

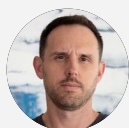


The Refrigerators Were Hacked.

Would Your Business Have Known?

When hackers manipulated supermarket refrigeration systems across France, the damage spread far beyond the network.

The harder question is how a business can recognize trouble when the equipment it trusts is no longer telling the full story.



A FIELD NOTE BY

Thomas Latiolais

Chief Marketing Officer



veea.com

Intelligently Connected™

PART I

THE INCIDENT

*At five in the morning, a baker arrived at a supermarket in Normandy, France, and discovered something was **terribly wrong**.*

The refrigeration equipment wasn't working properly, and temperatures inside some units had climbed to dangerous levels.

5:00*in the morning*

He called the store's director, and what should have been the beginning of an ordinary business day quickly became a race to understand what was happening and save whatever inventory they could.

122°F*store units*

The staff checked equipment, attempted restarts, and called technicians. Eventually, they learned that someone had remotely manipulated the refrigeration controls.

176°F*fish dept. units*

Temperatures had reportedly reached 122°F, with some equipment in the fish department reaching as high as 176°F. By the time the situation was brought under control, the store had lost approximately \$112,000 worth of food.

**\$112,000** *reported food loss*

The store was an Intermarché in La Haye-du-Puits. Its director, Julien Fréret, recounted the experience in [a first-person account](#) published by Business Insider. His supermarket was among hundreds affected by cyberattacks targeting refrigeration systems across France in October 2026.

Attackers reportedly manipulated refrigeration and defrost settings, causing extensive food losses and business disruptions. Fires were also reported at some affected locations.

One detail in the reporting particularly caught my attention. [Le Monde reported](#) that attackers extended defrost cycles from one hour to eight hours, delaying alarms and giving temperatures more time to rise. That detail came from the wider attacks, not necessarily this particular supermarket. Think about what that means. The controls responsible for operating the refrigeration equipment were manipulated, and the warning process that operators depended on could be delayed as well.

I've spent much of my career working at the intersection of software, networking, and the physical world. When I read about these attacks, I wasn't just thinking about the cybersecurity failure. I was thinking about the store owner, the employees who arrived that morning, and all the inventory that was lost before anyone understood what was happening.

And I kept coming back to one question.

What if the business had known something was wrong hours before anyone opened the doors?

Not because another screen was displaying information from the same compromised refrigeration controller. Not because another alarm depended on that controller behaving correctly. I mean an independent way to recognize that physical conditions inside the store were changing, regardless of what the refrigeration system was reporting.

That question gets to something much bigger than a cyberattack on refrigerators. It gets to how we should think about protecting the businesses, equipment, and operations we depend on every day.

PART II
THE BREACH

When connected equipment becomes a vulnerability

Most of us think of refrigeration as a fairly straightforward process. The refrigerator keeps things cold, and if something goes wrong, we expect it to tell us. Commercial refrigeration systems, however, are considerably more sophisticated than the appliance in your kitchen.

They use electronic controllers to manage compressors, fans, temperatures, defrost cycles, and other operating functions. Many are also connected to networks so technicians and operators can monitor, diagnose, and manage them remotely.

There are good reasons for that connectivity.

If you operate a hundred grocery stores, you don't want to send a technician across the country every time a refrigeration system needs an adjustment.

Remote management improves efficiency, reduces service costs, and gives operators greater control over equipment spread across multiple locations.

But the same connectivity that makes these systems convenient can also create opportunities for unauthorized access.

In the French attacks, criminals manipulated refrigeration controls, including settings associated with defrost operations. Commercial systems use defrost cycles to prevent ice buildup, but abusing those functions can cause temperatures to rise dangerously. French authorities identified affected Danfoss, Copeland, and Dixell controller families. The exact intrusion methods used across all affected sites have not been conclusively established.

