The ABI
Together Driving Change

pwc

UK Cyber Insurance Market Assessment

A report produced in association with PwC UK

August 2026

About the PwC UK Corporate Insurance Strategy Team

PwC UK's Corporate Insurance Strategy team helps organisations maximise the value they derive from insurance by providing independent strategic advice across insurance programmes, risk financing, claims and insurance governance. Working across the corporate and public sectors, we support organisations in aligning insurance arrangements with their risk appetite and wider business objectives, helping them strengthen resilience, optimise costs and improve decision-making.

Our expertise spans insurance strategy, broker reviews and tendering, claims management, insurance function/process transformation, use of captives and self-insurance, risk financing, and technology-led insurance and claims. Combining deep commercial insurance expertise with risk, actuarial and data capabilities, we work with clients to ensure insurance is viewed not simply as a mechanism for transferring risk, but as a strategic enabler that supports organisational resilience, protects value and facilitates sustainable growth.

PwC UK is an associate partner of the ABI, reflecting a longstanding relationship and commitment to supporting the UK insurance market. Through this collaboration, PwC UK contributes insights and expertise on key strategic issues affecting insurers and the wider insurance ecosystem.

REPORT AUTHORS

Alpesh Shah
Partner

Martin Murphy
Associate Director

Ross Aveyard
Manager

Amy Shaw
Senior Associate

Contents

Foreword

As our lives and our work become ever more digitised and interconnected, the potential impact of cyber incidents continues to grow. The government has calculated that cyberattacks cost the UK close to £15 billion each year, and the cost to individual companies can escalate to hundreds of millions from just one incident.

Against this backdrop, cyber insurance has never been more important. Over a short period, it has developed from being a limited product, focused on data breach liabilities, into an extensive offering that combines financial protection for a wide range of incidents with a suite of preventative and recovery services. This combination of financial indemnity and ongoing cyber support offers a powerful tool to improve our cyber defences.

Cyber risk evolves rapidly. In response, insurers continue to invest in new products, capabilities and partnerships. Through our assessment with PwC UK, we've found an innovative and competitive cyber insurance market, that is responsive to customer needs. Its ability to adapt and innovate has been a key factor in its development and remains one of its greatest strengths.

Our assessment also underlines the important contribution that cyber insurance can make to the UK's wider cyber resilience. While cyber insurance alone cannot absorb the full burden of systemic cyber risk, the industry can act as an important partner to businesses, government and regulators. Through risk insight, incident response capabilities and incentives for good cyber hygiene, insurers work to reduce the likelihood of incidents, help limit the damage if the worst does happen and support recovery afterwards.

The UK's cyber expertise is also a great commercial opportunity. We are home to a world-leading insurance market, a thriving cybersecurity sector and internationally recognised expertise in risk management and innovation. By bringing these strengths together, the UK can continue to develop cutting-edge solutions to emerging cyber challenges while reinforcing its position as a global leader in cyber risk transfer and resilience.

Looking ahead, the pace of technological change shows no sign of slowing. Frontier artificial intelligence will soon have a transformative impact on cybersecurity – both for defenders and attackers. At the same time, organisations are facing an increasingly volatile geopolitical environment. The cyber risk landscape is becoming more threatening and uncertain than ever.

In this context, strengthening collaboration between industry and policymakers will be essential if the UK is to meet the challenges posed by an increasingly digital world.

Chris Bose
Director of General Insurance Policy
The ABI

Executive Summary

Cyber risk now represents a systemic economic issue for the UK, with 31% of global business CEOs saying their company is "*highly or extremely exposed to the risk of a significant financial loss from cyber threats in the year ahead*"[1]. From a cyber insurance perspective, claims frequency and severity continue to rise, regulatory scrutiny is increasing, and cyber incidents increasingly demonstrate characteristics of aggregation and systemic risk.

Cyber insurance is already delivering significant economic value through increased access to incident response and recovery services and claims payments, although its future role as part of the national cyber resilience landscape is not assured without structural change and its involvement could take many forms. **Structural constraints mean cyber insurance cannot, on its own, act as a national backstop for systemic cyber risk**.

The Current State of the Market

The UK cyber insurance market has matured rapidly in recent years and is now competitive in nature. Policies are often increasingly service-led, rather than solely being a financial indemnity mechanism. The current market structure is clearly segmented:

Small/Medium-sized Enterprise & Mid-market firms largely access standardised, service-focused products via the open market	**Large & Complex** risks are typically placed through bespoke, layered programmes, predominantly in the Lloyd's or wider London market, with a reduced focus on services.

Capacity and appetite are currently at historically high levels following the post-COVID hard market conditions, with broader coverage and softer pricing often available for well-controlled risks. Analysis of Gross Written Premium by sector demonstrates that the mix of organisations and sectors purchasing cyber insurance is evolving at pace.

Based on market reports and publicly available data, a common observation is that claims are increasing in severity and cost:

- Average claim severity has increased significantly in recent years (with ABI data indicating 642% growth in the value of the average claims settlement between 2017-2025).
- Recent claims experience and inflation indicates that claims severity remains an important factor for market monitoring and underwriting discipline
- The threat landscape presents a fast-changing picture, with the causes of loss shifting significantly year-on-year despite the ongoing prevalence of ransomware and malware.
- There is an increasing recent trend in the number of non-malicious claims made.

[1] **PwC**. *29th Global CEO Survey*. 2026.

Innovation

Innovation has helped to start the transition of cyber insurance **from pure risk transfer to continuous risk engagement**, with insurers providing pre-incident monitoring, threat intelligence and incident response coordination. Data-driven underwriting processes and continuous risk assessment are increasingly prevalent. There is increasing adoption of scenario-based and risk quantification modelling to assess the exposure to cyber losses and support the tailoring of policy terms and limit sizes. Non-traditional capital has entered the market via Insurance-Linked Security (ILS) structures, cyber catastrophe bonds and parametric-style instruments.

Key Coverage Gaps and Constraints

Despite its evolution, **the market cannot sustainably insure all cyber risks**:

- SME protection gaps remain significant, with low penetration and at times limited understanding of cyber insurance products.
- Systemic and supply-chain risks (e.g. cloud providers, managed service providers (MSPs) remain structurally underinsured due to aggregation concerns and are fundamentally a key single point of failure in the digital supply-chain).
- Policy wordings in relation to operational technology (OT) and cyber-physical risks do not always reflect operational realities.
- Crime and social engineering losses often fall between cyber and crime policies, particularly for SMEs.
- Bodily injury, infrastructure failure and widespread systemic events (such as war or state-backed activity) are largely excluded to preserve market viability.
- Artificial intelligence is also influencing both the cyber threat landscape and underwriting approaches, increasing the importance of clear policy definitions and coverage boundaries as the technology becomes more widely adopted.
- Policy limit sizes are not always reflecting actual risk exposures.

These gaps do not diminish the role cyber insurance can play in supporting national cyber resilience, but they do underline that insurance cannot, on its own, address the full range of cyber risks facing the economy. Cyber insurance should be considered as an important component within the broader resilience landscape, rather than a complete solution.

Barriers to Adoption

Cyber insurance uptake, particularly in the SME market, remains constrained by the following themes:

- Insufficient understanding and/or awareness of cyber risks, the impact they can have and what cyber insurance can actually deliver in practice.
- Complex and inconsistent policy language and definitions.
- Onerous underwriting data requirements and processes.
- Price sensitivity, particularly for SMEs, as well as the cost of meeting minimum security standards.

As a result, cyber insurance remains under-embedded in supply chains and is **often treated as discretionary rather than a core component of insurance and risk management programmes**.

Strategic Implications for National Cyber Resilience

Cyber insurance already contributes to resilience through:

- Rapid access to specialist incident response and other risk identification and mitigation services, allowing practical support for faster operational recovery following incidents.
- Incentives for enhancing baseline cyber hygiene.
- Financial payments in the event of incidents and claims.

However, its contribution at scale is currently constrained by low penetration, aggregation risk, data gaps and a lack of standardisation. The introduction of the Cyber Security and Resilience Bill creates an opportunity to better align regulation and insurance by:

- Reinforcing minimum cyber standards through underwriting incentives.
- Increasing transparency of cyber incidents and losses.
- Clarifying the boundaries between private risk transfer and state responsibility.

