# Marks & Spencer faces £300m losses and leadership shakeup amid cyberattack fallout



Marks & Spencer (M&S) is contending with a challenging landscape following the resignation of its marketing director, Anna Braithwaite, a key figure in the brand's recent efforts to rejuvenate its image. Braithwaite's departure marks a significant moment for the retailer, which has worked diligently over the past four years to reshape perceptions from its previous dowdy reputation. Her tenure saw the introduction of collaborative advertising campaigns featuring high-profile personalities such as Alex Scott and Sienna Miller, aimed at appealing to a younger demographic and reinvigorating sales.

Despite these marketing triumphs, M&S is grappling with the repercussions of a recent cyberattack that has significantly disrupted its operations. The incident, attributed to the hacker group Scattered Spider, has halted online sales and limited payment processing capabilities, leading to a staggering projected loss of £300 million in operating profits. Such disruptions have posed considerable risks, including the potential compromise of customer data, which has resulted in a class action lawsuit against the retailer.

The implications of the cyberattack extend beyond immediate losses. As experts have pointed out, M&S’s challenges reflect a broader vulnerability within the retail sector, which has increasingly become a target for cybercriminals. This particular breach exploited vulnerabilities related to third-party suppliers, underscoring that human error remains a critical vulnerability in cybersecurity defences. CEO Stuart Machin highlighted that M&S cannot entirely rule out the possibility that its partner, Tata Consultancy Services (TCS), may have played a role in the breach, although the investigation is ongoing.

Customer sentiment, meanwhile, remains surprisingly resilient. Despite the ongoing operational turmoil, recent sales figures from NielsenIQ indicate that M&S's food division is outperforming expectations, with a year-on-year growth of 10.8% during the three months leading up to mid-May. This resilience suggests that while the brand faces significant operational hurdles, its core loyal customer base continues to support it. Analysts are optimistic about the brand's ability to bounce back, particularly as M&S is reportedly poised to reintroduce online shopping soon, potentially by next month.

Further complicating the narrative is the fact that M&S has taken proactive measures to reassure customers during this tumultuous period. By increasing in-store staffing and enhancing customer response times, the retailer aims to maintain trust and loyalty among its customers. Praise for its transparency in communication during the crisis has been vital in mitigating potential backlash, an approach that may set a positive precedent for handling future crises.

However, as M&S navigates this multifaceted crisis, the lessons learned from this cyberattack will likely shape its strategy moving forward. The emphasis on improving cybersecurity protocols, rigorous vetting of third-party vendors, and a comprehensive approach to employee training is becoming increasingly crucial. With many retailers facing a similar threat landscape, establishing robust cybersecurity measures may no longer be viewed merely as a technical need, but as a board-level priority essential for safeguarding the future.

In the aftermath of such trials, the road to recovery for Marks & Spencer will not only hinge on its marketing effectiveness and operational resilience but also on the retailer’s ability to restore its digital capabilities and ensure customer confidence in a landscape increasingly fraught with risks.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/money/markets/article-14766033/Fresh-blow-Marks-Spencer-marketing-chief-quits.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761), [[4]](https://www.ft.com/content/71bf35b0-740f-472f-96c6-86a9458e5844)
* Paragraph 2 – [[2]](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761), [[5]](https://www.reuters.com/business/retail-consumer/ms-food-sales-show-resilience-despite-cyberattack-says-nielseniq-2025-05-29/), [[6]](https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8)
* Paragraph 3 – [[3]](https://www.techradar.com/pro/security/m-and-s-hack-may-have-been-caused-by-security-issues-at-indian-it-giant-tata-consultancy-services), [[7]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/)
* Paragraph 4 – [[4]](https://www.ft.com/content/71bf35b0-740f-472f-96c6-86a9458e5844), [[5]](https://www.reuters.com/business/retail-consumer/ms-food-sales-show-resilience-despite-cyberattack-says-nielseniq-2025-05-29/), [[6]](https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8)
* Paragraph 5 – [[6]](https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8), [[7]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/)

