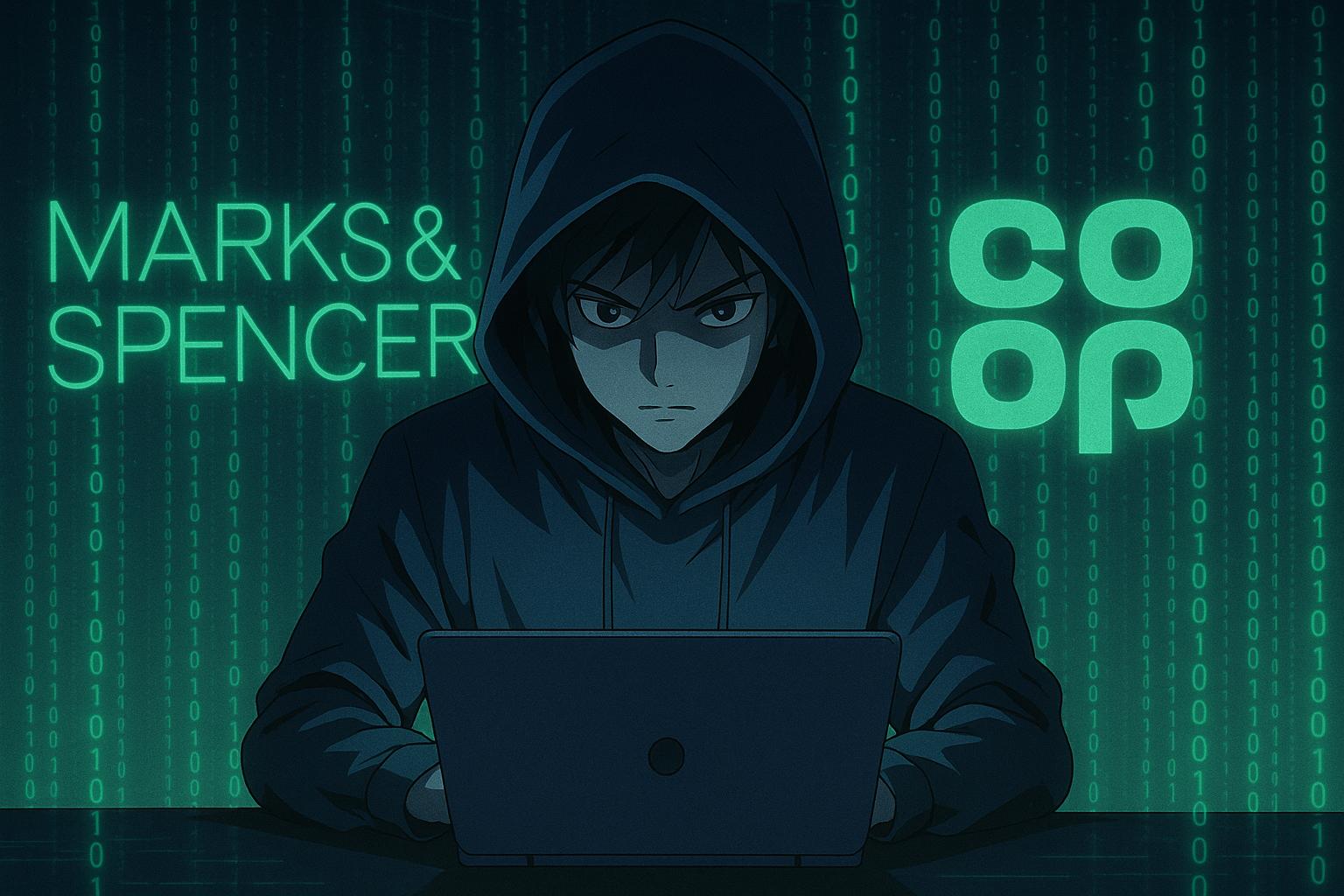
# DragonForce ransomware group exposes M&S and Co-op to crippling cyberattacks



Almost daily, my phone pings with messages from hackers of various stripes, each keen to share their exploits. As a seasoned cyber security correspondent, I have engaged with many over the years, though most conversations remain confidential. Recently, however, a message sparked my attention. “Hey. This is Joe Tidy from the BBC reporting on this Co-op news, correct?” the anonymous hackers wrote on Telegram. Intrigued, I initiated a dialogue that revealed the extent of their claims regarding recent cyber attacks on Marks & Spencer (M&S) and the Co-op.