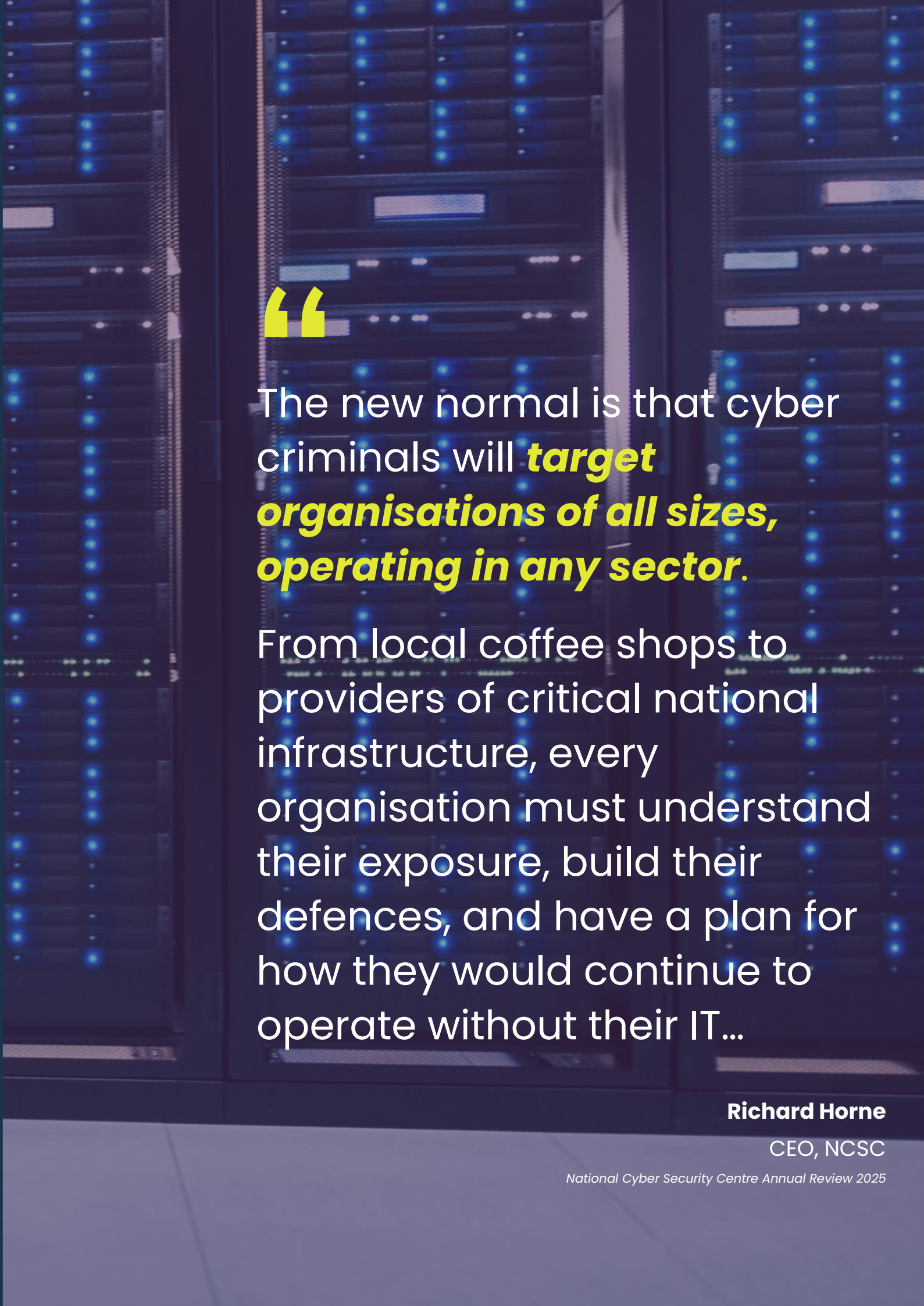
Opportunities and Future Role

To enhance the role of cyber insurance in national cyber resilience, this report identifies several priorities:

1. ***Reduce the protection gap**, particularly for SMEs, through consistent definitions, clearer policy language and improved broker capability.*
2. ***Align cyber insurance with public policy**, such as Cyber Essentials or alternatives, and forthcoming regulatory requirements.*
3. ***Improve data sharing and transparency** to strengthen modelling, aggregation management and evidence-based policy.*
4. ***Support elements of standardisation**, including adoption of consistent cyber event categorisation (e.g. via the Cyber Monitoring Centre).*
5. *Explore the pros and cons of **the spectrum of possible public-private mechanisms**, including potential backstop arrangements, to address low-frequency, high-severity systemic cyber events.*
6. *Continue the **shift in focus towards a risk-prevention-led approach**, focusing on enhancing the preparedness and readiness of policyholders, rewarding organisations that exceed baseline cybersecurity maturity.*

Overall Conclusion

Cyber insurance is an increasingly important component of the UK's cyber resilience ecosystem, offering practical value through incident response, recovery, claim payments and incentives for improved cyber hygiene. Whilst it cannot act as a provider of last resort for systemic cyber risk, **cyber insurance has the potential to play a more significant role in improving the wider cyber resilience across the economy**.



> The new normal is that cyber criminals will ***target organisations of all sizes, operating in any sector***.
>
> From local coffee shops to providers of critical national infrastructure, every organisation must understand their exposure, build their defences, and have a plan for how they would continue to operate without their IT...

Richard Horne

CEO, NCSC

National Cyber Security Centre Annual Review 2025

Introduction & Purpose

Introduction

Cyber risk has continued to become a significant and escalating issue for the UK insurance market and for the economy as a whole. Cyber risk is no longer a niche or emerging exposure for insurers, but a significant driver of claims volatility, aggregation risk and increasing regulatory scrutiny. ABI member data shows that insurers paid nearly £200 million in cyber claims in 2024, representing a 230% increase year on year, with ransomware and malware accounting for over half of all claims.

43%

UK businesses experienced a cyber breach or attack in the past 12 months (2025)[2]

The Department for Science, Innovation & Technology (DSIT) Cyber Security Breaches Survey 2025[2] reported that 43% of UK businesses experienced a cyber breach or attack in the past 12 months, equivalent to 600,000 businesses, with incidence remaining highest among medium (67%) and large (74%) organisations. The survey highlighted an increase in high-impact and disruptive incidents, including those affecting essential services and economic activity. For insurers, this reinforces concerns of shared dependencies and systemic exposure.

Cyber resilience across the UK economy remains inconsistent. Large organisations are more likely to demonstrate Board-level ownership of cyber risk, with formal incident response planning and significant investment in controls, whilst SMEs typically continue to rely on basic cyber hygiene measures and on external and third-party support. Government data shows there is a gradually increasing uptake of cyber insurance for smaller businesses , indicating an increased awareness of the access to expertise and recovery support that a cyber insurance policy facilitates.

At the same time, the regulatory and policy environment is shifting decisively. The Cyber Security and Resilience (Network and Information Systems) Bill represents the most significant expansion of the UK's cyber regulatory framework since the introduction of the Network and Information Systems Regulations (NIS) in 2018. The regulation brings new categories of organisations into scope, including managed service providers, data centres and critical suppliers. The Cyber Security and Resilience Bill strengthens requirements for incident reporting and provides the UK Government with increased powers to respond to emerging and national security-related cyber threats. The intention is to close regulatory gaps, improve visibility of national cyber risk and raise the baseline of resilience across the UK economy.

For the insurance market, this matters on several fronts. More prescriptive cyber regulation is highly likely to influence the behaviour of insurance buyers, minimum risk standards and transparency of losses. Cyber insurance is already delivering demonstrable economic value in supporting recovery and operational continuity following cyber-attacks. Continuing changes in claims experience, regulation and systemic risk considerations are likely to significantly impact how the insurance market contributes to the wider cyber resilience ecosystem. Policymakers increasingly view cyber insurance as part of the wider cyber resilience ecosystem, with a role in supporting prevention, incident response and recovery.

Industry appears to be aligning with this, for example the British Insurance Brokers Association (BIBA) released their 2026 Manifesto in January 2026, with one key "ask" of the Government and industry to "*promote cyber insurance as a key pillar of building cyber resilience*"[3], as well as

[2] **Department for Science, Innovation & Technology.** *Cyber security breaches survey 2025.* 2025

[3] **British Insurance Brokers Association.** *BIBA Manifesto 2026 – Economic Resilience.* 2026

making various commitments to enhance the level of industry training and standardise policy terminology. At the same time, there is growing understanding that commercial, prudential and systemic risk constraints mean the insurance market cannot absorb all cyber risk, or act as a cyber resilience provider of last resort.

