# Marks and Spencer faces £300m cyberattack hit while planning bold Homebase expansion



Despite the May bank holiday weekend typically being a quieter period for news, Marks and Spencer (M&S) continued to dominate headlines, notably in the wake of its recent annual results. CEO Stuart Machin has been prominent in public discussions, especially following an interview with the Mail on Sunday. In this interview, he opted to downplay the severe impact of a recent cyberattack on the company, which he described as merely “an incident, a setback, a bump in the road.” This attack has already been projected to wipe £300 million from the retailer's profit forecast for the upcoming year, a significant figure that raises questions about the extent of the damage inflicted.

The cyberattack, which emerged over the Easter break, was attributed to a hacking group named Scattered Spider, noted for employing advanced techniques such as phishing and SIM swapping. While Machin acknowledged that the attack was a shock, he expressed confidence in the company’s resilience, stating, “We intend to come back better and stronger than ever.” This sentiment echoes a broader narrative in the retail sector, with many firms showing a willingness to adapt and recover despite the mounting pressures of cyber threats.

Faced with operational disruptions including significant issues with contactless payments and online orders, M&S has since suspended its online services to address these vulnerabilities. Reports suggest the financial ramifications could total £30 million annually, with ongoing losses estimated at £15 million weekly. This has prompted a collaboration with cybersecurity experts and law enforcement, underscoring a wider imperative for UK retailers to bolster their cyber defenses amidst escalating threats.

Amid these challenges, M&S has also announced strategic moves intended to enhance its market presence. The company is set to acquire 12 former Homebase stores to convert them into larger branches specialised in M&S Food. This bold initiative is framed as part of the company’s recovery strategy and aims to employ hundreds of staff while introducing features like bakeries that compete with established names such as Gail’s. This reflection of forward-thinking management contrasts starkly with the ongoing cyber crisis, indicating that M&S is striving to balance recovery with growth.

Furthermore, the landscape for British retailers is complicated by external factors, particularly in relation to trade policies initiated under the Trump administration. Recent announcements concerning proposed tariffs on EU goods reflect a tumultuous trade relationship, set against an already complex backdrop of Brexit negotiations. Experts suggest these tariffs could exacerbate existing vulnerabilities, with analyses indicating that the UK’s trade performance remains critical, yet precarious. Despite some optimism among UK firms regarding international growth, the overarching sentiment is one of caution, reiterating concerns over rising business costs and market instability.

Meanwhile, in the realm of store security, developments around surveillance technology are generating substantial discussion. Tesco is the latest supermarket transitioning to advanced, AI-powered camera systems at self-checkout points, designed to alert customers if their scanning processes do not register items correctly. This innovation comes amid legal challenges facing Asda, where privacy advocates have raised alarms over its use of facial recognition technology, labelling it an infringement on data rights. These technological advancements and legal entanglements raise significant ethical questions about shopper privacy and the surveillance practices of major retailers.

In summary, while Marks and Spencer grapples with the aftermath of a major cyberattack, its efforts to expand and recover signal a commitment to resilience. The retail sector's structural shifts, combined with external pressures from trade policies and evolving security technologies, paint a complex picture of a marketplace in transition, underscored by challenges that require proactive adaptation and strategic foresight.

## Reference Map:

* Paragraph 1 – [[1]](https://www.thegrocer.co.uk/news/media-bites-27-may-mands-trade-deals-and-store-security/704890.article), [[2]](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it)
* Paragraph 2 – [[2]](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it), [[6]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos), [[7]](https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/)
* Paragraph 3 – [[1]](https://www.thegrocer.co.uk/news/media-bites-27-may-mands-trade-deals-and-store-security/704890.article), [[5]](https://www.reuters.com/breakingviews/trump-reciprocal-tariffs-are-key-test-eu-unity-2025-02-19/)
* Paragraph 4 – [[3]](https://www.ft.com/content/f0aa939f-b179-44e4-8420-68aca684ac63), [[4]](https://www.ft.com/content/9b1f982a-485c-4868-9a03-b7e58a6f5746)
* Paragraph 5 – [[1]](https://www.thegrocer.co.uk/news/media-bites-27-may-mands-trade-deals-and-store-security/704890.article), [[6]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos)

