Browne Jacobson

Exploring the impact of recent attacks on UK retailers and the future of cyber insurance

30 May 2025 Felicity Pallas

In light of the recent high profile cyberattacks on Marks & Spencer (M&S), Co-op and Harrods in this update we take a look at other recent cyber events and the significant vulnerabilities within the sector.

These recent attacks have cast a spotlight on significant vulnerabilities within the sector, igniting a broad discussion on cybersecurity preparedness. These incidents have disrupted operations and raised concerns about the protection of customer data and the financial stability of the companies involved.

M&S

The cyberattack on M&S was particularly severe, leading to substantial operational disruption and exposure of sensitive customer data. M&S has taken steps to tighten security, particularly around remote access protocols. This breach has led to a substantial financial impact, with M&S's market capitalisation dropping by approximately £1.3 billion. In response, M&S is preparing a cyber insurance claim that could reportedly reach up to £100 million to cover losses including reduced online sales and data breach liabilities.

Co-op

Following the detection of hacking attempts, Co-op took preventive measures by shutting down parts of its IT systems. This action primarily affected back-office functions and call centre operations, but customer-facing services continued without disruption. Co-op's response highlights the importance of swift action and the challenges of balancing security with operational continuity.

Harrods

Harrods also reported a cyberattack but managed to maintain normal operations in its flagship and other stores, as well as its online presence. The company took immediate action by restricting internet access at its sites to protect its systems. This incident underscores the need for rapid response mechanisms and the potential effectiveness of immediate containment measures

The National Cyber Security Centre's response

Richard Horne, Chief Executive of the National Cyber Security Centre (NCSC), has termed these incidents a "wake-up call" for the industry.

The NCSC is actively working with the affected companies to analyse the nature of these attacks and to provide expert advice to help protect the wider sector. The recent attacks are expected to increase demand for cyber insurance and lead insurers to reassess their coverage strategies. Despite a recent softening in the market due to increased capacity and a decrease in claims, these incidents underline the potential financial impacts and may contribute to a hardening of market conditions. The cyber threat landscape is undergoing significant transformations, marked by an increase in the complexity and frequency of attacks.

In response, the insurance industry is evolving to meet these new challenges. One such example of this is that Markel Insurance have introduced a pioneering cyber insurance product designed to cover up to US$5 million per risk for indirect losses caused by acts of war, filling a critical gap in traditional policies that often exclude such losses.

The Cyber Monitoring Centre's response

Furthermore, the Cyber Monitoring Centre's (CMC) newly developed cyber risk categorisation framework represents a significant advancement in the cyber insurance industry. Designed to address the complexities of quantifying cyber risks, the framework introduces a five-level severity scale that measures the economic impact of cyber incidents. This scale ranges from £100 million for category one events to over £5 billion for category five events, providing a clear and structured way to assess the financial implications of cyberattacks. Each level of the CMC's categorisation comes with a detailed event report that is made freely available, enhancing transparency and providing insurers with a robust basis for underwriting decisions, risk modelling, and policy pricing.

The framework not only benefits insurers but also serves as a valuable benchmark for businesses, guiding them in aligning their cybersecurity measures with the industry best practices reflected in insurers' policy requirements.

The landscape is also being shaped by regulatory changes aimed at enhancing cyber resilience, notably the UK's consideration of legislation to ban ransom payments for critical infrastructure and the Cyber Security and Resilience Bill.

What does this mean for insurers?

The 2024 Marsh UK Cyber Insurance Claims Trends Report highlighted a year fraught with cyber risk challenges, particularly from ransomware attacks which have shown both volatility and increased sophistication. The recent cyberattacks on prominent UK retailers such as M&S, Co-op, and Harrods have brought significant vulnerabilities in the retail sector to light, emphasizing the urgent need for robust cybersecurity measures and comprehensive cyber insurance coverage. These incidents have disrupted operations, compromised sensitive customer data, and led to substantial financial impacts, highlighting the sector's need for enhanced resilience against cyber threats.

For insurers, these events underscore the complexities of assessing and underwriting cyber risks. They necessitate a reassessment of coverage strategies to better accommodate the evolving nature of cyber threats, particularly as the demand for cyber insurance increases. Innovations such as Markel's new policy and the CMC's new risk categorisation framework, are critical developments.

The effectiveness of these innovations depends on their widespread adoption across the industry and the completeness of the data provided by participating companies. Insurers must collaborate closely with businesses, cybersecurity experts, and government agencies to continuously refine their approaches to cyber risk management. This collaboration is essential not only for addressing current threats but also for preparing for future challenges in an increasingly digital world.

‹ Previous
The Word, May 2025

Next ›
How accurate are your IPIDs?

Contents

AI hallucinations cover launched in first wave of new insurance products for AI →

PFAS exclusions: Are your exclusions robust enough? →

The FCA proposes removal of mandatory CPD hours for insurance sector →

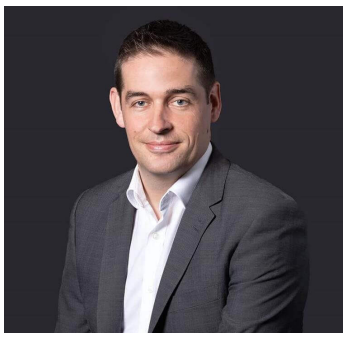
Author

Felicity Pallas

Paralegal

felicity.pallas@brownejacobson.com

+44 (0)330 045 1173



Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

Services

Cyber liability and data security insurance

Financial services and insurance advisory

Policy drafting and distribution