# Marks & Spencer faces £300 million hit after major cyber attack disrupts online sales



Marks & Spencer (M&S) recently encountered significant disruptions as its website was taken offline for several hours following a major cyber attack, the latest challenge in a series of ongoing operational issues. Customers attempting to access the site during the early hours of Thursday were met with a message apologising for the inconvenience and announcing that updates were in progress. By 7 am, browsing functionality had been restored, yet online orders remained suspended, and the company warned that full service restoration might not occur until July.

This incident is part of a larger cyber assault that first emerged over the Easter weekend, exposing vulnerabilities within M&S’s digital infrastructure. The attack has been attributed to the Scattered Spider hacking group, which is believed to have infiltrated M&S's systems through social engineering tactics directed at a third-party supplier. Such incidents underscore a growing concern within the retail sector regarding third-party dependencies that can create significant security weaknesses, even against robust internal cybersecurity measures. Despite M&S’s considerable investment to enhance its cyber defences, the breach reveals that human vulnerabilities remain a critical risk.

The financial ramifications of the attack are staggering, with M&S anticipating a £300 million hit to its profits this year. This loss mirrors a broader trend, as the UK government's Cyber Security Breaches Survey indicates that over 40% of businesses in the country have faced cybercrime in the past year. M&S’s predicament is particularly acute given that online sales typically account for around a third of its clothing and home revenue. As the company grapples with this latest setback, other retailers are reassessing their cybersecurity strategies to mitigate similar threats.

CEO Stuart Machin described the attack as the most formidable challenge his team has faced, highlighting the company's renewed commitment to a comprehensive recovery strategy. He confirmed that customer data, including names, addresses, and birth dates, had been compromised, although payment information and passwords were reportedly safe. The threat from the malware used in this incident echoes a broader trend, wherein sophisticated hacking strategies are employed to target weaknesses in human processes rather than solely relying on technical vulnerabilities.

In response to the attack, M&S has launched an extensive review of its systems. Approximately 600 applications and thousands of servers have been subject to scrutiny in an effort to restore and secure operations. The National Crime Agency is currently investigating the breach, and the retailer has declined to comment on any ransom demands in accordance with law enforcement advice. While facing such substantial operational hurdles, M&S's strategy of prioritising long-term security over rapid service recovery could lead to further delays and reputational damage, as ongoing disruptions have already affected the availability of various products both online and in-store.

Retail analysts are watching closely as this incident may spur heightened investor scrutiny of executive accountability regarding cybersecurity, potentially affecting decisions around bonuses or incentives. As M&S navigates this turbulent period, it serves as a sobering reminder of the vulnerabilities that can exist within even the largest and most established brands. The future of M&S's digital strategy will depend on its ability to enhance its cybersecurity framework, rebuild consumer trust, and navigate the evolving landscape of cyber threats effectively.

