National Insurance Alliance Limited

10th June, 2025

Navigating the Impact of State-Sponsored Cyber Attacks on the Insurance Industry

The proliferation of Cybercrime-as-a-Service platforms has made it easier for criminals to launch ransomware attacks, with artificial intelligence (AI) further amplifying the scale and sophistication of these threats. In addition to ransomware, scams such as Business Email Compromise (BEC) and Business Communication Compromise (BCC) continue to deceive individuals to extract money or sensitive information. Meanwhile, vulnerabilities in supply chains remain a critical point of weakness for both infrastructure and economies.

Recent High-Profile Attacks in the UK

The real-world consequences of cyberattacks are increasingly evident, particularly in the UK, where major retail brands have become targets. Notable incidents include suspected cyberattacks on Marks & Spencer (M&S), Harrods, and the Co-op. The M&S incident, which appears to be ransomware-related, resulted in a nearly £700 million drop in market value and disrupted essential operations such as online ordering and contactless payments. The outage lasted almost two weeks and could lead to insurance claims worth tens of millions in lost online revenue. Other retailers including JD Sports, Currys, and Morrisons, have also experienced breaches or operational disruptions due to cyberattacks.

Impact on the UK Cyber Insurance Market

These attacks are reshaping the UK's cyber insurance landscape. Retailers are likely to see premium hikes of up to 10%, and insurers are expected to impose stricter evaluations of policyholders' cybersecurity measures. In some cases, insurers may become reluctant to provide coverage to high-risk sectors like retail. Although cyber insurance premiums had eased during 2023 and 2024, the recent wave of attacks is anticipated to spark a trend reversal, with upward pressure on pricing across various industries, including healthcare, education, and transport.

Global Market Growth and Ongoing Protection Gaps

Globally, the cyber insurance market is reaching a more mature and resilient phase, with the capacity to absorb large-scale threats such as malware outbreaks or cloud service disruptions. In 2024, global cyber premiums reached approximately USD 15.3 billion, with North America leading in market share. Analysts forecast that this figure will more than double by 2030. Despite this growth, a wide protection gap persists, especially among small and medium-sized enterprises (SMEs), which often lack both sufficient coverage and robust cybersecurity measures. These smaller companies are frequently targeted due to their vulnerabilities, making them attractive to cybercriminals. Closing this protection gap remains a priority for leading insurers such as Munich RE, which emphasises the importance of risk assessment and adequate controls before underwriting.

Emerging Risks and Industry Response

Bearing in mind the recent high profile cyber attacks in the UK, several broader developments are expected to shape the cyber insurance sector. The use of AI by threat actors is becoming a major concern, as it enables more efficient, scalable attacks, including automated phishing and advanced malware creation. These AI-enhanced threats could lead

to more frequent insurance claims, particularly in areas like business interruption and data recovery. While current cyber insurance typically covers AI-driven attack damages, newer risks such as AI model manipulation or liability from faulty AI outputs are not always included. On the defensive side, AI is being adopted to bolster cyber defenses and improve threat detection. Additionally, geopolitical tensions are fueling state-backed cyber campaigns, often targeting critical infrastructure. The rise of AI-powered misinformation and disinformation campaigns also poses significant threats to both corporations and society.

Conclusion: Strengthening Cyber Resilience

In response to these growing challenges, insurers are evolving their offerings to include added-value services such as threat monitoring and cyber risk assessments.

There is a growing awareness among businesses about the need for proactive incident response planning and enhanced technical safeguards. Insurers are also investing in advanced analytics and strategic partnerships to better manage complex risks and reduce the cyber protection gap. As the pace of digital transformation continues, robust cyber insurance and protection measures are becoming essential components of business resilience.

Note: NIACE is an independent company and is not affiliated with any of the financial institutions (past and/or present) mentioned in our press releases unless otherwise specified. Views expressed in this article are purely for informational purposes only and do not act as nor constitute investment advice. Please refer to the prevailing regulations in your jurisdiction before making any regulatory decisions for yourself and/or your organisation. Past performance does not guarantee future returns. Clients and readers are advised to conduct your own due diligence or consult your financial advisor(s) before making any investment decisions.

Note: NIACE is an independent company and is not affiliated with any of the financial institutions (past and/or present) mentioned in our press releases unless otherwise specified. Views expressed in this article are purely for informational purposes only and do not act as nor constitute investment advice. Please refer to the prevailing regulations in your jurisdiction before making any regulatory decisions for yourself and/or your organisation.