CYBER

UK Cyber Market Report 2025

Gallagher

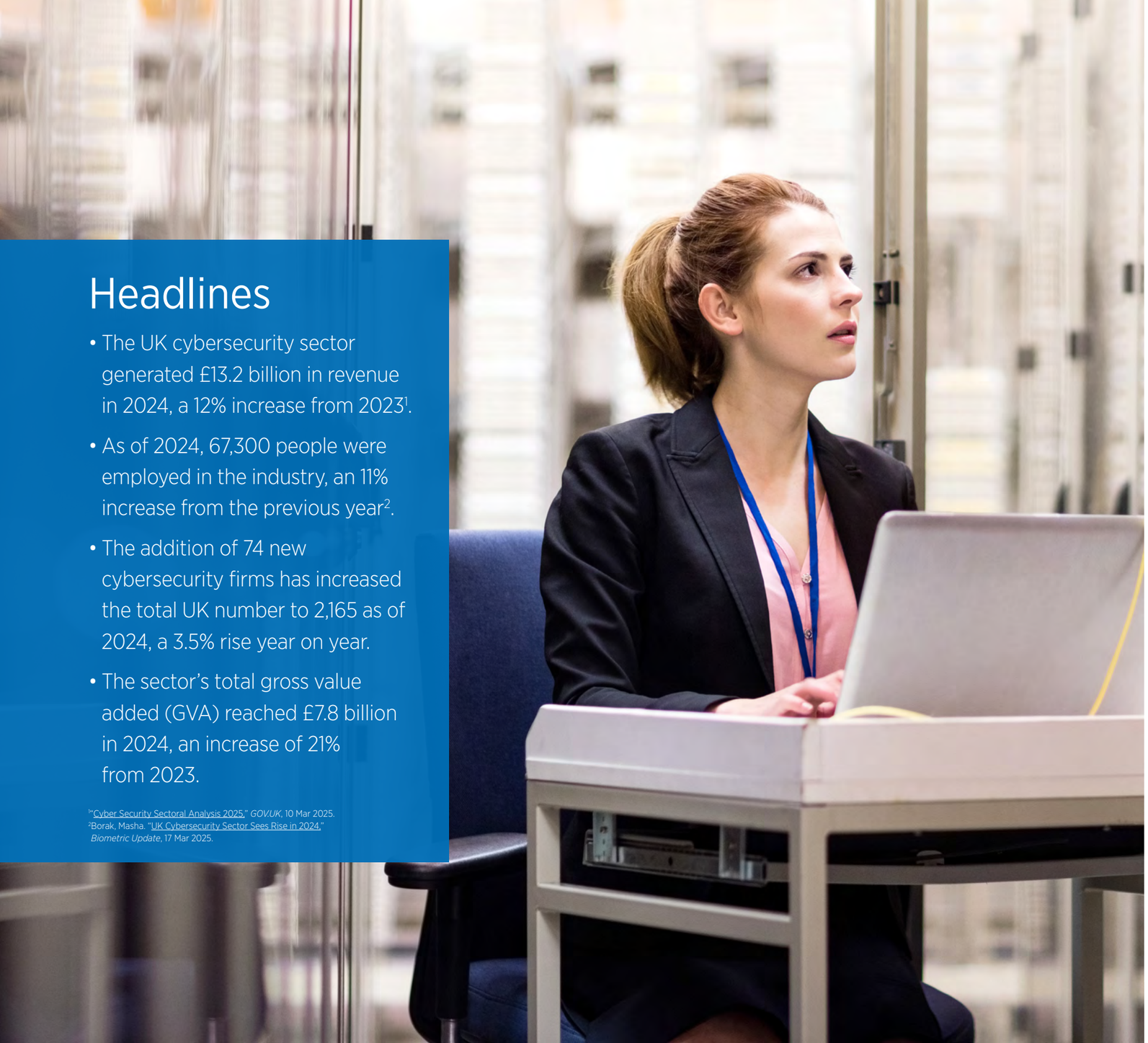
Insurance | Risk Management | Consulting

Foreword

As we progress through 2025, the cyber insurance market continues to experience significant transformation. Prices are decreasing as insurers seek to expand their reach, driven by businesses increasingly implementing security measures to manage and mitigate cyber risks, thereby improving their cybersecurity baseline. This shift has reduced entry barriers. The introduction of advanced technology in risk assessment has streamlined the underwriting process, allowing insurers to scan networks for vulnerabilities and enhance cybersecurity standards. Businesses prioritising robust security measures benefit not only from reduced premiums but broader coverage as well.