Over the course of a five-hour exchange, it became evident that these hackers were not only articulate masters of English but also likely involved in the attacks that significantly disrupted both retailers. They provided evidence suggesting the theft of vast amounts of private customer and employee information. I reviewed a sample of this data before securely deleting it, understanding the gravity of its potential ramifications.

Shoppers have faced widespread inconveniences, with empty shelves becoming a common sight in Co-op stores across the UK. Initially, the Co-op downplayed the incident as manageable; however, after my inquiry, the company admitted to stakeholders that a substantial data breach indeed occurred. The hackers, frustrated by the Co-op's resistance to their ransom demands, later sent me an aggressive letter detailing their grievances with the retailer's response and claiming that their efforts had narrowly averted a more catastrophic scenario.

The group responsible for these breaches is known as DragonForce. They function as a cyber criminal service on the darknet, where they offer ransomware-as-a-service. This business model allows them to retain a cut from the ransoms paid by affiliates seeking to utilise their malicious software for extortion. DragonForce's emergence follows a notable shift in the cybercriminal landscape; with previous ransomware services like LockBit facing crackdowns, new players have vied for dominance. This has led to an arms race of sorts, with groups like DragonForce aggressively promoting enhanced services such as 24/7 customer support and advanced negotiation tools for ransomware claims.

The ramifications of these attacks have been significant for both retailers. M&S's share price plummeted by 16%, erasing approximately £1.3 billion from its market value, while analysts predicted that the overall financial impact could exceed £125 million if disruptions continued. Cyber insurance may provide some respite, with M&S expected to claim up to £100 million to offset losses. Nevertheless, persistent operational challenges remain. Online services have been hampered, with customers grappling with limited access, prompting the company to pause its loyalty offers and reset customer passwords as a precautionary measure against further breaches.

As the situation unfolded, it was reported that DragonForce had used social engineering tactics to breach internal systems, impersonating employees to deceive IT help desks into resetting passwords. This method exemplifies the tactics cybercriminals employ, often exploiting basic vulnerabilities rather than complex technological exploits. Such incidents underscore the ongoing need for organisations to refine their security protocols.

This latest wave of cyber incidents strikes a chord with the broader theme of increasing cyberattacks targeting retailers in the UK. While M&S attempts to salvage operations, the Co-op recently announced that its systems have returned to normal following a similar breach, highlighting a pervasive trend that poses grave risks to businesses across the retail sector.

The evolving landscape of cyber threats reveals an urgent need for enhanced strategies in both prevention and response. As the reality of these digital attacks becomes more pronounced, it is imperative that organisations not only bolster their defences but also embrace a collaborative approach to mitigate risks and protect vital consumer information.

### Reference Map

1. Paragraphs 1, 2, 3, 4
2. Paragraphs 5, 6
3. Paragraph 7
4. Paragraphs 8, 9
5. Paragraph 10
6. Paragraph 11
7. Paragraph 12

