



CLIENT ALERT

French Supermarket Cyberattack Exposes Risks of Operational Technology

A recent cyberattack affecting hundreds of supermarkets across France is the subject of an ongoing investigation and highlights the growing risk that vulnerabilities in operational technology (OT) systems pose to retail operations and critical supply chains. French authorities are investigating reports that attackers compromised internet-connected commercial refrigeration management systems, allegedly manipulating temperature controls and causing refrigeration units to enter prolonged defrost cycles or operate at elevated temperatures. The resulting food spoilage and operational disruptions are believed to have impacted as many as 700 stores, raising concerns about inventory losses, business interruption, and potential insurance implications. While investigators have not established a direct connection to the 2025 cyberattacks against Marks & Spencer (M&S) and Co-op, all three incidents underscore a broader trend in which cyber threats are extending beyond traditional data theft to disrupt business-critical systems and day-to-day retail operations. Attribution for the French attack remains under investigation.

Unlike many recent cyber incidents, the attack does not appear to have involved ransomware, data theft, or extortion. Instead, the apparent objective was operational disruption and physical damage. Cybersecurity experts believe threat actors exploited weaknesses in connected refrigeration systems, including outdated firmware, unsupported equipment, and default credentials.

This event is another reminder that cyber threats are no longer limited to data breaches and ransomware. As organizations increasingly connect physical systems to business networks, cyber incidents can quickly create real-world operational and financial consequences.

Why This Matters for Cyber Insurance

The French supermarket attack reportedly resulted in:

- Inventory spoilage and product loss
- Business interruption and operational downtime
- Disruption to stock throughput and inventory replenishment processes
- Supply chain delays and reduced product availability
- Significant recovery and remediation expenses
- Lost sales resulting from inventory shortages and fulfillment challenges

While many organizations view cyber insurance primarily as protection against ransomware and privacy events, cyber incidents involving connected equipment can raise important questions regarding cyber, property, and business interruption coverage. Physical losses resulting from cyber events may trigger complex coverage considerations depending on policy language, exclusions, and the nature of the damage.

The incident highlights the importance of understanding how cyber insurance may respond to operational and physical losses, not just data theft. Organizations may benefit from reviewing their cyber, property, and marine cargo (or stock throughput [STP]) policies to identify potential coverage gaps and explore opportunities to mitigate exposures related to cyber-induced business interruptions.

Practical Risk Mitigation Tips

Strengthen Operational Technology Security

- Maintain an inventory of all internet-connected OT and IoT devices.
- Eliminate default passwords and implement MFA where feasible.
- Apply firmware updates promptly and replace unsupported equipment.

Improve Monitoring & Vendor Oversight

- Include OT systems within cybersecurity monitoring programs.
- Segment critical operational systems from corporate networks where possible.
- Evaluate cybersecurity controls of third-party vendors responsible for maintaining connected equipment.

Review Insurance Program Alignment

- Evaluate cyber, property, and marine cargo policies for cyber-related exclusions, sublimits, and carve-backs.
- Understand whether physical damage, inventory spoilage, and contingent business interruption losses resulting from cyber events are adequately addressed in your insurance program
- Work with experienced brokers and specialized insurers to understand how cyber-triggered physical losses would be handled across policies before an event occurs.

Bottom Line

The French supermarket incident demonstrates how a cyberattack can rapidly evolve into a property loss and business interruption event. Organizations that rely on connected equipment should view this as a timely reminder to assess OT security controls, understand potential third-party exposures, and review how their cyber and property insurance programs may respond to cyber-triggered physical losses.



Ready to be EPIC?

For more information about how EPIC can help your business, visit us at epicbrokers.com.