However, comprehensive cybersecurity is still in its relative infancy, and businesses are encouraged to stay proactive in enhancing their digital safety. The cyber insurance market presents great opportunities alongside evolving challenges. By leveraging the right strategies, companies can confidently navigate this dynamic landscape. At Gallagher, we are committed to supporting our clients, providing tailored solutions and specialist guidance to mitigate and safeguard operations.

Sam Cheshire
Cyber & Technology Practice Group Managing Director
UK Retail, Gallagher



Headlines

- The UK cybersecurity sector generated £13.2 billion in revenue in 2024, a 12% increase from 2023[1].
- As of 2024, 67,300 people were employed in the industry, an 11% increase from the previous year[2].
- The addition of 74 new cybersecurity firms has increased the total UK number to 2,165 as of 2024, a 3.5% rise year on year.
- The sector's total gross value added (GVA) reached £7.8 billion in 2024, an increase of 21% from 2023.

[1]"Cyber Security Sectoral Analysis 2025," *GOV.UK*, 10 Mar 2025.
[2]Borak, Masha. "UK Cybersecurity Sector Sees Rise in 2024," *Biometric Update*, 17 Mar 2025.

Introduction

The cyber market has rapidly become a critical driver for the global economy amid increasing digitisation and cyber threats.

As companies and governments worldwide invest heavily in cybersecurity measures, the market has expanded to include data protection, threat intelligence, cloud security and Internet of Things (IoT) security. The UK, as a major financial and technological hub, plays a pivotal role in this developing picture, and its cyber market reflects global trends alongside unique regional challenges.

2025 cyber market trends and growth projections

In the first quarter of 2025, the UK cyber market has seen increased demand for advanced cyber insurance products, driven by heightened awareness of cyber risks and regulatory pressures.

Market trends indicate a growing emphasis on data protection, cloud security and increased compliance with regulatory requirements, with businesses seeking tailored solutions to mitigate specific risks.

A notable trend is the ongoing softening of premiums. Following price hikes and stringent underwriting requirements between 2020 and 2023, the market is now more accessible. Insurers are engaging in a broader market, offering more affordable terms, especially for companies who have improved their cybersecurity significantly.

IoT security market to reach

$21.72bn

by end of 2025

Projected market size for cyber market niches

The market is growing fast, with sizeable growth forecast in key niches within the UK cyber market:

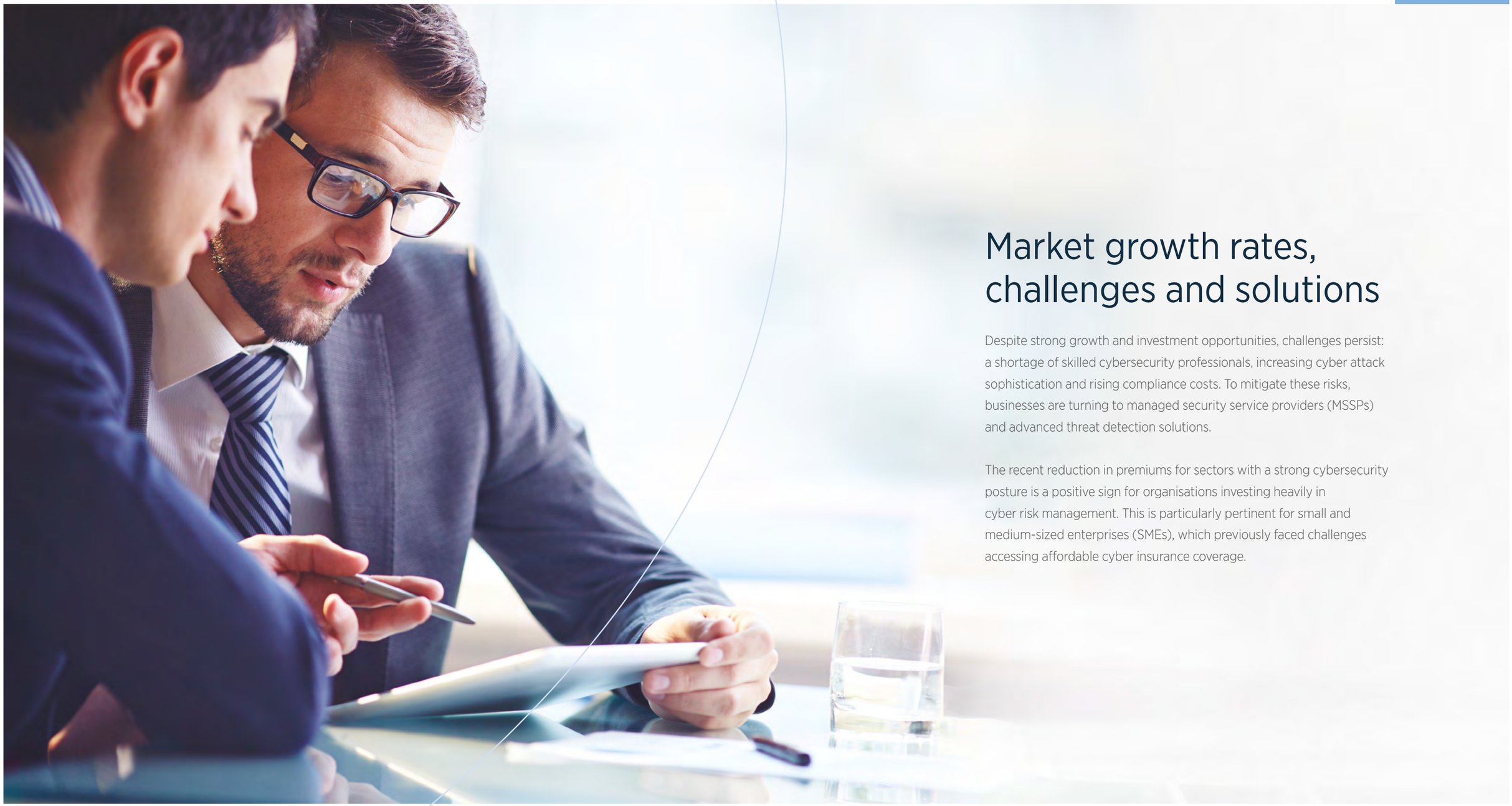
- **Data protection and encryption:** As data breaches continue to increase, businesses in the UK are investing heavily in encryption and secure data storage solutions. The market for data protection services is expected to exceed £2 billion by the end of 2025, with an annual growth rate of 12%[3].
- **Medical devices and healthcare cybersecurity:** With the rise of connected medical devices, healthcare cybersecurity is now a critical concern. GlobalData's latest report indicates that cybersecurity spending in the medical devices sector is set to increase significantly, with a projected growth of 12.9% year-on-year, rising from $631.2 million to $1.2 billion between 2022 and 2027[4].
- **Cloud security:** As cloud adoption accelerates, UK businesses are increasing their focus on secure storage environments. The cloud security market, currently valued at $163.39 million in 2025[5], is projected to reach a revenue of $3,781 million by 2030[6].
- **IoT protection:** The proliferation of connected devices heightens the importance of IoT protection. The UK IoT security market is forecast to reach $21.72 billion by the end of 2025[7].

[3] "UK Cyber Security Sectoral Analysis 2025," *Ipsos*, Mar 2025. PDF file.
[4] "Healthcare's Growing Reliance on Tech Demands Robust Cybersecurity Measures," *GlobalData*, 26 Jul 2024.
[5] "Cloud Security - United Kingdom," *Statista*, accessed 07 May 2025.
[6] "UK Cloud Security Market Size & Outlook, 2023-2030," *Horizon Grand View Research*, accessed 11 Apr 2025.
[7] "Internet of Things - United Kingdom," *Statista*, accessed 11 Apr 2025.

Emerging technologies and trends driving growth

Cloud-native security solutions are gaining traction as businesses migrate to the cloud. Artificial Intelligence (AI) and Machine Learning (ML) are being utilised in the detection of anomalous behaviour and the prevention of cyber attacks, while blockchain is enhancing data integrity and fraud prevention.

The cyber insurance market is becoming more adaptable as insurers leverage advanced technologies to enhance their risk assessments, offer dynamic pricing and provide customised coverage options. Data-driven underwriting tools and risk-scanning technologies are enabling insurers to streamline the quoting process and offer highly competitive premiums. This is particularly the case for organisations with investments in cybersecurity measures like multi-factor authentication, robust staff training and secure network configurations.



Market growth rates, challenges and solutions

Despite strong growth and investment opportunities, challenges persist: a shortage of skilled cybersecurity professionals, increasing cyber attack sophistication and rising compliance costs. To mitigate these risks, businesses are turning to managed security service providers (MSSPs) and advanced threat detection solutions.

The recent reduction in premiums for sectors with a strong cybersecurity posture is a positive sign for organisations investing heavily in cyber risk management. This is particularly pertinent for small and medium-sized enterprises (SMEs), which previously faced challenges accessing affordable cyber insurance coverage.

