

CYBER

UK Cyber Market Report

2026



Gallagher

Foreword

The UK cyber insurance market continues to show ample capacity and more transparent underwriting in 2026.

Despite major cyber incidents occurring over the summer period of 2025, especially affecting large retail and manufacturing companies, only a small share of the losses was insured.

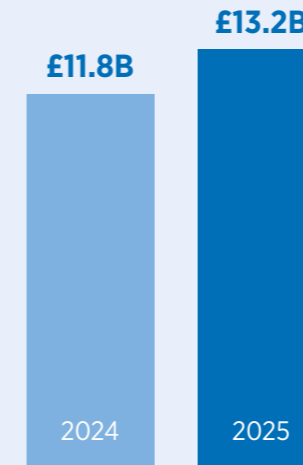
This gap has helped the market retain its capacity and keep prices steady for businesses that provide evidence of their cybersecurity controls. Third-party and supplier oversight is now central to how the market views cyber risk. Businesses are becoming more aware and leveraging advanced technology to continuously monitor their supplier networks for cyber vulnerabilities and to validate their controls in real time.

Insurers are loosening underwriting requirements, especially for small and medium-sized enterprises (SMEs) with turnovers below £50 million. Managing general agents (MGAs) also introduced coverage enhancements for SMEs. These enhancements are expected to continue, with composite markets catching up.

Policy wording improvements provide additional benefits, such as a shift to individual claim limits and introducing a pay-on-behalf model. New extensions are also emerging to address customer-side outages, which proved critical for suppliers last year.

Conditions remain favourable for well-managed risks. Firms that show measured improvement in their controls and practice active oversight are securing broader terms and are better placed if conditions evolve later in the year.

Headlines



+12%

The UK cybersecurity sector showed robust growth in 2025,

with revenue rising from approximately £11.8 billion in 2024 to £13.2 billion in 2025, reflecting a 12% year-on-year increase¹.

Security services are set to dominate the market, with a projected market volume of

\$7.2 billion¹

A 2025 cyber incident at a large automobile manufacturing business caused nearly

£2 billion

(\$2.5 billion) loss to the British economy².

Introduction

Digital operations now run through every part of business, and so do cyber risks.

With rising spend on building resilient systems, the UK cyber insurance market has evolved beyond basic cyber breach response to offer staff training, business interruption planning and practical risk management.

The UK's diverse mix of financial institutions, manufacturers, retailers and technology companies gives its cyber market a unique vantage point on emerging threats and incident patterns. This breadth of exposure is helping insurers strengthen their underwriting insight and adapt coverage to more accurately reflect the realities of modern cyber events and the growing influence of supply chain vulnerabilities.





2026 cyber market trends and growth projections

As we progress through 2026, the cyber insurance market is offering plenty of capacity. For smaller firms, applications are now less cumbersome than they were a year ago. Many insurers have reduced the number of required questions, lowering entry barriers for SMEs, though basic cyber hygiene must be in place. Businesses are encouraged to conduct regular staff training, establish a consistent patch routine and carry out continuous checks on key suppliers to manage risk.

With the proliferation of AI, its influence is evident on both sides of the risk equation. Attackers are now using automated content and voice tooling to scale phishing and vishing. At the same time, as threat actors refine their ability to identify cyber vulnerabilities and breach systems, AI is also helping businesses better prepare themselves for attacks and improve training and post-incident data review.

Supply chain disruptions are also shaping the availability of coverage. In 2025, we saw how losses can fall on suppliers, even though they were not directly breached, especially when a major customer pauses orders. New policy options are now recognising this exposure, alongside broader wordings.

Trends to look out for in 2026

Pricing and capacity

Conditions remain buyer-friendly at the start of the year. That could shift if loss ratios rise or a genuine insured loss cluster emerges.

Product design

Broader wordings are now commonplace (per claim limits, pay on behalf of ransomware, full limit bricking, longer Business Interruption (BI), shorter waits).

Dependency cover

Emerging customer BI extensions help address revenue loss when a customer's outage stops orders.

Operations

Markets are standardising faster claim handling and sharpening vendor panels to reduce time to recovery.

