# Co-op Group cyberattack sparks food supply shortages amid rising cybercrime threats



The recent upheaval within the Co-op Group, which has resulted in significant disruptions across various regional co-operative societies in the UK, stems from a sustained cyberattack that has raised alarm bells throughout the industry. Midcounties Co-op, Heart of England Co-op, and Lincolnshire Co-op have reported difficulties in maintaining food supply, signalling that the adverse effects of this breach are being widely felt.

This incident follows a growing trend of cyber intrusions targeting major retailers. In a similar case earlier this year, Marks & Spencer reported a breach where hackers impersonated employees to gain access to internal systems. This pattern underscores the increasing sophistication of cyber threats, as well as the vulnerabilities present in even the most established organisations. As seen in the Marks & Spencer attack, the repercussions can be severe; the company faced a substantial decline in its share price and estimated losses of around £30 million, with continuing damages of approximately £15 million weekly. Analysts have indicated that the group behind the recent attacks, known as DragonForce, claimed responsibility for assaults not only on Marks & Spencer but also on Co-op and Harrods, allegedly involving the theft of sensitive data including customer records.

The ramifications of such attacks extend beyond immediate operational challenges. In response to incidents like the Co-op Group's current situation, the UK's National Cyber Security Centre has issued recommendations for organisations to revise help desk protocols to fortify defences against social engineering tactics commonly employed by cybercriminals. These measures could mitigate the risks of future breaches, which have become alarmingly common across the sector.

In parallel, a similar scenario unfolded in Canada, where Federated Co-operatives Limited experienced a significant cyberattack that disrupted food ordering systems across several regions. Reports from Alberta indicated that grocery shortages emerged as a result of the incapacitated supply chain, with local news showing empty shelves as co-ops struggled to replenish stock. Despite the chaos, co-ops in Alberta managed to keep some operations running; for instance, cardlock fuel locations remained largely functional. This underscores a broader issue whereby the supply chains of co-operative businesses, like those operated by FCL and the Co-op Group, are becoming increasingly vulnerable to coordinated cyberattacks.

Interestingly, a related incident in Sweden showcased the devastating potential of supply chain attacks when a ransomware assault on the software supplier Kaseya caused widespread disruptions. The strike affected over half of Coop Sweden's stores, highlighting the cascading effects such breaches can precipitate throughout large networks. The UK's National Cyber Security Centre noted the inherent risks associated with outsourcing and interconnected systems, urging firms to improve their defensive measures and incident response strategies.

As the Co-op Group and its affiliated societies grapple with these challenges, they will undoubtedly need to consider how to not only restore operations but also strengthen their cybersecurity frameworks. Many affected co-ops have prioritised the replenishment of essential items and have publicly acknowledged the ongoing difficulties in maintaining stock levels due to the cyber incident. In addition, the potential leak of sensitive data was flagged by FCL in Canada, with threats of published files adding an unsettling layer to the fallout of these attacks.

In conclusion, the current cyberattack affecting the Co-op Group serves as a stark reminder of the vulnerabilities faced by modern businesses and the pressing need for robust cybersecurity measures. As the landscape of cyber threats continues to evolve, co-operative societies must adapt their strategies to safeguard both their operations and their customers' trust, ensuring resilience against future incidents.

