ASCM SAN DIEGO CHAPTER
Serving Greater San Diego-Imperial, Arizona, Baja CA & Sonora MX

Event: Navigating Logistics Disruption and Uncertainty: Logistics SIG Open Forum, (Aug 29th, 2025)

Case Study Summary –UNFI Cyberattack Disrupts Food Distribution (2025)

A cyberattack in June 2025 severely impacted United Natural Foods Inc. (UNFI), a major food distributor, disrupting its distribution network and leading to widespread impacts on grocery stores and the wider food supply chain in North America

Key points of the attack

- **Attack Vector and Response:** UNFI detected unauthorized activity on its systems on June 5, 2025, and responded by taking core systems offline to contain the breach. While UNFI didn't disclose the nature of the attack, experts suspect it was likely a ransomware attack targeting critical business systems like warehouse, transportation, and order management.
- **Operational Disruption and Impact:** The incident significantly disrupted UNFI's ability to fulfill and distribute customer orders, impacting over 30,000 retail locations, including major chains like Whole Foods Market and numerous independent grocery stores across the U.S. and Canada. This led to delayed deliveries, cancelled employee shifts, and empty store shelves in various departments. Smaller businesses, like Pattycake Bakery in Columbus, Ohio, faced difficulties obtaining essential ingredients.
- **Attribution**: While UNFI didn't officially attribute the attack, security researchers identified tactics, techniques, and procedures consistent with the Scattered Spider group, known for targeting retailers with sophisticated social engineering attacks.
- **Financial and Operational Recovery:** UNFI gradually restored its core systems, resuming normal operations and deliveries by late June. The incident is expected to result in a $350 million to $400 million reduction in fiscal 2025 sales and $65 million to $75 million in pre-tax costs, according to SecurityWeek and Distribution Strategy Group. UNFI expects its cybersecurity insurance to cover a significant portion of the losses.

- **Lessons Learned and Industry Implications:** The UNFI cyberattack highlighted the vulnerability of the food supply chain to cyberthreats. It underscored the need for businesses to invest in robust cybersecurity measures, develop strong business continuity plans, and diversify supply chains to mitigate the impact of such attacks. Regulatory bodies like the Food and Ag-ISAC have updated cybersecurity guidance for food and agriculture businesses in response.

Context & Impact

A cyberattack on United Natural Foods Inc. (UNFI)—the main distributor for Whole Foods and over 30,000 other stores—halted operations, delaying shipments and leaving shelves empty across the U.S. and Canada.

1. How Success Was Defined

- **Restoring IT systems** and operational transparency rapidly
- **Minimizing inventory outages**
- **Maintaining customer confidence and avoiding brand damage**

2. Best Practices Learned

- Transitioning quickly to **alternative suppliers and distribution channels** while core systems were offline. nypost.com
- Implementing **phased restoration of systems** to balance speed and stability during recovery.
- The disruption highlighted the necessity of **robust cyber-incident response and continuity planning** for logistics operations.

3. Benchmarks & Metrics

- **Downtime duration** (system & operational) — critical success metric
- **Percentage of inventory replenished** within X days
- **Customer satisfaction and brand impact**—e.g., headlines, social sentiment, or foot traffic trends
- **Operational resilience**: The ability to shift supply chains (e.g., the percentage of supply delivered via alternative routes)

🔑 **Key Takeaways from the UNFI Cyberattack**

1. **Cybersecurity is now a logistics risk, not just an IT issue**
    - Attack on United Natural Foods (UNFI) disrupted food distribution to Whole Foods and 30,000+ stores.
    - Logistics and supply chain operations are highly dependent on digital platforms (TMS, WMS, ERP, EDI).
2. **Supply continuity depends on contingency playbooks**
    - Initial outages halted shipments and left store shelves empty.
    - Those with backup suppliers, alternate distribution nodes, and manual workarounds restored partial flows faster.
3. **Time-to-recovery is the real benchmark**
    - The critical KPI isn't whether an attack occurs, but **how quickly IT and logistics operations are restored**.
    - Downtime → lost sales, customer dissatisfaction, and brand reputation hits.
4. **Cross-functional crisis management is essential**
    - Effective response required coordination between IT, supply chain, operations, and retail partners.
    - "War room" structures—linking logistics leaders with IT & security teams—speed recovery.
5. **Resilience investments pay back in brand trust**
    - Whole Foods/UNFI communicated "temporary supply challenges" publicly.
    - Transparent customer messaging prevented worse reputational damage.

Summary Table

Case	Success Defined By	Key Learnings / Best Practices	Benchmarks & Indicators
UNFI Cyberattack (2025)	Rapid systems recovery, inventory stability, customer trust	Alternate supplier routing; phased recovery; cyber resilience	Downtime days, replenishment %, sentiment metrics

---

❓ Key Questions for Discussion

- How should logistics define “success” in a cyber disruption?
- Which benchmarks (downtime, fulfillment %, customer sentiment) best measure resilience in logistics operations?
- Should resilience performance (e.g., recovery time, continuity) be part of supplier scorecards?
- What best practices and manual workarounds can be built into our contingency playbooks?
- What is one action you can take back to your team to improve readiness?

Sources:

- nypost.com
- Cyberattack leads to shortage at pharmacies, grocery stores
- https://www.forbes.com/sites/errolschweizer/2025/06/16/what-the-cyberattack-on-unfi-reveals-about-the-us-grocery-industry/
- https://www.youtube.com/watch?v=FrrY-ga25qk