ISS GLOBAL / COMPARATIVE INCIDENT ASSESSMENT

Cyberattacks on European supermarket refrigeration

France in October and the cross-border disruption in November

REPORTING / REVIEW WINDOW
11 October to 9 November 2026 · Europe/London

ISSUE DATE
2026-11-10

France attributed the October refrigeration sabotage to Iran. Similar incidents across Europe in November exposed the same kind of operational risk, but the public evidence does not establish a common attacker.

This assessment compares the 11–12 October attack on French food retailers with the 1–2 November incidents in several European countries. It covers public developments through 23:59 GMT on 9 November 2026, including France's attribution. The country and operator examples are selected cases, not a census. [1][2][3]

The comparison separates the physical cold-chain losses from Ahold Delhaize's October corporate IT disruption and identifies practical priorities for retailers, franchisees and refrigeration contractors. [10][11]

01 / EXECUTIVE SUMMARY

What happened and its threat significance

COUNTRY	WHERE	WHEN
France and several European countries	French retail sites; selected November cases include Belgium, Luxembourg, Sweden, Ireland, Estonia, Germany and Finland. [1][3][5][6][16]	11–12 October (France); 1–2 November (cross-border); 9 November (French attribution). [1][2][3]

What happened

France's Cyber Crisis Coordination Centre (C4) reported that the October attack targeted refrigeration controllers at around 700 French retail sites, with substantial stock losses and at least 15 fire outbreaks. In November, retailers in several countries reported disrupted refrigeration and removed affected stock from sale. [2][3][5][6][7]

Threat significance

The attacks turned a cyber compromise into a food safety, continuity and, in France, fire safety problem. An individual shop may lose chilled stock while checkouts and distribution remain functional. A shared controller or maintenance arrangement can expose independent stores to the same failure. [2][5][6][7]

> EXECUTIVE JUDGEMENT
>
> France named the Shahid Kaveh unit, linked to Iran's Islamic Revolutionary Guard Corps, for the 11–12 October attack. That attribution does not extend to the November incidents on the public evidence reviewed. Retailers should restrict remote access and check that independent temperature alarms reach staff who can act, including overnight. [1][2][3][4]

02 / RECONSTRUCTION

What happened

France | overnight 11–12 October

C4 says the attackers compromised refrigeration controls and changed defrost settings. It names Casino, Leclerc, Coopérative U, Metro, Carrefour and Intermarché among the affected retail groups and also reports effects on some other food businesses. The Gradignan Intermarché owner separately described discarding stock after the overnight incident. [2][9]

Several countries | overnight 1–2 November

The EU joint statement confirms a new wave across several member states. Swedish NCSC reported incidents in grocery refrigeration and contact with affected organisations. In Ireland, Musgrave said monitoring alerted staff and chilled and frozen items were withdrawn at 13 SuperValu stores as a precaution. The company reported resolution and restocking on 2 November. [3][4][7]

Parallel incident | Ahold Delhaize corporate IT

The group first disclosed its IT incident on 12 October and said it took some systems offline to protect its environment. It later identified effects on online services in the Benelux and US and on Benelux supply-chain operations. The group's November results provide no evidence tying that October IT outage to the refrigeration attacks. [10][11]

03 / GEOGRAPHIC COMPARISON

Where disruption was reported

The examples below have a named operator or national authority behind the reporting. Counts refer to each named operator, not the national total.

COUNTRY / AREA	OPERATOR EVIDENCE AND LIMIT
France · October	C4: around 700 retail sites targeted across several groups. No public site roster in the C4 report. [2]
Belgium / Luxembourg	Delhaize reported several dozen sites across both countries, mostly in Belgium. Carrefour reported 15 Belgian sites. Delhaize said distribution centres and deliveries were operating normally. [5]
Sweden	ICA told Reuters 23 stores were affected. Coop's count was six in early AP reporting and seven in a later Reuters report; use seven as the later operator count. [4][5][6]
Ireland	Musgrave reported 13 SuperValu stores affected. Stores remained open; replenishment started after the operator reported resolving the incident. [5][7]
Estonia	Selver confirmed one outlet to ERR; the Estonian Information System Authority (RIA) said it had received one notification at the time of its interview. [8][15]
Germany	Edeka confirmed one case to Reuters at Reisbach. This is an operator example, not a national tally. [6]
Finland	Yle quoted the national cyber authority confirming a cyberattack and reported disruption at a few smaller K Group shops. No exact count. [16]
Netherlands / Italy · adjacent	NOS cited a supplier reporting at least 17 Dutch businesses, including small shops and non-retail sites. ANSA cited Italy's cyber authority on a caterer and a frozen-food producer. Neither is a national supermarket tally. [17][18]
United Kingdom · adjacent	Trade body AIMS reported three affected British meat suppliers. This is supply-chain evidence, not a UK supermarket count. [13]

