2025, the Co-op found itself the target of a sophisticated, large-scale cyber-attack, reported to have cost it £206 million in lost sales. Alongside the operational impact, the Co-op subsequently reported that the personal data of 6.5 million of its members was stolen during the incident. It was reported to have only had limited insurance cover in place for immediate cyber response, rather than back-end losses.

Similarly, another major UK retailer, Marks & Spencer, was hit by a large-scale cyber incident that suspended its online shopping and disrupted operations over the Easter weekend. Online sales only resumed after 46-days of disruption, causing a reported business interruption loss of £300 million, against which it is said to have received a £100 million insurance payment. Customer data was also stolen.

In August 2025, Jaguar Land Rover ("JLR") was targeted by cyber-criminals, forcing it to shut down its computer networks. Vehicle production was suspended for approximately five weeks across major UK plants, causing losses of £50 million per week. The Cyber Monitoring Centre estimates the UK financial impact of the JLR attack to be in the region of £1.9 billion across 5,000 UK organisations, likely making it the most economically damaging cyber incident ever experienced in the UK, with all financial losses arising from operational disruption. The scale of the incident prompted the UK Government to intervene with a £1.5 billion loan guarantee to help stabilise the company and its supply chain. JLR has since reported that sensitive payroll data for its current and former employees was stolen during the attack, potentially putting thousands of staff at risk of identity fraud. In addition to potential data breach claims that may follow, it remains to be seen whether a potential shareholder action might also be pursued against JLR for its decision not to purchase cyber insurance before the breach.

The attack wave on UK retailers continued in September 2025, with cyber criminals infiltrating the IT system of Harrods, stealing the data of over 400,000 customers.

The takeaways? Each of the attacks likely started with sophisticated social engineering attacks, whereby hackers impersonate employees to deceive internal personnel, into resetting passwords or sharing information. This is a risk that will only increase as AI and deep fakes become more sophisticated and widespread.

The lesson learned? Operational disruption poses the biggest cyber risk for most businesses, far outweighing potential losses caused by data breach incidents. Companies should brace themselves for the increased risk of disruptive attacks on their operations. While some industry experts argue that the UK Government should backstop cyber insurance, guarantees such as those provided to JLR are likely to be few and far between, particularly for SMEs. Companies should therefore ensure that not only is cyber insurance in place, but that they are adequately covered for business interruption losses arising out of operational disruption, alongside immediate incident response costs.

From pandemic to cyber panic: lessons in business interruption

As the scope of business interruption coverage in cyber insurance policies comes into increased focus, so does the operation and impact of any exclusions within policy wordings or other limitations on coverage.

Insurance coverage disputes arising from the Covid-19 pandemic have dominated headlines in England and Wales since 2020, with the court providing helpful authority on the scope and application of business interruption insurance.

Our Policyholder Disputes team has been at the forefront of these disputes.

Composite insurance policies

Where there are multiple entities within a corporate group, a business will likely want its insurance policy to protect each individual subsidiary, as each subsidiary would be subject to different losses. This consideration applies equally to Covid-19 business interruption as it does to cyber risks for corporate groups.

Helpfully for policyholders, on behalf of our client, *Bath Racecourse*[3], the Court of Appeal has now confirmed, within the context of Covid-19 business interruption, that composite policies of insurance entitle each of the insured entities to its own separate limits of indemnity, under one policy document, on the basis that a composite policy is a series of insurance contracts. In practice, this means that where different businesses have suffered substantial losses, multiple limits of indemnity will be available to the individual subsidiary within the corporate group. This is an important clarification for group companies that have suffered substantial business interruption losses, particularly where different subsidiaries may operate warehouses or factories in different locations, with separate insurable interests.

Following the Court of Appeal's judgment, policyholders and their brokers should carefully check the wording of composite policies of insurance to ensure that they continue to provide adequate limits of indemnity for a group of insureds. That might include, for example, the following considerations:

1. the presentation of the risk and the definition of "insured" i.e. whether this encompasses just one entity or whether others in the group are additionally listed as insureds;
2. the description of "sums insured" and whether there is express language in the policy stating that the sums insured are to apply to all insureds, on a per insured basis, or with individual limits; and
3. whether any aggregate limit is said to be shared between group companies.

Another key takeaway from *Bath Racecourse* is whether a claim will be subject to a single deductible or to multiple deductibles. In *Bath Racecourse*, the trigger event was the government action that caused different losses from a single government action. Consequently, there was a single trigger event that formed part of a single loss, and so only one deductible applied. The same principle may well apply in the case of a cyber incident: for example, where malware is installed that systematically releases data and/or deletes files. It might be said here that the trigger event is the single entry of the malware, and the "loss" is the multiple immediate consequences of that singular event. As a result, only one deductible may apply, although this is, of course, fact-dependent. The Court of Appeal has provided similar helpful authority to policyholders on the aggregation of losses in *Sky & Mace v Riverstone*[4], which is addressed in our Construction chapter.

Proximate cause

The concept of proximate cause is also an issue that policyholders may need to get to grips with in the context of a cyber claim.

