# Co-op supply crisis persists weeks after DragonForce cyberattack despite restocking efforts



Co-op convenience stores across the UK are grappling with a crippling supply crisis three weeks after a significant cyberattack resulted in the theft of customer and employee data alongside major disruptions to the company’s IT infrastructure. Despite the company’s efforts to manage the fallout, many stores are still witnessing empty shelves, with customers frequently met by print-outs apologising for the shortages.

In early May, the Co-op initiated a damage control strategy following the breach, stating that they had begun a gradual restocking of their shops. They effectively halted access to their systems to prevent further data theft, a testament to the seriousness of the attack. Reports indicate that hackers, believed to be part of a group named DragonForce, accessed sensitive personal information of approximately 20 million members. While the Co-op reassured the public that financial data was not compromised, the breach still raised significant alarm among customers, leading CEO Shirine Khoury-Haq to express regret and emphasise ongoing protective measures.

The impact of this incident has not been isolated to the Co-op alone; it has also reverberated through other prominent UK retailers. Marks & Spencer, for instance, has faced comparable disruption, expecting financial repercussions that could reach £300 million. Likewise, luxury brands such as Harrods and supermarket distributor Arla similarly contend with the consequences of increasing cyber threats. The apparent targeting of multiple high-profile retail entities underlines a troubling trend in the retail sector.

In light of the ongoing challenges, Co-op's recovery progress has been slow. Initially, the company prioritised deliveries to rural areas attempting to mitigate the effects on isolated communities. However, reports from various locations show that many stores are still operating at significantly reduced capacity. For example, fresh produce may be available, yet shelves dedicated to frozen and dried goods remain sparse. One London Co-op employee noted that an anticipated delivery would include around a third fewer products than usual, illustrating the ongoing struggle to replenish essential stock.

Adding to the complications, the Co-op has faced logistical issues stemming from an IT error that allowed some customers to purchase items at considerably discounted rates, further muddling the retailer's recovery efforts. As part of their response strategy, Co-op has managed to restore contactless payment systems in all their outlets, addressing one of the more immediate concerns that arose from the cyberattack.

As supplies gradually become more stable, store employees express cautious optimism about returning to normality. Many expect shelves to be fully stocked within days, assuming deliveries proceed as promised. A spokesperson from Co-op reiterated their commitment, stating that while they are in a recovery phase, stock availability has improved, and the company will continue to collaborate closely with suppliers.

Although immediate concerns over IT operations and stock shortages dominate conversations, the broader economic implications of these supply issues are yet to be fully realised, leaving customers and stakeholders alike to wonder how such vulnerabilities will continue to shape the future of this cooperative giant and the retail landscape at large.

### Reference Map

1. Paragraphs 1-2, 4, 7
2. Paragraphs 3-4
3. Paragraph 4
4. Paragraphs 5-6
5. Paragraph 6
6. Paragraph 3
7. Paragraphs 3, 5-6

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

## Bibliography

1. <https://www.independent.co.uk/news/business/coop-shops-empty-cyber-hack-data-b2755116.html> - Please view link - unable to able to access data
2. <https://www.theguardian.com/business/2025/may/02/co-op-apologises-after-hackers-extract-significant-amount-of-customer-data> - The Co-op has apologized after hackers accessed and extracted personal data, including names and contact details, of a significant number of its current and past members. The National Cyber Security Centre and the National Crime Agency are assisting with the investigation. The Co-op emphasized that financial information such as bank or credit card details were not compromised. CEO Shirine Khoury-Haq expressed regret over the incident and assured members that steps are being taken to protect their data.
3. <https://www.theguardian.com/business/2025/apr/30/co-op-forced-to-shut-down-part-of-it-system-after-hack-attempt> - The Co-op was compelled to shut down parts of its IT system following an attempted hack, just days after Marks & Spencer faced a similar cyber incident. The company took proactive measures to safeguard its systems, leading to temporary disruptions in some services. Despite these challenges, all stores, including rapid home deliveries and funeral homes, continued to operate as usual. The National Cyber Security Centre is collaborating with the Co-op to support their response to the cyber incident.
4. <https://www.retailgazette.co.uk/blog/2025/05/co-op-reroutes-stock/> - In response to disruptions caused by a cyber attack, the Co-op is prioritizing deliveries to rural and island-based stores to minimize shortages in isolated communities. The retailer has asked suppliers to cancel deliveries to its warehouses due to technical issues with its Electronic Data Interchange system, impacting stock management and deliveries. Some stores have experienced empty shelves and shortages of core items, including milk, vegetables, and toilet paper.
5. <https://www.theguardian.com/business/2025/may/06/co-op-rushes-to-fix-contactless-payment-issue-in-some-stores-amid-cyber-attack-fallout> - The Co-op faced issues with contactless payment systems in up to 200 of its 2,300 stores across the UK due to a cyber attack. The problem was resolved by mid-afternoon, and contactless payment was restored in all stores. The retailer is working to address the fallout from the cyber attack, which has also led to product shortages and empty shelves in some locations.
6. <https://www.retail-week.com/grocery/co-op-cyber-attack-more-extensive-than-initially-reported/7048641.article> - The Co-op's cyber attack is more severe than initially acknowledged. Hackers, operating under the name DragonForce, have claimed to access personal information of 20 million Co-op members. The company had previously stated that there was no evidence of data being compromised. The hackers also claimed responsibility for ongoing cyber attacks on Marks & Spencer and an attempted attack on Harrods.
7. <https://www.retailgazette.co.uk/blog/2025/05/co-op-faces-delivery-chaos/> - The Co-op is experiencing delivery delays and empty shelves due to a sustained cyber attack that has forced the company to shut down some of its delivery systems. The attack has caused significant disruption to store availability, particularly in fresh categories such as fruit, vegetables, meat, and dairy. Some stores have posted notices apologizing for stock shortages, and pictures shared online show empty shelves and fridges.