FOIL
FORUM OF INSURANCE LAWYERS

Informing Progress - Shaping the Future

FOIL Update 27th October 2025

How UK Insurers are Responding to the Escalating Risk of Cyber Attacks

At a time when digital infrastructure supports every aspect of business and society, the threat of cyber attacks is intensifying and has become one of the most significant and persistent risks facing the UK. The National Cyber Security Centre (NCSC) reported assisting with 429 attacks between September 2024 and August 2025, with 204 of these categorised as 'nationally significant'. Of this number, 18 were seen to pose a 'highly significant' threat to central government, critical public services, a large number of the population or to the UK economy.

The scale, frequency and sophistication of cyber incidents are increasing rapidly, with national institutions and organisations of all sizes exposed to significant disruption and financial loss from ransomware, data breaches and other forms of attack. For insurers, this presents both a challenge and an opportunity: on one hand, growing exposure to systemic and correlated risks that test the limits of traditional models and on the other, growing demand for innovative cyber coverages.

The Growing Scale and Sophistication of Cyber Threats

Cyber attacks have evolved into a sophisticated, well-funded and often international enterprise and are no longer isolated incidents or perpetuated by opportunistic hackers. Recent large-scale incidents have demonstrated both the financial and operational damage such attacks can inflict.

High-profile UK organisations across multiple sectors have experienced major disruptions, including some of the UK's most prominent brands. Jaguar Land Rover is estimated to have lost up to £50 million per week due to operations being shutdown following a significant attack on its IT systems. The incident has inflicted substantial operational, financial and reputational damage.

Marks & Spencer and the Co-op both suffered major breaches in April 2025, with the Cyber Monitoring Centre (CMC) estimating the ransomware attacks caused combined financial damage of up to £440 million in lost revenues.

While the automotive and retail sectors have been in the spotlight, the aviation industry faces an accelerated threat landscape, with navigation systems, aerospace manufacturers and suppliers all exposed to attacks involving ransomware, credential theft or unauthorised access. Industry statistics from global technology leader Thales indicate a 600% year-on-year increase in ransomware attacks between January 2024 and April 2025 within the sector.

Cybercrime is estimated to cost the UK economy more than £27 billion annually, a figure projected to rise sharply given that the UK, as one of the most digitised economies, is particularly exposed. The most recent government data indicates that 43% of UK businesses experienced a cybersecurity breach in the last 12 months, with this data increasing dramatically for medium-sized and large organisations, which reported 70% and 74%, respectively.

The Expanding Cost of Cyber Incidents

The frequency of cyber incidents continues to grow, but their impact has also deepened. Modern attacks typically combine data theft, encryption and extortion, magnifying both direct financial losses and reputational damage. IBM’s UK edition of its 2025 Cost of a Data Breach Report puts the average cost of a cyber breach for a large UK organisation at £3.8 million. This figure drops to £3.1 million for firms extensively using AI and automation.

Ransomware remains the most disruptive form of attack, with threat actors shifting to more strategic campaigns that extend beyond IT infrastructure to target operational technology and industrial control systems. Even when no ransom is paid, the cost of rebuilding systems, restoring data and re-establishing trust can be substantial.

Data breaches and phishing attacks also continue to grow. The Information Commissioner’s Office (ICO) reports a steady stream of notifications of personal data breaches, with approximately 80% attributable to human error. For regulated industries such as finance, healthcare and utilities, the implications of regulatory violations are particularly severe under the UK GDPR and the Network and Information Systems (NIS) Regulations. Critical national infrastructure and aviation industries carry an extra safety and security dimension, as compromised systems can endanger lives or disrupt essential services.

Beyond direct losses, cyber attacks can trigger significant secondary effects, such as a dip in share price, downgrading of credit ratings and strained contractual relationships. The

complexity of modern supply chains means an attack on one firm is an attack on many. Companies like Jaguar Land Rover sit at the tip of a supply chain that involves multiple companies, some big and some very small. For the smaller ones, who may depend on a single customer like Jaguar Land Rover, the consequences can be devastating.

A Challenge for Insurers

Unlike traditional risks such as fire or theft, cyber incidents can occur simultaneously across thousands of organisations through a shared vulnerability. It therefore presents insurers with a complex and evolving challenge and one with the potential for systemic losses that could rival those of natural catastrophes.