It is possible that some insurers might seek to suggest that a business is not entitled to be indemnified for losses associated with certain customers if a customer's own production was suspended by the same malware (potentially in reliance on principles set out in *Orient Express v Generali*, where it was held that on a "but for" cause of loss analysis, if the insured would have suffered the same loss anyway, as a result of another cause, then the insured loss is not the proximate cause and is not covered). It is important to note that the Supreme Court overturned the decision in *Orient Express* in the FCA Covid-19 business interruption test case, and that it is therefore irrelevant whether there are concurrent proximate causes of the same losses. The fact that business orders might have been cancelled because a customer's production was suspended by the same malware for example, does not mean the cyber-attack on the insured entity was not a concurrent proximate cause of loss. Assuming there is no exclusion language, insurers should not be able to avoid liability.

3 *Bath Racecourse Company Ltd & Ors v (1) Liberty Mutual Insurance Europe SE (2) Allianz Insurance Plc (3) Aviva Insurance Limited* [2024] EWHC 124 (Comm)

4 *Sky UK Ltd & Anr v Riverstone Managing Agency* [2024] EWCA Civ 1567

Cyber Security and Resilience (Network and Information Systems) Bill

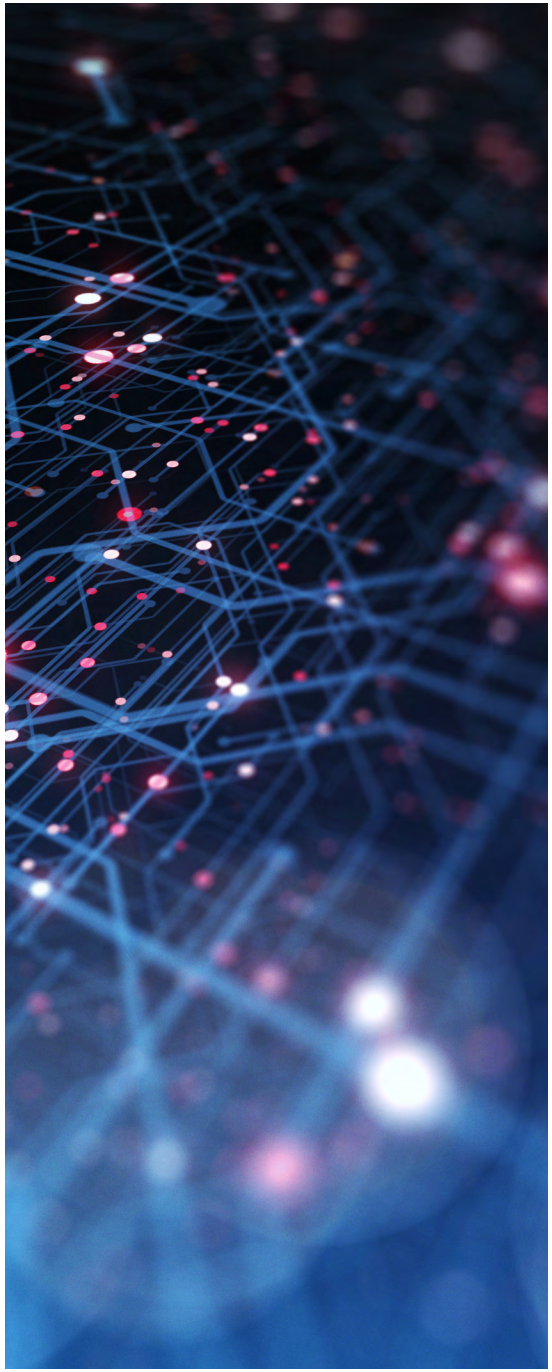
On 12 November 2025, the government introduced the Cyber Security and Resilience (Network and Information Systems) Bill (the "Bill") to the House of Commons[5]. In its explanatory notes, the purpose of the Bill is said to be to update the existing Network and Information Systems Regulations (NIS Regulations) by bringing more entities into their scope and equipping regulators with proportionate powers to better fulfil their duties. This is with the overall objective of better protecting the services and other activities that are essential to the day-to-day functioning of society and the UK economy. In discussing the evolving threat picture and the manner in which the technologies relied upon by essential services are changing, the Bill references the 204 cyber incidents in the year preceding September 2025 that were considered by the National Cyber Security Centre (part of GCHQ) as being "nationally significant – meaning that they had a substantial impact on national security, economic stability, or public safety". State-backed foreign actors targeting the UK are notably referenced, including Iran and Russia and a cyber threat group attributed to the People's Republic of China, some of which are reported to be hiding on critical infrastructure networks.