There's a second reason the story should concern anyone operating connected equipment. [The Register reported on October 15](#) that researchers had warned about serious weaknesses in certain refrigeration controllers months before the attacks. Claroty's Team82 documented issues including authentication bypass and the possibility of executing commands on affected equipment. U.S. cybersecurity advisories had also described vulnerabilities in these controller families.

According to scanning data quoted in that report, 1,506 IP addresses were exposing Danfoss StoreView administration interfaces to the public internet during September and early October; 820 were associated with French networks.

1,506

*IP Addresses exposing
administration views*

These were **exposed interfaces**, not a confirmed count of vulnerable or hacked devices. And investigators have not established that the specific flaws disclosed by researchers were the ones used in these incidents.

820

*of which were
located in France*

That distinction matters. I don't want to use an attack to imply that every exposed device was compromised. But the timeline makes something clear: publishing a warning, shipping a patch, and achieving protection in the field are three different things. Businesses need good maintenance and secure remote access, and they also need ways to reduce the consequences when prevention fails.

The obvious cybersecurity lessons are important. Equipment should be maintained, known vulnerabilities addressed, remote access protected, and unnecessary exposure to the internet eliminated. Those are basic practices every organization should take seriously.

But even with strong cybersecurity, we have to acknowledge something uncomfortable: no organization can guarantee that an attacker will never get through. A business can also experience mechanical failures, power problems, configuration errors, and human mistakes that have nothing to do with malicious activity.

That's why I think we need to approach the problem from two directions. First, how do we prevent unauthorized access and protect the systems that run the business? Second, if something goes wrong anyway, how quickly can we recognize it and respond? Those two questions lead us to a very different way of thinking about business protection.

FIELD NOTE

*Known risk
does not equal
protection.*



Vulnerabilities had been described before the France incidents.

Protecting the network is the first line of defense

Let's imagine walking into a typical retail store. There are payment terminals, employee computers, wireless networks, security cameras, printers, and perhaps dozens of connected devices operating behind the scenes. Some of those devices support everyday business activities. Others may control equipment that's essential to keeping the store operational. They all need connectivity, but that doesn't mean they should all be allowed to communicate with one another.

Think of your network like a building. Customers can enter the lobby, employees can access their workspaces, and managers may have access to restricted offices. But allowing someone into the lobby shouldn't automatically give them the keys to the stockroom or the safe. A business network should follow the same principle.



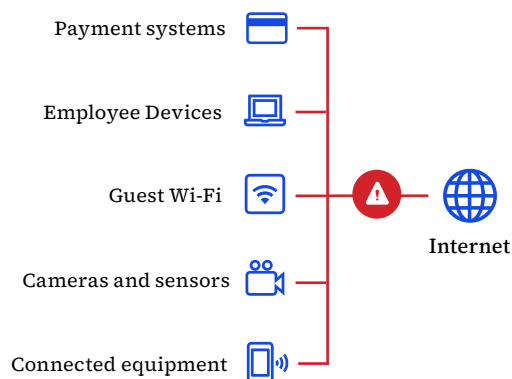
This is one of the problems we're addressing at Veeva with SecureConnect, our cybersecurity and managed networking solution. SecureConnect allows businesses to organize connected devices into different security profiles and establish policies controlling what those devices can access.

Guest Wi-Fi users can be isolated from payment systems, sensitive business equipment can operate in protected network segments, and unknown devices can be restricted until they're authorized. The technical term for this is network segmentation, but the business value is simple: just because something connects to your network doesn't mean it should have access to everything on it.

SecureConnect also provides firewall capabilities, traffic filtering, access controls, network visibility, and AI-driven anomaly detection designed to identify unusual patterns of activity. If a device that normally communicates with a predictable group of systems suddenly begins generating unexpected traffic, that behavior may warrant investigation. Depending on how policies are configured and which traffic passes through the protected network path, prohibited connections can be blocked and suspicious behavior can be surfaced for review.