Purpose of the Report

The purpose of this report is to provide a structured strategic assessment of the UK cyber insurance market, as well as its current and potential contribution to national cyber resilience.
This report will:

- Provide an assessment of the current structure of the market, its capacity and appetite across the UK insurance market.
- Examine the common features of cyber insurance products available in the market, including common coverage, exclusions and services.
- Identify gaps between policy expectations of cyber insurance and what the market currently provides.
- Explore how cyber insurance products and services contribute to prevention, response and recovery beyond pure risk transfer.
- Explore how regulatory changes, specifically the Cyber Security and Resilience Bill, may shape future demand, underwriting expectations and insurer roles in national cyber resilience.

Scope & Limitations

This report focuses on the current UK cyber insurance market, with explicit differentiation where relevant between ABI members and the wider London Market, and between SMEs and large corporate organisations. It considers market capacity, underwriting appetite, product features, services, exclusions, and claims experience at a strategic level, alongside the interaction between cyber insurance, cyber resilience, and public policy objectives.

The report does not provide legal or clause-by-clause policy interpretation, make claims coverage determinations for specific incidents, or undertake actuarial pricing or capital modelling. Any discussion of policy features or exclusions is intentionally high-level and descriptive.

The analysis draws on a combination of empirical data, industry insight, and informed professional judgement. Where evidence is limited or evolving, particularly in relation to systemic cyber risk and uninsured losses, the report explicitly highlights this uncertainty and avoids definitive conclusions. Given the pace of change in cyber risk, regulation and insurance market practice, findings should be interpreted as directional and contextual rather than static or exhaustive.

Acknowledgements

This report has drawn on input from across the insurance, broking and wider corporate communities. Special thanks are due to Ross Aveyard, Martin Murphy, Amy Shaw and Alpesh Shah from PwC UK's Corporate Insurance Strategy team, and to Chris Bose, Jonathan Fong and Harry Burnham from the ABI General Insurance team, all of whom made valuable contributions to the development of this report. Thanks also go to the ABI member institutions and their stakeholders who agreed to be interviewed, and provided data as part of the research process for this report.

Overview of the UK Cyber Insurance Market

The UK cyber insurance market is no longer a niche segment. Over recent years, it has become increasingly stratified by customer size, distribution channel and underwriting model, with recent growth in the number of participants competing for defined risk bands. This structural segmentation has created diversification, providing improved choice and bringing innovation, but has also reinforced fragmentation in coverage depth, pricing and resilience outcomes.

1. Market Participants & Structure

A segmented market by insured size and complexity

The most fundamental structural segmentation in the UK cyber insurance market is between:

SME and **mid-market** risks**,** typically accessing cyber cover through standardised "off-the-shelf" type products with lower limits and prescriptive cyber security control requirements.

Large corporate and **complex** risks**,** including multinational businesses and those with material operational technology, data aggregation or supply-chain exposures, purchasing bespoke, layered programmes potentially with significantly higher limits and a more tailored coverage structure.

This market bifurcation is visibly reflected in the prevalence of cyber insurance within insurance programmes and in claims experience. The consensus across UK survey data shows that SME and mid-market businesses account for the largest volume of policies and claims notifications[4,5,6], and that whilst large organisations account for a smaller proportion of losses, they experience losses at a far higher severity[4].

SME and mid-market targeted policies increasingly focus on a service-led proposition, enabling access to pre- and post-loss support that is often not a part of the business' formal cybersecurity framework. For these organisations, this service component is arguably more important than the financial indemnity aspect of the policy, as the focus on prevention and rapid recovery is vital. For larger organisations, the service-led component is typically not given the same priority due to a generally more consistent level of cybersecurity maturity and/or existing access to providers of these services.

[4] **Coalition.** *2025 Cyber Claims Report.* 2025
[5] **Department for Science, Innovation & Technology.** *Cyber security breaches survey 2025.* 2025
[6] **Aviva.** *"UK SMEs face rising cyber exposure, but the smallest firms are the least prepared".* 2025

Distinct roles for the Lloyd's Market and UK Open Market

Cyber insurance in the UK is placed through two structurally different mechanisms:

Lloyd's of London	Open Market
A subscription-based market, which remains core to large, complex and multinational cyber placements.	Which dominates SME and mid-market distribution through direct, broker-led and delegated authority placements.

Whilst Lloyd's of London and the open market are distinct structural mechanisms for placing cyber risk, the boundary between them is not absolute in practice. There is overlap between Lloyd's and the open market, where insurers often participate across both channels depending on underwriting strategy, particularly for SME and mid-market business.

This dual structure has enhanced the capability of the market to contribute to national resilience, and the market's own, by spreading a highly volatile and significant area of risk across a number of insurer balance sheets and diversifying the concentration of cyber exposure. This is particularly evident in the subscription market where risks are typically spread across a much greater number of insurers, facilitating confidence that has sustained growth. The two approaches have resulted in different focuses on building resilience. The large subscription placements focus on tailored response frameworks, higher limits and a more in-depth underwriting process, with the open market typically placing reliance on more standardised coverage modules, tighter security prerequisites and lower levels of flexibility in the underwriting process.

Both distribution markets have seen new entrants in recent years (Lloyd's of London adding two new syndicates writing cyber insurance in 2025[7]), with many occupying both distribution channels. The role of the Lloyd's market is clear, with the subscription basis providing a strong mechanism for minimising the impact of significant or systemic events, but only where there is careful management of "silent" aggregation. With an increasing number of syndicates underwriting cyber cover, how insurers gain visibility of market-wide aggregation exposures (particularly when considering the reliance on common reinsurance providers to many new entrants), is fundamental in order for the market itself to be resilient.

Any singular narrative of the insurance market and its role in wider cyber resilience risks oversimplifying the place that it currently has, as reflected by the nature of the two distribution channels. Any regulatory or policy expectations of cyber insurance need to contemplate both aspects of the market in a tailored fashion if the objective is to enhance the market's role in national resilience. This reflects that both channels have the ability to contribute in different ways to different organisations, which is particularly relevant in relation to any introduction of minimum standards or incentives.

Increasing number of participants and competitive intensity

The number of active cyber insurance market participants has increased steadily since 2022, across all distribution lines, in part supported by an increasing confidence in the cyber risk controls established by insurance buyers. There has been a sustained volume of new entrants and re-entrants into the cyber market. This is alongside the expansion of cyber lines by existing participants, such as through the development and introduction of more niche coverage products to address the different ways cyber interfaces with other lines of cover, such as combined cyber/technology errors and omissions products.

[7] **Lloyd's of London.** *Lloyd's Insight Hub.* 2026. (data as of January 2026)

A notable structural development has been the emergence of smaller specialist insurers, often MGAs (managing general agents), backed by substantial balance sheet capacity from established insurers. These specialty insurers have driven the evolution and innovation of the market towards the service-led proposition, with a heavy focus on pre-loss mitigation and risk management services. Leading offerings in the market centre around attack-surface monitoring, threat intelligence and vulnerability monitoring, providing remediation support to policyholders often in a fashion more akin to a cybersecurity company than an insurer.

Competition across both the SME/mid-market and large corporate segments has grown, resulting in a recent softening of market conditions. Underwriting terms have broadened for well-controlled risks, and insurers are increasingly needing to compete on value-add services and risk management support rather than purely on price. Whilst the increased competition is generally driving improved buyer outcomes, which should benefit national resilience in the form of more robust coverage and wider uptake, it also raises the question of longer-term underwriting discipline. If market conditions deteriorate, such as resulting from a systemic event, maintaining underwriting discipline will remain vital as competition increases and products continue to evolve.

Implications for market resilience and policy relevance

Based on the current trajectory and the competitive environment, it is likely that market segmentation will continue to develop, as shown in recent years, as the focus continues to be on creating products that break into the cyber insurance penetration gap. Systemic risk and concentration risk continue to be underlying areas that are not fully understood, and present a significant barrier to the resilience of the market and its ability to contribute to national resilience in the event of major losses.