Against that background, the following are some of the key changes proposed by the Bill:

1. **Relevant Managed Service Providers ("RMSPs")** will be regulated by the Information Commissioner (through the Information Commissioner's Office ("ICO")) and will be subject to the same obligations as other relevant digital service providers, such as search engines, online marketplaces, and cloud systems. The definition of an RMSP is broad and will include medium or large-sized businesses that offer the ongoing management of IT systems to third-party customers.
2. **Data centres** are to be classed as regulated "essential services", which is a fitting and perhaps overdue label given that the Bill itself states that data centres underpin almost all economic activity and innovation in the UK. This was seen first-hand with the Amazon AWS outage in October 2025, which caused disruption to online services nationwide, including HMRC.
3. **Designated Critical Suppliers.** Certain high-impact suppliers, being those whose services must be so critical that any issue could cause significant disruption to essential services, can be classified as Designated Critical Suppliers. Designation will be subject to a high threshold, and, consequently, only a small percentage of suppliers will likely be categorised as such, particularly given that it does not include suppliers regulated elsewhere.
4. **Enhanced regulatory powers.** The Bill will provide enhanced monitoring, information gathering and inspection powers to regulators. It introduces a more prescriptive two-stage reporting structure, requiring in-scope entities to submit an initial notification of a serious incident within 24 hours of first awareness, followed by a full report within 72 hours. The government (the Secretary of State) might also give specific directions to individual entities where it considers such directions to be necessary in the interests of national security. The Bill provides an example of the government requiring the operator of an essential service to take specified action to confirm the presence of a hostile state actor on its network and, if necessary, remediate. A failure to comply with a government direction can be subject to a maximum financial penalty of up to £17 million, or 10% of worldwide turnover, if higher.
5. **Extra-territorial reach.** The Bill extends to the whole of the UK and applies whether the relevant goods or services are supplied from within or from outside the UK. If an RMSP has its principal office outside the UK, then it must nominate a UK representative to the Information Commissioner within three months of the Bill coming into force.

The Bill will likely be relevant to all organisations, given the increasing reliance on service providers. While the Bill remains under consideration, one thing is clear: the UK Government is committed to enhancing the nation's cyber security and cyber resilience in the face of an increasingly threatening landscape.

5 *HC Bill 329*



Held hostage: ransomware in the age of digital exploitation

Throughout 2025, ransomware remained the primary cause of cyber loss, impacting business in the UK.

In January 2025, the UK Government launched a consultation that set out its legislative proposals on ransomware payments, including a ban on ransomware payments by all public sector bodies, including local government, and by owners and operators of critical national infrastructure ("CNI"). The government's motivation is clear: to make UK public entities and essential infrastructure unattractive to ransomware gangs by sending a strong message that they simply will not get paid.

The consultation sets out a three-pronged strategy, including the implementation of:

1. **A targeted ban on ransomware payments for CNI and public sector entities**, with the intention of making it unattractive for cyber criminals to attack those entities.
2. **A ransomware payment prevention regime** that would cover all potential ransomware payments from the UK. In practice, the regime would require a victim to report ransomware to authorities along with their intention to make the payment. On receipt, the UK Government would provide support to discuss "non-payment options" to ascertain whether the payment needed to be blocked, for example, due to UK sanctions. If the conclusion is that the payment does not need to be blocked, then the victim will need to decide whether or not the payment should be made. However, our view remains that this approach will likely face inherent difficulties. The requirement to pay a ransom is often immediate, with losses incurred while payment is outstanding, and the UK Government would need to introduce a targeted rapid-response team to deal with any reports expeditiously, which could be problematic.
3. **A ransomware incident reporting regime** that would be threshold-based. Subject to falling within the threshold, the victim would be required to report a ransom demand, any recovery measures and whether the attacker has been identified.

Ultimately, the broad-brush banning of ransom payments, or mandating reports, is, in our view, unlikely to ensure the safety of organisations. The consultation clearly aims to strike a balance between impactful measures and not creating unreasonable or disproportionate burdens on ordinary individuals and organisations. However, for large incidents, it potentially removes options for speedy remediation that could otherwise reduce significant operational disruption, causing losses (and indemnity payments) to escalate.

There might also be potential difficulties from both a government assessment and a coverage perspective if the ransom wallet is suspected, but not confirmed, to be connected to an individual designated under UK sanctions. Sanctions regimes can evolve rapidly, and the coverage position can become complex, particularly for a global business with a multinational insurance programme. As is clear from *Mamancochet Mining v Aegis*[6], however, it is not simply the case that insurers can refuse to pay a claim in a sweeping reliance upon sanctions. If an insurer wants to rely on a sanctions clause to avoid coverage, it must demonstrate, on the balance of probabilities, that the payment would be prohibited and would breach sanctions, rather than simply expose the insurer to a risk that sanctions would be breached. It is also worth noting here that a sanctions clause simply suspends, rather than extinguishes, an insurer's liability, meaning that the liability revives once the prohibition is lifted.

Overall, it is crucial that businesses continue to focus on developing their cyber resilience, including putting in place any necessary infrastructure and cyber incident response plans. This includes maintaining up-to-date security systems and offline backups, as well as rolling out cyber security defences. In particular, cyber insurance policies typically require multi-factor authentication (MFA) to be implemented across all devices, whether at the employee or executive level. Insureds should be aware of any such policy conditions, and IT teams and employees must work together to ensure compliance. All of that said, even with the best cyber security in place, a business is not immune to loss: 90% of insurance claims involve some form of human error, as demonstrated by the fact that social engineering is being utilised by cyber criminal organisations around the globe.

