# Cyber attacks on Marks & Spencer and Co-op expose critical food sector vulnerabilities



Crippling cyber attacks on prominent UK retailers Marks & Spencer and Co-op have exposed significant vulnerabilities within the food and beverage sector, prompting a scramble to bolster cybersecurity measures. Nearly three weeks after the attacks, both companies are still contending with severe operational disruptions, resulting in empty shelves and suspended online shopping capabilities.

These recent incidents represent not only individual corporate crises but also a worrying trend in which the food sector has become a prime target for cybercriminals. Richard Werran of BSI articulated this shift, noting, “Cyber attackers have moved on from trying to attack banks and car manufacturers; they’re targeting the food sector because it’s such a weak sector.” This shift away from traditional targets underscores a rapidly evolving threat landscape that many within the industry have been slow to address.

Despite warnings from security experts, many companies within the sector have prioritised other operational needs over cybersecurity. David Mudd from BSI remarked earlier this year that there exists a damaging attitude: “The opinion seems to be, ‘We could spend these millions on security and something bad might not happen, alternatively we could spend the same millions somewhere else in the organisation and something good is going to happen.’” Yet, as the recent attacks demonstrate, the consequences of neglecting cybersecurity can be catastrophic.

Cabinet minister Pat McFadden echoed this sentiment, suggesting these incidents should serve as a wake-up call. During a government-organised meeting on cybersecurity, he stated, “Cybersecurity is not a luxury but an absolute necessity.” His comments were particularly poignant given that Marks & Spencer has not processed online orders since the attack on its IT systems, an infrastructure failure that has generated serious financial repercussions estimated at £30 million.

The attacks have also prompted a remarkable spike in interest surrounding cybersecurity—Bionic reports an increase of 320% in queries for cybersecurity support since the incidents. Google searches for the term “cyber attack” have surged by a staggering 588%, indicating widespread concern among businesses and the public alike. Laura Court-Jones from Bionic provided timely advice, emphasising that investing in preventative measures, such as regular software updates and employee training, is crucial in mitigating the risk of future attacks.

Concerns are not limited to large retailers; small businesses remain particularly vulnerable due to often inadequate security infrastructures. However, the incidents involving Marks & Spencer and Co-op have highlighted that even well-established corporations are not infallible. Furthermore, the situation complicates the relationship between retailers and cyber insurance providers. Holly Waszak, head of cyber claims UK at Marsh, noted that insurers are closely monitoring developments, with an expectation that retailers may soon need to demonstrate a minimum level of cybersecurity to qualify for insurance.

Adding to the complexity of this crisis, the UK’s National Cyber Security Centre (NCSC) has issued warnings about sophisticated social engineering tactics being employed by attackers—methods that involve tricking IT personnel into resetting passwords. This approach was reportedly used in the recent cyber incidents affecting Marks & Spencer and Co-op, with hackers impersonating employees to breach security protocols. Although Signs of a coordinated effort among hackers remain unconfirmed, such tactics underline the evolving sophistication of cyber threats.

As retailers such as Tesco prepare for increased scrutiny over their cybersecurity measures—citing ongoing efforts to enhance threat preparedness—the overarching message from government officials and industry experts is clear: the time for complacency has passed. The introduction of a new cybersecurity strategy highlights the government’s proactive stance, with McFadden linking the rise in cyber threats to the increasing adoption of artificial intelligence technologies. As these tools become more prevalent, they are expected to exacerbate existing vulnerabilities and create new avenues for attacks.

In summary, the cyber attacks on Marks & Spencer and Co-op have not only precipitated immediate operational chaos but have also ignited a broader industry reassessment of cybersecurity policies and practices. As the retail sector grapples with these challenges, the stakes have never been higher, demanding that both businesses and consumers remain vigilant in the face of an evolving and relentless cyber threat landscape.

