# Marks & Spencer faces up to £300m hit from cyber attack that exposed supplier vulnerabilities



Marks and Spencer (M&S) recently found itself in the challenging grip of a cyber attack that has not only disrupted its operations but is also set to significantly dent its financial outlook. Just as the FTSE 100 retailer was celebrating strong annual results, including a 22% increase in adjusted pre-tax profits to £875.5 million, CEO Stuart Machin revealed the grim reality that the company could see a reduction in this year’s operating profits by up to £300 million. The unexpected safety breach, disclosed on April 22, has forced M&S to shut its online clothing business for over three weeks, leading to substantial losses and the theft of customer data.

The breach occurred through social engineering tactics targeting a third-party supplier, a revelation that CEO Machin shared pointedly with analysts. He noted the unexpected vulnerability that arose from relying too heavily on external partners for IT services, emphasising that while M&S had invested in robust cybersecurity measures over recent years, the attack highlighted a significant blind spot in its security architecture. Rafe Pilling, threat intelligence director at Secureworks, remarked that social engineering often proves to be the "Achilles' heel" even for well-resourced organisations.

As M&S battles to regain footing, it is not alone in facing such threats. Other prominent UK retailers, including the Co-op and Harrods, have recently reported similar attacks, underscoring a turbulent landscape for retail cybersecurity. The rise of cybercrime is alarming, with recent statistics indicating that over 40% of UK businesses have experienced a cyber incident in the past year. This broadening threat has led insurers to demand better disclosure of risk controls from their clients, particularly those with considerable reliance on third-party services.

The immediate financial implications for M&S are stark. Following the announcement of the attack, the retailer saw its market capitalisation plunge by over £750 million, with its shares falling by 13%. Analysts estimate that the total losses could reach up to £125 million if issues persist. In response, M&S is not only focused on recovering lost ground but is also intent on accelerating its technological transformation. The company aims to compress a planned two-year overhaul into six months, a decision that reflects both urgency and an acknowledgment of evolving consumer expectations in the digital retail space.

Machin described the attack as one of the most challenging situations he and his team have ever faced, noting the emotional toll on employees who worked tirelessly to address the breach. As they navigate the recovery, M&S has prioritised cybersecurity enhancements, increasing its cybersecurity investments and quadrupling its cyber team over the past two and a half years. Yet, even with these measures in place, the company’s experience serves as a sobering reminder of the precarious balance between convenience, digital imperative, and security.

The protracted recovery process from the attack is expected to extend into July, with Machin stating that the firm has initiated a comprehensive sanitation of its digital systems to mitigate any further vulnerabilities. Surprisingly, he has indicated a cautious optimism about returning approximately 85% of its product range to online availability "quite quickly." Nevertheless, the long-term impacts of the incident on M&S's brand reputation and operational strategy remain uncertain. The company will have to work diligently to regain customer trust and shore up its digital infrastructure against future threats.

The issue of cybersecurity is not confined to M&S it has now become a focal point for businesses across various sectors. Executives are increasingly recognising the need to bolster their cybersecurity frameworks as they wrestle with the growing intertwining of retail with technology. The current landscape, shaped not only by financial imperatives but by shifting consumer demands, presents a complex challenge that requires a dual focus on innovation and security.

Ultimately, the incident at M&S exemplifies the critical nature of robust cybersecurity measures in an increasingly digital world, where the cost of complacency can be detrimental. As Machin reflects on the past weeks, he, alongside other industry leaders, is compelled to reassess their exposure and resilience in the face of evolving cyber threats, reinforcing that in today's business environment, it is essential to remain vigilant and prepared.

