# Cyber-attack costs Marks and Spencer £300 million and forces urgent network overhaul



The recent cyber-attack on Marks and Spencer (M&S) underscores a growing concern for the retail sector amid increasing technological integration. Once perceived as a bastion of strong cyber defences, M&S now finds itself at the mercy of sophisticated cybercriminals. The company estimates that this incident will cost it around £300 million, a substantial blow that could have been channelled into further business development and operational growth. Instead, this financial setback is prompting M&S to expedite its network upgrades, aiming to enhance its cyber resilience in an era where digital threats loom large over enterprises.

Cyber-attacks on major retailers are becoming increasingly common, posing significant risks not only to corporate reputations but also to investor confidence. The M&S incident, which reportedly disrupted contactless payments and forced the suspension of online orders, is a stark reminder of the vulnerabilities inherent in today’s digital landscape. In a statement following the attack, M&S assured customers that it was working closely with the National Cyber Security Centre and cybersecurity experts to mitigate the fallout and restore operations. However, this disruption has already led to a reduction in physical store product availability, compounding the difficulties faced by the retailer during a critical sales period.

The attack has implications not just for M&S's immediate financials but for the broader retail industry as well. Market analysts noted that the company's stock value has taken a significant hit, with estimates indicating a £30 million reduction in underlying profits due to the incident. Nevertheless, experts maintain a cautiously optimistic outlook, suggesting that immediate communication and the absence of customer data breaches may mitigate long-term damage to the brand. The swift responses and operational adjustments implemented by M&S are indicative of a company keen to not only address the crisis but also prevent future occurrences.

The rising trend of cyber threats is not solely damaging; it is also reshaping investment landscapes. Companies specialising in cybersecurity, such as Palo Alto Networks and CrowdStrike, have benefitted from heightened awareness and demand for robust security solutions. London-listed firms, including NCC and Softcat, also stand to gain from the increasing need for protective measures against cybercrime. As the market's focus intensifies on how companies manage cyber risks, investor confidence may increasingly hinge on demonstrable capabilities in cybersecurity resilience.

Moreover, the insurance market is likely to see a surge in demand as businesses recognise the necessity of protecting themselves against breaches. Insurers, such as Beazley and Hiscox, are anticipating this uptick, particularly in the realm of cyber risks, where claims are often capped to avoid unbridled financial exposure. However, companies such as M&S need to be cautious in their approach to cybersecurity spending, ensuring that investments translate into meaningful security enhancements and not just perceived costs.

Ultimately, the repercussions of such cyber incidents reach far beyond the immediate financial losses. The M&S attack serves as a clarion call for retailers and investors alike: a reminder that security measures must be prioritised in a digitised economy. Understanding and investing in cybersecurity not only protect a company’s assets and data but also fortify its market standing in an increasingly competitive landscape. As larger businesses may face scrutiny over their defensive capabilities, it is imperative for all companies to take proactive measures to safeguard against these persistent threats.

The lessons learned from M&S's experience will likely reverberate throughout the retail sector and beyond, reinforcing the necessity of robust cyber defences to protect against not only financial damage but also the erosion of consumer trust.

### Reference Map

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

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

## Bibliography

1. <https://www.ft.com/content/5a577869-00f8-4a82-95d4-c7f737d3d73f> - Please view link - unable to able to access data
2. <https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders> - Marks & Spencer (M&S) experienced a cyber incident affecting contactless payments and online orders. The company reported the issue to the National Cyber Security Centre and engaged cybersecurity experts to investigate. M&S apologized for the inconvenience and implemented temporary operational changes to protect customers and the business. Despite the disruptions, physical stores remained open, and the website and app continued to operate normally. The incident highlights the increasing prevalence of cyber-attacks targeting major retailers.
3. <https://www.theguardian.com/business/2025/apr/30/marks-and-spencer-cyber-attack-products-run-short-in-some-stores> - Following a cyber-attack, Marks & Spencer (M&S) faced disruptions leading to product shortages in some stores. The company took systems offline to manage the incident and worked to restore normal availability. The Metropolitan Police's cybercrime unit and the National Crime Agency investigated the attack, which was linked to the hacking collective Scattered Spider. M&S paused online orders and deliveries of certain food items to Ocado, resulting in a significant decline in the company's market value.
4. <https://www.theguardian.com/business/2025/apr/28/m-and-s-marks-spencer-warehouse-staff-cyber-attack> - Marks & Spencer (M&S) paused online orders and deliveries of some food items to Ocado following a cyber-attack. The disruption led to the temporary closure of its online store, affecting daily sales of approximately £3.8 million. M&S apologized for the inconvenience and took actions to protect its network. The cyber-attack, attributed to the Scattered Spider hacking group, resulted in significant financial impact and operational challenges for the retailer.
5. <https://www.theguardian.com/business/2025/apr/25/marks-and-spencer-pauses-online-orders-cyber-attack-fallout> - Marks & Spencer (M&S) paused online orders due to a cyber-attack affecting contactless payments and online services. The company engaged cybersecurity experts and took systems offline to manage the incident. M&S apologized for the inconvenience and implemented measures to protect its network. The attack, linked to the Scattered Spider hacking group, underscores the escalating threat of cybercrime to retailers. M&S is working to restore normal services and prevent future incidents.
6. <https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it> - Marks & Spencer (M&S) and Harrods were targeted by cyber-attacks, leading to significant disruptions. M&S faced a cyber-attack that halted online shopping, affecting daily sales of approximately £3.8 million. The attack, attributed to the Scattered Spider hacking group, resulted in a market value loss of over £700 million for M&S. Both retailers are working with cybersecurity experts and law enforcement to investigate the incidents and restore services. The attacks highlight the growing threat of cybercrime to major retailers.
7. <https://www.proactiveinvestors.com/companies/news/1070597/marks-spencer-falls-further-as-analysts-calculate-30m-hit-from-cyber-attack-1070597.html> - Analysts estimate that Marks & Spencer (M&S) faces a £30 million hit to underlying profits due to a cyber-attack. The disruption has led to a decline in the company's stock value, with shares falling over 9% since the incident. Despite the financial impact, analysts believe there is no long-lasting damage to the brand, citing M&S's effective communication and the absence of evidence that customer data was compromised. The company is working to resolve the issue and restore normal operations.