When data costs: the rising price of privacy breaches

The extent to which cyber insurance policies may indemnify regulatory fines is an issue that is yet to be determined by the court. Throughout 2025, there were astonishing levels of fines issued by the ICO and the Irish supervisory authority, the Data Protection Commission ("DPC"). Between 2018 and 2025, EU data protection authorities issued fines totalling $5.6 billion.

The sheer size of the fines is attracting worldwide attention and criticism. In early 2025, the Trump administration issued an executive order that criticised regulatory fines and other measures the administration viewed as designed to "plunder" US companies. It is notable that a report by the Centre for Data Innovation has suggested that US companies have accounted for 83% of the $5.6 billion in fines issued.

Overall, the magnitude of General Data Protection Regulation (GDPR) fines means that a business potential exposure to regulatory fines could be higher than a ransom request or business interruption losses after a large-scale cyber incident. In 2023, for example, Capita suffered a cyber security incident, following which the ICO proposed a fine of £45 million for GDPR infringements (albeit reduced to £14 million upon submissions from Capita and after it agreed to a voluntary settlement).

The question, therefore, arises as to whether such fines are indemnifiable, an issue that we discussed in detail in The Policyholder Review 2025. As noted there, some London market policies contain exclusions stating that the insurer will not indemnify any civil or regulatory fines, penalties or sanctions that the business is obliged to pay. There remain, however, numerous policies across the market that do explicitly insure civil fines and penalties, subject to the proviso "to the extent insurable by law". Certain insurers have also expressly confirmed they will provide broader wording or cyber liability extensions that indemnify regulatory costs and fines.

Despite that, a number of insurers continue to adopt a sweeping stance that GDPR fines are not insurable for public policy reasons, on the grounds that an insured cannot benefit from their own wrongful act (the *ex turpi causa* principle), arguably rendering explicit coverage for civil fines by a regulatory agency in the context of a cyber policy illusory.

While we continue to await judicial authority from the English courts as to whether regulatory fines are insurable within the context of GDPR fines, we discussed the existing case authorities in detail in The Policyholder Review 2025. In summary, the key question for any policyholder facing issues around the insurability of a GDPR fine is whether the conduct giving rise to the fine should be uninsurable as a matter of public policy. This is, in our view, a question that is highly fact-dependent. The character of the infringement must be reviewed with regard to whether it was negligent, rather than intentional (or reckless, rather than deliberate). The level of the fine issued might also provide some guidance on its considered severity. Arguably, regulatory fines arising from negligent conduct, where there is no turpitude or act of "wickedness", do not engage the public interest in the same way as a deliberate wrongful act. Consequently, policyholders should resist any suggestion by insurers that GDPR fines and similar penalties are uninsurable as a matter of law.

6 *Mamancochet Mining Limited v Aegis Managing Agency Limited and Ors* [2018] EWHC 2643 (Comm)

War risks in a cyber universe

In May 2024, we saw the introduction of Lloyd's second state-backed cyber bulletin (Y5433), which sought to further regulate and refine the scope and extent of cyber coverage written by the market. Additionally, from 1 January 2025, Lloyd's made clear that coverage for state-backed cyber-attacks carried out as part of a conventional war would sit outside the market's standard risk appetite (such that syndicates wishing to write that risk would need to do so with its explicit approval and on a clear and distinct basis, potentially via a separate product).

A year on, where does that leave us? At the time of writing, there are 48 approved versions of Lloyd's cyber war exclusions in circulation, each with different wording and potential issues. Such a lack of standardisation will inevitably lead to uncertainty, and it is an issue that we expect to give rise to coverage disputes.

Attribution

While it is generally straightforward to ascertain whether war was a factual cause of loss in relation to physical loss or property damage (including who the perpetrator was), this question becomes much more complex in the case of a cyber-attack. There is often no formal attribution of a cyber-attack to a government of a state, and investigating and establishing with certainty whether the origin(s) and perpetrator(s) are state-backed is rife with difficulties.

For that reason, the Lloyd's Market Association (LMA) model clauses include a mechanism by which state-backed cyber operations are to be identified primarily on the basis of attribution by another state. Pending any such attribution, insurers are relieved from paying the loss. There are obvious problems with that approach from a coverage perspective.

Generally, it is rare for the victim of a cyber-attack to be able to ascertain with absolute certainty that the perpetrator(s) are state-backed. This is becoming increasingly difficult in circumstances where cyber-criminals are beginning to align with states and there are emerging risks posed by 'state-aligned' adversaries (being non-state backed actors who have expressed a desire to cause a disruptive impact for political reasons). Unless a perpetrator or state expressly states that the cyber-attack can be attributed to a particular state, it will be difficult to prove that cover is triggered. Very rarely are express acknowledgements by states forthcoming, and it may not be unusual for states to manipulate reports of events to suit their own interests at the time of reporting.