The evolving claims landscape

The cyber claims landscape has experienced a moderate increase, reflecting the growing sophistication and proliferation of cyber threats. Ransomware and distributed denial of service (DDoS) attacks remain prevalent. The Pinsent Masons report, 'Insights from our Cyber Team Annual Report 2025,' reveals that ransomware was the most common type of incident managed by their cyber specialists in 2024, with ransom demands varying between $40,000 and $70 million. Only 25% of Pinsent Mason clients elected to pay the ransom, all of whom held cyber insurance[8].

From ransomware incidents leading to substantial financial losses to operational disruptions, the range of ransom demands has broadened, highlighting the unpredictable nature of such attacks.

[8] "Insights From Our Cyber Team Annual Report 2025," *Pinsent Masons*, accessed 11 Apr 2025.

Social engineering attacks are also rising; these include tactics like phishing, pretexting and baiting, and are becoming increasingly sophisticated. Additionally, other tactics such as vishing (voice phishing), smishing (SMS phishing) and whaling (targeting high-profile individuals) are also becoming more common. These methods exploit human psychology and cognitive biases, making them highly effective tactics and tough to defend against.

Law enforcement plays a crucial role in tackling cybercrime but faces significant challenges due to the global interconnectedness of the digital world. Jurisdictional issues, the rapid evolution of technology and the overwhelming volume of digital data complicate efforts to address these threats. Legal and technical constraints further hinder access to critical information. Meanwhile, supply chain risks have escalated, as demonstrated by attacks on sectors like healthcare, retail and defence, highlighting vulnerabilities from third-party partnerships.

Cyber insurance has become increasingly crucial in mitigating financial losses from ransomware attacks. And keeping abreast of the evolving cyber regulatory landscape across various jurisdictions is also crucial for businesses to both ensure compliance and strengthen their cybersecurity preparedness.

2024 Incident type

10% Ransomware
2% Misdirected communications
2% Active directory attack
4% Application fraud
26% Attempted or potential compromise
4% Business email compromise
2% Credential stuffing
2% Third-party incident
48% Malicious access

IoT security market to reach

$21.72bn

by end of 2025

Coverage impact

Scope of coverage

The scope of cyber insurance can vary widely, covering data breaches, business interruption and cyber extortion. However, coverage for cyber warfare risks remains limited, highlighting the need for clear communication between clients and brokers regarding policy breadth.

Renewals and clarity

The rate at which businesses renew their cyber insurance policies is increasing as they recognise the ongoing importance of maintaining comprehensive coverage. However, this trend is nuanced and influenced by sector-specific risk profiles and the level of cybersecurity integration by clients. These factors play a crucial role in determining whether insurers can offer competitive premiums.

‘The rate at which businesses renew their cyber insurance policies is increasing as they recognise the ongoing importance of maintaining comprehensive coverage.’

Future forecasts

The UK cyber insurance market is set to grow through 2025 and beyond, fuelled by increasing demand for protection against escalating threats. This growth is expected to continue with a softening trend due to intensified competition, especially from new entrants targeting the underserved SME sector. 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.

Integrating innovative technologies and data-driven underwriting approaches is anticipated to improve accessibility, making it easier for businesses to obtain coverage. However, the market remains susceptible to disruptions from major global cyber events which could significantly alter pricing and coverage dynamics.

Future development relies on the collaborative efforts of key stakeholders, including insurance carriers, reinsurance providers, brokers, cybersecurity vendors and regulators. Cooperation is crucial in addressing emerging threats and ensuring the market's steady evolution. Understanding and analysing the behaviour of threat actor groups is pivotal in the development of effective defence mechanisms and improving cybersecurity strategies.

The increasing rates for cyber reinsurance underscore the critical need for substantial investment in this area to effectively mitigate risks, while the current market position reflects a strong foundation for future expansion.

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 the most effective solutions. Our dedicated team of cyber insurance and risk management specialists work closely with organisations to identify and address their unique risks, guiding them through the complexities of the cyber insurance landscape, securing the necessary coverage for business protection.

1. **Staff training and awareness:**
Conduct regular training sessions and phishing simulations to enhance employee awareness and preparedness against cyber threats.

2. **System vulnerability scans:**
Perform vulnerability scans regularly to identify and address outdated or vulnerable software, preventing potential security breaches.

3. **Maintain basic IT hygiene:**
Implement multi-factor authentication and ensure reliable data backups to safeguard against data loss.

4. **Develop a well-defined incident response plan:**
Create a comprehensive response plan for cyber attacks, clearly defining roles and responsibilities to ensure quick and effective action during incidents.

5. **Regular review and update:**
Review and update risk management strategies to adapt to evolving threats, engaging with experts to refine and enhance practices.

AJG.com/UK **The Gallagher Way.** Since 1927.

Gallagher

Insurance | Risk Management | Consulting