# Marks & Spencer cyberattack reveals urgent need for UK retail cybersecurity overhaul



The recent cyberattack on Marks & Spencer (M&S) has unveiled significant vulnerabilities within the UK's retail sector, an alarming development in the ongoing battle against cybercrime. The attack, attributed to the cybercrime group DragonForce, has not only disrupted M&S’s operations—rendering its click and collect service unavailable—but has also exposed the broader implications of corporate cyber insecurity. Indeed, this incident encapsulates the multifaceted threats faced by retailers today, particularly those with extensive customer databases and digital infrastructure.

DragonForce, which claims a mandate of levying financial penalties rather than outright destruction, asserted responsibility for the attack, citing a protective stance towards the former Soviet Union and warning against the misuse of their ransomware in that region. The group has stated that it will “punish any violations” by hackers who might use their tools against critical infrastructure, which underscores a complex interplay of motivations amongst cybercriminals. Their declaration hints at a quasi-regulatory posture over the intricacies of the ongoing cyber-war, as they navigate alliances and enmities in the shadowy landscape of the dark web.

M&S disclosed the cyber incident on April 22, which has led to an alarming 12% decline in its stock prices and an estimation that the financial repercussions could reach upwards of £30 million. Analysts predict that ongoing disruptions could cost the retailer around £15 million per week, with full recovery expected to take weeks or even longer due to the intricate reconstruction needed for its compromised networks. The National Cyber Security Centre (NCSC) has since advised retailers to rethink their cybersecurity protocols, particularly around IT help desk operations, as the attackers successfully impersonated M&S employees to gain access to internal systems.

This incident is not isolated; it is part of a worrying trend highlighted by the NCSC, which has reported a surge in cyberattacks targeting major retailers such as the Co-op and Harrods. Retailers present attractive targets due to their reliance on legacy systems along with the vast quantities of customer data they hold. Experts believe that the modus operandi employed in the M&S attack might involve social engineering tactics, where attackers manipulate individuals into breaching security protocols. In the case of Co-op, hackers extracted customer details after initially misleading staff about the severity of the breach, an approach that echoes vulnerabilities exposed in the M&S incident.

Furthermore, the ongoing challenges posed by the hacking group Scattered Spider add another layer of complexity. Known for their sophisticated tactics, which reportedly involve leveraging tools from more established ransomware factions like BlackCat and ALPHV, Scattered Spider has been implicated in numerous high-profile attacks. Notably, they have orchestrated disruptive actions against major organisations, including MGM Resorts and Caesars Entertainment, evidencing a widespread and damaging operational footprint. Recent investigations have suggested that their operations are not purely opportunistic, as evidence points to a potential collaboration with DragonForce illustrating a shared modus operandi focused on financial gain rather than outright sabotage.

The UK government is now reinforcing the need for improved practices across sectors, having recognised cybersecurity as a paramount concern following incidents like these. At an upcoming CyberUK conference, Cabinet Office Minister Pat McFadden is expected to emphasise the necessity of treating cybersecurity as an “absolute priority,” following calls for more stringent measures under new legislation aimed at fortifying national defence against cyber threats.

As the dust settles on the M&S incident, it serves as a stark reminder of the growing sophistication of cybercriminal operations and the urgent need for retailers to innovate their cybersecurity measures. While M&S scrambles to regain control of its systems, the increased scrutiny from regulators and the public at large highlights a crucial juncture for the retail sector. Ensuring robust cybersecurity isn't merely an operational necessity; it’s a fundamental component of sustaining trust in an increasingly digital consumer landscape.

### Reference Map

* Paragraph 1: (1), (4), (5)
* Paragraph 2: (1), (7)
* Paragraph 3: (2), (3)
* Paragraph 4: (4), (5)
* Paragraph 5: (3), (6)
* Paragraph 6: (6), (4)
* Paragraph 7: (6)