Taking the LMA 5564A war exclusion as an example, that exclusion confirms that there is no coverage for loss or damage arising from a cyber operation at the direction or control of a state. In determining attribution to a state, the clause further confirms that "the insured and the insurer will consider such objectively reasonable evidence available to them"; and that evidence may include "formal or official attribution by the government of the state in which the computer system affected by the cyber operation is physically located, to another state". The starting point here is that, as an exclusion clause, the insurer bears the burden of proof.

Commentary by government advisories and industry bodies that suggest a cyber campaign is "most likely" state-linked, would be unlikely to suffice. Even if it could be said that a government had attributed the incident to another state, on the wording of the exclusion, the attribution needs to originate from the government of the state in which the computer system is located physically, to the other state, which would reduce the relevance of commentary by outside administrations, including "tweets". Equally, the policy might define the meaning of a "state" as a "sovereign state", and there may not be consensus as to whether the policy definition of a state is met.

War risks in the English courts

There have been a number of recent case authorities as to the general treatment of war risks in the English courts, including: *University of Exeter v Allianz*[7]; *Hamilton v Afghan Global*[8]; and, perhaps most notably, *AerCap v AIG*[9]. While none of these authorities consider war risks in the context of cyber insurance policies, each is helpful in determining how cyber policies may well be constructed in the event of a cyber-attack.

Firstly, in *University of Exeter v Allianz*, the court determined that the wording "occasioned by war" was equivalent to a test for proximate causation. Consequently, a war that had ended before the property damaged was even built was found to be a concurrent proximate cause of loss. The University of Exeter's entire claim was therefore determined to be excluded on the basis that the relevant policy contained an exclusion for loss occasioned by war, applying the *Wayne Tank* principle. The *Wayne Tank* principle is that where a loss has two concurrent causes and one of them is excluded under the policy, the insurer is not liable for the loss even if the other cause would otherwise be covered.

Similarly, the recent case of *AerCap v AIG*, which is considered in detail in the War and Political Risk chapter provides a helpful examination of political and governmental perils. Unlike *University of Exeter v Allianz*, in *AerCap*, the court rejected arguments of concurrent proximate causation, with Mr Justice Butcher determining that if there were concurrent causes of loss, one of which was an all risks peril and the other a war risks peril, the *Wayne Tank* principle dictated that the exclusion would prevail. That was the case even if it could be demonstrated that each peril operated independently rather than interdependently.

Perhaps most interesting to the consideration of cyber coverage and the issues around attribution is *Hamilton v Afghan Global*. In that case, the claimant reinsurer sought a declaration of non-liability under two reinsurance policies issued to Anham, the owners of a warehouse in Afghanistan. The defendant and Anham had lost possession of the warehouse following seizure by the Taliban. The court was asked to determine, among other issues, whether the exclusion for "loss or damage directly or indirectly caused by a seizure" applied only to a seizure by a "governing authority".

Anham argued that the exclusion only applied to seizure by a "governing authority", which it argued the Taliban was not. The words "by law, order decree or regulation of any governing authority" appeared later in the drafting of the relevant exclusion, and Anham suggested that this therefore qualified the word "seizure". The court rejected this argument. Anham then argued that the meaning of "seizure" should derive its context from the exclusion clause, which included the words "confiscation, nationalisation" etc, which are typically acts of a governing authority. The court also rejected this argument, finding that the exclusion referred to both acts likely to be carried out by a governing authority and those that were not.