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

## Bibliography

1. <https://www.grocerygazette.co.uk/2025/05/22/ms-website-back-online/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2> - Marks & Spencer (M&S) faced a significant cyber attack that compromised its operations and is expected to cut up to £300 million from this year’s operating profit. The attack forced the shutdown of its online clothing business for over three weeks, resulting in stolen customer data and a £750 million market capitalisation loss. The breach occurred due to social engineering tactics directed at a third-party supplier, allowing cybercriminals to bypass M&S’s internal defenses. Although M&S had significantly increased its investment in cybersecurity and expanded its security team, the incident exposed its vulnerability through third-party dependencies — a common risk for multinational retailers. In response, M&S is undertaking a comprehensive cleansing of more than 600 applications and thousands of servers, with full e-commerce operations expected to resume by July. CEO Stuart Machin described the attack as the most difficult challenge faced by his team, and the company is now focusing on a controlled and thorough recovery to ensure long-term security. The incident has also raised questions about potential cuts to executive bonuses and has heightened scrutiny of third-party IT partnerships in the retail industry.
3. <https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/> - Marks & Spencer (M&S) disclosed that a recent cyberattack on its systems was carried out through a third-party contractor, bypassing its own digital defenses via social engineering tactics. CEO Stuart Machin revealed that despite increasing tech investment threefold over the past three years, the attackers exploited human vulnerabilities, gaining access through the contractor rather than a technical weakness. Although M&S has an IT contract with Tata Consulting Services (TCS), Machin did not confirm if TCS was the specific target. The breach was discovered over Easter weekend (April 19-20), and M&S promptly involved cybersecurity experts and authorities. The company halted online sales, anticipating full service restoration by July. The UK’s National Crime Agency is investigating a group of young English-speaking hackers believed to be responsible. So far, around 600 systems have been scanned and are being restored. M&S has not commented on any ransom demands due to law enforcement advice. The retailer, with annual sales of nearly £14 billion ($19 billion), emphasized the importance of vigilance against increasingly sophisticated cyber threats.
4. <https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8> - British retailer Marks & Spencer (M&S) has estimated the cost of a recent cyberattack at approximately £300 million ($400 million). The attack, described as highly sophisticated and targeted, began around the Easter weekend and has significantly disrupted operations, particularly online sales of food, home, and beauty products. The disruption is expected to continue until July. The suspension of online shopping and the need for manual processes in stores have led to reduced food availability, increased waste, and higher logistics costs, adversely affecting profits. CEO Stuart Machin emphasized the company's focus on system recovery and declined to provide details about the attackers. M&S also revealed that hackers accessed customer personal data, including names, emails, addresses, and birth dates. The cyberattack is part of a broader wave affecting other British retailers, including Harrod’s and Co-op.
5. <https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b> - A recent cyber attack on Marks & Spencer (M&S) is projected to cost the company £300 million, or about 30% of its previous year's operating profit. This incident underscores the rising threat of cybercrime, which more than 40% of UK businesses have encountered in the past year, according to the UK government's Cyber Security Breaches Survey. While retail headlines dominate, other sectors are even more exposed. For tech companies, however, such breaches are creating business opportunities as organizations invest heavily in cybersecurity—global spending on anti-hacking software is seeing double-digit annual growth and is projected to reach $300 billion by 2028. The evolving nature of cyber threats complicates the defensive landscape. Malware has declined to 20% of attacks, while 'vishing' has surged, and generative AI presents both risks and defensive potential. M&S had already doubled its cybersecurity spending since 2021 and is now accelerating its digital initiatives. Experts suggest that corporate boards need better cyber literacy, especially considering vulnerabilities caused by third-party access, which contributed to the M&S breach. Online sales at M&S will remain impaired for weeks, severely impacting its integrated retail strategy and reputation. The attack serves as a wake-up call for executives to enhance their cybersecurity frameworks.
6. <https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/> - A month after a cyberattack crippled Marks & Spencer's (M&S) online operations, the UK retailer is still struggling to fully recover, prioritizing cybersecurity over rapid system restoration. The attack, attributed to the ransomware group Scattered Spider and DragonForce, has already cost M&S an estimated £60 million in lost profits and over £1 billion in market value. Online clothing and home orders remain suspended, and some in-store products have also been affected due to disrupted supply operations. The company is gradually bringing systems back online and has resumed food stock forecasting. M&S refused to pay the ransom in line with government guidance, opting to rebuild its systems, a move that may prolong disruptions and potentially lead to reputational harm. Analysts warn continued delays risk customer frustration, rising operational costs, and reduced morale among staff. The breach reportedly involved credentials of Tata Consulting Services employees, though TCS has not commented. With online sales typically comprising a third of M&S’s clothing and home revenue, the disruption could result in substantial losses. Meanwhile, other UK retailers are urgently reassessing cybersecurity to avoid a similar fate, acknowledging the widespread vulnerability in the retail sector.
7. <https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders> - Marks & Spencer has apologised to customers after a 'cyber incident' affected contactless payments and the pick up of online orders in its stores in recent days. The retailer told shoppers that delays to click and collect orders have continued but it was 'working hard to resolve' the issue. It told customers and staff they did not need to take any action, suggesting their data has not been accessed. In a statement to the stock exchange M&S said it had found it 'necessary to make some minor, temporary changes to our store operations to protect customers and the business' and was 'sorry for any inconvenience experienced'. It said stores remained open and its website and app were operating as normal. 'Customer trust is incredibly important to us, and if the situation changes an update will be provided as appropriate,' the company said in a statement to the City. M&S said it had reported the incident to the National Cyber Security Centre and hired cybersecurity experts to help investigate and manage the issue and was 'taking actions to further protect our network' to ensure it could continue serving shoppers. The incident began on Monday with contactless payments and click and collect orders affected in stores across the country. However, there was a separate technical problem on Saturday, which only affected contactless payments. A shopper at the retailer’s Plymouth store posted on X on Saturday 'could not collect my online purchase today, previous visit could not return an item as tills were down …please sort out your poor IT situation'.