The traditional model

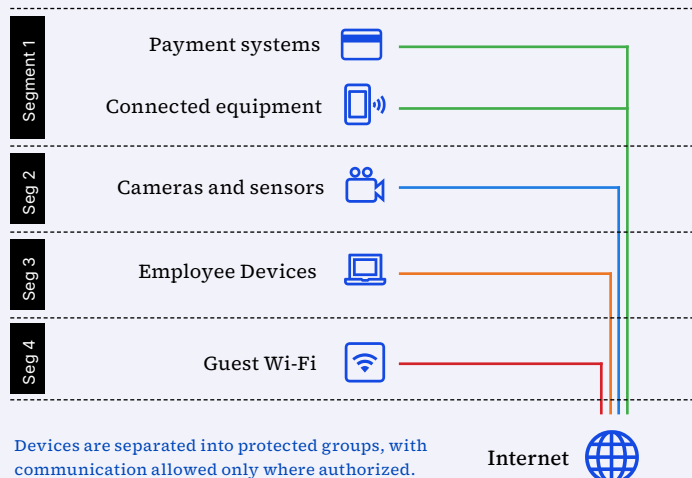
A flat, shared network with direct Internet access that increases the risk significantly.



If one device gets compromised, the rest of the network can be accessed by the hackers easily.

The SecureConnect™ model

A segmented, monitored, and protected network that controls communication between device groups and helps contain threats.



Devices are separated into protected groups, with communication allowed only where authorized.

Consider how this relates to the French supermarket attacks. Refrigeration controllers should not be freely accessible from unrelated devices or exposed to unnecessary network traffic. Proper segmentation, access policies, and secure remote connectivity can reduce some attack paths and limit an intruder's ability to move between systems. They do not automatically protect a controller if an attacker reaches it through an otherwise permitted management connection.

Could SecureConnect have prevented the exact incidents in France? We can't make that claim without knowing the specific configurations and methods used at each affected location. But the underlying principle is sound: control access, limit unnecessary communication, and look for behavior that doesn't belong.

Now let's consider the situation that makes this story particularly interesting. What happens if those defenses aren't enough?



What if the refrigerator had its own set of eyes?

Imagine that an attacker has successfully manipulated a refrigeration controller in the middle of the night. The controller is no longer operating as intended, and the equipment's normal warning mechanisms may not be functioning correctly. The store is closed, the employees have gone home, and no one is there to notice the temperature beginning to rise.

In a traditional setup, the business may be relying entirely on the refrigeration system to report its own condition. If the controller has been compromised or its alarms are delayed, the owner might not receive a meaningful warning until the damage is already done.

Now imagine placing a small, appropriately specified wireless temperature sensor inside that refrigerator, independent of its existing controller. Rather than asking the refrigeration system to report its own temperature, we're measuring the actual physical conditions through a separate device.

Let's say the refrigerator normally operates around 37°F. Something goes wrong, and the temperature begins climbing outside its approved operating range. Our independent monitoring system recognizes the change and, based on the rules we've configured, alerts the appropriate person.

We no longer have to depend exclusively on the refrigeration controller to acknowledge that it has a problem. We have another source of information, one that measures the environment rather than trusting the equipment's own assessment. That independence is specifically from the refrigeration controller; sensors, the hub, power, and communications must still be installed, monitored, and maintained properly.

The system responsible for controlling something shouldn't always be the only system responsible for telling you whether it's working correctly.

That idea is familiar in critical infrastructure and data centers, where independent monitoring provides visibility into equipment and environmental conditions. But the same thinking can benefit a grocery store, restaurant, pharmacy, warehouse, or virtually any other business that depends on physical equipment.

And temperature is only one part of the picture.

PART III
THE SOLUTION

Recognizing the warning signs before they become disasters

When I think about designing a monitoring solution, I don't stop at the most obvious measurement. I ask what else might tell us something useful about the condition we're trying to protect.

