# Marks & Spencer faces £200 million hit from Scattered Spider cyberattack amid sales disruption



Marks & Spencer (M&S) faces a significant challenge as it prepares to unveil its annual financial performance, following a cyber attack last month that has disrupted operations and potentially cost the retailer millions in lost revenue. The incident, attributed to the hacking group Scattered Spider, has placed immense pressure on the company, which has been forced to suspend all online orders for nearly three weeks. Financial analysts estimated that the breach could be costing M&S around £4 million a day in lost sales, particularly detrimental as the disruptions coincide with a critical period for spring and summer clothing sales.

Despite the turmoil, M&S reported that its physical stores remained operational, although in-store availability was briefly impacted due to changes in IT systems. Recent updates indicate a swift improvement in food supply availability, with distributions returning to normal levels. However, the broader implications of the cyber attack are significant. Customer data, including names, email addresses, and dates of birth, was compromised, sparking concerns about security and consumer trust.

When M&S announces its annual results, investors will be keen to assess the full extent of the damage and the company’s plans for recovery. The retailer has not disclosed a precise financial cost of the breach but has reportedly missed out on tens of millions in sales. Susannah Streeter, head of money and markets at Hargreaves Lansdown, noted that while the annual numbers may not fully reflect the impact of the operational outages—since they occurred later in the financial year—guidance for the upcoming year is anticipated to be cautious.

Analysts from Barclays have projected a staggering £200 million impact on profits for the 2025/26 financial year, though much of this may be offset by a claim of up to £100 million from the company’s cyber insurance policy. Insurers, including Allianz and Beazley, are expected to cover substantial portions of the damages, although it is worth noting that M&S's insurance premium—currently under £5 million—could potentially double unless the retailer enhances its cyber risk management practices.

The immediate implications extend beyond financial loss; the incident has triggered a turbulent period for M&S, leading to a 16% decline in its share price, erasing approximately £1.3 billion of the company's market value. This has occurred following a period of relative stability and growth under the leadership of CEO Stuart Machin, who only last month saw shares reach nearly a nine-year high.

The ramifications of this attack echo throughout the retail sector, which has witnessed a surge in cyber threats. Google recently highlighted the aggressive tactics of Scattered Spider, suggesting that retailers in both the UK and the US may become increasingly vulnerable as this hacking group seeks new targets. The vulnerability of the retail industry, coupled with high volumes of consumer data, has raised alarms about future cyberattacks and the need for fortified security measures across the board.

In light of this incident, the broader trend of rising cyber insurance premiums is expected to escalate. Following the recent string of high-profile attacks—including incidents at retailers like Harrods and the Co-op—experts anticipate that insurers will reassess risk in the sector. This shift may compel businesses to expedite the acquisition of cyber insurance are looking to safeguard their operations and customer trust.

As M&S grapples with the fallout from this cyberattack, the retailer's recovery strategy and future digital resilience will be closely scrutinised by stakeholders keen on understanding the implications for the company's long-term viability in an increasingly digital world.

### Reference Map

1. Lead article on M&S's financial performance and the impact of the cyber attack.
2. Details on the insurance claims potential after the cyber breach.
3. Confirmation of the nature of the attack and its effects on sales.
4. Information regarding the hacking group's ongoing activities and threats to US retailers.
5. Updates on food supply recovery following the cyber incident.
6. Discussion on increased premiums and cybersecurity scrutiny in the retail sector.
7. Insights on the possibility of lost sales quantified against M&S's past performances.

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

## Bibliography

1. <https://www.independent.co.uk/tech/marks-spencer-cyber-attack-orders-latest-b2752588.html> - Please view link - unable to able to access data
2. <https://www.ft.com/content/723b6195-1ce7-4b5f-94f5-729e9152c578> - Marks & Spencer (M&S) is set to claim up to £100 million from its cyber insurance following a recent cyberattack that 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.
3. <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.
4. <https://www.reuters.com/business/google-says-hackers-that-targeted-uk-retail-sector-are-now-targeting-us-2025-05-14/> - Google has warned that the hackers responsible for major cyberattacks on UK retailers, specifically linked to the group known as "Scattered Spider," are now targeting US retail companies. John Hultquist, a cybersecurity analyst at Google's cybersecurity division, stated that US retailers should be on alert as these attackers are highly aggressive, innovative, and capable of bypassing even well-established security measures. Scattered Spider is described as a loosely connected collective of hackers with varying expertise, previously attributed to a paralyzing hack of UK retailer Marks & Spencer, which disrupted its online operations since April 25. The group is known for concentrating on specific sectors, suggesting the retail industry will remain a focus. In 2023, related hackers gained infamy for cyberattacks on US casino giants MGM Resorts and Caesars Entertainment. Efforts to counter Scattered Spider have proven difficult due to the group’s decentralized nature, the young age of its members, and the limited cooperation from businesses affected by the cyberattacks.
5. <https://www.reuters.com/business/retail-consumer/uks-ms-says-food-availability-improving-every-day-2025-05-15/> - British retailer Marks & Spencer (M&S) announced that food supplies from its distribution centers to stores have returned to normal levels following a cyberattack that disrupted operations last month. The company reported that, particularly in chilled food sections, customer needs are being met, and deliveries to grocery departments are stabilizing, leading to daily improvements in product availability. The cyberattack, first acknowledged on April 22, led to the temporary shutdown of systems, affecting stock availability across food, clothing, and home departments. Additionally, M&S revealed that some personal customer information was compromised during the breach. Online clothing orders remain suspended since April 25, with no current update on when they will resume.
6. <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.
7. <https://www.nationalworld.com/business/consumer/marks-and-spencer-cyber-attack-how-long-online-ordering-down-how-much-losing-day-5118983> - It’s difficult to say exactly how much the company will lose from the outage - the website is still working, so is still acting like a catalogue rather than a platform for ordering - and it will be difficult to quantify how many people who would have ordered online will have visited a store instead. But having said that, a look at Marks & Spencer’s most recent annual report, released in September last year, does give some indicators of how big a hole this outage will punch in its revenues. The report says that up to the end of the 2023/24 financial year, in its clothing and home departments, M&S saw £1,268.4m - so £1,268,400,000 or £1.27bn - online sales, with more than 9m customers and more than 33m transactions. Using the blunt tool of averaging out the online sales per day (and with 2024 being a leap year), that gives a figure of £3,465,573 in clothing and home sales alone every day. At time of writing, the cyber attack had been going on for 18 days - so the company could have lost £62.5m from clothing and home sales alone so far. But to stress again, this does not take into account the number of people who will have visited a store instead of ordering online. The in-store comparison for clothing and home sales is £2,642.3m - £2,642,300,000, or £2.64bn - for the financial year before last, so was still much higher. M&S Food reports its sales through Ocado Retail so does not include them in its annual financial reports.