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

## Bibliography

1. <https://www.bbc.com/news/articles/cgr5nen5gxyo> - Please view link - unable to able to access data
2. <https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e> - Marks and Spencer (M&S) CEO Stuart Machin is set to lose up to £1.06 million from his pay package due to a cyber attack that triggered a 14% drop in the company’s share price. The cyber attack, disclosed in April 2025, compromised customer data, disrupted online orders for three weeks, and led to stock shortages in stores. Analysts estimate the retailer may have already lost around £75 million in revenue, with potential losses rising to £125 million if disruptions continue through May. While M&S may claim up to £100 million in insurance, the incident risks affecting its broader transformation efforts, including back-end automation and digital improvements. Despite the setback, M&S posted a strong financial year prior to the attack, with expected pre-tax profits of £840 million and a 14.7% year-on-year sales increase. However, the damage from the cyber incident may weigh heavily on first-quarter 2026 performance and long-term strategy execution.
3. <https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems> - Marks & Spencer (M&S) continues to face serious operational disruptions following a cyberattack that occurred over the Easter weekend. Online orders through its website, app, and phone have been suspended since April 25, with no confirmed restart date. The attack compromised some customer data, including names, contact information, and order histories, though no payment details or passwords were exposed. As a security measure, customers will be prompted to reset their passwords upon their next login. Services including Sparks loyalty offers have been paused, and in-store stock availability remains inconsistent, as illustrated by images of empty shelves shared by shoppers online. The cyberattack has severely impacted M&S financially, with an estimated £4 million a day in lost online sales and an 18% drop in share value, erasing over £1 billion in market capitalization. While some affected customers have been compensated with gift cards, broader investor confidence is shaken due to limited communication from M&S. The ransomware group “DragonForce” has claimed responsibility for the breach. Despite these challenges, M&S's core food business and partnerships like Ocado remain unaffected, providing a silver lining during this crisis. The company is actively working to resolve the issue though no timeline has been confirmed.
4. <https://www.ft.com/content/55221f2d-00b3-4856-9158-dfdd0263bd0c> - The article, written by the director of the Cambridge Cybercrime Centre, critiques the glamorization of cybercriminal groups like 'Scattered Spider.' Despite recent disruptions to UK retailers such as Marks and Spencer, the Co-op, and Harrods speculated to be linked to this group, its actual methods rely more on basic social engineering tactics than advanced technical skills. These include phishing, SIM swapping, and exploiting weak verification processes to gain unauthorized access. The cybersecurity industry, aiming to market its products, often assigns dramatic names to such groups—Scattered Spider being coined by CrowdStrike—which helps sensationalize their impact and sells fear-based solutions. These names can unintentionally bolster the criminals' status and recruitment appeal, especially among young offenders seeking prestige. The article argues for a shift away from inflated narratives toward a mature approach to cybersecurity, emphasizing early intervention, better detection, law enforcement training, and international cooperation. It stresses that addressing cybercrime effectively requires both reducing vulnerabilities and increasing the likelihood of prosecution for offenders.
5. <https://www.reuters.com/business/retail-consumer/uks-co-op-says-systems-now-running-normally-after-cyber-incident-2025-05-14/> - UK grocery retailer Co-Op announced that its systems are now fully operational following a recent cyber incident. The company reported that payment systems are functioning, and stock availability—both in stores and online—is expected to improve by the weekend. The breach, disclosed last month, involved an attempted hack that prompted Co-Op to restrict system access as a protective measure. The company, which operates over 2,300 stores and also provides funeral care, legal, and insurance services, is currently in a recovery phase, restoring systems in a controlled manner. This incident comes amid a broader trend of cyberattacks targeting UK retailers. Marks and Spencer, another major retailer, recently ceased online orders due to a suspected ransomware attack, which also led to the compromise of some customer information. The UK's National Cyber Security Centre has not confirmed whether these attacks are connected.
6. <https://www.ft.com/content/723b6195-1ce7-4b5f-94f5-729e9152c578> - Marks and Spencer (M&S) stands to claim up to £100 million from its cyber insurance following a recent cyberattack, which compromised some customer data and severely disrupted operations, especially online orders for almost three weeks. The personal data exposed includes contact details, dates of birth, and order histories, though not payment details or passwords. Insurers involved include Allianz, expected to cover at least £10 million initially, and Beazley. The incident may have resulted in lost revenues exceeding £60 million and contributed to a 16% drop in share price, erasing £1.3 billion of its market value. M&S's cyber insurance, arranged by WTW, is likely to cover all losses, including both direct and third-party liabilities, even if a third-party vendor is implicated in the breach. However, M&S may see its insurance premium—currently under £5 million—double unless it improves cyber risk management. This breach, along with recent cyberattacks on other UK retailers such as Harrods and the Co-op, may lead to increased cyber insurance premiums across the sector. The M&S payout could validate the value of cyber insurance and encourage wider adoption among smaller businesses. UK businesses have suffered approximately £44 billion in cyber-related revenue losses over the past five years.
7. <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 retailers Marks & Spencer (M&S) and the Co-op Group were initiated by hackers impersonating employees and deceiving IT help desks into resetting passwords, according to BleepingComputer. This allowed the 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.