# Co-op cyber attack leaves remote communities facing critical food shortages



# Co-op Cyber Attack Disrupts Food Supplies in Remote Communities

A recent cyber attack on Co-op stores has caused significant supply shortages in several locations across Argyll, the Highlands, and the Western Isles, leaving shelves bare of essential items such as fresh fruit, bread, and milk. In regions like Tobermory, Skye, and the surrounding islands, where the Co-op often serves as the sole local grocery option, the disruption has raised serious concerns about food availability for residents.

While mainland communities may have more grocery alternatives, island inhabitants are feeling the impact acutely. In the wake of this cyber incident, many have turned to smaller independent and community-focused shops that have stepped in to fill the void left by the Co-op's reduced stock. For example, Buth Bharraigh, a community-run shop on Barra, has quickly adapted its supply chain to meet local demands, highlighting the resilience of these smaller retailers.

Real-time updates about the situation have flooded social media, with locals sharing photos of empty shelves and seeking reassurance from shop staff. In a bid to communicate openly with customers, Ricky Johnston, the manager of the Co-op in Tobermory, expressed gratitude for their understanding during this difficult period. “Thank you all for your patience during this difficult time at the Co-op. We are working hard to get stock to the store as quickly and as frequently as possible while our systems are down,” he stated.

Community support has been tangible, with local figures like former councillor Mary-Jean Devon praising the Co-op staff’s efforts. She noted that despite the logistical challenges, the team has managed to keep some items in stock, including the bakery's homemade bread and the usual supply of fresh fruit and milk. This commitment to service has been crucial as residents grasp for reliable food supplies during the disruption.

According to Shirine Khoudry-Haq, the CEO of the Co-op Group, the cyber attack was serious enough to necessitate significant operational shutdowns. In her communication to members, she confirmed the breach had allowed hackers to access a limited amount of member data, raising concerns about potential data safety issues. The incident highlights broader vulnerabilities not just within the Co-op’s infrastructure but also across retail supply chains more generally. As noted in previous cases, such as a similar attack impacting the Swedish supermarket chain Coop in 2021, the risks associated with cyber threats on essential services can have far-reaching implications for food security.

As the community grapples with these shortages, some residents on Skye have voiced hopes for more diverse grocery options, suggesting the introduction of retailers like Lidl or Aldi to mitigate the Co-op's market dominance. Others echo the sentiment of supporting local businesses, which have proven to be more resilient due to different supply chains.

The current supply challenges underscore the necessity of robust cybersecurity measures within the retail sector. Cyber incidents not only disrupt the flow of goods but can compromise the overall operational effectiveness of a business, leading to customer dissatisfaction and reduced trust. The Co-op’s management has expressed their commitment to rectify these issues swiftly and ensure that essential items become readily available once again.

As important supplies dwindle in these remote communities, the unfolding situation serves as a stark reminder of the reliance on local grocery outlets and the need for steady, reliable supply chains. The ramifications of this cyber attack may extend beyond immediate supply issues, challenging the viability of local economies in regions already vulnerable due to geographic isolation.

## Reference Map:

* Paragraph 1 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/)
* Paragraph 2 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/), [[6]](https://regina.ctvnews.ca/co-op-operations-and-systems-fully-restored-following-cybersecurity-incident-1.6970648)
* Paragraph 3 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/)
* Paragraph 4 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/), [[4]](https://www.ckom.com/2024/07/02/shortage-on-shelves-in-midst-of-co-op-cybersecurity-incident/)
* Paragraph 5 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/), [[2]](https://www.timescolonist.com/local-news/co-op-struggles-to-re-stock-in-wake-of-cyberattack-9210692)
* Paragraph 6 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/), [[3]](https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/)
* Paragraph 7 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/), [[5]](https://www.ctvnews.ca/saskatoon/article/it-was-empty-co-op-stores-deal-with-cyberattack-affecting-supply/)
* Paragraph 8 – [[1]](https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/), [[7]](https://panow.com/2024/07/10/uncertainty-remains-after-co-op-cybersecurity-incident/)

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

## Bibliography

1. <https://www.pressandjournal.co.uk/fp/news/6750849/co-op-cyber-attack-hits-food-supplies-on-islands/> - Please view link - unable to able to access data
2. <https://www.timescolonist.com/local-news/co-op-struggles-to-re-stock-in-wake-of-cyberattack-9210692> - In July 2024, Federated Co-operatives Limited (FCL) experienced a cyberattack that disrupted their internal operations, leading to challenges in restocking grocery items. The Peninsula Co-op Food Centre in Victoria reported difficulties in maintaining inventory levels, particularly affecting dairy, dried, canned, and frozen foods. The store emphasized efforts to source local produce to fill the gaps and appreciated customers' understanding during this period. The cyberattack also raised concerns about potential data breaches, with threats of sensitive information being released, prompting ongoing investigations.
3. <https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/> - In July 2021, Swedish supermarket chain Coop was severely impacted by a ransomware attack targeting its supplier, Visma Esscom, which managed Coop's point-of-sale systems. The attack led to the closure of approximately 500 Coop stores as cash registers became inoperable. Coop acknowledged the issue, stating that an IT attack on one of their suppliers had rendered cash registers non-functional, and they were working to reopen stores promptly. The incident highlighted the vulnerabilities in supply chain dependencies and the broader impact of cyberattacks on retail operations.
4. <https://www.ckom.com/2024/07/02/shortage-on-shelves-in-midst-of-co-op-cybersecurity-incident/> - Following a cybersecurity incident in July 2024, Federated Co-operatives Limited (FCL) reported inventory shortages across several Co-op locations. The Warman Co-op store experienced empty shelves in produce and frozen food sections. FCL acknowledged the disruption, attributing it to internal system issues caused by the cyberattack, and apologized for the inconvenience. The company assured customers that efforts were underway to restore regular stock levels and expressed gratitude for the community's patience during the recovery process.
5. <https://www.ctvnews.ca/saskatoon/article/it-was-empty-co-op-stores-deal-with-cyberattack-affecting-supply/> - In July 2024, Co-op stores in Saskatoon faced significant supply disruptions due to a cyberattack. Shoppers reported empty shelves, particularly in essential items, as the attack affected the retailer's ability to restock. The incident led to operational challenges, with some stores unable to process transactions, further impacting customer experience. The cyberattack underscored the vulnerabilities in retail supply chains and the critical importance of robust cybersecurity measures to maintain service continuity.
6. <https://regina.ctvnews.ca/co-op-operations-and-systems-fully-restored-following-cybersecurity-incident-1.6970648> - Federated Co-operatives Limited (FCL) announced in July 2024 that its grocery operations, inventory, and delivery systems had been fully restored following a cybersecurity incident. The company expressed gratitude to customers for their patience and understanding during the disruption. FCL had previously reported system outages affecting internal and customer-facing systems, including Co-op cardlock fuel locations, and had been working to bring all systems back online safely. The restoration marked a significant recovery from the cyberattack's impact on operations.
7. <https://panow.com/2024/07/10/uncertainty-remains-after-co-op-cybersecurity-incident/> - In July 2024, Federated Co-operatives Limited (FCL) continued to address the aftermath of a cybersecurity incident that led to operational disruptions, including empty grocery shelves and closed Co-op Cardlocks across the country. FCL acknowledged circulating statements about potential data breaches but stated it was too early to confirm such claims. The company emphasized ongoing investigations with third-party experts and assured customers that appropriate actions would be taken if data was compromised. The incident highlighted the complexities and uncertainties following significant cyberattacks on retail operations.