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

## Bibliography

1. <https://www.thegrocer.co.uk/news/media-bites-27-may-mands-trade-deals-and-store-security/704890.article> - Please view link - unable to able to access data
2. <https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it> - In April 2025, British retailers Marks & Spencer (M&S) and Harrods suffered cyberattacks disrupting their operations. M&S faced issues with contactless payments and online orders, leading to a suspension of online services and significant financial losses. The attack was linked to the hacking group Scattered Spider, known for using techniques like phishing and SIM swapping. Harrods also confirmed a cyberattack but assured customers that its operations continued as normal. Both companies are collaborating with cybersecurity experts and law enforcement to investigate the incidents. ([aljazeera.com](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it?utm_source=openai))
3. <https://www.ft.com/content/f0aa939f-b179-44e4-8420-68aca684ac63> - In early 2025, U.S. President Donald Trump proposed a 'reciprocal' tariff plan aimed at addressing the U.S. trade deficit by imposing tariffs equivalent to those levied on U.S. goods by other countries, including the EU. This plan targets non-tariff barriers such as the EU's VAT and digital services taxes. The proposal has raised concerns about potential violations of World Trade Organization rules and marks a shift from traditional U.S. trade policy. The EU is considering responses, including lowering car tariffs to avoid punitive U.S. actions, though significant changes to VAT regimes remain unlikely. ([ft.com](https://www.ft.com/content/f0aa939f-b179-44e4-8420-68aca684ac63?utm_source=openai))
4. <https://www.ft.com/content/9b1f982a-485c-4868-9a03-b7e58a6f5746> - The European Union (EU) is preparing a two-pronged trade plan to respond to potential actions by Donald Trump if he wins a second term as U.S. president. The strategy involves offering a swift trade deal to avoid conflict or, alternatively, implementing targeted retaliatory tariffs if Trump enforces his proposed 10% minimum tariff, which could impact EU exports by €150bn annually. European Commission officials are planning early negotiations with Trump's team to explore increasing purchases of U.S. goods. However, if negotiations fail and tariffs are imposed, the EU is ready to impose substantial tariffs on selected U.S. imports. During Trump's first term, the EU faced tariffs on steel and aluminium, leading to responses targeting key Trump constituencies. EU Trade Commissioner Valdis Dombrovskis stresses the importance of cooperation but affirms readiness to defend the EU's interests. Previous EU-U.S. trade adjustments included deals on lobsters, beef, and soybeans. The EU maintains a trade surplus and notes challenges in substantially increasing U.S. exports. Economic experts predict that a tariff war could be more detrimental to the EU’s economy than the U.S.’s, though it would also heighten U.S. inflation. ([ft.com](https://www.ft.com/content/9b1f982a-485c-4868-9a03-b7e58a6f5746?utm_source=openai))
5. <https://www.reuters.com/breakingviews/trump-reciprocal-tariffs-are-key-test-eu-unity-2025-02-19/> - Donald Trump's proposed 'reciprocal' tariffs pose a serious challenge to the European Union's unity. These tariffs enable Trump to arbitrarily target specific countries within the EU, potentially creating division among the 27 member states. For example, a 25% levy on European car imports, which largely affects Germany and Italy, could lead to friction as countries like Spain, which don't benefit as much, may see such a response as wasted effort. Additionally, if Trump imposes tariffs on individual member states, like a hypothetical 50% tariff on Denmark, other members might be reluctant to retaliate, fearing economic repercussions. This fragmentation could be exploited by Trump to pressure individual EU states or gain concessions, such as encouraging more U.S.-based manufacturing. Although the EU can respond with countermeasures, coordinating a united trade response becomes difficult and could weaken internal solidarity. ([reuters.com](https://www.reuters.com/breakingviews/trump-reciprocal-tariffs-are-key-test-eu-unity-2025-02-19/?utm_source=openai))
6. <https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> - The cyberattack on Marks & Spencer (M&S) in April 2025 led to significant operational disruptions, including issues with contactless payments and online orders. The company suspended online services and faced financial losses, with estimates suggesting a £30 million impact on annual profits and ongoing losses of about £15 million per week. The attack was linked to the hacking group Scattered Spider, known for using techniques like phishing and SIM swapping. The National Cyber Security Centre (NCSC) is working with affected companies, urging all UK businesses to strengthen their cybersecurity measures. The incident has raised concerns about the vulnerability of UK retailers to cyberattacks and the need for enhanced security protocols. ([theguardian.com](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos?utm_source=openai))
7. <https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/> - Marks & Spencer (M&S) experienced a cyberattack in April 2025, leading to widespread disruptions, including issues with contactless payments and online orders. The attack is believed to have been conducted by the hacking group 'Scattered Spider,' known for deploying ransomware to encrypt key systems. The company has engaged external cybersecurity experts to investigate and manage the incident, taking actions to further protect its network and maintain customer service. M&S stores, website, and app remain operational, but some services, such as Click and Collect, have been affected. The company has notified data protection supervisory authorities and the National Cyber Security Centre. ([bleepingcomputer.com](https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/?utm_source=openai))