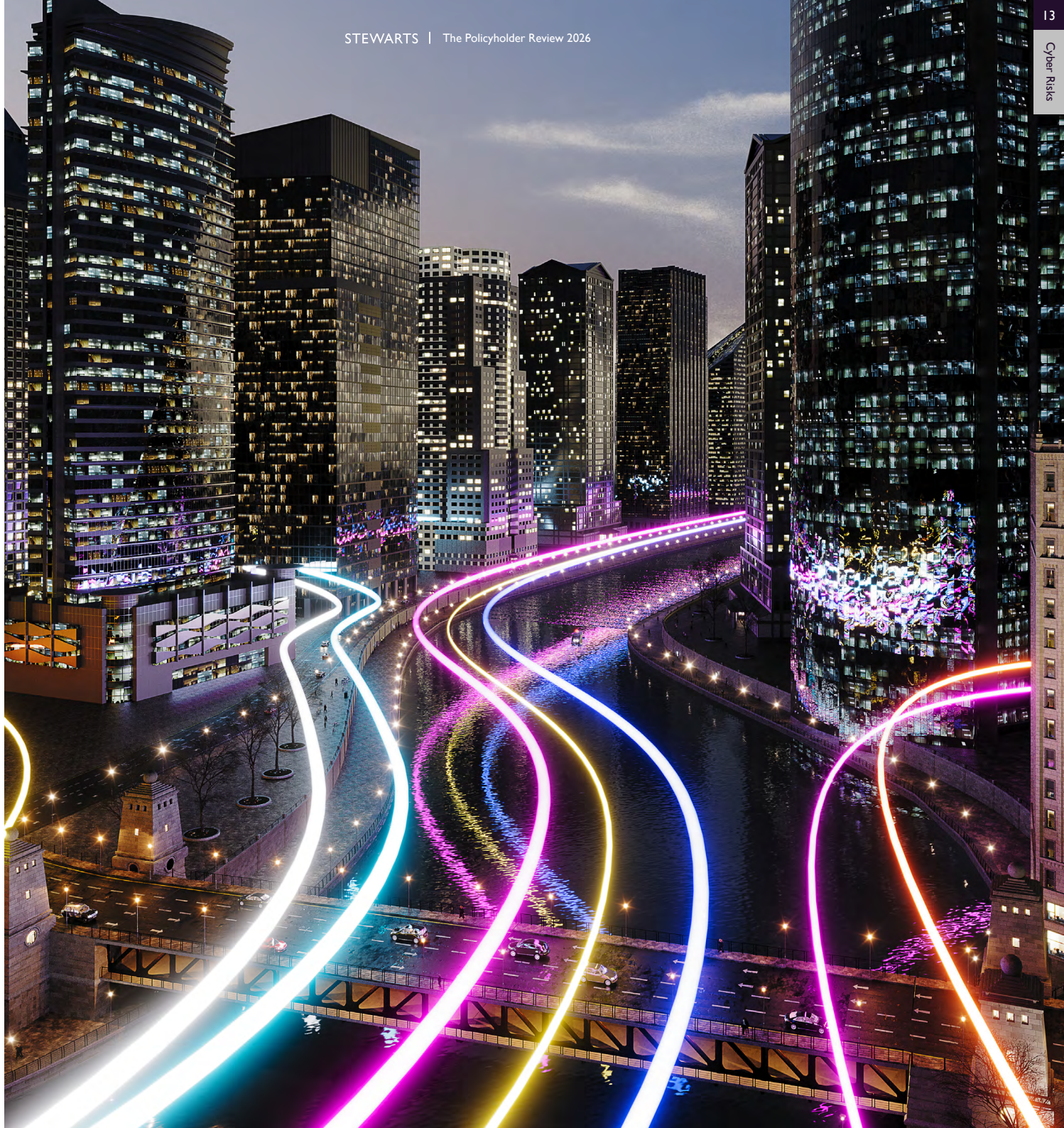
Finally, Anham sought to persuade the court that the exclusion was intended to be limited to acts of a governing authority as a matter of commercial purpose, relying on the distinction found in the market as to the risks insured under political risk policies as opposed to political violence policies. The court held that the recognised market practice was not sufficient to rewrite the terms of the exclusion as drafted, and that the policyholder's interpretation of "seizure" failed. Instead, the word "seizure" was found to have its ordinary meaning and was not limited to acts of a legitimate government or a sovereign power. Reinsurers were therefore granted a declaration of non-liability. Albeit an unwelcome judgment for the policyholder, this case may be relevant in a cyber context when considering what a "governing authority" or "state" is for the purposes of attribution.

7 *University of Exeter v Allianz Insurance Plc* [2023] EWCA Civ 1484
8 *Hamilton Corporate Member Ltd v Afghan Global Insurance Ltd* [2024] EWHC 1426 (Comm)
9 *AerCap Ireland Ltd v AIG Europe SA & Ors* [2025] EWHC 1430 (Comm)

Looking ahead to 2026

It is undoubtedly the case that the lack of standardisation across cyber policies will continue to give rise to coverage issues. While the ABI Lloyd's Cyber Working Group has published guidance aimed at creating a framework for insurers to consider when developing their policy wordings, measures to standardise cyber policies are in their infancy.

Ultimately, cyber coverage remains an emerging line of business, and there is a wide variance of coverage available in the market. Not all policies are created equal, and businesses should continue to review their policies carefully to ensure they are comfortable with the coverage provided, including in relation to the scope and limit(s) of any business interruption coverage. Against a landscape of increasing fines, the policy language around regulatory fines and penalties should also continue to be subject to careful review.



Cyber claims: A broker perspective

Marsh

Marsh's UK Cyber Claims and Incident Management team dealt with around 600 notifications in its 2024 retail and wholesale books, and 2025 appears to be tracking to roughly the same number. However, cyber incidents have undoubtedly received greater media attention this past year.

This is due in part to the high-profile attacks by hacking groups Scattered Spider, UNC6040 and ShinyHunters. Although the UK press focus has been on victims in the UK retail sector, no industry has been immune, and we have seen organisations from the insurance, aviation and manufacturing industries affected. These incidents have once again brought to the fore how vital the "human" defence can be, given the use of social engineering as an initial entry point for these attacks or "hacking the human", as it has been described. Their success in duping IT helpdesk staff into resetting accounts quickly, preying on their eagerness to help the end customer and hit the efficiency metrics against which their service has been measured, has been a key to their success.

Though exploiting human vulnerabilities is not new, these incidents were among the first in which threat actors reached out directly to the UK media to "tell their side" of the incident, undoubtedly in a bid to put pressure on their victims. This successfully stoked the media furore and demonstrates that the motivations of threat actor groups are not solely financial. They are also keen to garner kudos for their exploits, so they can promote their success on dark web forums. Notoriety, it appears, is as much a driver as monetary gain.

