2026 Cyber-insurance

Market Outlook

After a period of price hikes and stricter underwriting from 2020 to 2023, the cyber-insurance market has softened since 2024, with this trend set to continue. According to risk management company Marsh, cyber-insurance rates declined by 11% in the third quarter of 2025. Softening conditions stem from several factors. Data-driven underwriting practices are enabling insurers to access exposures more precisely, and policyholders are adopting stronger cyber-hygiene measures. Together, these aspects have helped stabilise loss ratios, despite the rising severity of cyber-attacks. Increased competition and expanded capacity, particularly from new entrants targeting small and medium-sized enterprises (SMEs), have further contributed to favourable buying conditions.

However, several large-scale cyber-attacks in 2025, including those targeting Marks & Spencer, Jaguar Land Rover and the Co-op, could reduce insurers' appetite for risk. Additionally, various market developments could prompt a return to unpredictable claims patterns and threaten ongoing stabilisation.

Developments and Trends to Watch

Artificial Intelligence (AI) Exposures

Cyber-criminals are increasingly exploiting AI to conduct sophisticated social engineering campaigns and automate infiltration tactics, enabling malicious attacks with unprecedented speed and scale. Within minutes, threat actors can generate convincing phishing emails, fraudulent websites or deepfake videos that closely mimic legitimate businesses. For example, UK Finance reported that almost £100 million was lost to investment scams in the first half of 2025, with many of these scams being fueled by AI-driven deepfake videos. As AI threats grow, insurers may redefine policy language to clarify how cover applies, particularly for losses from social engineering. In contrast, they may broaden cover for organisations that incorporate AI-powered threat detection into their cyber-security frameworks. Therefore, AI is poised to be both an asset and a risk in 2026.

Ransomware Risks

Ransomware attacks have been a leading claims driver across the cyber-insurance market for much of the past decade, causing significant losses across various sectors. According to research by insurance and reinsurance group QBE, the number of ransomware victims publicly named on leak sites is projected to rise by 40% by the end of 2026. Notably, adversaries are increasingly targeting SMEs within supply chains as gateways into larger organisations. Ransomware losses could leave SMEs with claims that exceed their insurance cover limits, resulting in significant out-of-pocket expenses.

Skills Shortages

According to the government's 2025 Cyber Security Breaches Survey, 49% of businesses and 59% of charities lack basic cyber skills, such as setting up firewalls, data management and malware detection. Advanced skills—such as penetration testing and malicious code analysis—are also lacking in 30% of businesses and 29% of charities. If left unaddressed, these gaps could increase the likelihood of cyber-breaches in 2026. Additionally, premiums could rise for organisations unable to demonstrate adequate cyber-resilience.

Regulatory Concerns

Compliance will be a significant concern for organisations in the coming year. The Cyber Security and Resilience Bill is expected to be enacted in 2026, expanding on the existing Network and Information Systems regulations and imposing stricter incident-reporting requirements. Alongside regulatory penalties, organisations that fail to comply with evolving legislation may face higher insurance premiums or reduced capacity as insurers reassess their risk appetite.

Tips for Insurance Buyers

- Adopt a zero-trust approach by subjecting network requests to strict access controls. Maintain isolated backups, establish a cyber incident response plan and conduct regular recovery drills to minimise damages in the event of a breach.
- Work with an insurance professional to examine policy terms and conditions, especially regarding how social engineering scams and ransomware attacks are defined and covered.
- Upskill IT teams to address skills gaps and implement robust employee training to help staff proactively spot cyber-security concerns. Consider managed security service providers or consultants to bridge gaps in penetration testing, malware analysis and other advanced capabilities.
- Consult insurance and legal professionals to determine regulatory exposures. Vet third-party vendors and their cyber-security practices before entering a partnership to reduce supply chain risk.

MACKAY
Corporate Insurance Brokers