EU authorities did not publish a harmonised site count in their joint statement. These selected cases cannot establish which countries escaped disruption or rank national exposure. [3]

04 / CHRONOLOGY

Event and reporting timelines

EVENT DATE	WHAT OCCURRED OR WAS DETECTED
11–12 Oct · local time	France: overnight compromise of retail refrigeration controls. C4 was alerted on 12 October. [2]
12–13 Oct · local time	Le Monde later described a smaller second French episode the following night. Its inclusion in the public attribution is unclear. [12]
1–2 Nov · local time	EU authorities date the later wave to this window. The time of detection varied by operator; no common minute of onset is established. [3][5][7]

PUBLICATION DATE	WHAT BECAME PUBLIC
12 / 19 Oct	Ahold Delhaize first disclosed its corporate IT issue on 12 October, then explained its precautionary shutdowns on 19 October. [10]
2 / 3 Nov	National and operator reports identified November refrigeration disruption and updated some shop counts. [4][5][6][7][8]
4 Nov	EU bodies issued a joint call to reduce exposure. Ahold Delhaize published its financial estimate separately. [3][11]
9 Nov	France publicly named Shahid Kaveh. The Paris prosecutor reported seeking international arrest warrants; France said it would propose EU sanctions. [1][2][12]

Event dates above use local civil time. The research cutoff is 9 November, 23:59 GMT. A reporting date or time of detection does not establish when access first occurred.

05 / ATTRIBUTION

What the attribution covers

Official position | high confidence that France made the attribution

France attributes the 11–12 October refrigeration sabotage to Iran. C4 identifies the Islamic Revolutionary Guard Corps (IRGC) as directing the operation and Shahid Kaveh as carrying it out. The ministry and C4 are one coordinated attribution family. They are authoritative for the French position, but the underlying logs and complete chain of evidence were not released. [1][2]

Weight of the public indicators | ISS Global assessment

C4 cites overlap in attack infrastructure and previously observed activity, references to the attack in a media outlet associated with the unit, and traces of Persian in the infrastructure. Infrastructure overlap carries more weight when independently validated. Language traces and media amplification cannot establish responsibility by themselves. Le Monde reported the Paris prosecutor's warrant requests; requests are not issued warrants or convictions. [2][12]

November | actor undetermined

Timing, sector and effects make a connection worth investigating, but similar failures can arise when different actors target the same class of equipment. The EU statement confirms the November wave without assigning responsibility. SVT reported claims by pro-Russian groups; the public reporting does not verify those claims or establish who carried out the incidents. [19] The C4 report also discusses a separate Iranian unit, Shahid Shoostari, in connection with other operations; that is not the unit France named for the October refrigeration attack. [1][2][3]

> WHAT WOULD CHANGE THE ASSESSMENT
>
> Authenticated cross-border matches in logs, infrastructure or other distinctive evidence, confirmed by independent investigators, would carry more weight than the similarity of the damage.

06 / CONSEQUENCES

Physical damage and business impact

France | scale and accounting

C4 gives approximately 700 retail sites targeted; the foreign ministry says more than 700. Both describe targeting, not a count of fires, closures or verified losses at every site. C4 reports at least 15 fire outbreaks. The ministry's food loss estimate is in the tens of millions of euros; no audited breakdown appears in the cited releases. [1][2]

November | local disruption

The operator accounts show stock withdrawals and reduced availability at affected shops. Delhaize reported that deliveries continued; Musgrave reported same-day resolution. At the Estonian site, ERR reported a changed controller setting. A setpoint is not a measurement of cabinet air or product temperature. The selected sources do not establish a Europe-wide loss figure or count of injuries. [3][5][7][8]

Ahold Delhaize | separate financial estimate

On 4 November the group estimated a €200–250 million reduction in net sales and €75–100 million reduction in underlying and IFRS operating income from its October corporate IT incident. These are forward estimates of different financial measures; they should not be added together or treated as refrigeration damage. The company said most disruption was contained within two weeks, with restoration still in progress at the update. [11]

Beyond retail | separate records

The November British reports concern meat suppliers. France also reported an incident involving blood-storage refrigeration; its health ministry said no blood products were compromised, according to AP. Neither is counted as a supermarket incident or treated here as evidence of common authorship. [13][14]