For refrigeration equipment, one of those measurements could be electrical power consumption.

Commercial refrigeration systems use electricity to operate compressors, fans, defrost heaters, and other components. With properly rated metering equipment installed for the application, we may be able to observe changes in their power consumption. A unit might begin drawing substantially more power than expected, operate for unusually long periods, or show an unexpected reduction in consumption. Those patterns are useful clues, not automatic diagnoses.

None of those changes automatically means a cyberattack. There could be a mechanical problem, a defrost cycle operating differently, or another legitimate explanation. But imagine observing an unusual power pattern at the same time an independent temperature sensor begins reporting rising temperatures. We now have two separate observations telling us something deserves attention.

The value becomes clearer when we consider other possible explanations.

Perhaps an employee accidentally left the refrigerator door open. A small wireless contact sensor could tell us whether the door is open or closed. Maybe someone was working in the storage room after hours.

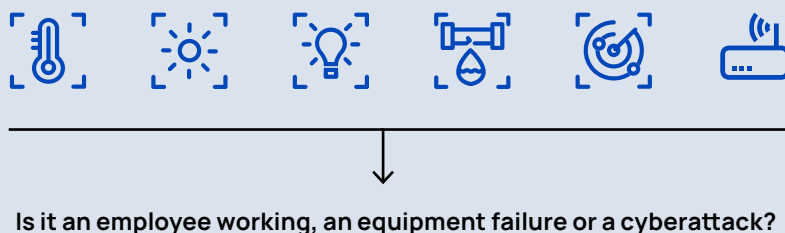
A motion sensor could provide additional information about activity in the monitored area. If a camera covers that location, the operator could review an available image or recording to better understand what was happening.

Now consider a scenario in which the refrigerator temperature is rising, the power consumption has changed, the refrigerator door remains closed, and no motion has been detected in the storage room. The available camera footage shows no obvious physical activity around the equipment.

That doesn't prove someone has launched a cyberattack. We could still be dealing with an equipment failure or another operating problem. But it gives the person responding to the incident much more useful information than a single alarm saying the temperature is too high.

FIELD NOTE

No single sensor explains everything.



Different observations can reveal different aspects of a developing incident, providing context.

We might also monitor for water leaks near refrigeration equipment, unexpected access to storage areas, or changes in environmental conditions. Each sensor provides a different piece of information about the physical world.

The important thing is that these measurements don't have to depend on one another to be useful. A critical temperature alert should still be issued even if a power reading is unavailable or a camera isn't responding. Additional information should help someone understand the situation, not delay a warning. And none of these connected sensors replaces dedicated equipment safety controls or a required fire protection system.

What we're creating is a more complete picture of what's happening inside the business. One measurement tells us about temperature. Another tells us about power. Others help establish whether someone opened a door, entered an area, or was physically present when an event occurred.

Individually, these are relatively simple capabilities. Together, they can provide the context needed to make better decisions, faster.

Turning separate signals into useful intelligence

Let's return to our hypothetical supermarket in the middle of the night.

An attacker has manipulated a refrigeration controller. Perhaps our cybersecurity system detected suspicious network activity, or perhaps the attack used a permitted connection and wasn't immediately recognized. Either way, the physical conditions inside the refrigerator have begun changing.