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14699457/hackers-target-Marks-Spencers-political-allegiance.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> - Cyberattackers targeted Marks & Spencer (M&S) and the Co-op Group by impersonating employees to deceive IT help desks into resetting passwords, granting them access to internal networks. The UK's National Cyber Security Centre has advised organizations to revise their help desk protocols to prevent similar breaches. M&S disclosed the cyber incident on April 22, leading to a 12% share decline and suspension of online clothing and home orders. Analysts estimate the financial impact at approximately £30 million, with ongoing losses of around £15 million weekly. Full recovery may take weeks due to the complexity of rebuilding networks.
3. <https://www.ft.com/content/602e10e7-00b3-4c9b-bb27-6480d7246f37> - The UK's National Cyber Security Centre (NCSC) has issued a warning to retailers about an increase in cyberattacks involving criminals impersonating IT help desks. This alert follows recent attacks on major retailers including Marks and Spencer (M&S), Co-op, and Harrods. The NCSC emphasized the risk of social engineering tactics, in which attackers deceive IT personnel into resetting passwords, thereby gaining unauthorized access to systems. Co-op revealed that hackers extracted customer names and contact details, after initially claiming the attack was unsuccessful. As a result, Co-op is facing store shortages due to operational disruptions. M&S, similarly affected, has been unable to process online orders for over a week and is also experiencing limited stock availability. Rafe Pilling, threat intelligence director at Secureworks, noted that the attacks likely involved account takeovers facilitated through social engineering rather than malware. Although the NCSC has insights into the incidents, it has not yet determined whether they are related or the result of a coordinated effort by a single threat actor.
4. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - Several major UK retailers, including Marks and Spencer (M&S), the Co-op, and Harrods, have recently been targeted by cyber attacks, highlighting the increasing vulnerability of the retail sector. M&S has faced significant operational disruptions and a £600 million drop in value due to these attacks. Investigations are ongoing, and experts suspect a common supplier or technology could link the incidents. Cybersecurity professionals suggest a potentially coordinated effort, possibly involving the group Scattered Spider, known for manipulating individuals to gain system access. The National Cyber Security Centre has expressed concern, urging businesses to treat cybersecurity seriously. Retailers are attractive targets due to their vast customer data, real-time operations, and reliance on legacy systems. Although some customer data was accessed, sensitive financial information reportedly remains secure. Cybersecurity apathy, especially among large UK retailers, has been noted in recent industry research. Experts warn that even without paying ransoms, attackers could profit by selling stolen data. The incidents serve as a stark reminder of the growing sophistication and impact of cybercrime on the retail landscape, with recovery potentially taking months.
5. <https://apnews.com/article/7d3c01faa7380775598a517df4db1250> - British retailers are facing a wave of cyberattacks, with Marks & Spencer (M&S) and Harrods among the latest high-profile victims. M&S has been grappling with an ongoing cyber incident since Easter weekend, disabling its ability to process online orders, hire new staff, or maintain regular website functions. Although some services like contactless payments have been restored, the disruption continues as M&S works intensively to resolve the issue. Meanwhile, Harrods acknowledged a cyber threat and has taken precautionary steps, including limiting internet access. The attacks, which may be linked to a group called Scattered Spider, have raised concerns in the UK retail sector following a similar incident at Co-op. Authorities, including London’s Metropolitan Police and the UK’s National Cyber Security Centre, are investigating and providing support. Experts across the cyber defense industry warn that the growing use of generative artificial intelligence is intensifying the cyber threat landscape and urge organizations to strengthen their digital defenses.
6. <https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/> - The British government is set to urge all UK businesses to prioritize cyber security following recent cyberattacks on major retailers Marks & Spencer (M&S), the Co-op Group, and Harrods. Cabinet Office Minister Pat McFadden, in coordination with national security officials and Richard Horne, CEO of the National Cyber Security Centre, outlined governmental support for affected companies. At the upcoming CyberUK conference in Manchester, McFadden will stress the need for heightened cyber precautions, describing the attacks as a 'wake-up call' and advocating for cyber security to be treated as an 'absolute priority.' New measures, including the Cyber Security Bill, are being introduced to strengthen national defense. M&S experienced significant disruption on April 25 due to a suspected ransomware attack by the group 'Scattered Spider,' which affected their online and contactless services. This incident follows a growing trend of cyberattacks causing extensive financial and operational damage across UK industries.
7. <https://www.axios.com/2024/11/20/scattered-spider-us-arrests> - The U.S. Justice Department has charged five men, Ahmed Hossam Eldin Elbadawy, Noah Michael Urban, Evans Onyeaka Osiebo, and Joel Martin Evans, who are allegedly part of the Scattered Spider hacker group. This group is accused of targeting multiple U.S. corporations, stealing millions of dollars in cryptocurrency, and deceiving employees with phishing texts. The charges include aggravated identity theft, conspiracy to commit wire fraud, and conspiracy to commit a crime. Scattered Spider has been linked to high-profile attacks on MGM Resorts and Caesars Entertainment, among others, with estimates suggesting the group has targeted around 100 organizations in total. If convicted, each defendant could face up to 20 years in federal prison for the wire fraud charges alone.