### Reference Map

1. Paragraphs 1, 2, 3, 4
2. Paragraphs 1, 2
3. Paragraph 4
4. Paragraphs 5, 6
5. Paragraphs 7, 8
6. Paragraphs 9, 10
7. Paragraph 11

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

## Bibliography

1. <https://www.foodnavigator.com/Article/2025/05/12/marks-and-spencer-co-op-attacks-spike-cybersecurity-interest/> - Please view link - unable to able to access data
2. <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.
3. <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> - Cyberattacks on UK's Marks & Spencer (M&S) and Co-op Group were initiated by hackers impersonating employees and deceiving IT help desks into resetting passwords, according to BleepingComputer. This allowed intruders 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, having disclosed the cyber incident on April 22, witnessed a 12% share decline and subsequently suspended online clothing and home orders; food product availability has also been disrupted. Analysts from Deutsche Bank estimate the financial impact at approximately £30 million ($40 million), with ongoing losses of around £15 million weekly, though cyber insurance is anticipated to cover most of the initial losses. Full recovery may take weeks, as rebuilding networks is a complex process. Meanwhile, a group named DragonForce claimed responsibility for attacks on M&S, the Co-op, and Harrods, alleging theft of staff and potentially 20 million customer records. The attack on M&S has also been tentatively linked to the hacking group 'Scattered Spider' using DragonForce ransomware, though the National Cyber Security Centre has not confirmed any direct connection between these incidents.
4. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - UK retailers are facing significant cyber insurance premium increases, up to 10%, following high-profile cyber attacks on major chains such as Marks and Spencer (M&S), Harrods, and the Co-op. These attacks are prompting insurers to reassess cyber risk in the retail sector, which had enjoyed falling rates in 2023 and 2024. Experts warn cyber security scrutiny will intensify and some insurers may withdraw from the retail market. M&S may claim tens of millions of pounds for business interruption, after losing over £40 million in online sales during a lengthy system outage. The Co-op confirmed a data breach affecting numerous customers. The sector is particularly vulnerable due to large amounts of consumer data and outdated IT systems. Tesco acknowledged ongoing cyber threat preparedness in its annual report, citing crisis simulations involving ransomware. Insurance might cover not only ransomware payments but also costs associated with crisis response. However, insurers face challenges if attackers are linked to sanctioned entities. The UK’s cyber security agency has also issued warnings about attackers impersonating IT help desks in sophisticated social engineering scams. Brokers urge businesses to secure cyber insurance now before premiums rise further.
5. <https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/> - As AI technology becomes more widespread, the United Kingdom is expected to face an increase in both the frequency and severity of cyberattacks, according to Cabinet Office Minister Pat McFadden. Speaking at the CyberUK 2025 conference, McFadden announced the declassification of an intelligence assessment revealing that AI will escalate cyber threats in the coming years. In 2024, the National Cyber Security Centre (NCSC) received nearly 2,000 cyberattack reports, with 90 considered significant and 12 classified as highly severe—a threefold increase in major incidents from the previous year. Recent ransomware attacks have targeted notable British retailers including Marks & Spencer, the Co-op Group, and Harrods, resulting in significant operational disruptions. McFadden emphasized that cybersecurity is a vital necessity, not a luxury, and urged both public and private sectors to strengthen their defenses. The government plans to introduce a new cyber security strategy and legislate new powers under the upcoming Cyber Security and Resilience Bill. NCSC CEO Richard Horne also advocated for ending ransom payments to undermine the attackers' business model.
6. <https://www.reuters.com/sustainability/boards-policy-regulation/britains-co-op-says-hackers-have-extracted-customer-data-2025-05-02/> - On May 2, 2025, Britain's Co-operative Group reported that it had suffered a sustained cyberattack resulting in unauthorized access and extraction of customer data. The breach affected a significant number of current and former Co-op members, with compromised data including personal information such as names, contact details, and dates of birth. Importantly, the Co-op confirmed that no passwords, financial information (such as bank or credit card numbers), transaction data, or customer product or service details were compromised. The retail group, which operates more than 2,300 food stores across the UK and also offers funeral, legal, and insurance services, is working with the UK's National Cyber Security Centre and the National Crime Agency to investigate the incident. The attack follows a similar cyber incident recently targeting Marks & Spencer. The Co-op issued an apology to those affected by the breach.
7. <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.