# M&S and Co-op cyberattacks reveal rising retail vulnerabilities and £125 million potential losses



In a world increasingly fraught with cyber threats, two recent high-profile hacks have underscored the precarious nature of retail security in the UK. Joe Tidy, a cyber correspondent, shared his unsettling interaction with hackers who claimed to have compromised both Marks & Spencer (M&S) and the Co-op. Through a series of messages on Telegram, the hackers divulged details of their operation, asserting that they had stolen substantial amounts of customer and employee data from these retailers. The extent of their claims was corroborated by evidence they provided, indicating a troubling reality for both companies and their customers.

The cyber incidents at M&S and the Co-op have had severe repercussions. M&S has suffered operational disruptions since the attack occurred over the Easter weekend, when it was forced to suspend online orders spanning nearly three weeks. The situation not only resulted in a staggering £4 million loss per day in online sales but also caused a significant 18% drop in the company’s share price. Analysts estimate that the total revenue loss could reach £125 million if the disruptions persist. While M&S maintains that no payment details or passwords were compromised, customer data—including names and order histories—was put at risk, leading to heightened consumer concerns.

Co-op has also faced its share of turmoil. Initially, the company attempted to downplay the severity of the breach, but soon admitted that a substantial data breach had occurred. Customers reported encountering empty shelves in stores, a direct result of the operational chaos stemming from the hack. Industry experts have observed that this increase in cyber incidents highlights the vulnerabilities of retailers in a sector already burdened by outdated IT systems and insufficient cyber security measures.

According to the hackers, the group behind these attacks identifies as DragonForce—a cybercrime cartel offering a range of malicious services in exchange for a cut of any ransoms paid. This model of ransomware-as-a-service has proliferated in recent years, particularly following the dismantling of the notorious LockBit group. As DragonForce seeks to solidify its position in a fragmented landscape of cybercriminal operation, it has recently expanded its offerings, including support services and negotiation tools for ransoms.

In the wake of these attacks, M&S disclosed the impact on its financials. CEO Stuart Machin stands to lose up to £1.06 million due to the strike on the company's market performance. Even before the cyber incident, M&S had reported a strong financial position, with pre-tax profits expected to reach £840 million. However, the fallout from the cyber attack threatens to derail its ongoing transformation efforts, which rely heavily on back-end automation and digital enhancements.

Alongside M&S, other retailers like the Co-op and even Harrods have also faced similar operational disruptions, prompting a re-evaluation of cyber insurance within the sector. Insurance premiums are projected to rise significantly, potentially increasing by up to 10% as insurers reassess the risks associated with cyber threats. M&S, set to claim up to £100 million from its cyber insurance, faces the challenge of improving its cyber risk management strategies to avoid skyrocketing premiums in the future.

The cyber security landscape for retail is alarming. The UK’s National Cyber Security Centre reports that businesses across the country have incurred approximately £44 billion in cyber-related losses over the past five years. This worrying trend compels retailers to reinforce their digital fortifications and adopt more robust crisis response strategies. As M&S and Co-op navigate these turbulent waters, their experiences serve as cautionary tales for the wider industry, prompting urgent calls for enhanced cybersecurity measures across the retail sector.

While M&S continues working with cyber experts and law enforcement to restore its systems, the reality remains that customer trust has been shaken. For consumers, this spells uncertainty in an industry that already faced scrutiny over its data protection measures. In an age where digital interactions have become the norm, the threats posed by cybercriminals will only continue to evolve. The lessons learned from these attacks may reverberate well beyond M&S and the Co-op, offering crucial insights into securing retail operations against future breaches.

### Reference Map

1. Lead article summarising Joe Tidy's interactions with hackers and their claims regarding M&S and Co-op.
2. Financial implications of the attack on M&S, including CEO pay losses and overall revenue impact.
3. Details on operational disruptions affecting M&S and Co-op post-hack.
4. Statements from M&S regarding the nature of the data compromised.
5. Overview of M&S's insurance claims and potential financial ramifications of the breach.
6. Co-op's response and operational recovery following the cyber incident.
7. Broader implications of rising cyber insurance premiums in the wake of recent cyberattacks.