Marsh's Claims and Incident Management team have not only been supporting clients through live incidents and the end-to-end claims process but also educating them. This focus on education emphasises the importance of cyber incident preparedness. This ranges from reviewing incident response plans and providing access to Marsh Central (an out-of-band communication platform) to sharing intel through webinars and bulletins on everything we have seen and practical tips to reduce cyber risk.

As a team, though Scattered Spider et al stole the headlines, we have continued to see ransomware events perpetrated by numerous threat actor groups using a more scattergun approach with less thought and focus behind their actions. It remains clear that it is not a matter of "if" but "when" in relation to cyber-attacks, so general cyber resilience and preparedness are vital. With government ministers, the National Cyber Security Centre ("NCSC") and the National Crime Agency ("NCA") writing to FTSE 350 boards last October to remind them of their duty to build cyber resilience, it is clear that inaction is not an option.

Holly Waszak
Head of Cyber Claims
HollyWaszak@marsh.com

Business interruption

Many attacks on organisations impact their ability to continue trading, so business interruption has accounted for a large proportion of the claims we have handled. With so many supply chain disruptions, contingent business interruption coverage has received renewed focus, which can cover losses caused by disruptions at critical suppliers.

As a team, we have worked with numerous insureds to obtain reimbursement for business interruption claims (both direct and contingent). Working alongside our forensic accounting colleagues, we have successfully advocated for interim payments during the adjustment phase to ensure clients have a steady cash flow. With threat actor groups now seeking to cause as much chaos as possible, disruption to organisations and business interruption claims remain a trend we expect to continue in 2026.

Why now is a good time to buy cyber insurance

Despite this backdrop of incidents and claims activity, cyber insurance rates are decreasing across the board, creating a buyer-friendly market. We have seen numerous clients increase their limits this year, with 16% of Marsh clients extending their limits in the first quarter of 2025. With an ever-changing threat landscape, it's crucial to check that cyber coverage reflects the current risk environment. A thorough review of an organisation's policy can help identify any gaps in coverage, ensuring it is protected against a wide range of cyber incidents, including data breaches, ransomware attacks and business interruption.

Meet the team

Aaron Le Marquer

Head of Policyholder Disputes

With over twenty years' experience in insurance law on both the policyholder and insurer side, Aaron is a leading advocate for policyholders in diverse sectors including financial services, hospitality and retail, energy and construction, and sports and entertainment. Known for leading a series of high-profile Covid-19 business interruption test case litigation in recent years, he is experienced in all commercial lines of business, including business interruption, directors and officers, professional liability, cyber, environmental risks, and construction. Aaron spent eight years practising in the Asia Pacific region and is particularly experienced at resolving international and reinsurance disputes, often via arbitration.

Aaron has been ranked as a leading insurance practitioner in the Legal 500, Chambers, and Lexology Index (formerly Who's Who Legal) since 2013. He was named as The Times Lawyer of the Week in 2023, and listed in The Lawyer Hot 100 in 2025.

Aaron Le Marquer
Partner and Head of Policyholder Disputes
T +44 (0)20 7822 8150
E alemarquer@stewartslaw.com

> **Aaron Le Marquer is genuinely outstanding. … A standout name in the market."**
>
> *Legal 500 2026*

Chloe Derrick

Partner

Chloe specialises in insurance coverage and professional negligence. Having previously acted for insurers, she now acts exclusively for businesses and individuals in high-value disputes against the insurance market and the financial and professional services sectors. Chloe has successfully recovered significant funds for clients across insurance lines, and has represented clients in disputes spanning a number of jurisdictions (including the United States, Canada, South Africa, Mauritius, Gibraltar, and countries across the Channel Islands and Europe).

Before joining Stewarts, Chloe advised Lloyd's and London market insurers on their high-profile market loss exposures and drafted policy wordings for existing and new insurance products. Chloe is ranked by both Chambers and Legal 500.

Chloe Derrick
Partner
Policyholder Disputes
T +44 (0)20 7822 8098
E cderrick@stewartslaw.com

> **Chloe is wonderful to work with. She has deep expertise in her specialism and is very personable and conscientious. She is able to explain things in a clear way to non-lawyers and lawyers alike."**
>
> *Chambers 2026*

James Breese

Partner

James is ranked by Chambers and Legal 500 as an 'Up and Coming' and 'Next Generation Partner'. He has represented policyholders in the UK and internationally for eight years, having previously acted on the insurer-side. James uses his knowledge of both sides of the market to strategically advance policyholders' complex insurance disputes.

James' clients range from listed companies, private equity houses, asset managers and multinational enterprises, to high-net-worth individuals and directors of companies. He is regularly instructed to resolve coverage disputes under W&I, D&O, cyber, and investment management insurance policies.

Since 2020, James has also represented policyholders in the leading Covid-19 insurance litigation in the Commercial Court and Court of Appeal. James is widely regarded for his strong business interruption insurance expertise having recovered tens of millions from insurers, including for distressed or insolvent businesses.

