# Co-op grapples with operational chaos after cyberattack disrupts logistics and data security



British retail giant Co-op is currently navigating significant operational disruptions following a recent cyberattack that has raised alarm bells not only within the company but across the retail sector. Reports indicate that some hackers may still have access to Co-op's systems, prompting cautious measures such as the temporary shutdown of critical IT networks. As a consequence, staff have struggled to restock certain products, severely affecting logistical operations crucial for a smooth retail experience.

The Co-op has been actively engaged in mitigating the impact of the attack, with CEO Dorothy Thompson confirming that "a limited amount of customer data" had been accessed by the criminals. In an official statement, she expressed her distress at the breach, emphasising the organisation's commitment to data protection, especially in her leadership of a member-owned entity. “This is obviously extremely distressing for our colleagues and members, and I am very sorry this happened,” she said, recognising the heightened responsibility that comes with handling sensitive member information.

Despite these setbacks, the company has reassured its customers that all stores remain open. However, they acknowledge that some locations may not have their usual stock levels, as deliveries from depots are reported to be operating at less than 20% of their typical capacity. A spokesperson noted that an increased level of deliveries was being made, but still cautioned customers against expecting full product availability in every store. This situation underscores how deeply cyberattacks can disrupt not just operational efficiency, but also consumer trust in major retail brands.

This cyber incident is not isolated. It has occurred in conjunction with other significant attacks in the retail space, such as the recent disruption faced by Marks & Spencer, which was likely due to ransomware efforts linked to the notorious group ScatteredSpider. Such cyberattacks highlight a troubling trend in the retail sector, where criminals increasingly target large organisations with far-reaching impacts.

The ramifications of cyberattacks in the retail sector can be severe. A historical context is provided by the closure of nearly 800 Co-op stores in Sweden following a breach related to Kaseya, which disrupted payment processing systems extensively. These events illustrate the vulnerabilities inherent in modern supermarket operations, emphasising the necessity for robust cybersecurity measures as a priority rather than a luxury.

Moreover, the experience of co-ops in other regions showcases the broad spectrum of challenges faced post-breach. For instance, following a third-party vendor hack, Blue Ridge Energy in North Carolina found itself accessing the dark web and establishing a 'situation room' to mitigate damages and protect member data. This proactive approach underscores the importance for all co-ops and similar entities to deploy comprehensive strategies for safeguarding their information and operational integrity.

In a more alarming narrative, data breaches within other sectors, like that of Mr. Cooper, a major U.S. mortgage loan servicer, unveiled personal information of nearly 14.7 million individuals, spotlighting the real and pervasive risks associated with cyberattacks across all industries. Such breaches illuminate the pervasive nature of cyber threats, which extend beyond retail and affect vast swathes of consumer and institutional trust.

As Co-op strives to restore full functionality to its operations, the industry watches closely, aware that this incident is emblematic of wider cybersecurity challenges. The path to recovery may be marred with complexities, but the shift towards increased investment in cybersecurity measures is becoming ever more essential for safeguarding not only operational resilience but also customer confidence.

### Reference Map

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

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

## Bibliography

1. <https://www.techradar.com/pro/security/co-op-hackers-may-still-be-in-the-system-as-cyberattack-disruption-continues> - Please view link - unable to able to access data
2. <https://www.cooperative.com/news/Pages/North-Carolina-Co-op-Advice-After-Third-Party-Breach.aspx> - This article discusses the experience of Blue Ridge Energy, a North Carolina co-op, following a third-party vendor hack. It details their response, including setting up a 'situation room' to access the dark web and locate stolen data, and emphasizes the importance of co-ops taking proactive measures to protect their data.
3. <https://therecord.media/supermarket-chain-coop-closes-800-stores-following-kaseya-ransomware-attack> - This report covers the closure of nearly 800 Coop stores in Sweden after a ransomware attack on one of its contractors, linked to the Kaseya security incident. The attack disrupted payment processing systems, leading to store closures and highlighting the broader impact of such cyberattacks on retail operations.
4. <https://therecord.media/mr-cooper-cyberattack-data-breach-notifications> - This article details a cyberattack on Mr. Cooper, a major U.S. mortgage loan servicer, in October 2023. The breach exposed personal information of nearly 14.7 million individuals, including names, addresses, and Social Security numbers, underscoring the significant risks of cyberattacks in the financial sector.
5. <https://saskatoon.ctvnews.ca/it-was-empty-co-op-stores-deal-with-cyberattack-affecting-supply-1.6950576> - This news piece reports on Co-op stores in Saskatoon experiencing supply shortages due to a cyberattack. Shoppers reported empty shelves, particularly in the produce section, highlighting the operational challenges faced by retailers during such incidents.
6. <https://thecyberexpress.com/coop-cyberattack-swedish-giant-in-crisis/> - This article discusses the cyberattack on Coop Sweden, which began on December 22, 2023. The attack led to payment processing issues in Coop Värmland stores, causing operational disruptions and prompting the company to seek expert assistance to address the problems.
7. <https://therecord.media/coop-varmland-sweden-supermarket-chain-cyberattack> - This report covers the cyberattack on Coop Värmland, a Swedish supermarket chain, detailing the involvement of the Cactus ransomware group. The article highlights the group's history of targeting large entities and the impact of the attack on Coop's operations.