# Co-op faces ongoing supply chain shortages following cyber attack disruption



The recent cyber attack on the Co-op grocery chain has raised considerable alarm as supermarkets contend with significant supply chain disruptions. The West Way Square store in Botley, among those impacted, has witnessed bare shelves, prompting an apology to customers for the inconveniences caused. Signs have been placed alongside empty fridge units, informing shoppers of persistent supplier shortages linked to the nationwide issue affecting many Co-op locations.

Customers expressing concern noted the visible gaps in stock, with one shopper hopeful that services would soon normalise. Meanwhile, the Co-op branch on West St Helen Street in Abingdon reported less severe disruptions, albeit also experiencing delays in product availability.

In response to the attack, the Co-op has stated that recovery efforts are well underway. The chain has assured its customers that stock availability, both in-store and online, will start to improve as systems are progressively restored. The company is working closely with suppliers, having taken "early and decisive action" to limit access to its systems following the breach. This measure was aimed at safeguarding the integrity of its operations, with the spokesperson emphasising the importance of a safe and controlled recovery process.

Historically, cyber attacks have demonstrated a crippling effect on the retail sector. For instance, in July 2021, Coop Sweden suffered a massive ransomware attack that led to the closure of over half of its stores. This attack disrupted cash registers and highlighted vulnerabilities in supply chains, particularly when they rely on third-party managed service providers. The knock-on effect illustrates how interconnected these systems are, where a breach in one part can incapacitate the entire operation.

The Co-op's situation follows a growing trend within the UK retail sector, which is grappling with rising cyber insurance premiums up to 10%, partly in response to recent high-profile breaches. Insurers are becoming increasingly vigilant, and some may be reconsidering their presence in the retail market altogether. This shift is exacerbated by outdated IT systems and the extensive consumer data many retailers manage, rendering them prime targets for malicious attacks.

The implications of these incidents extend beyond immediate operational disruptions. They underscore a broader concern regarding the cybersecurity posture of grocery retailers, which often face unique challenges in protecting their supply chains. Recent attacks on federated co-operatives have similarly disrupted operations, leading to significant delays in restocking essential grocery items. As stores recover from technological setbacks, the industry remains on high alert, recognising that safeguarding against such attacks is crucial for long-term stability.

As the Co-op emerges from this cyber incident, it faces the challenge of restoring both its operational integrity and consumer confidence. With the company actively addressing these disruptions, customers can expect improvements by this weekend as measures are implemented to ensure better stock availability and payment systems. Yet, the event serves as a sobering reminder of the vulnerabilities that lie within the retail sector's increasingly digital landscape, emphasising the need for robust cybersecurity measures to protect both retailers and consumers alike.

### Reference Map

1. Paragraph 1: [[1]](https://www.oxfordmail.co.uk/news/25162064.oxford-co-op-supermarket-shelves-empty-cyber-attack/?ref=rss)
2. Paragraph 2: [[1]](https://www.oxfordmail.co.uk/news/25162064.oxford-co-op-supermarket-shelves-empty-cyber-attack/?ref=rss)
3. Paragraph 3: [[1]](https://www.oxfordmail.co.uk/news/25162064.oxford-co-op-supermarket-shelves-empty-cyber-attack/?ref=rss)
4. Paragraph 4: [[3]](https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/), [[4]](https://www.ibm.com/blogs/nordic-msp/how-a-supply-chain-attack-closed-one-of-swedens-largest-supermarket-chains/)
5. Paragraph 5: [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1)
6. Paragraph 6: [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[5]](https://www.timescolonist.com/local-news/co-op-struggles-to-re-stock-in-wake-of-cyberattack-9210692)
7. Paragraph 7: [[2]](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1), [[6]](https://www.truesec.com/cases/back-in-business-after-the-largest-ransomware-attack-of-all-time), [[7]](https://www.bbc.co.uk/news/technology-57707530)
8. Paragraph 8: [[1]](https://www.oxfordmail.co.uk/news/25162064.oxford-co-op-supermarket-shelves-empty-cyber-attack/?ref=rss)

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

## Bibliography

1. <https://www.oxfordmail.co.uk/news/25162064.oxford-co-op-supermarket-shelves-empty-cyber-attack/?ref=rss> - Please view link - unable to able to access data
2. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - UK retailers, including the Co-op, are facing significant cyber insurance premium increases, up to 10%, following high-profile cyber attacks. These incidents have prompted insurers to reassess cyber risk in the retail sector, which had previously seen falling rates. Experts warn that cyber security scrutiny will intensify, and some insurers may withdraw from the retail market. The Co-op confirmed a data breach affecting numerous customers, and the sector's vulnerability is attributed to large amounts of consumer data and outdated IT systems.
3. <https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/> - In July 2021, Swedish supermarket chain Coop closed approximately 500 stores after being affected by an REvil ransomware attack targeting managed service providers through a supply-chain attack. The attack disrupted Coop's cash registers, leading to store closures. Coop's supplier, Visma Esscom, was compromised, affecting Coop's point-of-sale systems. The incident highlights the risks of supply-chain attacks and their impact on retail operations.
4. <https://www.ibm.com/blogs/nordic-msp/how-a-supply-chain-attack-closed-one-of-swedens-largest-supermarket-chains/> - A supply chain attack involving the REvil ransomware group exploited a zero-day vulnerability in Kaseya's VSA software, affecting Coop's managed service provider, Visma Esscom. This led to the encryption of Coop's systems, causing store closures. The attack was sophisticated, using a malicious update to distribute ransomware, and underscores the importance of securing supply chains to prevent such incidents.
5. <https://www.timescolonist.com/local-news/co-op-struggles-to-re-stock-in-wake-of-cyberattack-9210692> - In June 2024, Federated Co-operatives Limited (FCL) experienced a cyberattack affecting internal operations, leading to challenges in restocking grocery items. The attack impacted the ordering process, causing delays in shipments and empty shelves in some stores. FCL prioritized key grocery items for delivery and worked to restore operations, highlighting the broader impact of cyber incidents on supply chains.
6. <https://www.truesec.com/cases/back-in-business-after-the-largest-ransomware-attack-of-all-time> - In July 2021, Coop, one of Sweden's largest grocery chains, was severely impacted by a supply chain attack involving the Kaseya ransomware incident. The attack led to the closure of approximately 700 of Coop's 800 stores. Truesec's Incident Response Team assisted Coop in restoring operations, and within six days, all stores were reopened, demonstrating the resilience and recovery capabilities in the face of significant cyber threats.
7. <https://www.bbc.co.uk/news/technology-57707530> - In July 2021, Coop Sweden closed over half of its 800 stores due to a cyberattack that disrupted point-of-sale systems. The attack targeted Kaseya, a software supplier used by Coop, leading to store closures. The incident highlights the risks of supply chain attacks and their potential to cause widespread operational disruptions in the retail sector.