# Co-op prioritises remote stores after major cybersecurity breach impacting 20 million customers



## Co-op Responds to Cyber Attack by Prioritising Supply to Remote Stores

In the wake of a significant cyber attack on its systems, Co-op has initiated urgent measures to divert supplies to some of the UK's most remote supermarkets, ensuring that these communities are not left without essential food and drink. The attack has led to reports of empty shelves in various locations, particularly in Scotland's island communities where the Co-op is a primary retailer.

Customers across the Scottish Isles have expressed concerns as rows of shelves once stocked with fresh produce now stand bare. The retailer, which operates around 2,500 stores nationwide, was compelled to deactivate essential computer systems following the attack, which hackers claimed had compromised personal data from approximately 20 million customers. In an effort to manage the crisis, Co-op is prioritising deliveries to rural and island areas, such as Portree on the Isle of Skye and several stores in Glasgow and Aberdeen, among others.

The cyber attack prompted Co-op to issue a statement acknowledging potential product shortages. “Some of our stores might not have all of their usual products available,” the company noted, as it grapples with the ongoing impact of the breach. Customers in larger cities like London and Manchester have similarly reported disruptions, with some stores being unable to process card payments, leading to a temporary cash-only policy.

Amid these challenges, Co-op's chief executive, Shirine Khoury-Haq, expressed regret over the incident, describing it as “extremely distressing” for both staff and customers. Reports indicate that while a limited amount of sensitive data was stolen, the company had initially downplayed the extent of the breach, suggesting only a minor impact on operations. However, external assessments have painted a grimmer picture, with cybersecurity experts suggesting that the hackers, linked to a group known as Dragonforce, had deeper access and capabilities than initially acknowledged.

The attack on Co-op is part of a troubling trend affecting the retail sector, with similar incidents reported at major retailers like Marks & Spencer and Harrods. M&S recently paused online sales for over two weeks due to a ransomware attack that disrupted their operations significantly, highlighting the vulnerabilities faced by large retailers reliant on digital systems for everyday transactions.

Experts attribute these breaches to a relatively new generation of cybercriminals, including groups like Scattered Spider, reportedly comprising British and American teenagers, who exploit social engineering tactics to manipulate company employees into compromising security protocols. Nathaniel Jones, vice president of security and AI strategy at Darktrace, emphasised the uniqueness of these hackers, who, unlike many cybercriminals from Eastern Europe, are native English speakers. This linguistic proficiency may have afforded them a level of credibility that facilitated their attempts to infiltrate corporate systems.

The severity of these cyber incidents has rallied the National Cyber Security Centre (NCSC) and the National Crime Agency to assist affected retailers. Recent statistics from NCSC reveal a doubling in hacking incidents over the past months, attributed largely to increased ransomware activities by "hostile nation-states" and opportunistic criminal gangs. Richard Horne, acting as NCSC's spokesperson, remarked that the incidence of attacks on UK businesses could be costing upwards of £64 billion annually, signifying a crucial need for improved cybersecurity measures across the retail sector.

As Co-op continues to work diligently to restore stability, the incident serves as a wake-up call for retailers to bolster their cybersecurity protocols. With the increasing reliance on interconnected digital systems, experts warn that the repercussions of such attacks could escalate, potentially leading to complete operational shutdowns for vulnerable organisations. In the meantime, Co-op reassures its customers that it is "working around the clock" to mitigate the disruption and restore its supply chains.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://saskatoon.ctvnews.ca/it-was-empty-co-op-stores-deal-with-cyberattack-affecting-supply-1.6950576)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[4]](https://regina.ctvnews.ca/co-op-operations-and-systems-fully-restored-following-cybersecurity-incident-1.6970648)
* Paragraph 3 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[6]](https://teckpath.com/the-latest-ransomware-incident-at-co-op-a-wake-up-call-for-retail-cybersecurity/)
* Paragraph 4 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490)
* Paragraph 5 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[3]](https://www.truesec.com/cases/back-in-business-after-the-largest-ransomware-attack-of-all-time)
* Paragraph 6 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[7]](https://globalnews.ca/news/10598617/co-ops-saskatchewan-recovering-cybersecurity-incident/)
* Paragraph 7 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[6]](https://teckpath.com/the-latest-ransomware-incident-at-co-op-a-wake-up-call-for-retail-cybersecurity/)
* Paragraph 8 – [[1]](https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[5]](https://regina.ctvnews.ca/co-op-websites-back-online-following-cybersecurity-incident-1.6967134)

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14690925/Co-op-divert-supplies-remote-shops-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://saskatoon.ctvnews.ca/it-was-empty-co-op-stores-deal-with-cyberattack-affecting-supply-1.6950576> - Co-op stores in Saskatoon and surrounding areas are experiencing supply shortages due to a cyberattack. Customers have reported empty shelves, particularly in the produce section. The company has acknowledged the issue and is working to restore normal operations. Experts emphasize the importance of transparent communication during such incidents.
3. <https://www.truesec.com/cases/back-in-business-after-the-largest-ransomware-attack-of-all-time> - Truesec assisted Coop through a significant ransomware attack that led to the temporary closure of over 500 stores. The attack exploited a vulnerability in Coop's POS software, causing widespread disruption. With Truesec's support, Coop restored operations within six days, reopening all stores and resuming services.
4. <https://regina.ctvnews.ca/co-op-operations-and-systems-fully-restored-following-cybersecurity-incident-1.6970648> - Federated Co-op Limited (FCL) announced the full restoration of its grocery operations, inventory, and delivery systems following a cybersecurity incident. The company thanked customers for their patience and understanding during the downtime, which had previously led to empty shelves and operational challenges.
5. <https://regina.ctvnews.ca/co-op-websites-back-online-following-cybersecurity-incident-1.6967134> - FCL reported that its corporate and local Co-op websites are back online after a cybersecurity incident. The company had previously shut down many systems as a precaution, leading to supply issues and empty shelves in some locations. Customers are encouraged to visit their local websites for updates.
6. <https://teckpath.com/the-latest-ransomware-incident-at-co-op-a-wake-up-call-for-retail-cybersecurity/> - The recent ransomware attack on Co-op highlights the need for robust cybersecurity measures in the retail sector. The attack led to store closures, financial losses, and customer inconvenience. Co-op's response included activating an incident response team, collaborating with authorities, and working on system recovery to prevent future incidents.
7. <https://globalnews.ca/news/10598617/co-ops-saskatchewan-recovering-cybersecurity-incident/> - Co-ops across Western Canada are recovering from a cybersecurity incident that impacted internal and customer-facing systems, leading to inventory shortages and closed cardlock fuel locations. The company is investigating the incident and working to restore normal operations, with some systems gradually coming back online.