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

## Bibliography

1. <https://www.bbc.com/news/articles/cgr5nen5gxyo> - Please view link - unable to able to access data
2. <https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e> - Marks and Spencer (M&S) CEO Stuart Machin is set to lose up to £1.06 million from his pay package due to a cyber attack that triggered a 14% drop in the company’s share price. The cyber attack, disclosed in April 2025, compromised customer data, disrupted online orders for three weeks, and led to stock shortages in stores. Analysts estimate the retailer may have already lost around £75 million in revenue, with potential losses rising to £125 million if disruptions continue through May. While M&S may claim up to £100 million in insurance, the incident risks affecting its broader transformation efforts, including back-end automation and digital improvements. Despite the setback, M&S posted a strong financial year prior to the attack, with expected pre-tax profits of £840 million and a 14.7% year-on-year sales increase. However, the damage from the cyber incident may weigh heavily on first-quarter 2026 performance and long-term strategy execution.
3. <https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems> - Marks & Spencer (M&S) continues to face serious operational disruptions following a cyberattack that occurred over the Easter weekend. Online orders through its website, app, and phone have been suspended since April 25, with no confirmed restart date. The attack compromised some customer data, including names, contact information, and order histories, though no payment details or passwords were exposed. As a security measure, customers will be prompted to reset their passwords upon their next login. Services including Sparks loyalty offers have been paused, and in-store stock availability remains inconsistent, as illustrated by images of empty shelves shared by shoppers online. The cyberattack has severely impacted M&S financially, with an estimated £4 million a day in lost online sales and an 18% drop in share value, erasing over £1 billion in market capitalization. While some affected customers have been compensated with gift cards, broader investor confidence is shaken due to limited communication from M&S. The ransomware group “DragonForce” has claimed responsibility for the breach. Despite these challenges, M&S's core food business and partnerships like Ocado remain unaffected, providing a silver lining during this crisis. The company is actively working to resolve the issue though no timeline has been confirmed.
4. <https://www.reuters.com/business/retail-consumer/uks-ms-says-customer-information-was-taken-cyber-attack-2025-05-13/> - British retailer Marks and Spencer (M&S) confirmed it suffered a cyber attack that compromised some customer personal data, though no usable payment information or passwords were taken. The attack, widely identified as a ransomware incident, has significantly disrupted M&S's online operations, halting online orders since April 25. Despite the breach, M&S emphasized there is no evidence the stolen data has been shared and reassured customers that no action is required from them at this time. The company is working with cybersecurity experts, law enforcement, and government agencies to restore operations and secure its systems. While its 1,000 physical stores remain operational, M&S has seen a 15% drop in share price and is facing substantial financial impact, particularly as online sales represent about a third of its clothing and home revenue. Deutsche Bank analysts estimate the profit loss could be at least £30 million, with weekly losses around £15 million. M&S noted that cyber insurance may cover most of the damages, though typically for a limited period.
5. <https://www.ft.com/content/723b6195-1ce7-4b5f-94f5-729e9152c578> - Marks and Spencer (M&S) stands to claim up to £100 million from its cyber insurance following a recent cyberattack, which compromised some customer data and severely disrupted operations, especially online orders for almost three weeks. The personal data exposed includes contact details, dates of birth, and order histories, though not payment details or passwords. Insurers involved include Allianz, expected to cover at least £10 million initially, and Beazley. The incident may have resulted in lost revenues exceeding £60 million and contributed to a 16% drop in share price, erasing £1.3 billion of its market value. M&S's cyber insurance, arranged by WTW, is likely to cover all losses, including both direct and third-party liabilities, even if a third-party vendor is implicated in the breach. However, M&S may see its insurance premium—currently under £5 million—double unless it improves cyber risk management. This breach, along with recent cyberattacks on other UK retailers such as Harrods and the Co-op, may lead to increased cyber insurance premiums across the sector. The M&S payout could validate the value of cyber insurance and encourage wider adoption among smaller businesses. UK businesses have suffered approximately £44 billion in cyber-related revenue losses over the past five years.
6. <https://www.reuters.com/business/retail-consumer/uks-co-op-says-systems-now-running-normally-after-cyber-incident-2025-05-14/> - UK grocery retailer Co-Op announced that its systems are now fully operational following a recent cyber incident. The company reported that payment systems are functioning, and stock availability—both in stores and online—is expected to improve by the weekend. The breach, disclosed last month, involved an attempted hack that prompted Co-Op to restrict system access as a protective measure. The company, which operates over 2,300 stores and also provides funeral care, legal, and insurance services, is currently in a recovery phase, restoring systems in a controlled manner. This incident comes amid a broader trend of cyberattacks targeting UK retailers. Marks and Spencer, another major retailer, recently ceased online orders due to a suspected ransomware attack, which also led to the compromise of some customer information. The UK's National Cyber Security Centre has not confirmed whether these attacks are connected.
7. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - UK retailers are facing significant cyber insurance premium increases, up to 10%, following high-profile cyber attacks on major chains such as Marks and Spencer (M&S), Harrods, and the Co-op. These attacks are prompting insurers to reassess cyber risk in the retail sector, which had enjoyed falling rates in 2023 and 2024. Experts warn cyber security scrutiny will intensify and some insurers may withdraw from the retail market. M&S may claim tens of millions of pounds for business interruption, after losing over £40 million in online sales during a lengthy system outage. The Co-op confirmed a data breach affecting numerous customers. The sector is particularly vulnerable due to large amounts of consumer data and outdated IT systems. Tesco acknowledged ongoing cyber threat preparedness in its annual report, citing crisis simulations involving ransomware. Insurance might cover not only ransomware payments but also costs associated with crisis response. However, insurers face challenges if attackers are linked to sanctioned entities. The UK’s cyber security agency has also issued warnings about attackers impersonating IT help desks in sophisticated social engineering scams. Brokers urge businesses to secure cyber insurance now before premiums rise further.