Projected market size for cyber market niches

£2.3 billion

Data protection and encryption

As data breaches continue to increase, businesses in the UK are investing heavily in encryption and secure data storage solutions. The broader security software market, which covers encryption software, is projected to reach £2.3 billion (\$3.18 billion) in 2026, with a growth rate of 19.3%³.

£18 billion

IoT protection

The proliferation of connected devices heightens the importance of IoT protection. The projected revenue from the UK IoT security market reached £18 billion (\$24.10 billion) by the end of 2025⁵.

£156 million

Cloud security

Cloud adoption is accelerating, and UK businesses are increasing their focus on secure storage environments. The cloud security market is expected to experience substantial revenue growth, with projections indicating that it will reach £156 million (\$210.50 million) by 2026⁴.

Emerging technologies and trends driving growth

AI has now become part of day-to-day operations, reshaping both preparation and response.

It is being used to enhance phishing detection measures and accelerate post-incident data scoping for regulators and customers.

Recently, a first-of-its-kind case surfaced when an AI inbox monitoring tool interacted with a phishing link before a user followed it, prompting discussion about how cyber cover should respond. Existing policies do not exclude AI-related mistakes that result in breaches, but specific endorsements are beginning to clarify such anomalies.

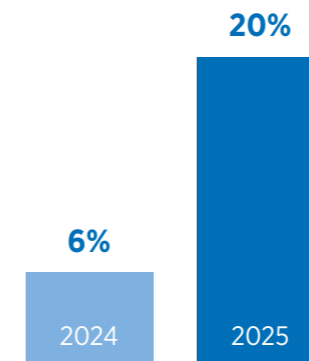
Firms are tracking vulnerabilities more closely and increasing investments in cybersecurity measures such as multi-factor authentication, robust staff training and secure network configurations.

This has led insurers to offer broader terms and, in some cases, support to keep those improvements moving, encouraging more first-time buyers to come to market.





Market growth, challenges and practical fixes



While the market continued to grow through 2025, cyber breaches across supply chains surged, rising from 6% in 2024 to nearly 20% in 2025⁶.

Buyers are responding with practical measures. Contracts with key suppliers now spell out security expectations and the right to timely cooperation and access to logs during an incident.

Insurers are rewarding businesses that can show progress. Companies with strong training and ongoing supplier checks are securing lower premiums and better terms. That's especially helpful for small and mid-sized businesses, who previously struggled to access affordable cyber cover but are now finding it easier to do so through evidence of steady improvement.

Underwriting and controls

Over the past year, policy wordings have evolved to address changing claims requirements. The most significant change is the shift from annual aggregate limits to individual claim limits. Each claim now draws from its own limit, providing mid-market insureds with more consistent protection across multiple events.

Ransomware handling has also changed. Many policies now include settlements in which insurers pay on behalf of the policyholder rather than seeking reimbursement, removing a cash flow hurdle for businesses during a stressful time.

Business interruption coverage now offers longer indemnity periods and quicker response times. Indemnity periods have increased from a maximum of 90 or 180 days to up to 365 days. Waiting periods have shortened, with some policies responding after just 8 hours and covering the entire outage, including the initial hours.

In the mid-market and corporate space, underwriters reward buyers with better premiums that optimise areas, including:

People

Regular training and a no-blame reporting culture reduce dwell time.

Vulnerability management

Visible patch cadence and disciplined remediation.

Third-party oversight

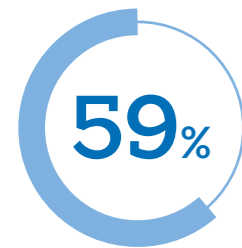
Continuous supplier due diligence, not just onboarding checks.



The evolving claims landscape

Despite more incidents, market conditions remained competitive into early 2026 as the insured share of loss remained small and capacity held.