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

## Bibliography

1. <https://www.dailymail.co.uk/money/markets/article-14766033/Fresh-blow-Marks-Spencer-marketing-chief-quits.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761> - A recent cyber attack on Marks & Spencer (M&S) underscores the growing vulnerability of businesses to cyber threats. The attack, attributed to the hacker group Scattered Spider, disrupted services including online clothing sales and contactless payments, with the company facing a potential £300 million hit to operating profits. The breach, linked to third-party human error, exposed customer data and has prompted a class action lawsuit. M&S is still recovering, expecting full operational restoration by July. Experts stress the need for better cybersecurity practices to mitigate such risks.
3. <https://www.techradar.com/pro/security/m-and-s-hack-may-have-been-caused-by-security-issues-at-indian-it-giant-tata-consultancy-services> - In April 2025, British retailer Marks & Spencer (M&S) experienced a major cyberattack, later confirmed as a ransomware incident. The breach disrupted store operations, forced the shutdown of contactless and Click and Collect services, and halted online orders. This led to a market loss of £1 billion and potentially compromised customer data. The cybercriminal group Scattered Spider is believed to be responsible. Tata Consultancy Services (TCS), a long-term IT partner of M&S, is now investigating whether its infrastructure was the entry point for attackers. TCS, part of India’s Tata Group, has been previously targeted in other cyber incidents, including attacks on Tata Power and Tata Technologies. Scattered Spider, part of the broader hacking community known as 'the Com,' employs methods ranging from social engineering to SIM swapping and ransomware. The ongoing investigation aims to determine the extent of TCS's involvement or vulnerabilities, with results expected by June 2025. Both M&S and TCS have yet to issue official statements.
4. <https://www.ft.com/content/71bf35b0-740f-472f-96c6-86a9458e5844> - Marks & Spencer (M&S) is grappling with a major cyberattack, potentially costing the company £300 million in profits and severely disrupting online operations for over a month. The incident led to halted online orders, inventory shortages, and stolen customer data, with full system recovery possibly delayed until July. Despite this, the FTSE 100 retailer reported strong results in food and fashion, underscoring a business resurgence. To mitigate investor concerns, M&S raised its dividend by 20%, though its share price has dropped by approximately £750 million. Customer sentiment remains surprisingly positive, with many loyal shoppers expressing support rather than outrage. The company’s transparent crisis communication, including prompt warnings and apologies, has helped maintain trust. Other retailers like the Co-op and Harrods were also targeted, deflecting blame to a third-party supplier. M&S has boosted in-store staffing and ensured rapid customer service response times. Analysts caution against rushing restoration efforts, emphasizing the importance of getting it right. Despite the setbacks, M&S retains top rankings in customer trust surveys. The situation highlights the brand’s resilience and the key role of frontline staff in preserving customer loyalty. Going forward, rewarding Sparks loyalty members could help restore goodwill and drive online traffic upon relaunch.
5. <https://www.reuters.com/business/retail-consumer/ms-food-sales-show-resilience-despite-cyberattack-says-nielseniq-2025-05-29/> - Despite a recent cyberattack, Marks & Spencer's food business demonstrated strong performance, with sales increasing by 10.8% year-on-year in the 12 weeks leading up to May 17, 2025, according to NielsenIQ. The retailer’s share of the UK grocery market rose by 20 basis points to 3.8%. However, the growth rate slowed compared to the 14.7% increase reported in the previous NielsenIQ period. The cyberattack forced M&S to halt online clothing orders and shut down other systems, negatively affecting food availability and increasing waste and logistics costs. As a result, the company projected a loss of about £300 million ($404 million) in operating profit, with service disruptions likely to continue until July. NielsenIQ’s data aligns with findings from Kantar, which showed strong sales growth from competitors like Aldi, Lidl, Tesco, Sainsbury’s, and Ocado. Notably, M&S is not fully represented in Kantar's market data.
6. <https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8> - Recent cyber attacks, including a significant one on British retailer Marks and Spencer (M&S), highlight that humans remain the weakest link in cybersecurity. M&S reportedly lost up to £300 million in profits and saw its market value drop by £750 million after criminals exploited social engineering tactics through a third-party supplier. These methods involved deceiving IT staff into resetting passwords or authentication processes. Other UK retailers like the Co-op and Harrods have also been targeted by a group known as Scattered Spider, previously linked to attacks on major US companies. Unlike traditional state-linked cybercriminals, Scattered Spider includes English-speaking hackers based in the UK and US and uses human manipulation tactics such as impersonation and SIM swapping. Despite M&S increasing cybersecurity investment and staffing, their systems were still breached, underscoring the vulnerability of supply chains and human error. Businesses are urged to prioritize cybersecurity at the board level, enforce stricter identity verification, improve staff training, impose standards on third-party vendors, and maintain a robust, rehearsed incident response plan. As commercial entities increasingly become targets, the cost of inadequate cybersecurity can far outweigh preventive investments.
7. <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.