Market segmentation matters for resilience: cyber insurance provides many of the mechanisms to reinforce organisational resilience. Cyber insurers can play an important role in raising understanding of cyber hygiene by linking underwriting, risk mitigation support and access to services with proportionate expectations in relation to baseline controls. It also brings the question of how public policy, alongside the insurance market, can also drive an increase in the baseline of business cybersecurity controls in a manner that builds systemic resilience against future cyber threats.

The insurance market has the option to provide incentives in relation to cyber hygiene, but its role in reinforcing resilience needs to sit alongside wider regulation. These regulations and policies need to be tailored to the two segments of the insurance market. Progress has been seen with Government-backed schemes such as Cyber Essentials for SMEs. This now includes free insurance cover starting at a limit of £25,000 and includes the option to increase it for a relatively low premium to a limit of up to £250,000, dependent on revenue banding. Whilst this represents a positive move to address the protection gap, the coverage levels in question run the risk of providing false reassurance to businesses who do not understand their exposure, and may quickly find the limit exhausted in the event of a loss.

2. Market Coverage & Appetite

The UK cyber insurance market is currently characterised by historically high levels of available capacity and an increasingly broad underwriting appetite, particularly for well-managed risks. Following several years of hard market conditions where policyholders saw tightening coverage and premium volatility, stabilisation alongside growing capacity is an indication of a maturing market capacity position.

Multiple industry reports[8,9,10] indicate that cyber insurance capacity available to UK insurance buyers is as large as it has been historically, following a period of sustained expansion from 2023-25. A continued level of moderate softening of rates and increased policy limits have been observed throughout 2024-25.

Claims ratios appear to have stabilised following the introduction of more stringent security and data requirements during the hard market, increasing the willingness for insurers to deploy capital into the market.

> "The expanding market cap helps stabilise premium rates despite more claims, enabling insurers to keep premiums competitive and making cyber insurance more accessible to a wider range of businesses
>
> **Gallagher**
> *UK Cyber Market Report 2025*

Emerging capital and alternative risk transfer

In addition to traditional capacity, growth in capacity has been fuelled by an increasing level of non-traditional capital entering the market via Insurance-Linked Security (ILS) structures, cyber catastrophe bonds, captives and parametric-style instruments.

These mechanisms remain nascent, with the availability and quality of the data required to properly assess their viability and sustainability still lacking. Historical data for cyber events is typically less predictive than for other traditional insurance lines, which presents a modelling challenge when compared to a traditional catastrophe peril such as wind. The correlated losses that can result from a single cyber event are also difficult to assess based on the lack of comprehensive data, where rather than traditional factors such as geography, a much greater granularity of data is required to understand exposure (for example at a software vendor level).

Alternative capital remains supplementary, and market signals do not indicate a shift in this position. It is expected that as modelling sophistication, data availability and quality, and standardisation continue to evolve, alternative capital may play an increasingly important role. This could include the use of well-capitalised captives as an alternative risk transfer tool for organisations seeking to retain risk and structure their cyber risk financing approach more efficiently. This could be supported by public policy, in a manner similar to that seen with terrorism insurance products, where there is a clearly defined requirement for an event to be categorised by Government to trigger coverage.

Appetite and coverage

Underwriting appetite is widely regarded as the broadest it has been since the pre-COVID period, with a shift to exposure-led rather than loss-led growth. Insurers are increasingly willing to provide higher primary and excess limits and reduce sub-limits for specific coverages. This expanded appetite is, however, conditional on compliance with minimum cyber hygiene standards, in particular:

- Multi-factor authentication (MFA) deployment
- Immutable backups
- Incident response and recovery planning

[8] **Gallagher.** *UK Cyber Market Report 2025.* 2025
[9] **Howden.** *Rebooting growth.* 2025.
[10] **CyberCube.** *Cyber Predictions Report 2026.* 2026

Notable developments include the selective removal or reduction of sub-limits and coinsurance for specific coverage elements, seen with ransomware and incident response cover. These are both clearly key components in the context of building organisational resilience to cyber events. Despite this, data exfiltration, business interruption and recovery costs continue to be material drivers of loss severity, and markets are reflecting this with coverage amendments as they look to continue control of their exposure.

What is clear, however, is that the market has the most appetite for businesses that meet the minimum control requirements and, vitally, are willing to engage proactively with insurers and brokers. With insurers increasing the range of pre-incident services available, businesses that fully engage with reducing and mitigating risk in partnership with their insurers are best placed to take advantage of the widened appetite of the market.

3. Known Market Gaps & Cover Constraints

Whilst the UK cyber insurance market has matured significantly in underwriting sophistication, discipline and claims handling, there remain structural gaps between the evolving cyber risk landscape and what the market can sustainably insure. Market gaps are most pronounced where risks are systemic or operationally complex in nature.

Limited coverage for systemic supply chain and contingent/customer business interruption

Cyber losses are increasingly arising from key single points of failure within the supply chain, particularly the digital supply chain. This includes managed service providers, cloud platforms and common software dependencies often concentrated within business sectors and organisation sizes. As a result of this, there is a growing trend of cyber events that cascade across multiple insureds, particularly seen in SME and mid-market sectors, where the lack of diversification in supply chain service providers presents an appetising target for threat actors seeking to inflict maximum disruption. They also highlight the importance of cyber risk being understood and owned at Board and C-suite level, particularly where decisions on investment, risk appetite, business continuity and insurance purchasing are closely interconnected.

It is therefore challenging for the insurance market to provide a consistent, meaningful and affordable coverage that addresses this situation, without creating a significant aggregation risk that is difficult to price or reinsure. Contingent or Customer Business Interruption coverage are important means of insuring against supply chains or third-party risks. However, these are typically restricted, sub-limited or excluded, particularly in respect of the rapid integration of cloud-based services within business models.

The scale and aggregation characteristics of major supply-chain events continue to present challenges for insurers in providing broad and affordable cover. Further development of market mechanisms, data and approaches to accumulation management may support future evolution of coverage in this area.

Accommodating manufacturing, industrial and OT environments

Due to the origin of cyber insurance (focusing on data breach type events), policy structures and wordings have typically been IT-centric in scope, often with limited granularity on operational technology (OT) systems, legacy systems and cyber-physical interaction.

Manufacturing, engineering and industrial business are often susceptible to significant impacts from cyber events; digital disruption quickly becomes physical operations disruption. This can be compounded by a common reliance on legacy-type systems and the inappropriateness of many common IT security controls in an OT environment. As a result, an IT-focused cyber insurance policy

that centres on data-type loss drivers often inadequately contemplates the reality of the operational and physical impacts these business face through loss of production, spoilage and contractual penalties.

The lines often blur within these cyber-attacks, where policy definitions typically assume a clear boundary between computer/IT systems and physical operations. Where OT is impacted, however, IT has often played a role as the initial access or within the attack chain, bringing ambiguity and complexity to how the policy applies for the claim. Following a cyber event, quantifying the business interruption costs is often difficult. Layering on the complications brought by cyber-physical coverage ambiguity and policy wordings not always addressing the relevant OT-specific recovery costs (e.g. OT restart and safety processes) only increases this challenge.

Constrained appetite and coverage for OT presents a significant question for the market in its role of supporting national cyber resilience, given the large role of manufacturing/industrial business in the UK economy, paired with its appeal as a target for disruption. Developing policy wordings or new products that adequately define and address the cyber-physical interaction in this environment, and the differing profile of loss drivers, will be necessary to support the resilience of this sector.

SME protection gap

Despite an ever-increasing public profile and greater awareness of cyber risk and its impacts, cyber insurance penetration amongst UK businesses remains relatively low, particularly for SME and mid-market businesses. Many businesses underestimate their exposure, lack confidence in cybersecurity, or view cyber insurance as a particularly complex and/or unaffordable product . In many cases, this is reinforced by limited Board- or owner-level engagement with cyber risk, with it often being viewed as a predominantly technical matter as opposed to a strategic business issue.

For organisations that have not been a victim of a cyber-attack, there is a prevalence of the belief that they are "too small to be targeted", despite claims data demonstrating to the contrary. In the context of national cyber resilience, this segment of the UK economy is one of the most concerning. Balance sheets of SME and even mid-market businesses often do not have the strength to absorb significant losses or prolonged periods of downtime. Whilst the overall quantum of losses in these parts of the market is lower, attack frequency drives concerns. If resilience across this market segment were improved more broadly, there could also be wider benefits for the economy through a form of cyber "herd immunity", whereby stronger baseline resilience across a larger number of firms reduces the overall effectiveness and spread of common attack methods.