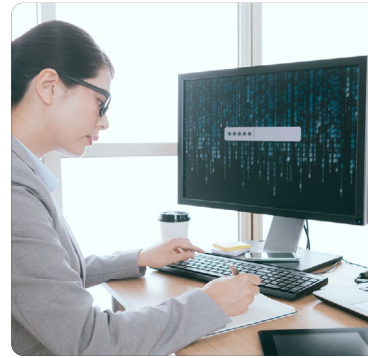
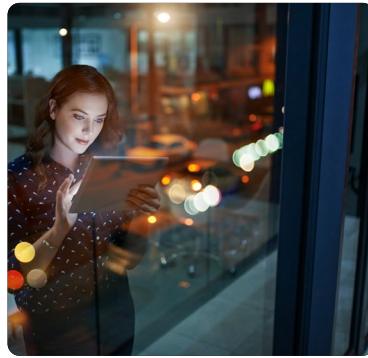
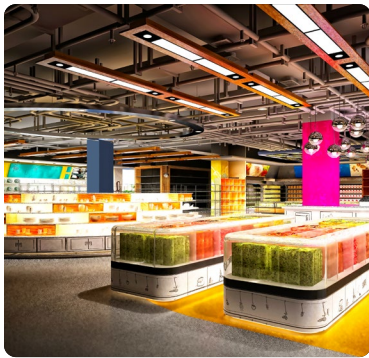
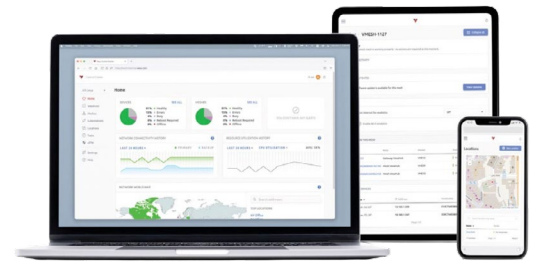
With independent monitoring in place, the temperature sensor continues measuring the actual conditions. A power monitor may identify a change in equipment behavior, while contact sensors and cameras provide additional context about the area.

Instead of waiting until someone opens the store the following morning, a monitoring rule could recognize that the temperature has moved outside the acceptable range and generate an alert.

More importantly, the alert could include relevant information that helps the operator understand why it matters.



Imagine receiving a notification indicating that a cold storage unit has exceeded its approved temperature threshold. The associated information shows that power consumption has changed, the refrigerator door remained closed, and no motion was detected in the monitored area. A camera recording is available for review.



This is an illustrative scenario, not an account of what Veea did at any affected French supermarket. Exact incident, notification, and camera-evidence workflows depend on the devices, application integrations, and configuration supplied to the location.

But the principle is important: an alert is more valuable when it arrives with relevant context.

Someone can assess the information, investigate the cause, contact a technician, or initiate the appropriate response before the situation deteriorates further.

There's no guarantee that every problem can be stopped in time. Some failures happen quickly, and alerts only create value when someone is available and prepared to respond. But earlier awareness creates an opportunity that doesn't exist when the first indication of trouble arrives after the damage is done.

It gives the business something incredibly valuable.

Time to act.

PART IV
THE ECOSYSTEM

Bringing everything together with Veeva VigiLynx™

At this point, we've talked about cybersecurity, network segmentation, temperature monitoring, power consumption, wireless sensors, cameras, and alerts.

It might sound like a complicated collection of separate systems, each requiring its own hardware, software, and management tools.

Traditionally, that is exactly how many businesses have accumulated technology.

They have a router from one vendor, cameras from another, sensors managed through a separate application, and cybersecurity tools that don't necessarily know anything about the physical environment.

The result can be a collection of systems that individually perform useful tasks but provide limited context when something goes wrong.

At Veeva, we've taken a different approach.

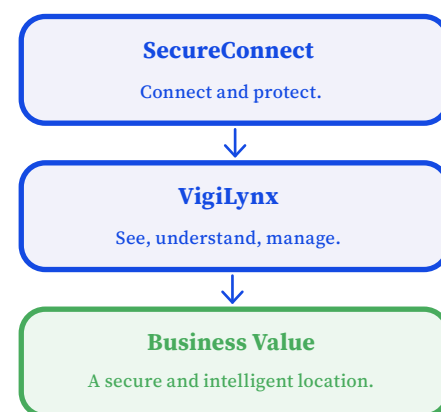
Our Veeahub is a compact edge computing platform that brings together networking, connectivity, security capabilities, local processing, and support for compatible connected devices.

