# Cyber insurance premiums set to rise sharply after attacks on UK retailers



# Rising Cyber Insurance Costs Amid UK Retail Sector Attacks

The recent surge in cyberattacks targeting major UK retailers, including Marks and Spencer (M&S), Harrods, and the Co-op, is expected to trigger significant increases in cyber insurance premiums, as industry experts predict rate hikes of up to 10%. This evolving threat landscape comes as the retail sector is already grappling with rising insurance costs, following a previous period of competitive pricing that saw premiums fall by nearly 20% in 2023 and 15% in 2024.

Dan Leahy, head of cyber at broker BMS, noted that these incidents are likely to prompt underwriters to take a more stringent approach to assessing cyber security controls and pricing policies accordingly. As demand increases and market conditions tighten, it may lead some insurers to reconsider their willingness to provide coverage to retailers altogether. Currently, businesses are paying around £20,000 for every £1 million of coverage, but this amount may soon escalate.

For M&S, the ramifications of a recent cyber incident have been particularly severe. As the organization battles to regain operational stability following the disruption that began on April 25, it faces estimated losses exceeding £40 million due to halted online sales during a period of high consumer demand. According to analysts from Deutsche Bank, M&S's market value has dropped by about £600 million as a direct consequence of this breach, which has prompted the company to work closely with governmental and law enforcement bodies. Despite some services being restored, the company’s recovery is expected to remain protracted, with potential ramifications for staffing and product availability persisting for months.

The Co-op has similarly acknowledged breaches, revealing that hackers accessed and extracted personal customer information. Initially painting a picture of control, the retailer had to concede to the reality of the situation as the details started to surface. The volume of consumer data held by these retailers, combined with outdated technology and exposed helpdesk protocols, has rendered them particularly vulnerable to attacks. The Co-op’s challenges echo those experienced across the sector, which has highlighted fundamental weaknesses that many organisations were previously unaware of.

In response to these escalating threats, Tesco has taken proactive measures, implementing rigorous cyber security protocols. Their annual report underscores the significance of regular tests carried out in collaboration with independent agencies to fortify defences against potential breaches. During crisis simulations, senior leaders faced scenarios that imitated real cyberattacks, including a drill conducted in partnership with PwC in 2023 that involved ransomware aimed at critical operational systems such as payment processes.

Experts advise that despite the current volatility, companies should consider investing in cyber insurance while premiums remain comparatively low. Policies may cover a myriad of expenses, from ransom payments to crisis management costs, although the decision to pay a ransom remains a contentious one. This complexity is underscored by the dilemmas companies face, especially if ransom demands are connected to sanctioned entities, which could complicate insurance claims.

Compounding these challenges, the UK's National Cyber Security Centre has issued warnings about increasingly sophisticated social engineering campaigns. Cyber criminals are employing deceitful tactics, such as impersonating IT helpdesk personnel to reset passwords and gain system access. This trend reflects a broader rise in cyber threats across UK retail, prompting both industry leaders and policymakers to advocate for enhanced cyber security measures.

As the landscape evolves, the need for immediate action has never been clearer. Cabinet Office Minister Pat McFadden emphasized the importance of prioritising cyber security in light of these recent incidents, framing them as a crucial wake-up call for the sector. With mounting pressure from both the public and government, UK retailers must confront their vulnerabilities and adopt a more proactive stance towards cyber defence.

In a market where the impact of cyber attacks is becoming increasingly pervasive, the combination of steeply rising premiums and the persistent threat of new incidents serves as a stark reminder of the urgent need for comprehensive, fortified cyber security measures in the UK retail sector.