The market has made efforts to provide more standardised insurance products that meet the needs of the SME market, resulting in a consistently increased level of uptake, however the gap remains at a size (between 17%[11] and 35%[12] of SMEs purchase a standalone cyber policy) that limits the insurance market's current ability to contribute significantly to national resilience. Closing this gap is relevant not only at the level of individual firm protection, but also because broader improvements in resilience and response capability across SMEs could help reduce aggregate vulnerability across the wider economy. Improving take-up is likely to depend not only on product accessibility and affordability, but also on stronger leadership awareness of cyber risk, so that cyber insurance is considered as part of wider resilience planning rather than as a discretionary purchase.

One possible avenue to improving penetration has been proposed by BIBA within their 2026 Manifesto: an Insurance Premium Tax (IPT) carveout for cyber insurance[13]. However, it is clear that a wider and more substantial effort will be required by the market, and perhaps policymakers, to achieve penetration levels that can support a more resilient economy at a wider scale.

[11] **Department for Science, Innovation & Technology.** *Cyber security breaches survey 2025.* 2025
[12] **Howden.** *The Cyber Security Gap.* 2025
[13] **British Insurance Brokers Association.** *BIBA Manifesto 2026 – Economic Resilience.* 2026

Crime and social engineering cover gaps in multi-vector attacks

Business email compromise (BEC), funds transfer fraud and social engineering continue to represent frequent drivers of volume losses, particularly for SMEs . These types of attack sit at a conflicting intersection between cyber liability insurance and crime insurance, due to the combination of a cyber-enabled attack, but an actual loss derived from theft or fraud. [14]

Cyber policies will commonly include carve-out exclusions for crime, theft of money, loss of funds via intentional/voluntary transfer, and social engineering fraud, despite the fact that many of these attacks rely on attack mechanisms common to other cyber losses. Traditional crime policies were designed to cover the acts of rogue employees, forgeries and physical theft. As the nature of crime has changed, crime policies now often include an exclusion for computer fraud, but also typically require any instructions to a bank for funds transfer to be "unauthorised".

29%

of Business Email Compromise events resulted in Funds Transfer Fraud[14]

Whilst it is possible to obtain affirmative cybercrime coverage extensions to most cyber insurance policies, there is no consistent treatment on this area, with a variety of sub-limiting and carve-out exclusions applied. Within the SME market, there is a general assumption that BEC and social engineering are covered by cyber insurance products, despite this not always being the case. This ambiguity often manifests in an affected business bearing the loss on their balance sheet, to significant detriment. With the proliferation of AI, the barrier to entry for threat actors has never been lower, fuelling a rise in more sophisticated social engineering attacks, broadening this gap.

Sufficiency of limits and underinsurance

The costs of a cyber-attack continue to rise, reflected in claims data that shows a greater increase in severity of losses than frequency. Incident response, legal expenses, forensic investigation costs and recovery services continue to rise in cost, eroding policy limits quicker than ever before.

To "right-size" a cyber insurance policy limit, businesses are either reliant on cyber risk quantification exercises (which are often onerous and complex for SMEs) necessary to model the quantum of possible financial exposure, or on historical benchmarks. Purchasing cyber insurance based on historical patterns is difficult to justify as historical performance and limit adequacy, given the rapidly evolving landscape, are not typically indicative of a forward-looking view.

The significant cost of cyber insurance for many organisations has historically constrained the size of limits being sought in policies. Regardless of market conditions, underinsurance remains a consistent concern, particularly when paired with the low penetration rates. Underinsurance potentially creates a significant problem in the context of resilience, where a portion of UK businesses that has purchased the product are not fully aware of the extent or bounds of their coverage, and risk finding themselves insufficiently indemnified in the event of a cyber loss. In practice, this is a governance issue: where Boards and leadership do not sufficiently understand key cyber exposures, incident scenarios and recovery requirements, insurance purchasing decisions may not reflect the organisation's actual risk profile, risk appetite or needs.

[14] **Coalition.** *2025 Cyber Claims Report.* 2025

Cyber-physical harm and bodily injury ambiguity

Technology continues to evolve at a pace faster than has been seen before, becoming increasingly embedded in everyday life, as well as in business processes. Transport, healthcare and manufacturing have seen the greatest growth in this area, and also present key sector targets for threat actors aiming to cause maximum disruption.

As previously discussed, there are already boundaries in the cyber-physical interaction that present a gap in the context of OT, but the increasing prevalence of technology in areas that could have a propensity to cause physical bodily harm is a further extension of this concern.

Cyber policies typically exclude bodily injury and physical damage. When this is paired with traditional liability and motor policies typically excluding cyber-related losses, this potentially creates a gap in cover with life-critical consequences. A key example of this is the expanding integration of technology into motor vehicles; should a cyber-attack target these modules it is unclear as to how insurance coverage would respond, if at all. Given the limited number of car manufacturers and their technology suppliers, any such attack could have a broad reach and a significant impact.

Inconsistency for SaaS- and cloud-native business models

More and more businesses, both new and old, are starting with or aligning to SaaS- or cloud-native business models. The needs of these organisations often differ greatly to traditional business models, with losses driven by service and system outages, contractual liabilities and a growing level of dependency risk.

Policy wordings on the market vary significantly in how they address system or service outages and interruption, particularly in a shared-responsibility environment. This brings an ambiguity as to the appropriateness of cover for these businesses, and a question as to how this could impact the resilience of the SME sector, where insurance and cyber security maturity is often limited.

Infrastructure exclusions

One point of clear consistency across the market is the incorporation of an infrastructure exclusion. This limits coverage in respect of failures of large-scale, shared or critical infrastructure systems, such as utility services or financial institutions. This clearly presents a constraint for contribution to national resilience, but is considered necessary, reflecting the challenges associated with managing highly aggregated cyber risks.

It is unclear how this position may move following the Cyber Security & Resilience Bill, which brings more businesses into the scope of “critical infrastructure”, such as managed service providers and data centres. A significant infrastructure event affecting these types of organisations could create significant accumulation challenges for the insurance market. The insurance market is not structured to be the financial backstop for significant global infrastructure failure at scale.

Expanding “non-attack” surface

In addition to the wider exposure to system and service failure/outage claims discussed previously, the wider non-attack surface continues to expand with inconsistent clarity on the future of coverage.

Privacy regulation and litigation claims are also on the rise, representing another non-malicious source of claims. With a growing diversity of AI and privacy-related regulation, UK businesses that operate on a global scale have a complex problem to navigate, especially where they hold or handle large volumes of data from key jurisdictions such as the US. Cyber insurance wordings will need to keep pace with this regulatory change, ensuring that coverage language remains appropriate for global businesses.

AI-enabled cyber risk and emerging exclusionary language

Artificial intelligence is becoming increasingly relevant to cyber insurance both as a tool that may be used in cyber attacks and as a technology deployed by insured organisations. In cyber insurance policy terms, the key issue is not simply whether AI is involved in an incident, but whether the loss arises from a recognised cyber peril, such as a security breach, system failure, privacy event (e.g. data loss/theft) or cyber-enabled fraud, or from the performance, output or governance of an AI system itself.

The NCSC has assessed that AI will impact the effectiveness of cyber operations and the cyber threat landscape over the near term, including by increasing the volume and impact of some types of cyber attacks. The NCSC has also highlighted that frontier AI tools can make it easier, faster and cheaper for attackers to discover and exploit weaknesses, while also supporting defensive activity. This reinforces the importance of the cyber hygiene controls already considered by insurers, including vulnerability management, access controls, monitoring, incident response planning and governance of third-party technology dependencies[15].

From a coverage and product perspective, the principal issue is wording clarity. The increasing prevalence of AI creates the need for a distinction between AI-assisted cyber events, and AI-system performance risks. Where AI is used as a tool to commit an otherwise conventional cyber event, such as AI-assisted phishing, deepfake-enabled impersonation, credential compromise, or malware development, existing cyber wordings may respond if the incident falls within the relevant insuring clause. Where the loss arises from the operation of an AI system itself, such as autonomous decisioning, defective chatbot output, model hallucination, algorithmic error, or discrimination, insurers may be more likely to address the exposure through covers such as technology errors and omissions, professional indemnity, or through specific endorsements, sub-limits or exclusions.