Ransomware continued to be the main cause of major losses in 2025. Ransomware cases in the UK rose slightly to 52%, up from 48% in 2024,



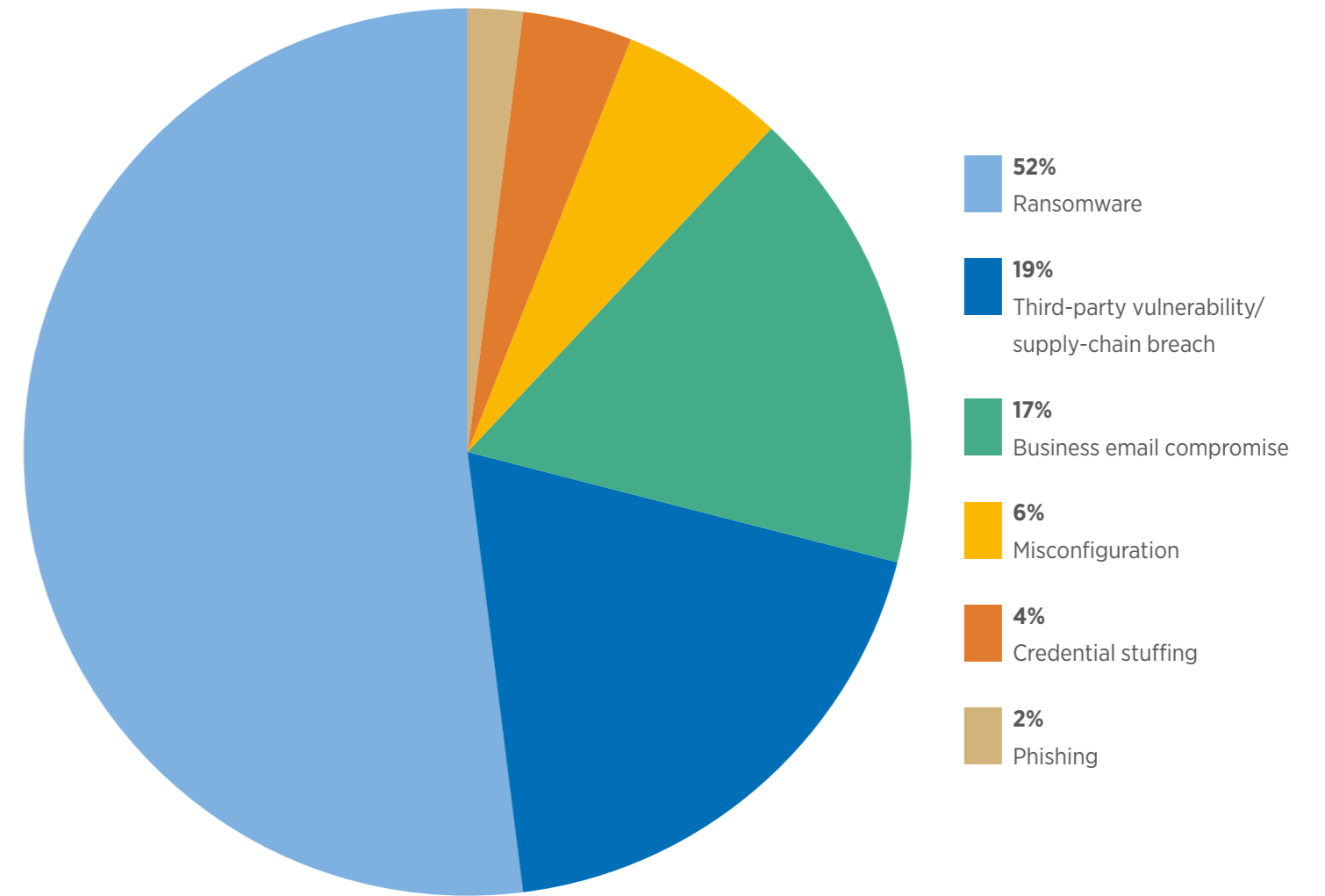
with 59% of these cases involving data exfiltration, highlighting the need to protect data⁶.

Ransom amounts have decreased as threat actors lower their demands. The largest demand observed was approximately £5 million, down from £25 million the previous year. Insurers connected clients to specialist teams, including a team to manage ransomware negotiations quickly, alongside other organisations stress-tested their response plans. As a result, claims were managed more effectively, and the financial impact was reduced.

