# Cyber attacks on M&S and Co-op expose high-stakes vulnerabilities in UK retail sector



The recent wave of cyber attacks on major UK retailers, notably Marks & Spencer (M&S) and the Co-op, has revealed alarming vulnerabilities in the cybersecurity landscape. These incidents, attributed to a group claiming ties with the DragonForce hacking syndicate, have sent shockwaves through the retail sector, prompting urgent calls for enhanced security measures.

The hackers have positioned themselves as a new breed of cybercriminals, announcing their activities through Telegram under the banner of a 'Blacklist', aptly named after the popular US crime series. In a series of communications, they expressed frustration over the Co-op's resistance to their ransom demands, yet provided enough evidence of their claims to suggest a robust operation behind them. Through these exchanges, the group, which appears to model its tactics after the notorious Scattered Spider group, indicated that they were not merely after monetary gain but also sought notoriety.

The implications of the cyber attacks have been profound. M&S has faced severe operational disruptions, leading to an estimated £600 million loss in value, as their systems went down for an extensive recovery phase. Customers reported empty shelves and halted online sales, reflecting a chaotic response to the breach. While M&S struggled to restore functionality, Co-op appeared to navigate the storm with quicker recovery strategies, effectively yanking the plug on compromised systems before the situation escalated further.

The National Cyber Security Centre has called attention to the rising sophistication of such attacks, urging UK businesses to bolster their cybersecurity protocols. Alan Woodward, a cybersecurity professor at the University of Surrey, noted that M&S's delay in reinstating online sales suggested a lack of preparedness for such incidents. His remarks highlighted a critical aspect of the ongoing crisis—retailers must leverage better security practices to guard against potential breaches.

Security experts have indicated that the DragonForce group operates within a ransomware-as-a-service model, which commodifies cybercrime, making it accessible even to less skilled hackers. The BBC's cyber correspondent indicated that the group's tactics mirror those of Scattered Spider, suggesting a loosely coordinated effort aimed at exploiting weaknesses in the retail sector. This pattern of operation reflects an evolving threat landscape where attackers are increasingly adept at navigating corporate security frameworks.

Since these attacks, retailers across the UK are on high alert, fearing further breaches. The hackers have not ruled out additional strikes, stating their intention to name and shame victims if ransoms are not paid. Everyday customers and retailers alike have been left reeling as they navigate the new normal—heightened vigilance surrounding personal data security, and the sobering reality that the digital landscape continues to be a target for malicious actors.

As investigations unfold, the Information Commissioner's Office is looking into the breaches to ascertain the full extent of the damage. With reports of sensitive data being exfiltrated dating back to February, the urgency for comprehensive cybersecurity strategies has never been more pronounced. As the retail sector grapples with the aftermath, the focus now turns to enhancing defenses against a backdrop of evolving cyber threats.

In this rapidly shifting landscape, the lessons from these incidents will likely resonate well beyond the confines of the retail sector, prompting a collective effort to cultivate resilience against future cyber onslaughts.

### Reference Map

* Paragraph 1: (1), (2)
* Paragraph 2: (1), (5)
* Paragraph 3: (3), (4)
* Paragraph 4: (7), (6)
* Paragraph 5: (2), (4)
* Paragraph 6: (5), (3)
* Paragraph 7: (6), (7)
* Paragraph 8: (1), (4)

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14728533/Cyber-attack-hackers-op-Marks-Spencers-Blacklist-show.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - This article discusses recent cyber attacks targeting major UK retailers, including Marks & Spencer (M&S), the Co-op, and Harrods. It highlights the operational disruptions faced by M&S, which experienced a £600 million drop in value due to these attacks. The piece explores the possibility of a coordinated effort by threat groups like Scattered Spider and emphasizes the need for enhanced cybersecurity measures in the retail sector. The National Cyber Security Centre has urged businesses to take cybersecurity seriously, given the increasing sophistication of cyber threats.
3. <https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/> - This report details the cyber attack on Marks & Spencer, attributed to the Scattered Spider ransomware group. The attackers gained access to M&S's systems as early as February, exfiltrating sensitive data, and deployed the DragonForce ransomware in April, leading to significant operational disruptions. The article provides insights into the tactics used by Scattered Spider and the impact of the attack on M&S's operations and reputation.
4. <https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> - This article provides an in-depth look at the aftermath of the cyber attack on Marks & Spencer. It describes the operational challenges faced by the retailer, including empty shelves and disrupted services. The piece also discusses the financial implications, estimating a £30 million loss in annual profits and ongoing weekly losses of about £15 million. It highlights the broader impact of the attack on the retail sector and the need for improved cybersecurity measures.
5. <https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/> - This article examines the DragonForce cybercriminal syndicate, which has claimed responsibility for attacks on Marks & Spencer, the Co-op, and Harrods. It provides background on DragonForce's origins and evolution into a ransomware-as-a-service operation. The piece also discusses the potential involvement of the Scattered Spider group and the implications of these attacks for the retail sector's cybersecurity landscape.
6. <https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s> - This report focuses on the DragonForce ransomware believed to have been used in the cyber attack on Marks & Spencer. It details the operational disruptions caused by the attack, including issues with contactless payments and online orders. The article also highlights the financial impact, estimating daily losses of up to £3.5 million, and discusses the broader implications for cybersecurity in the UK retail sector.
7. <https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/> - This article discusses the UK's National Cyber Security Centre (NCSC) issuing guidance to strengthen cybersecurity defenses following cyber attacks on major retailers like Marks & Spencer, the Co-op, and Harrods. It details the nature of the attacks, including the use of DragonForce ransomware and tactics associated with Scattered Spider. The piece emphasizes the need for businesses to take cybersecurity seriously and provides recommendations for enhancing security measures.