This gives rise to the emerging issue of "silent AI": the risk that policies do not expressly state whether AI risks are covered, often having been drafted before the recent acceleration in AI adoption. The issue is analogous to the insurance market's earlier treatment of non-affirmative cyber exposure, where policy language evolved to explicitly define whether cyber risk was intended to be covered or excluded. AI-related exclusionary language is therefore better understood as part of a "market clarification" phase rather than a settled market-wide exclusion standard. Some insurers are beginning to clarify AI-related coverage through affirmative wording, endorsements, sub-limits or exclusions.

For policyholders, the risk is that AI-related losses may fall between cyber, crime, technology errors and omissions, professional indemnity and other liability policies if wordings are not coordinated. For insurers, the risk is that policies may respond to AI-related losses that were not expressly contemplated, underwritten or priced. This makes definitions increasingly important in determining whether an AI-linked loss is covered, limited or excluded.

[15] **National Cyber Security Centre.** *The near-term impact of AI on the cyber threat.* 2024

Products, Services & Exclusions

1. Common Coverage Features

Across the cyber insurance market, policy wordings have begun to demonstrate a convergence around the core first-party (the insured's own losses and costs) and third-party coverages (the insured's liability to others arising from a cyber event). Almost all policies centre around an incident response framework as the foundation of cover:

- Legal expenses
- Forensic Investigation Costs
- Incident response costs
- IT restoration/recovery costs
- Crisis management
- Public relations expenses

First-party indemnity provided by the policy typically focuses on the business interruption component, typically triggered by security breaches, ransomware and system failures. The underlying basis, loss of income and increased costs of working, are consistent across most available policy wordings. Several market options extend business interruption cover to include dependent/contingent business interruption, reflecting the increasing reliance on cloud and outsourced service providers, although this is typically subject to sub-limits and defined waiting periods for coverage to trigger, as well as often being at greater cost.

Cyber extortion and ransomware cover are now standard market features, providing coverage for the ransom payment itself (where legally permissible), as well as negotiation costs. Cybercrime and social engineering coverage components are available, but are less widely included and are often sub-limited, providing coverage for funds transfer fraud, impersonation and invoice manipulation.

Third-party liability cover centres on network security and privacy liability, addressing claims arising from malware transmission, unauthorised access, or misuse of personal data. Naturally, this is typically supplemented by regulatory investigation and defence costs coverage, particularly GDPR and ICO proceedings.

Despite the increasing consistency of core covers, policies are increasingly differentiating themselves through the incorporation of coverage extensions, though there are several common features seen, including coverage for:

- PCI liabilities
- Crisis communication costs
- Criminal rewards funds
- Court attendance compensation

2. Common Exclusions

Policy wordings are featuring a more consistent set of coverage exclusions designed to preserve the boundaries of insurability, particularly in the management of systemic accumulation risk. The most common exclusions seen include:

- War/terrorism/state-linked cyber operations
- Bodily injury
- External infrastructure/utility/telecoms failure
- Property damage
- Betterment
- Sanctions and territorial/jurisdictional restrictions

In alignment with other "financial lines" coverages, cyber insurance policies also typically include exclusions for prior known circumstances, dishonest/fraudulent/criminal acts by employees, and insolvency-related causations. These are typically defined by retroactive dates, and specific conduct triggers.

The market has attempted to manage the cross-class boundaries that cyber often interfaces with, through the common inclusion of contractual liability and professional services/professional indemnity exclusions, as well as intellectual property/patent/trade-secret cover exclusions.

3. Add-on Services & Risk Mitigation

"Add-on services" are now a core aspect of most cyber insurance policies, focussing on incident prevention, containment and the reduction of impact. Consistent features across market wordings include:24/7 notification lines

- IT forensic investigation services
- Legal/regulatory support
- Incident coordination/response
- Customer notification service
- Credit/Identity monitoring

Whilst many of these common services focus on the post-incident response, the market has shown a clear shift towards the incorporation of risk mitigation and preparedness services. Proactive vulnerability identification, threat alerts and remediation advice are all often available without reducing the size of policy limits. Attack-surface monitoring, cyber risk assessments and consulting support are also typically offered either within policy structures or as an at-cost service.

Overall, the shift from a standard indemnity-based product to a service-led enabler and risk-reduction tool makes the product of cyber insurance unique. This presents the opportunity for cyber insurance to become a significant differentiator for UK national cyber resilience, through access to speed, quality and increased certainty as part of incident response and mitigation services.

4. Variation in Definitions

One key component of cyber insurance policies that we have discussed throughout this report is the variability in policy definitions and terminology. Whilst overall policy architecture has converged, the breadth of definitions can significantly impact the scope and cover of available policy wordings.

Across the wordings analysed, core definitions such as "**cyber event**" vary from broad umbrella wording to more restrictive definitions based on specific event types (for example security breach but not system failure). This extends to the aggregation of claims from a single event, where policies contemplate multiple incidents arising from a common origin to varying degrees, fundamentally impacting the appropriateness of coverage limits.

For other core definitions such as **data, systems** or **assets**, we see a continuation of ambiguity. These span from including or excluding software, firmware, backups, digital assets, and third-party hosted environments, significantly impacting the interpretation and appropriateness of products in the increasingly cloud-native, SaaS-enabled business environment.

The definition of **security compromise** differs greatly, with several policy wordings defining a breach as "unauthorised access" only. This definition can enable the repudiation of claims resulting from misuse of authorised credentials, depending on the exact wider wording of the policy.

Privacy breach definitions can range from personal data only, to a "protected data" wording that expands to include confidential commercial information and trade data. Wordings may provide coverage for inadvertent loss or destruction, alongside the standard unauthorised disclosure of data.

Waiting periods typically tied to losses such as system outages follow this pattern of inconsistency, where they can be defined as starting at the moment of interruption, the point of discovery or at the time of notification to the insurer, having a significant impact on the extent to which interruption costs may be recoverable.

5. Barriers to Adoption

From both a qualitative and quantitative perspective, cyber insurance market penetration rates remain constrained. Cyber insurance can only support national resilience if it is widely adopted, correctly understood and operationally usable at the point of a cyber event. Current adoption rates limit the extent to which insurance can act as a stabilising force, particularly for SME and mid-market firms that make up the bulk of the economic supply chain.

The "understanding gap" and the "language problem"

A persistent barrier to adoption is often the limited understanding of what cyber insurance actually provides in practice. Many organisations continue to view cyber insurance narrowly as a post-incident payout, akin to other indemnity policies, rather than as a mechanism to reduce risk and accelerate response and recovery efforts through the access to practical services provided within policies[16].

Survey evidence, from UK Government research[17], indicates that whilst awareness of cyber risk is relatively high amongst businesses, understanding of cyber insurance products is significantly weaker. 28% of SME respondents to the survey cited a "l*ack of knowledge or perceived lack of necessity*" as a reason for not purchasing cyber insurance[18].

[16] **Department for Science, Innovation & Technology.** *Cyber security breaches survey 2025.* 2025
[17] **UK Government & Grant Thornton.** *Insuring Resilience – The State of SME Cyber Insurance.* 2025
[18] **Department for Science, Innovation & Technology.** *Cyber security breaches survey 2025.* 2025

Further compounding this issue is the structural disconnect between insurance and cyber security. Cyber insurance is often procured by finance, procurement or in-house insurance functions, whilst cyber risk responsibility is owned by CISOs, IT leads or external parties. This disconnect only grows in light of the differing terminologies used by both groups when talking about risk: insurance focuses on limits, triggers, exclusions and sub-limits; cybersecurity on threat actors, controls and vulnerabilities. These two communities often struggle to align during the insurance purchasing process, particularly in relation to the completion of technically burdensome insurer questionnaires. This can result in mis-specified coverage and a misunderstanding of what is covered and what is not.

Product variety and lack of standardisation

Unlike other long-established commercial insurance lines where there is a widely understood baseline, cyber insurance policies remain highly diversified despite some recent increased convergence of policy wordings. Policies differ materially in definitions of insured events, treatment of business interruption, inclusion and scope of services, and the application of sub-limits.

Lack of standardisation makes it difficult for buyers to compare products, for brokers to provide consistent advice that ensures a product is appropriate for their client, and for Boards to develop confidence that cyber insurance delivers predictable outcomes.

With too much differentiation, the cover landscape becomes fragmented, meaning application of coverage across a supply chain is uneven and often opaque, making it challenging for the product to have a significant contribution to national cyber resilience. To address this, some element of policy standardisation (for example in relation to common definitions) is necessary, without restricting insurers' ability to provide innovative and differentiated coverage which meets policyholder requirements.

