# Marks & Spencer faces £1.3 billion hit amid prolonged cyberattack by DragonForce



Marks & Spencer (M&S) finds itself embroiled in a continuing cyber crisis that has significantly disrupted operations and eroded shareholder value. As the retailer crosses into the fourth week marked by this cyber incident, the firm has witnessed a decline in market value of approximately £1.3 billion. Shares have experienced a notable drop, falling nearly 16 per cent since news of the attack broke, with a decrease of 3.3 per cent reported recently.

The attack has been linked to DragonForce, a hacking group that claims to have stolen sensitive data of millions of customers and threatens to impose ransom demands. They assert that similar attacks have also targeted other notable retailers like the Co-op and Harrods. The repercussions from the security breach have been dire, forcing M&S to suspend online shopping for both fashion and homeware—an essential service for the retailer, particularly during peak shopping seasons. Reports indicate that M&S has faced an estimated loss of £68 million in online revenue due to the disturbances.

Justin Kuruvilla, a supply chain security expert at Risk Ledger, remarked on the challenge of predicting when M&S’s website will be fully operational again. "The last thing M&S will want is to have overlooked a backdoor left open by the attackers that can then be used to regain entry," he said. This highlights the precarious balance M&S must strike between restoring services swiftly and ensuring the integrity of its systems is fully secured.

Reports attribute the cyber assault not solely to DragonForce but also hint at possible involvement from the Scattered Spider hacking group, known for employing advanced techniques such as social engineering and SIM swapping. This group has previously targeted significant corporations, indicating a trend towards larger-scale cyber assaults. In fact, they were implicated in the breach of MGM Resorts International in September 2023, which raises questions about the evolving landscape of cyber threats businesses face today.

Amid these developments, M&S is not new to such troubles. In October 2015, the retailer undertook a temporary suspension of its online services after a technical glitch exposed personal information of customers, though at that time, the company emphasized that no financial data was compromised. The current situation, however, involves far graver ramifications, both in terms of financial loss and customer trust.

As M&S navigates this challenging landscape, the ramifications extend beyond immediate operational difficulties. The incident may invoke legal obligations under the UK Data Protection Act, particularly concerning the extent of data compromise and customer notifications. Given the heightened sensitivity surrounding data privacy, customer apprehensions about the safety of their personal information could have lasting implications for M&S's brand reputation.

In addition to the issues encountered by M&S, similar breaches have been reported across various sectors. For instance, Capita, a company providing administration services for the M&S Pension Scheme, experienced a cyber incident that wrought minor data leaks earlier this year. Members of the pension scheme were advised to remain vigilant about their communications, underpinning the importance of data protection in the current climate.

As the retailer faces mounting challenges, including the suspension of online job advertisements, M&S has pledged to work diligently to restore services and reinforce security measures. A spokeswoman stated that the company is committed to reinstating normal operations as swiftly as possible, although the timeline remains uncertain.

The repercussions of this cyber crisis at M&S serve as a cautionary tale for the retail industry, illustrating the critical need for robust cyber defences and proactive crisis management. The ongoing saga is a stark reminder that the evolving threats posed by cybercriminals may reshape the landscape of retail, both in terms of operational sensitivity and customer interactions moving forward.

### Reference Map

1. Paragraph 1, 2, 3, 4, 5, 6, 7
2. Paragraph 2, 4
3. Paragraph 3
4. Paragraph 4
5. Paragraph 4
6. Paragraph 6, 7
7. Paragraph 7

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

## Bibliography

1. <https://www.dailymail.co.uk/money/markets/article-14704375/Cyber-crisis-stings-M-S-shares-fourth-week-firms-value-1-3bn-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.cybersecurityintelligence.com/blog/scattered-spider-hacking-group-is-behind-the-attack-on-mands-8392.html> - This article discusses the cyber attack on Marks & Spencer (M&S) attributed to the Scattered Spider hacking group. The attack led to significant disruptions, including empty shelves and delays in online shopping services. The group, known for targeting large organizations, employed tactics like social engineering and SIM swapping. The article also mentions previous exploits by the group, such as the MGM Resorts International breach in September 2023. The extent of data compromise in the M&S attack is still under investigation, with potential legal obligations for reporting under the UK Data Protection Act.
3. <https://www.bbc.com/news/technology-34656818> - In October 2015, Marks & Spencer (M&S) temporarily suspended its website after a technical issue allowed customers to view other users' personal information upon logging in. The glitch exposed details like names, dates of birth, and previous orders. M&S clarified that no financial details were compromised and attributed the problem to an internal error, not an external hack. The company apologized for the inconvenience and restored the website after a two-hour suspension.
4. <https://www.mandspensionscheme.com/news/news/2023/04/message-from-the-trustee-capita-cyber-incident/> - In April 2023, Capita, which provides administration services to the M&S Pension Scheme, experienced a cyber incident. Capita informed the scheme that a limited amount of data was leaked. The M&S Pension Scheme emphasized the importance of protecting member data and advised members to stay vigilant, especially regarding communications about their pensions. The scheme assured members that the annual increase to pensions in payment for 1 May 2023 was applied on time and that pension increase letters would be available by 28 April.
5. <https://www.bbc.com/news/articles/cv22e5vx5djo> - In May 2024, Marks & Spencer's website and app experienced a technical issue that rendered them inaccessible for several hours. Customers encountered error messages and were unable to navigate the site. An M&S spokeswoman attributed the problem to a third-party provider and apologized for the inconvenience caused. The website and app were restored by 18:15 BST on the same day.
6. <https://www.upday.com/uk/m-and-s-working-day-and-night-to-manage-impact-of-cyber-attack> - This article reports on Marks & Spencer's response to a significant cyber attack in April 2025. CEO Stuart Machin expressed regret over the impact on customers and stated that the company was working tirelessly to manage the situation. The attack led to the suspension of online orders and affected contactless payments in stores. M&S apologized for the inconvenience and assured customers that normal services would resume as soon as possible.
7. <https://www.bishopsstortfordindependent.co.uk/national/m-s-stops-hiring-after-systems-taken-offline-due-to-cyber-attack-145398/> - In May 2025, Marks & Spencer halted all online job advertisements following a cyber attack that disrupted its operations. The company confirmed that it had removed job listings from its website as technical experts worked to resolve issues across its online systems. A spokeswoman stated that job adverts would be reinstated in due course. The cyber attack had previously led to the suspension of online orders and impacted contactless payments in stores.