07 / EVIDENCE AUDIT

What remains unresolved

CLAIM OR DISCREPANCY	DISPOSITION AT CUTOFF
October French scope	Prefer C4's approximate count for the analytical baseline and keep the ministry's wording distinct. Obtain site-level records before counting spoilage, closures or fires by retailer. [1][2]
Second French night	Press reporting describes 12–13 October separately. C4's named attribution is dated 11–12 October. Hold the later episode apart pending clarification from French investigators. [2][12]
November country totals	Operator counts are snapshots and may use different definitions. Do not add incident reports, shop counts, device counts or suppliers. Confirm site and incident identifiers before aggregation. [3][5][6][13][15]
Ahold vs Delhaize	The parent's October corporate IT event and the Delhaize banner's November refrigeration report differ in date, scope and effects. Keep separate records unless a link is evidenced. [5][10][11]
Scene evidence	Published photographs associated with Caen and Lucan show store conditions as described by their publishers. No original metadata, site-wide coverage or reproduction rights were established; no image is used to prove attribution or temperatures. [7][9]

ANALYTICAL LIMITS

This is an open-source review of selected cases. It cannot determine the total number of affected sites, independently reproduce the French attribution, or rule out a connection between the waves.

08 / OPERATOR PRIORITIES

Protect stock and keep stores operating

Today | estates, IT security and contractors

Name one accountable owner for each site's refrigeration, including franchises. Confirm whether external service access is needed. Remove direct internet exposure, restrict necessary access to authenticated and monitored routes, and arrange any change with refrigeration engineers to preserve safe local operation. [3][4]

Today | store management and food safety

Test independent temperature sensing, alarm delivery and overnight escalation. If readings cannot be trusted, hold affected stock and record the time and temperature evidence before deciding whether to release, transfer or discard it under established food safety procedures. Escalate signs of overheating through site safety procedures.

This week | engineering and incident response

Inventory controllers and maintenance dependencies; prioritise updates and unsupported equipment. Preserve configuration history, access logs and independent sensor data where safe. Record local time and UTC, when the anomaly was detected, and what was measured versus commanded. Test recovery and stock replenishment as separate steps.

For investigators | distinguish linked events from similar failures

Request a deduplicated site register, original logs from operators and service providers, and fire-service records for the French incidents. Ask national cyber authorities to compare November evidence across borders. Record common equipment as context; keep actor linkage provisional until evidence supports it. [2][3][4]

> MEASURE THE RESPONSE
>
> Track sites with an accountable owner, verified restricted access and a successfully tested independent alarm. Restore stock only after the responsible food safety lead signs off.

SOURCE REGISTER

Sources 01–05

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

01 Déclaration d’attribution à l’Iran de cyberattaques visant la France

France Diplomatie · 2026-11-09

Family: French government attribution · Accessed 10 Nov 2026. French statement read; state position and estimates.

https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/declaration-d-attribution-a-l-iran-de-cyberattaques-visant-la-france

02 Activités cyber offensives ciblant la France menées par des acteurs iraniens liés au CGRI

C4 / **CERT-FR** · 2026-11-09

Family: French government attribution · Accessed 10 Nov 2026. French public report read; underlying forensic data not released.

https://www.cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-009.pdf

03 Joint statement on cyber incidents in refrigeration systems across the EU

European Commission / **EU cyber partners** · 2026-11-04

Family: Joint EU authority statement · Accessed 10 Nov 2026. English statement read; no victim census or actor finding.

https://digital-strategy.ec.europa.eu/en/news/joint-statement-cyber-incidents-refrigeration-systems-across-eu

04 Cyberangrepp mot uppkopplade frys- och kylsystem

Nationellt cybersäkerhetscenter (Sweden) · 2026-11-02

Family: Swedish national cyber authority · Accessed 10 Nov 2026. Swedish notice read; no chain totals.

https://www.ncsc.se/sv/aktuellt/cyberangrepp-mot-kylsystem

05 Supermarket freezers in several European countries hit by apparent cyberattacks

Associated Press · 2026-11-02

Family: AP reporting / named operators · Accessed 10 Nov 2026. English text read; early operator and news agency accounts.

https://apnews.com/article/a8ea5b30d67da47957769f29101fe686

SOURCE REGISTER

Sources 06–10

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

06 European supermarkets rush to patch vulnerabilities after region-wide fridge hack

Reuters via Investing.com · 2026-11-03

Family: Reuters reporting / named operators · Accessed 10 Nov 2026. English syndicated text read; site counts from operators.

https://www.investing.com/news/stock-market-news/european-supermarkets-rush-to-patch-vulnerabilities-after-regionwide-fridge-hack-4995896

07 SuperValu says issues after cyberattack on its fridge systems ‘fully resolved’

The Irish Times · 2026-11-02

Family: Irish Times reporting / Musgrave · Accessed 10 Nov 2026. English article read; recovery as stated by Musgrave.

https://www.irishtimes.com/technology/data-security/2026/11/02/supervalu-removes-frozen-and-chilled-food-from-13-stores-after-cyber-attack-on-fridges/

08 Hackers raised freezer temperature at Selver supermarket to +50°C

ERR · 2026-11-02

Family: ERR reporting / Selver and service provider · Accessed 10 Nov 2026. English article read; headline describes a setting, not a measured product temperature.