Data and process burden

Cyber underwriting has historically been defined by data-intensive and onerous insurer quotation processes. Whilst reflective of the technical nature of the risk, lengthy and detailed proposal forms have provided an insurmountable barrier for many businesses who lack the expertise and/or time to adequately understand, collate and disclose the required information.

Outsourcing of IT and security functions presents an obstacle, particularly for SME businesses, where organisations often do not control or fully understand the controls that an insurer requires disclosure of. The market has evolved in recent years, with a stronger push towards a more insurer-led approach, with a number of markets integrating vulnerability scanning, attack-surface assessments and other "outside-in" assessment techniques to reduce this burden on insurance buyers. Despite this, reducing the SME penetration gap may still rely on more tiered and proportionate underwriting processes.

Price and perceived affordability

Arguably still the most prominent barrier is one of cost. Approximately 36% of SMEs without cyber insurance cited cost as the primary reason for not purchasing cover19. Price sensitivity is closely linked to the understanding gap. Cyber insurance is often viewed as a complex product with low probabilities of payout. Premiums are often unfavourably compared to more tangible costs within the security budget, sometimes compounded by a lack of experience where a business has not experienced a past cyber event.

[19] **UK Government & Grant Thornton.** *Insuring Resilience – The State of SME Cyber Insurance.* 2025

For SMEs and mid-market businesses, high premiums are combined with the additional investment costs required to meet the qualification criteria for cyber insurance. Whilst improving the posture of organisations directly improves the national resilience position, these requirements can often be seen as too burdensome and deter adoption rather than improve this maturity.

One way of addressing this is to identify ways to help organisations to assess the potential financial impact of a cyber event on their business, as well as the affordability of cyber insurance in light of not only the potential financial indemnity provided by the policy, but also the range of risk reduction/pre-incident and recovery/post-incident services included in the policy. The insurance market more proactively providing transparent, objective data and insights into practical examples of how cyber insurance has aided response and recovery could be a powerful tool.

Innovation & Opportunities

1. Innovation

Service-driven insurance

The widespread services included within cyber insurance policies clearly differentiates it from other lines of insurance cover. With a cyber risk landscape in a constant state of dynamic evolution, insurers have and continue to respond with a move from static risk transfer to continuous risk engagement, bringing together traditional underwriting with areas such as threat monitoring and incident response capabilities.

Data-driven underwriting and continuous risk assessment

The underwriting process for cyber insurance has also evolved with the product structure. A historic reliance on proposal forms and historic loss data is gradually being left behind for a more proactive underwriting approach with the adoption of externally sourced, near-real-time data and signals:

- External attack surface monitoring
- Vulnerability scanning
- Security ratings
- Threat intelligence to inform underwriting posture
- Mid-term risk reviews

Cyber risk is far from static, and the underwriting approach has moved to one that supports earlier intervention as the market recognises the need to reduce event severity and likelihood in order to improve long term market sustainability.

Scenario-based loss modelling and risk quantification

Risk quantification for cyber risk is intrinsically difficult due to the volatile nature and likelihood of events. The market is increasingly adopting scenario-based modelling to assess the potential of cyber losses, with a recent focus on ransomware business interruption, data exfiltration and systemic service outages. Stochastic modelling approaches such as “value-at-risk” models are increasingly being used to quantify exposure by the insurance market, with policyholders also using them at times to make more informed, data-driven decisions on insurance limits and to aid internal communication. Traditional insurance approaches, centred around geography, sector and loss experience, are increasingly deemed as being insufficient for understanding the potential of cyber losses.

Emerging and evolving products

As outlined earlier in this report, the policy wordings available within the market have evolved over time to address new and emerging areas of exposure as the threat landscape changes. Service-driven innovation has been driving pre-incident support, the embedding of incident response, as well as the emergence of more novel cover types such as non-malicious triggers and customer business interruption.

2. Opportunities

Product and distribution simplification

The complexity of cyber insurance products remains a significant barrier to increased uptake. Despite this there is clear opportunity to simplify both how cyber insurance is explained and how it is accessed.

There is a growing recognition across the market that the quality of distribution is now as important as the design of the product itself. Strengthening the capabilities of brokers, through accreditation and training, provides a practical route to improving buyer confidence and decision-making. Better-equipped brokers are more likely to be able to encourage their clients to consider and purchase cyber insurance within their insurance programme, not only as an insurance policy but as part of the wider business resilience conversation.

The development of a clearer, shared terminology on cyber risk presents a further opportunity. Reducing excessive jargon, providing clarity and certainty on core coverage and service concepts, and improving consistency in base policy definitions across the market would lower barriers to entry without undermining underwriting discipline and, importantly, without reducing the ability of cyber insurers to develop and provide a range of differentiated products necessary to meet different policyholder needs.

> “To work with the Lloyd’s Market Association, the ABI and other insurance trade bodies on common terminology and to demystify cyber policy language to encourage greater take-up of cyber insurance.
>
> **British Insurance Brokers Association**
> *BIBA Manifesto 2026 – Annual Objectives*

These steps are necessary in order to continue to reposition cyber insurance from a perceived niche or discretionary product to one that is a core component of a standard commercial insurance programme.

Aligning cyber insurance with regulation

The Cyber Security and Resilience Bill presents a further development in an evolving global regulatory landscape, and an opportunity to better align cyber insurance and the market with public policy objectives on cyber resilience. In this context, alignment should be understood not as insurance replacing regulation, but as ensuring that underwriting expectations, risk assessment approaches and insurance-supported risk improvement activities are more clearly connected to the resilience outcomes that regulation is seeking to promote. Cyber insurance as a product already aligns with many of these objectives in practice. For example, the focus on pre-incident mitigation services and incident response both contribute to helping businesses prevent incidents and return to operations as quickly as possible where incidents do occur. However, the role of cyber insurers in this space is not always visible outside of the market. There is scope to articulate more clearly how insurers’ underwriting standards, control expectations and risk management dialogue with insureds can support wider resilience objectives, helping organisations to prepare for, mitigate, respond to and recover from cyber events, alongside and in alignment with the wider regulatory framework.

Cyber insurance should not, however, become relied upon as a regulatory enforcement tool. Rather, this highlights an opportunity for mutual reinforcement: regulation clearly sets minimum expectations, duties and accountabilities, whilst insurance can reinforce these through underwriting standards that recognise and reward stronger cyber hygiene, governance and resilience measures. This is alongside insurance providing financial protection, operational support and practical incentives, including through differentiated pricing, risk improvement services and broader cover for businesses that meet and exceed the established baseline.

Data sharing and market transparency

The lack of transparency and availability of cyber risk and loss information has been highlighted earlier in this paper, and presents a key opportunity to contribute to the resilience of the market and the wider national resilience agenda. Insurers collectively hold extensive data on incidents, claims, near-misses and loss drivers, although much of this information remains fragmented or inaccessible outside of the individual firms.

There is a clear opportunity for a more structured approach to achieving an aggregated, anonymised data-sharing approach. This has the potential to improve underwriting confidence and the management of accumulation risk, and to better aid public understanding of cyber risk. Enhanced transparency would enable Government and regulators to develop more evidence-based public policy, particularly with growth of systemic and supply chain risk only set to accelerate. For this to be effective in practice, Government would need to clearly articulate the value proposition for insurers if they contribute data to this initiative. This could include how shared insights, improved threat understanding and better-informed resilience policy would flow back to the market, potentially building trust and making the purchase of insurance more desirable for organisations.

Expanding transparency and accessibility of data can only aid the market itself, supporting innovation in modelling. This is particularly the case where substantial progress is required to develop approaches to modelling cyber risk in order to provide further reassurance and confidence in a view of the economy's cyber exposure. Any future data-sharing framework would, however, likely need to rely on anonymised and appropriately aggregated data so that it is sufficiently useful to the wider market, Government and national resilience objectives, without requiring insurers to relinquish the competitive advantage embedded in proprietary firm-level data. In this respect, the objective should not be to eliminate differentiation between insurers, but to enable a shared evidence base on cyber risk and loss trends that strengthens market understanding, supports better public policy, and improves the collective management of cyber risk across the economy.