## Reference Map

1. Paragraph 1: [[1]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2), [[2]](https://www.ft.com/content/fa80b540-c836-4c45-a77f-38aa1693c656), [[3]](https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/)
2. Paragraph 2: [[1]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2), [[3]](https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/)
3. Paragraph 3: [[1]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2), [[4]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[5]](https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/)
4. Paragraph 4: [[2]](https://www.ft.com/content/fa80b540-c836-4c45-a77f-38aa1693c656), [[4]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[6]](https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e)
5. Paragraph 5: [[1]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2), [[5]](https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/), [[7]](https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders)
6. Paragraph 6: [[2]](https://www.ft.com/content/fa80b540-c836-4c45-a77f-38aa1693c656), [[4]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[6]](https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e)
7. Paragraph 7: [[4]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[5]](https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/), [[6]](https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e)
8. Paragraph 8: [[5]](https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/), [[6]](https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e)
9. Paragraph 9: [[5]](https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/), [[6]](https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e), [[7]](https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders)

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

## Bibliography

1. <https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2> - Please view link - unable to able to access data
2. <https://www.ft.com/content/fa80b540-c836-4c45-a77f-38aa1693c656> - Marks & Spencer (M&S) anticipates a £300 million hit to its operating profits this year due to a cyber attack attributed to 'human error'. The attack, which has severely disrupted M&S's operations, has resulted in the theft of personal customer data and the shutdown of its online clothing business for over three weeks. It also impacted the supply of food items and caused nearly £750 million in market capitalisation losses. CEO Stuart Machin revealed that the breach occurred due to social engineering tactics targeting a third-party supplier, rather than flaws in M&S’s IT infrastructure. While the company declined to comment on whether a ransom was paid, it is working to mitigate losses through cost management, insurance, and other measures, hoping to recover half the anticipated losses. Despite the disruption, M&S remains committed to accelerating its technology overhaul, compressing a planned two-year timeline into six months. The setback has overshadowed strong annual financial results, including a 22% rise in adjusted pre-tax profits to £875.5 million and a 6.1% increase in sales to nearly £14 billion, though reported pre-tax profits dropped 24% due to a significant impairment in Ocado Retail.
3. <https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/> - Marks & Spencer (M&S), a major British retailer, announced that a sophisticated cyberattack will reduce its operating profit by approximately £300 million ($403 million), with disruptions expected to persist into July. The attack temporarily shut down M&S's online clothing operations, disrupted food supplies, and wiped over £1 billion from its market value. Although online sales in the fashion, home, and beauty sectors were heavily impacted, in-store sales remained stable. The food division experienced reduced availability and higher logistics costs due to reverting to manual operations but has since shown signs of recovery. M&S aims to mitigate half of the profit loss in the 2025/26 fiscal year through insurance and cost management. Shares in the retailer fell by 13% since the incident. Despite the setback, the company remains committed to accelerating its technology transformation and recovery efforts. CEO Stuart Machin emphasized resilience and customer support. The incident follows an increasing trend of cyberattacks targeting UK businesses, which have also affected Co-op, Harrods, and the British Library. Meanwhile, M&S reported strong financial results prior to the attack, including a 22.2% rise in adjusted pretax profit and a 6.1% sales increase, benefitting food and clothing segments. Competitors like Next, Tesco, and Sainsbury’s may gain from M&S's online setbacks.
4. <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.
5. <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.
6. <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. Machin, appointed in 2022, stands to lose £831,000 from a performance share plan and £233,000 from a deferred bonus vesting in July, with total potential losses reaching around £2.4 million when considering his remaining incentive shares. 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.
7. <https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders> - 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”. Another customer posted on the same platform on Monday: “Nothing working Beckenham [in] London either, no pick ups or returns.” The attack on M&S follows a run of similar incidents in recent years. In September, Transport for London was forced to close down many online services after a cyber-attack. In 2023, Royal Mail was forced to ask customers to stop sending parcels and letters to overseas destinations after a cyber incident caused “severe service disruption” to international mail, and WH Smith was hit by an attack in which company data was accessed illegally, including the personal details of current and former employees. That came less than a year after a cyber-attack on WH Smith’s Funky Pigeon website forced it to stop taking orders for about a week. In 2022, the Guardian asked most of its staff to work from home after it was hit by a ransomware attack in which the personal data of UK staff members was accessed.