### Reference Map

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

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

## Bibliography

1. <https://www.thegrocer.co.uk/news/co-op-societies-hit-by-availability-issues-amid-ongoing-cyberattack-on-co-op-group/704305.article> - 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/> - Cyberattacks on UK's Marks & Spencer (M&S) and Co-op Group began with hackers impersonating employees to deceive IT help desks into resetting passwords, granting 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. 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.
3. <https://www.thealbertan.com/beyond-local/federated-co-op-cyber-attack-affecting-northern-alberta-towns-grocery-supply-9210365> - A cyberattack on Federated Co-operatives Limited (FCL) in late June 2024 disrupted food ordering systems, leading to empty shelves and limited orders in Barrhead, Alberta. Pembina West Co-op reported challenges in processing food orders due to the attack. The FCL's website was down, displaying a 'This site can't be reached' message. On June 27, Pembina West Co-op announced a system-wide outage, causing continued disruptions while customer-facing services remained open. Cardlocks in Barrhead, Mayerthorpe, and Whitecourt were fully operational as of June 27. The attack also affected Co-op Gas Bar stores, leading to shortages of tobacco and other items due to challenges in ordering products. The Co-op Home Centre faced difficulties in receiving flyer feature products. The issues were ongoing, with FCL working diligently to rectify the situation. A sign posted at the Co-op entrance on July 8 stated that FCL was experiencing a cybersecurity incident impacting some internal and customer-facing systems, potentially affecting the inventory of certain grocery items. There was no evidence at that time that consumer data was compromised. The technical issues caused longer phone wait times and delayed transaction times. FCL issued an update on July 3, stating significant progress in restoring some operations and prioritizing key grocery items and consumer goods for delivery to local Co-ops. Co-op cardlock fuel locations were widely impacted, but teams continued to get more cardlocks pumping fuel every day. Fuel supply to Co-op retail gas bars remained relatively unaffected, and customers could fill up at all Co-op retail locations.
4. <https://www.townandcountrytoday.com/barrhead-news/federated-co-op-cyber-attack-affecting-barrhead-grocery-supply-9203774> - A cyberattack on Federated Co-operatives Limited (FCL) in late June 2024 disrupted food ordering systems, leading to empty shelves and limited orders in Barrhead, Alberta. Pembina West Co-op reported challenges in processing food orders due to the attack. The FCL's website was down, displaying a 'This site can't be reached' message. On June 27, Pembina West Co-op announced a system-wide outage, causing continued disruptions while customer-facing services remained open. Cardlocks in Barrhead, Mayerthorpe, and Whitecourt were fully operational as of June 27. The attack also affected Co-op Gas Bar stores, leading to shortages of tobacco and other items due to challenges in ordering products. The Co-op Home Centre faced difficulties in receiving flyer feature products. The issues were ongoing, with FCL working diligently to rectify the situation. A sign posted at the Co-op entrance on July 8 stated that FCL was experiencing a cybersecurity incident impacting some internal and customer-facing systems, potentially affecting the inventory of certain grocery items. There was no evidence at that time that consumer data was compromised. The technical issues caused longer phone wait times and delayed transaction times. FCL issued an update on July 3, stating significant progress in restoring some operations and prioritizing key grocery items and consumer goods for delivery to local Co-ops. Co-op cardlock fuel locations were widely impacted, but teams continued to get more cardlocks pumping fuel every day. Fuel supply to Co-op retail gas bars remained relatively unaffected, and customers could fill up at all Co-op retail locations.
5. <https://www.bbc.co.uk/news/technology-57707530> - A cyberattack on a large software supplier, Kaseya, led to the closure of over half of Coop Sweden's 800 stores. The attack, believed to be carried out by the Russia-linked REvil ransomware gang, affected around 200 businesses globally. Coop Sweden's point-of-sale tills and self-service checkouts stopped working, prompting the company to close more than half of its stores. The attack highlights the growing concern over supply chain attacks, where hackers target suppliers to claim multiple victims. The US Cybersecurity and Infrastructure Agency urged users of Kaseya software to shut it down, and the UK's National Cyber Security Centre acknowledged the incident and advised organizations to implement robust defenses against such threats.
6. <https://www.timescolonist.com/local-news/co-op-struggles-to-re-stock-in-wake-of-cyberattack-9210692> - A cyberattack on Federated Co-operatives Limited (FCL) in late June 2024 disrupted food ordering systems, leading to empty shelves and limited orders in Victoria, British Columbia. Peninsula Co-op reported challenges in keeping shelves stocked due to the attack, which affected internal IT systems and the ordering process. Dairy items, dried and canned goods, and frozen foods were most affected. The Co-op worked to ramp up local produce to fill in the gaps. A threat on July 8 on the dark web claimed that 80 gigabytes of data from FCL would be available for download, including human resources files, confidential business files, financials, and client information. FCL stated that it was investigating the allegations with third-party experts and would take appropriate action if data was compromised. FCL provided updates via social media and stated it would not conduct interviews until the investigation was complete.
7. <https://www.sasktoday.ca/southwest/co-op-experiencing-empty-shelves-shipment-delays-from-ongoing-cyberattack-9173448> - A cyberattack on Federated Co-operatives Limited (FCL) in late June 2024 disrupted food ordering systems, leading to empty shelves and limited orders in Saskatchewan. Co-op cardlocks across the province remained out of service until further notice. FCL prioritized key grocery items and consumer goods for delivery to local Co-op retailers. Many Co-op cardlock fuel locations were impacted, but teams worked to bring them back online. Fuel supply to Co-op retail gas bars remained relatively unaffected, and customers could fill up at all Co-op retail locations. FCL acknowledged statements online about data being allegedly copied and released but stated it was still investigating with third-party experts. If data was compromised, appropriate action would be taken. FCL thanked Co-op members, customers, and the public for their patience and understanding during the recovery process.