The interface of public-private cooperation

As cyber events continue to demonstrate characteristics of systemic risk, and the impact they can have across the economy, there is a growing opportunity to formalise the interface between insurers and the Government by addressing the gap between private risk transfer and national resilience. This includes greater scope for cyber insurance to be recognised within the wider resilience landscape as one tool that can support preparedness, response and recovery, alongside regulatory, operational and security measures.

Recent events have demonstrated the ability for a cyber event to generate correlated losses across a number of organisations simultaneously, concentrating risk within an insurer's portfolio through indirect impacts. The way this occurs challenges the traditional insurance assumption of diversification. The Cyber Security and Resilience Bill emphasises the importance being placed on systemic dependencies and the continuity of essential services. There is scope for the insurance market to support this through the provision of the loss data it holds, which could inform any subsequent updates in a data-driven manner. There may also be value in Government and public authorities more clearly and proactively acknowledging and promoting the role that cyber insurance can play as part of broader national resilience, particularly in supporting organisational preparedness, access to incident response capabilities and financial recovery following significant events. There is an opportunity within the current Cyber Essentials framework to do so, where businesses are already taking steps to improve their resilience and build awareness of cyber risks, which may make them more receptive to the consideration of cyber insurance options beyond the complementary cover available upon gaining Cyber Essentials accreditation as part of their resilience toolkit.

The second opportunity is one with no clear current market consensus. In selected other lines of cover which are susceptible to low frequency, high severity events, the Government has recognised that the insurance market cannot sustainably absorb the "tail risk" without the support of a public-private "backstop". The goal of such a backstop has to be clearly articulated, often involving the state not wishing to take an active role in the market, but to enable insurers to participate with increased confidence. In the cyber context, however, this remains a more exploratory consideration than an immediate market priority, given there is currently no established consensus on the role or structure of any potential cyber backstop arrangement.

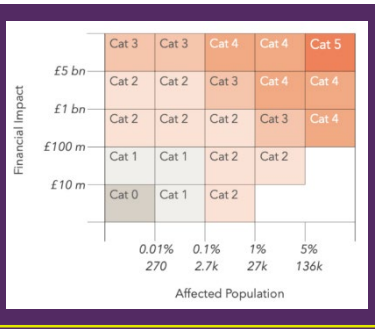
A cyber insurance backstop could look fundamentally different depending on how it is established. It could take the shape of regulation that enables "mutualisation" within the market which allows it to address the need collectively. Alternatively, it could take the form of a structure similar to existing backstops with a more significant role for Government. Any backstop would need a clear framework for event categorisation and established conditions, but could provide significant reassurance to the market and enable competition in a manner that drives uptake. At present, the more immediate opportunity may reside less in the detailed consideration of formal backstop structures, and more in strengthening dialogue between Government and the insurance market on how cyber insurance can support national resilience objectives within the existing market framework. Continued dialogue between Government, regulators and the insurance market may help clarify potential approaches before a significant systemic event occurs.

Developing standard categorisation of cyber events

Whilst cyber insurance displays unique characteristics as a coverage line, one opportunity aligns with a traditional concept from natural catastrophe risk: developing a shared and defined framework for categorising cyber events akin to that for windstorm and earthquake events.

At present, market participants, regulators, Government and the general public often describe similar cyber events using different terminology, classifications and severity thresholds. This fragmentation limits the ability to intuitively understand events, compare losses, assess risk aggregation and communicate clearly with stakeholders.

The development of the Cyber Monitoring Centre (CMC) and the classification system it is developing represents a significant opportunity to address this gap. The CMC is establishing an independent framework to classify cyber incidents based on their severity, impact and systemic relevance, with the explicit aim of supporting a consistent understanding of cyber events for a broad range of stakeholders. The framework provides a more graduated and structured view of cyber events, and inferred consequences, and provides an opportunity for the market to support its development and use.



Cyber Monitoring Centre
Event Categorisation Methodology- "The CMC Scale"

A consistent categorisation methodology also benefits the market through simpler identification of correlated events and accumulation, and improving the taxonomy used for claims data. It would provide a consistent platform to engage with policyholders, regulators and Government, especially with the heightened focus on systemic cyber risk. It also presents the opportunity for further evolution of policy coverage, helping coverage to be more clearly and explicitly tailored to the extent of its impact.

Conclusion

1. Summary

Cyber insurance already makes a tangible, albeit inconsistent, contribution to UK cyber resilience. This contribution extends beyond post-incident financial indemnity into areas of risk mitigation, preparedness and recovery. However, the insurance market's ability to support resilience at a national scale is constrained by relatively low insurance policy uptake, the lack of availability of systemic event capacity, affordability, coverage gaps, data limitations and aggregation risk considerations. Understanding both the value and the limitations of the insurance market's contribution to cyber resilience is essential for setting realistic expectations of the market's role within a wider national cyber resilience framework.

As a product, cyber insurance has evolved into a service-led proposition, and with increasing competition in the market and innovation in offerings. The pace of this evolution has come at a cost, with a lack of consistency and standardisation adversely impacting the uptake of the product, particularly in the SME and mid-market sectors. With its position as Europe's largest cyber insurance market, however, the UK cyber insurance market has the opportunity to continue this evolution in a manner that capitalises on its unique insight into complex threats and risks, and enhances its contribution to national cyber resilience.

2. The Role for Industry to Support National Cyber Resilience

For the insurance market to increase its role in supporting national cyber resilience, **the primary objective is to reduce the protection gap**. Whilst there have been significant efforts by many parts of the market to achieve this, there is substantial progress still to be made. This requires a broader and more transparent level of collaboration within and outside of the insurance market.

As uptake rates continue to grow, there are some clear ways for the market to enhance and define its role in national resilience, alongside public policy:

1. **Aligning underwriting standards with public policy** - The Cyber Security and Resilience Bill highlights the importance of strengthening cyber resilience on a broader scale. Underwriting has driven the creation of general minimum cybersecurity standards, and can continue to evolve by developing proportionate, risk-based control expectations for firms operating in or alongside critical sectors.

2. **Raise the profile of recognised assessment frameworks** - The UK already has a Government-backed framework for promoting baseline cyber hygiene through Cyber Essentials (CE) and Cyber Essentials Plus (CE+). The market is well placed to drive awareness of these and similar frameworks, taking a more active role alongside the NCSC in boosting awareness of cyber risks and options to mitigate this risk, whilst aligning with public policy objectives. More broadly, recognised frameworks such as CE and CE+ can help provide a clearer baseline for cyber hygiene, establish a more consistent language for discussing cyber controls, and support wider understanding of how organisations can improve resilience. As one example of this, the ABI has convened Government and cyber insurers to create good practice guidance on cybersecurity, to increase understanding of what options organisations have to protect themselves based on insights drawn from cyber insurers' data.

3. **Supporting the Cyber Monitoring Centre (CMC)** – There is a clear need for increased elements of standardisation within the market, and the categorisation system created by the CMC provides a strong opportunity. The industry has substantial amounts of loss data that would prove invaluable in supporting the development of classification models and would have a significant positive impact on how public policy is shaped, but also serve the market in creating a consistent method and terminology for defining cyber events.

4. **Improve the quality, transparency, and availability of data** – Enhancing visibility with structured sharing of anonymised UK-focused cyber insights between insurers, public bodies and service providers can only strengthen the contribution to national resilience. Consistent taxonomies and increased visibility with confidentiality safeguards would support a more evidence-led decision-making process grounded in greater understanding of the likelihood and impacts of cyber events for organisations, the market, regulators and policymakers. This would reinforce the role of cyber insurance as a partner for strengthening UK cyber resilience, without relinquishing competitive advantage for individual market participants.

5. **Continue shifting the focus to preparedness** – In the context of national cyber resilience, a risk prevention-led model is key. Widespread adoption of a consistent basic level of controls, increased threat visibility and access to specialist support has the potential to reduce the frequency and severity of cyber incidents. This could also lower the likelihood of disruption cascading through the supply chain. There is an opportunity for the insurance market to more proactively promote and encourage this model, through providing clearer incentives for good cyber hygiene and greater use of services that reduce the likelihood and severity of incidents. Incorporating technical validation of controls, vulnerability identification and support, and ongoing engagement with policyholders can represent a significant shift for many organisations from reactive cyber risk management to a more preventative and informed approach.

Together Driving Change

@PwC_UK
/pwc-uk
pwc.co.uk

@the_abi_uk
/the-abi
abi.org.uk

The ABI In collaboration with **PwC UK**