https://news.err.ee/1610183296/hackers-raised-freezer-temperature-at-selver-supermarket-to-50-c

09 A disastrous day for French supermarkets after massive cyberattack targets refrigeration systems

Le Monde · 2026-10-13

Family: Le Monde reporting / store owner · Accessed 10 Nov 2026. English subscriber preview read; direct account from Gradignan.

https://www.lemonde.fr/en/economy/article/2026/10/13/a-disastrous-day-for-french-supermarkets-after-massive-cyberattack-targets-refrigeration-systems_6758535_19.html

10 Ahold Delhaize update on status of cybersecurity incident

Ahold Delhaize · 2026-10-19

Family: Ahold Delhaize corporate disclosures · Accessed 10 Nov 2026. English update read; describes containment, not a finding of shared cause.

https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/

SOURCE REGISTER

Sources 11–15

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

11 Ahold Delhaize reports resilient Q3 2026 results and updates 2026 guidance to reflect business disruption caused by recent cybersecurity incident

Ahold Delhaize · 2026-11-04

Family: Ahold Delhaize corporate disclosures · Accessed 10 Nov 2026. English release read; financial effects are forward estimates.

https://newsroom.aholddelhaize.com/ahold-delhaize-reports-resilient-q3-2026-results-and-updates-2026-guidance-to-reflect-business-disruption-caused-by-recent-cybersecurity-incident

12 Cyberattaque contre des réfrigérateurs de supermarchés : la justice ouvre une enquête contre un groupe iranien lié aux gardiens de la révolution

Le Monde · 2026-11-09

Family: Le Monde reporting / Paris prosecutor · Accessed 10 Nov 2026. French article read in updated form; used for prosecutor's announcement of 9 November.

https://www.lemonde.fr/pixels/article/2026/11/09/cyberattaque-des-refrigerateurs-de-supermarche-la-justice-ouvre-une-enquete-contre-un-groupe-iranien-jean-noel-barrot-souhaite-des-sanctions-a-l-echelle-europeenne_6808673_4408996.html

13 British businesses caught in Europe-wide supermarket fridge attacks

The Record · 2026-11-03

Family: The Record reporting / AIMS · Accessed 10 Nov 2026. English article read; trade body account concerns suppliers.

https://therecord.media/british-businesses-caught-in-europe-wide-supermarket-fridge-attacks

14 Cyberattack hits French blood bank site but no blood products are compromised

Associated Press · 2026-11-04

Family: AP reporting / French health ministry · Accessed 10 Nov 2026. English wire account read; health ministry account, outside retail scope.

https://apnews.com/article/12b80bcf93b8404264209e519c204919

15 Kraft: millised on rünnakute motiivid, pole praegu teada

ERR · 2026-11-02

Family: ERR interview / Estonian RIA · Accessed 10 Nov 2026. Estonian interview read; only one report received by RIA at interview time.

https://www.err.ee/1610183710/kraft-millised-on-runnakute-motiivid-pole-praegu-teada

SOURCE REGISTER

Sources 16–19

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

16 Kyberturvallisuuskeskus vahvistaa: kauppojen kylmälaitehäiriöt johtuivat kyberhyökkäyksestä

Yle · 2026-11-04

Family: Yle reporting / Finnish cyber authority · Accessed 10 Nov 2026. Finnish article read; authority confirms attack, no exact shop count.

https://yle.fi/a/74-20255142

17 Ook koelsystemen in Nederland aangevallen, bij 17 bedrijven temperatuur aangepast

NOS · 2026-11-02

Family: NOS reporting / refrigeration supplier · Accessed 10 Nov 2026. Dutch article read; company count from vendor, includes non-retail sites.

https://nos.nl/artikel/2637734-ook-koelsystemen-in-nederland-aangevallen-bij-17-bedrijven-temperatuur-aangepast

18 Attacchi hacker ai supermercati, alert Agenzia cyber in Italia

ANSA · 2026-11-02

Family: ANSA reporting / Italian cyber authority · Accessed 10 Nov 2026. Italian article read; cited cases are food-sector operators, not supermarkets.

https://www.ansa.it/sito/notizie/cronaca/2026/11/02/attacchi-hacker-ai-supermercati-alert-agenzia-cyber-in-italia_6a838d5b-aef2-48ac-b082-37c487819ded.html

19 Pro-ryska grupper påstår sig ligga bakom flera kylattacker

SVT Nyheter · 2026-11-04

Family: SVT reporting / public claims · Accessed 10 Nov 2026. Swedish article read; reports unverified claims, not an attribution.

https://www.svt.se/nyheter/utrikes/pro-ryska-grupper-pastar-sig-ligga-bakom-flera-kylattacker