James Breese
Partner
Policyholder Disputes
T +44 (0)20 7822 8118
E jbreese@stewartslaw.com

> **James is easy to work with, pragmatic and clear, and he produces great results."**
>
> *Chambers 2026*

Hebe Swain
Senior Associate
Policyholder Disputes
T +44 (0)20 7936 8068
E hswain@stewartslaw.com

Arjun Dhar
Associate
Policyholder Disputes
T +44 (0)20 7903 7993
E adhar@stewartslaw.com

Zara Okereafor
Associate
Policyholder Disputes
T +44 (0)20 7936 8199
E zokereafor@stewartslaw.com

Jesal Parekh
Associate
Policyholder Disputes
T +44 (0)20 7903 7912
E jparekh@stewartslaw.com

Claudia Seeger
Associate
Policyholder Disputes
T +44 (0)20 7903 7908
E cseeger@stewartslaw.com

Sara Palinska
Trainee Solicitor
T +44 (0)20 7903 7987
E spalinska@stewartslaw.com

May Critchfield
Senior Paralegal
Policyholder Disputes
T +44 (0)20 7822 8186
E mcritchfield@stewartslaw.com

Bruno Ponte
Senior Paralegal
Policyholder Disputes
T +44 (0)20 7822 8104
E bponte@stewartslaw.com

Policyholder Disputes at Stewarts

We act exclusively for policyholders in high-value, complex insurance disputes.

Our market-leading Policyholder Disputes team represents businesses in insurance coverage disputes, including cyber, financial and professional risks, construction, business interruption and property losses.

We only represent policyholders in disputes against insurers. Our team has experience acting for local and multinational clients in all sectors, including financial services, entertainment, property, construction, hospitality, retail, logistics, manufacturing, energy and sports.

We do not act for London market insurers, and so are free to pursue claims against the insurance market.

We are one of the largest dedicated policyholder teams in the UK market, and all three of our partners are ranked as leading practitioners in the main legal directories. Our team's cases have been listed in The Lawyer's Top 20 Cases and Top 10 Appeals for the last four years consecutively.

Stewarts is a litigation powerhouse, and we leverage the firm's broader resources where subject matter experts are required, including in tax, insolvency and asset recovery, securities, fraud and employment law. Our combined resources in these areas provide a unique one-stop-shop for insured companies and their directors and officers.

We regularly act in English litigation and arbitration for clients based in overseas jurisdictions with insurance placed through the London market. Our team is experienced in handling disputes with a broad international reach with a particular focus on the US, and Middle East and Asia Pacific regions.

Our firm has unrivalled experience in putting together innovative costs arrangements to help with insurance disputes. The use of third-party funding, after-the-event insurance and risk-sharing fee agreements enables our clients to manage risk and litigate from a position of financial strength.

> **Stewarts' insurance team is one of the leading policyholder teams in the country."**
>
> *Legal 500 2026*

> **Stewarts know how to get the best possible results for their clients. The team are extremely knowledgeable and we have complete trust in their ability to handle the most complex insurance matters."**
>
> *Chambers 2026*

About Stewarts

Stewarts is the UK's largest disputes-only law firm acting in some of the most high-profile and ground-breaking cases.

Specialist expertise

We are widely recognised for our innovative and cutting-edge approach to high-value and complex litigation. Clients instruct us when the stakes are high and where genuine disputes experts are needed.

Our strength and depth rivals that of many disputes teams across the elite UK, US and international firms.

Conflict-free status

As a disputes-only firm, we are conflict-free and uniquely placed to advise where other law firms may be conflicted.

Client service

We get to the core of the dispute at hand as well as our clients' underlying commercial and strategic objectives so that our advice is tailored and holistic.

Our lawyers handle a small number of cases to ensure that they give our clients the care and responsiveness they need to go against the most well-resourced opponents.

Reputation

Our reputation is confirmed by our rankings in the leading legal directories as well as The Times Best Law Firms. We are consistently recognised as a "truly client-focused outfit whose calibre and experience is second to none".

International reach

The great majority of our work is international. As an independent law firm, we are free to work with our clients' existing advisers and can also draw on our strategic alliances with leading international law firms. This enables us to work in a global counsel role to coordinate complex multi-jurisdictional

Depth

We have over 200 lawyers, including 90 partners, and 480 staff across our London and Leeds offices.

Clients

We act for corporates and individuals in high-value and complex disputes in the UK and around the globe.

Practices

We have 15 practice areas across Commercial Disputes, Private Client Disputes and Injury Disputes.

Rankings

All of our practices are highly ranked in the Chambers and Legal 500 guides

Stewarts would like to thank the following for their contributions to The Policyholder Review 2026:

- Howden
- Hemsley Wynne Furlonge Partners Limited
- Lockton
- Marsh
- Solomonic
- Westgate Communications
- Simon Manuel

STEWARTS

London
5 New Street Square
London EC4A 3BF
T +44 (0)20 7822 8000

Leeds
9 Bond Court
Leeds LS1 2JZ
T +44 (0)113 222 0022

stewartslaw.com