# M&S faces £300 million profit hit after cyberattack but eyes recovery



For many businesses, the prospect of a £300 million dent to profits would be catastrophic, if not insurmountable. Yet, Marks & Spencer (M&S) finds itself in a somewhat unique position. As one of only four UK retailers to surpass annual profits of £1 billion, it is navigating these turbulent waters with a mix of resilience and strategic foresight. In a recent announcement, M&S reported a pre-tax profit of £875.5 million for the year ending on 29 March 2025, marking its most robust performance in over 15 years. However, alongside this commendable financial strength, the shadow of a significant cyberattack looms large, leading to heightened scrutiny of the retailer’s operational integrity.

The cyber breach, attributed to social engineering tactics that compromised a third-party supplier, has severely disrupted M&S’s operations, particularly its online clothing business, which was offline for over three weeks. Chief Executive Stuart Machin referred to the situation as “challenging,” but remained optimistic, asserting that M&S is committed to recovering from this setback and accelerating its technology transformation efforts. He stated, “It has been challenging, but it is a moment in time, and we are now focused on recovery, with the aim of exiting this period a much stronger business.”

This focus on recovery is crucial, especially as M&S prepares for the significant operational and reputational repercussions of the attack. Approximately £1 billion in market value was wiped out as a direct consequence of the incident, which highlights the considerable impact of cyber threats on corporate performance. M&S has stated that it aims to offset half of its projected £300 million profit loss through insurance claims and cost management strategies. Given that the UK has witnessed a notable rise in cyberattacks, with over 40% of businesses acknowledging such incidents in the past year, this breach serves as a stark reminder of the vulnerabilities that even established companies face.

The cyberattack has also raised questions about M&S’s preparedness. Analysts have pointed out that while the company had increased its cybersecurity budget by 75%, vulnerabilities stemming from reliance on third-party service providers remain a significant concern. The use of social engineering tactics highlights a method of intrusion that exploits human error rather than technical failings, suggesting that a multifaceted approach to cybersecurity may be necessary for robust protection.

Despite the immediate fallout, there are indications that M&S's underlying business remains on solid ground. For instance, while its online sales have been severely affected, in-store sales have held steady, and the retailer has managed to secure a 6.1% increase in overall sales. Aarin Chiekrie, an analyst with Hargreaves Lansdown, noted that the situation may offer a “compelling entry point” for investors, suggesting that capitalising on the company’s current valuation—which reflects the ongoing turmoil—could yield benefits in the long run.

The company's strategy will likely be scrutinised in light of the potential for regulatory repercussions. With the Information Commissioner’s Office (ICO) enforcing stringent data protection regulations, the possibility of fines for inadequate data security measures looms large. As Dan Coatsworth from AJ Bell remarked, “It suggests hackers have caused considerable damage to the company from a financial and reputational perspective.” This regulatory uncertainty is coupled with M&S's intent to proactively enhance its systems and practices in the wake of the breach.

While the fallout from the attack will remain a pressing concern in the near term, M&S appears determined to leverage this moment of crisis as a catalyst for organisational growth. As the retailer embarks on its recovery journey, the resilience attributed to its 140-year history will be put to the test. Only time will reveal the full impact of this incident on M&S’s reputation and market standing. Nonetheless, the company’s commitment to harnessing this challenge as an opportunity may ultimately define its path forward, ensuring that it emerges not merely intact, but fortified for the future.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6
2. Paragraphs 4, 5
3. Paragraphs 1, 2, 4
4. Paragraphs 1, 4, 5
5. Paragraphs 1, 2, 4
6. Paragraphs 2, 3, 5

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

## Bibliography

1. <https://www.heraldscotland.com/news/25181946.marks-spencer-looks-move-300m-cyber-hit/?ref=rss> - 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 has severely disrupted M&S's operations, resulting in the theft of personal customer data and the shutdown of its online clothing business for over three weeks. 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. The company 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://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/19dcd993-877e-43c5-aab4-c727e574e3f2> - Marks & Spencer (M&S) fell victim to a significant cyberattack just as it was reporting strong financial performance. The attack, which began over the Easter holidays, disrupted its online clothing business for more than three weeks, compromised customer data, and wiped £750 million off its market value. M&S now estimates a potential reduction of up to £300 million in this year’s operating profit. CEO Stuart Machin revealed that cybercriminals used 'social engineering' tactics to infiltrate through a third-party supplier, bypassing M&S's direct cyber defenses. This method involves deceiving IT personnel into granting access by impersonating employees. M&S, like other retailers recently targeted—including Harrods and the Co-op—relies heavily on external IT service providers such as Tata Consultancy Services. Although M&S had increased its cybersecurity investment by 75% over the past year and expanded its cyber team, vulnerabilities via third-party providers remain a concern. Full restoration of ecommerce operations may take until July as the company meticulously cleanses over 600 applications and thousands of servers. The incident has triggered internal reviews, with the possibility of executive bonus reductions. Despite the setback, Machin emphasized that M&S is committed to a careful recovery to prevent long-term damage.
6. <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.