## Reference Map:

* Paragraph 1 – [[1]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1)
* Paragraph 2 – [[1]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[3]](https://www.reuters.com/business/retail-consumer/britains-ms-enters-second-week-sales-disruption-after-cyberattack-2025-05-02/), [[4]](https://apnews.com/article/7d3c01faa7380775598a517df4db1250)
* Paragraph 3 – [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[5]](https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/)
* Paragraph 4 – [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[6]](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9)
* Paragraph 5 – [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[4]](https://apnews.com/article/7d3c01faa7380775598a517df4db1250)
* Paragraph 6 – [[5]](https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/), [[6]](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9)
* Paragraph 7 – [[4]](https://apnews.com/article/7d3c01faa7380775598a517df4db1250), [[7]](https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/)
* Paragraph 8 – [[4]](https://apnews.com/article/7d3c01faa7380775598a517df4db1250), [[7]](https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - Please view link - unable to able to access data
2. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - UK retailers are facing significant increases in cyber insurance premiums following recent cyber attacks on major companies like Marks and Spencer (M&S), Harrods, and the Co-op. Industry experts predict rate hikes of up to 10%, reversing previous years’ declines of up to 20% in 2023 and 15% in 2024. These attacks have worsened an already challenging insurance environment, with underwriters now scrutinizing cyber security controls more closely and some reconsidering providing coverage to retailers altogether. The cost of cyber insurance currently stands at around £20,000 per £1 million of coverage, but this may rise further. M&S's operations were severely affected, with losses potentially surpassing £40 million due to disruptions to online sales, and recovery could take months. The Co-op also reported that cyber criminals accessed a significant number of customer records. Retailers are particularly vulnerable due to large volumes of customer data, outdated IT systems, and exposed helpdesk protocols. Tesco has implemented robust cybersecurity exercises, acknowledging rising threats. Experts advise companies to invest in cyber insurance while rates are relatively low, as expenses from ransom demands and crisis management could potentially be covered depending on policy terms. Meanwhile, UK authorities warn of increasing sophisticated social engineering threats targeting the sector.
3. <https://www.reuters.com/business/retail-consumer/britains-ms-enters-second-week-sales-disruption-after-cyberattack-2025-05-02/> - Marks & Spencer (M&S), one of Britain’s leading retail giants, has entered a second week of disrupted online clothing and home sales due to a major cyberattack. The attack, which began on April 25, disabled contactless payment and click-and-collect services, impacting sales during a period of unusually warm weather and high consumer demand. Since the incident, M&S has suffered a £700 million loss in market value. CEO Stuart Machin apologized to customers, stating efforts are ongoing to restore normal operations, though a timeline remains unclear. The disruption has also affected food product availability and led to the removal of job postings from the M&S website. Around one-third of the company's clothing and home sales are generated online, suggesting a notable short-term profit hit. The attack is part of a broader wave of cyber threats affecting UK organizations, prompting the National Cyber Security Centre and law enforcement agencies to launch investigations and urge stronger cybersecurity measures. The incident has drawn calls from industry leaders and lawmakers for enhanced governmental response and corporate vigilance against increasingly sophisticated cyber threats.
4. <https://apnews.com/article/7d3c01faa7380775598a517df4db1250> - British retailers are facing a wave of cyberattacks, with Marks & Spencer (M&S) and Harrods among the latest high-profile victims. M&S has been grappling with an ongoing cyber incident since Easter weekend, disabling its ability to process online orders, hire new staff, or maintain regular website functions. Although some services like contactless payments have been restored, the disruption continues as M&S works intensively to resolve the issue. Meanwhile, Harrods acknowledged a cyber threat and has taken precautionary steps, including limiting internet access. The attacks, which may be linked to a group called Scattered Spider, have raised concerns in the UK retail sector following a similar incident at Co-op. Authorities, including London’s Metropolitan Police and the UK’s National Cyber Security Centre, are investigating and providing support. Experts across the cyber defense industry warn that the growing use of generative artificial intelligence is intensifying the cyber threat landscape and urge organizations to strengthen their digital defenses.
5. <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> - Cyberattacks on UK retailers Marks & Spencer (M&S) and the Co-op Group were initiated by hackers impersonating employees and deceiving IT help desks into resetting passwords, according to BleepingComputer. This allowed the intruders access to internal networks. The UK's National Cyber Security Centre has advised organizations to revise their help desk protocols to prevent similar breaches. M&S, having disclosed the cyber incident on April 22, witnessed a 12% share decline and subsequently suspended online clothing and home orders; food product availability has also been disrupted. Analysts from Deutsche Bank estimate the financial impact at approximately £30 million ($40 million), with ongoing losses of around £15 million weekly, though cyber insurance is anticipated to cover most of the initial losses. Full recovery may take weeks, as rebuilding networks is a complex process. Meanwhile, a group named DragonForce claimed responsibility for attacks on M&S, the Co-op, and Harrods, alleging theft of staff and potentially 20 million customer records. The attack on M&S has also been tentatively linked to the hacking group "Scattered Spider" using DragonForce ransomware, though the National Cyber Security Centre has not confirmed any direct connection between these incidents.
6. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - Several major UK retailers, including Marks and Spencer (M&S), the Co-op, and Harrods, have recently been targeted by cyber attacks, highlighting the increasing vulnerability of the retail sector. M&S has faced significant operational disruptions and a £600 million drop in value due to these attacks. Investigations are ongoing, and experts suspect a common supplier or technology could link the incidents. Cybersecurity professionals suggest a potentially coordinated effort, possibly involving the group Scattered Spider, known for manipulating individuals to gain system access. The National Cyber Security Centre has expressed concern, urging businesses to treat cybersecurity seriously. Retailers are attractive targets due to their vast customer data, real-time operations, and reliance on legacy systems. Although some customer data was accessed, sensitive financial information reportedly remains secure. Cybersecurity apathy, especially among large UK retailers, has been noted in recent industry research. Experts warn that even without paying ransoms, attackers could profit by selling stolen data. The incidents serve as a stark reminder of the growing sophistication and impact of cybercrime on the retail landscape, with recovery potentially taking months.
7. <https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/> - The British government is set to urge all UK businesses to prioritize cyber security following recent cyberattacks on major retailers Marks & Spencer (M&S), the Co-op Group, and Harrods. Cabinet Office Minister Pat McFadden, in coordination with national security officials and Richard Horne, CEO of the National Cyber Security Centre, outlined governmental support for affected companies. At the upcoming CyberUK conference in Manchester, McFadden will stress the need for heightened cyber precautions, describing the attacks as a "wake-up call" and advocating for cyber security to be treated as an "absolute priority." New measures, including the Cyber Security Bill, are being introduced to strengthen national defense. M&S experienced significant disruption on April 25 due to a suspected ransomware attack by the group "Scattered Spider," which affected their online and contactless services. This incident follows a growing trend of cyberattacks causing extensive financial and operational damage across UK industries.