

THE ALS GROUP

Managing Risk to Influence Successful Outcomes

Hacked Freezers and "Silent" Cyber: Would Your Property Policy Pay?

Key Takeaways

- Hackers turned supermarket freezers across Europe up to 50°C (122°F) through old, internet-connected refrigeration controls. It's a textbook case of "silent" cyber: a cyber cause behind a physical loss your policies may not clearly address.
- Silent cyber means a property, liability or equipment policy neither clearly covers nor clearly excludes a cyber event, so you don't know if it pays until the claim. Read your property, cyber and spoilage forms side by side now.
- Before it happens here: list every connected device, lock down contractor remote access, and put security and insurance requirements in your vendor contracts.

On November 2, refrigerators and freezers at supermarkets in Belgium, Sweden, Ireland, the Netherlands, Estonia, Luxembourg and other countries were switched into a heating mode overnight (The Record). It was the second wave in about three weeks. In October, a similar attack hit hundreds of supermarkets in France, and the Paris prosecutor counted around 700 victims. This isn't just a European grocery story. It's a preview of a risk sitting in buildings across the U.S.

The insurance industry has a name for the coverage problem behind it: "silent" cyber. Here's what it is, why it matters to your business and what to do about it.

1. The attackers went through equipment, not computers

The target was the remote controllers that run refrigeration systems:

- **Old, unsupported devices:** Danfoss and Copeland said the units hit in France were mainly discontinued products that no longer get security updates.
- **Weak access:** Danfoss said some affected Dutch systems weren't on a secure network and still used default passwords (The Hacker News).
- **Built for the contractor:** These controls are often connected to the internet so refrigeration contractors can monitor and repair them remotely.

One Belgian refrigeration contractor said some units need physical changes, not just a software update. No group has claimed the attacks, and Belgium's cybersecurity agency said the attackers may never be identified.

2. Your building probably has the same kind of exposure

Grocery stores aren't the only ones running connected equipment. Restaurants, hotels, healthcare facilities, warehouses, office buildings and apartment communities rely on systems like these:

- Refrigeration and walk-in coolers



- HVAC and building management systems
- Access control, elevators and fire panels

Many were installed by a contractor, connected for remote monitoring and never added to IT's list of devices to protect. When nobody owns a system, nobody updates it.

3. This is "silent" cyber, and it can hide in your property policy

A hacked freezer creates a physical loss (spoiled inventory, damaged equipment, lost sales while you restock) from a cyber cause. When a traditional policy, such as property, general liability or equipment breakdown, doesn't clearly cover or clearly exclude a loss like that, the industry calls it "silent" cyber. No one priced the risk, and no one knows if the policy pays until there's a claim. Here's where it gets tricky:

- **Property policies** may exclude or limit losses caused by a cyber event.
- **Cyber policies** often exclude physical damage to tangible property, like the food and the equipment.
- **Spoilage and equipment breakdown coverage** may carry its own exclusions or low limits.
- **Business income** while you clean, restock and reopen depends on which policy, if any, responds to the underlying loss.

Many insurers have rewritten their property and liability forms in recent years to state plainly whether cyber is covered or excluded. That's progress, but the answer is often "excluded," and if your policy is still silent, you don't know where you stand. Read together, these forms can leave a gap no one notices until the claim. We read the forms!

4. Vendors with remote access need contracts and insurance to match

If a contractor installs and monitors your equipment, your contract should cover more than service calls:

- **Security duties:** changing default passwords, connecting only through a secure network or VPN, applying updates and flagging end-of-life equipment
- **Notice:** how quickly they must tell you about a suspected breach
- **Insurance and indemnity:** technology errors and omissions and cyber coverage from vendors with remote access, plus clear indemnification language

France's cybersecurity agency even advised businesses to check their insurance terms before cutting off a contractor's data feed. That's how tightly the equipment, the contract and the coverage are tied together.

5. Three steps to take now

1. **Find what's online:** List every piece of equipment that connects to the internet, who installed it and who can reach it remotely.
2. **Lock down remote access:** Change default passwords, require a secure connection, apply updates and replace equipment that no longer gets security patches.
3. **Read your property, cyber and spoilage coverage side by side:** Confirm which policy pays if a hack spoils your inventory or shuts down your operations, and whether any of them is silent on cyber.



How ALS Helps

We look at risk first and insurance second. We review your property, cyber and equipment breakdown policies side by side to find where a cyber-caused physical loss could fall through or where a policy is silent on cyber, check your vendor contracts and insurance requirements for contractors with remote access, and add connected equipment to your enterprise risk picture. Because we're independent and fee-based, our only interest is making sure your coverage responds when you need it.

There you have it: what "silent" cyber is, why Europe's freezer attacks put it in the spotlight, and the three steps to take before it happens here.

Frequently Asked Questions

What is silent cyber insurance? "Silent" cyber is cyber exposure inside a traditional policy, such as property, general liability or equipment breakdown, that the policy doesn't clearly cover or clearly exclude. Because it was never priced, whether it pays comes down to how the claim is argued. Many insurers now add wording that affirms or excludes cyber, so it's worth checking which way yours went.

How did hackers get into supermarket freezers? Through internet-connected refrigeration controllers. Reports point to older devices that no longer received security updates, some left on open networks with default passwords. Many were connected so contractors could monitor them remotely.

Does cyber insurance cover physical damage from a cyber attack? Often not. Many cyber policies exclude damage to tangible property, such as spoiled inventory or broken equipment. Some offer limited coverage by endorsement, so the policy wording matters.

Does property insurance cover spoilage caused by a hack? It depends on the policy. Some property and spoilage coverages exclude or limit losses caused by a cyber event. Reading the property, spoilage and cyber forms together is the only way to know.

Who is responsible if a contractor's remote access is used in an attack? That comes down to your contract. Clear security duties, notice requirements, indemnification and insurance requirements for the contractor decide who pays. Without them, the loss is likely to land on you.

Which businesses should be concerned? Any business with connected building equipment: grocery, restaurants, hospitality, healthcare, warehousing and property owners with HVAC or building management systems. If a contractor can reach it remotely, so can someone else.

If you need more information on any of the topics covered here, or are interested in a Risk Management Assessment ("RMA"), please contact our Managing Principal, Albert Sica, at asica@thealsgroup.com or at 732.395.4251.