

To: Meat Institute Member Executives; Cyber Community; Communications Community

From: Casey Gallimore, Senior Director of Regulatory Policy

Subject: Cyberattacks Highlight Risks to Food Industry Operations

Overview

A recent cyberattack targeting supermarket refrigeration systems in France is highlighting how cybersecurity incidents can disrupt food operations, cause product losses and create potential food safety risks. The incident comes amid a broader rise in cyberattacks against the food and beverage industry, underscoring the importance of protecting both corporate networks and operational technology (OT), including connected equipment used to monitor and control production and refrigeration.

French Supermarket Refrigeration Systems Targeted

According to the [Associated Press](#), a cyberattack affected hundreds of supermarkets in France, manipulating refrigeration settings and forcing some stores to discard fresh and frozen products. Authorities are investigating, and the perpetrators have not been identified as of the latest reporting.

The French government's cybersecurity agency reported that the affected systems were directly exposed to the internet without VPN or firewall protection. [Many were older Danfoss refrigeration controllers](#) running end-of-life software that no longer receives security updates. The European agencies and the Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC) are monitoring the incident for indications that similar systems in other countries may be affected.

Cyberattacks Against the Food Industry Are Increasing

The incident comes amid a broader increase in cyberattacks. The Food and Ag-ISAC recorded 227 attacks against food and beverage companies in the first half of 2026, a 62% increase

over the same period in 2025. The Food Institute provides further context regarding the rise in attacks in [a recent article](#).

Cyberattacks can disrupt production, delay shipments, cause product waste and compromise systems used to verify food safety conditions and maintain traceability. Experts note that many attacks are opportunistic, with criminals scanning for exposed systems and exploiting vulnerabilities or using phishing and social engineering to gain access. If companies cannot verify that required food safety conditions were maintained, they may need to hold or discard affected products.

Food and Ag-ISAC Recommendations

In its [Oct. 14 situational update](#), the Food and Ag-ISAC urged organizations using similar refrigeration and control systems to assess their exposure and review security measures. Recommendations include:

- Remove direct internet exposure from refrigeration controls and other operational technology.
- Secure remote access through a VPN or another appropriately protected network.
- Install available security updates and evaluate whether outdated equipment should be upgraded or replaced.
- Review system settings and restore known-good configurations if necessary.
- Strengthen access controls and assess whether network segmentation or firewalls can protect legacy equipment.

Key Takeaway for Meat and Poultry Companies

The French incident reminds us that cyberattacks can affect physical equipment and food operations, not just corporate data. Meat and poultry companies should work with IT, cybersecurity, engineering and plant operations teams to assess connected equipment, review remote-access practices and identify outdated or internet-exposed systems. Members can access the Food and Agriculture Sector Cybersecurity [Guide for Small and](#)

[Medium-Sized Businesses](#) on the Meat Institute website. For further guidance or information about the Meat Institute's cybersecurity committee, reply to this email.