Insurers need to therefore balance the growing demand for cyber coverage with practical underwriting and risk accumulation management. The UK cyber insurance market has grown rapidly in the past five years, recording a CAGR of 16% and gross written premiums estimated to exceed £600 million.

However, profitability has been volatile, and several global insurers have adjusted pricing or coverage terms in response to the rising frequency and severity of claims. Retail insureds, for example, face possible premium increases of as much as 10% following losses from high-profile cyber incidents.

Some insurers have narrowed their coverage by introducing exclusions due to the growing threat of state-sponsored or war-related cyber attacks, reflecting concerns about establishing who is responsible and the potential for escalating tensions between nations. Others are refining existing policy wording to clarify what constitutes a cyber attack or to limit liability for systemic outages caused by failures at large-scale service providers.

Insurers are also investing in data analytics, threat intelligence and cyber modelling to drive improvements in pricing accuracy and portfolio management. Integrating advanced hazard, exposure, and vulnerability data helps to quantify exposures under specific attack scenarios and inform decision-making.

Insurers' Response

Traditional indemnification remains central to the proposition, but many UK insurers are progressively emphasising prevention and resilience, recognising that cyber risk relates as much to preparedness as it does recovery. This is leading to carriers developing their role from passive risk transfer to active risk management.

- **Proactive Approach**

  Insurers now require policyholders to meet minimum cybersecurity standards before coverage is granted or renewed. Stronger IT security, response and recovery plans, incident response teams, redundancy, and staff training are typical examples. Some

insurers provide diagnostic tools or risk audits as part of the underwriting process to support clients in benchmarking their defences against industry standards.

- **Incident Response and Crisis Support**

  Modern cyber policies typically include 24/7 access to a network of response specialists following a breach, meeting the costs of forensic investigation, crisis communications, system restoration, and legal counsel to direct regulatory notifications and compliance. This integrated approach can help organisations restore operations faster to limit financial and reputational harm.

- **Collaboration and Intelligence Sharing**

  The UK insurance industry works closely with the National Cyber Security Centre (NCSC), the London Market Group, and other government agencies to enhance the sharing of intelligence and threat awareness. Collaborative initiatives such as the Cyber Defence Alliance and the CyberAcuView consortium coordinate anonymised claims data from the sector to build insights on attack methods, sector vulnerabilities and loss patterns that can improve defence strategies.

- **Policy Innovation**

  Insurers are extending policy structures beyond traditional areas of indemnity, with emerging products extending coverage to areas including reputational rehabilitation, system restoration, and contingent business interruption. Some are exploring parametric models to simplify claims and reduce uncertainty, enabling payouts to be initiated automatically based on measurable cyber events.

- **Promoting National Cyber Resilience**

  At a systemic level, insurers are being viewed as stakeholders in the UK's cyber resilience ecosystem and through their underwriting standards and data insights, they influence corporate behaviour and investment. Industry groups have called for greater alignment between insurers, regulators, and government to develop a coherent framework that encourages both innovation and practicality in cyber insurance.

Future Outlook

The threat landscape will continue to evolve as technologies expand the attack surface, making cyber attacks an unavoidable feature of the modern economy. Deepfakes, synthetic identities, and automated phishing campaigns powered by generative AI are already testing defences, while geopolitical tensions and state-linked cyber operations increase the likelihood of large-scale, multi-sector disruptions. The question for many businesses is no longer if they will be targeted, but when.

Insurers have a key role in helping organisations manage, mitigate, and recover from incidents and face the challenge of keeping pace with these developments while maintaining a sustainable market. Pricing has to reflect the growing risk, but if excessive, it could push smaller firms out of coverage and leave a protection gap that undermines national resilience.

To address this, a public-private partnership will be vital; preliminary discussions have taken place on whether a form of government-backed cyber backstop may be needed for catastrophic events, similar to Pool Re for terrorism. Regardless, cyber resilience must now be treated as core to operational risk management, with investment in prevention, rapid response and ongoing security now essential. The FOIL working group focused on cyber liabilities meets regularly to share insights into the latest trends impacting the sector, and continues to work closely with other industry bodies such as the ABI, the LMA, the IUA and all its members' clients on this issue.