Manufacturing and retail remained the most targeted sectors. Incidents in factories led insurers to ask more questions about manufacturing control systems, data control measures and how production can continue if systems fail. Targeted attacks on retail in 2025 further reinforced the need for rehearsed responses and clearer communication across large, distributed teams.

Police involvement became more visible than in prior years. The UK law enforcement worked closely with affected businesses to identify the perpetrators. After the attacks on major retail chains, officers set up live group chats with the affected IT teams so businesses could gain insights from firms that were a few hours ahead.

2025 Incident Type



Outlook for the rest of 2026

Demand for coverage is expected to continue to increase through 2026 as businesses become more aware of their Cyber Risk and look to control this. We could see a further increase in this if the frequency of losses rises or a major outage triggers widespread covered claims.

Underwriters will continue to prioritise factors that influence outcomes: they seek evidence of regular staff training, a no-blame reporting culture and ongoing monitoring of key suppliers. As the market expands, insurers can maintain competitive premiums and broaden access to cyber insurance for more businesses.

Threat actors are refining tactics rather than inventing new ones. The late 2025 pattern of online intruders targeting cyber vulnerabilities to break in and sell access to ransomware groups is likely to continue. Short bursts of cyber-attacks should be treated as staging for a second phase that may follow weeks later.

Governance watch

In October 2025, the UK government wrote to FTSE leaders with three concrete asks:

- Make cyber a board-level priority using the Cyber Governance Code of Practice
- Register for the national cyber security centre's (NCSC) Early Warning service
- Establish cyber essentials across your supply chain

These steps serve as immediate actions that build resilience and closely align with what underwriters reward at renewal.

How Gallagher can help

Gallagher provides clients with access to various insurance markets, helping them to secure coverage tailored to their specific needs. We leverage our network and expertise to ensure clients receive effective solutions. Our specialists guide you in implementing robust cybersecurity measures and developing a strategic approach tailored to safeguard your organisation's future.

For better insurance premiums and conditions, Gallagher recommends:

- Staff training and awareness building
- Conducting system vulnerability scans
- Ensuring basic IT hygiene as a safeguard
- Developing a well-defined incident response plan
- Regularly reviewing and updating risk management strategies

If you would like to discuss your organisation's cyber and insurance considerations, our specialists are available to support you.

[CONNECT WITH US](#) →





¹Cyber security sectoral analysis 2025," *GOV.UK*, 10 Mar 2025.

²Jones, David. "Jaguar Land Rover attack cost British economy \$2.5 billion," *Cybersecurity Dive*, 22 Oct 2025.

³"Data Security - United Kingdom," *Statista*, accessed 26 Feb 2026.

⁴"Cloud Security - United Kingdom," *Statista Market Forecast*, accessed 26 Feb 2026.

⁵"Internet of Things - United Kingdom," *Statista*, accessed 26 Feb 2026.

⁶"Insights from our Cyber Team Annual Report 2026," *Pinsent Masons*, accessed 26 Feb 2026. PDF file.

The sole purpose of this report is to provide guidance on the issues covered. This report is not intended to give legal advice, and, accordingly, it should not be relied upon. It should not be regarded as a comprehensive statement of the law and/or market practice in this area. We make no claims as to the completeness or accuracy of the information contained herein or in the links which were live at the date of publication. You should not act upon (or should refrain from acting upon) information in this publication without first seeking specific legal and/or specialist advice. Arthur J. Gallagher Insurance Brokers Limited accepts no liability for any inaccuracy, omission or mistake in this publication, nor will we be responsible for any loss which may be suffered as a result of any person relying on the information contained herein.

AJG.com/uk The Gallagher Way. Since 1927.

Arthur J. Gallagher Insurance Brokers Limited is authorised and regulated by the Financial Conduct Authority. Registered Office: Spectrum Building, 55 Blythswood Street, Glasgow, G2 7AT.
Registered in Scotland. Company Number: SC108909. FP522-2026a Exp. 27.03.2027.

© 2026 Arthur J. Gallagher & Co. | GGBRETUK108084



Gallagher