It can provide managed Wi-Fi, enforce network segmentation through SecureConnect, communicate with supported wireless sensors, and run local applications on the same device. This is why the networking, security, and physical monitoring functions don't each need their own separate computer.

Built on that foundation, VigiLynx brings together SecureConnect, physical monitoring through IoT Pulse, and camera capabilities through VeeaNvision. Rather than treating the network, sensors, and cameras as unrelated technologies, VigiLynx is designed to organize their information around the business location and the assets being monitored.

For a supermarket, that asset might be a refrigerator or cold storage room. We can associate compatible temperature sensors, door contacts, power monitoring equipment, and cameras with that location, then establish rules governing which conditions should trigger attention.

For a business owner, the experience becomes much more straightforward. Instead of checking several unrelated systems to understand one incident, the objective is to provide an operating view that brings the relevant information together.



*What makes this powerful isn't any one sensor, camera, or security feature.
It's what happens when they work together.*

Cybersecurity tells us what's happening on the network. Sensors tell us what's happening in the physical environment. Cameras help us see what's happening. Together, they give us a much better opportunity to understand what's happening to the business.

A firewall can't tell you whether the milk is getting warm. A temperature sensor can't tell you whether an unknown device is attempting to access your payment network. A camera can't determine whether a compressor is consuming an unusual amount of electricity.

But when these capabilities operate within a common environment, they can complement one another in ways that isolated products cannot.

That's the value we're trying to deliver. Not simply more connected devices, but useful information that helps people recognize and respond to situations that matter.



What happens if the internet connection fails?

There's another part of this conversation that's especially important when we're protecting critical business operations.

Suppose the monitoring system recognizes a serious problem, but the location's primary internet connection has failed. How does the notification reach someone who isn't physically at the site?

The Veeahub supports different connectivity arrangements depending on the hardware and service configuration. A business may use wired broadband as its primary connection, with cellular connectivity available as a backup. Alternatively, 5G may serve as the location's primary connection from the beginning.



For a business with wired broadband, properly configured 5G failover can provide another route for communications if the primary connection becomes unavailable. And because Veeahub's platform supports local applications and locally enforced security policies, some important on-site functions can continue operating without continuous cloud access. A cellular connection on the same hub isn't automatically a fully independent, out-of-band management system; it is an alternate path when the deployment is configured to use it that way.

That doesn't mean a cellular connection solves every possible outage. The hub still requires power, cellular coverage must be available, and remote alerts depend on functioning communications services. These arrangements need to be designed and tested around the particular location.

But the principle is the same one we've been discussing throughout this article: avoid depending on a single component when losing that component could leave the business without critical visibility.

A backup connection is another way to improve resilience, particularly when an owner or service provider needs to monitor equipment remotely.

PART V
THE FOUNDATION

It's not really about refrigerators

The more I think about the French supermarket incident, the more I see it as an example of a much broader opportunity.

When I talk with someone about monitoring their business, I don't want to begin by asking how many sensors they want to buy. I want to understand what matters to them, what could go wrong, and what information would help them respond.

Imagine walking into a pharmacy. Perhaps they have temperature sensitive inventory that must remain within a specified range. They might also want to know when someone enters a restricted storage area, whether the back door opens after hours, or whether equipment is behaving abnormally. A combination of appropriate sensors, cameras, security policies, and alerts could help address those needs.

A restaurant might have different priorities. Walk-in refrigeration, freezer temperatures, delivery entrances, water leaks, and other operating conditions may be important. A warehouse might care about humidity, vibration, environmental conditions, loading areas, or access to valuable inventory. Specialized equipment, including cooking systems, requires appropriate sensors and validated integrations; the platform shouldn't be represented as a substitute for equipment safety systems.

But the underlying approach remains consistent.

We identify what needs protection, determine which conditions matter, and choose the appropriate technology to monitor those conditions.

It's almost like putting together building blocks. A temperature sensor provides one kind of information. A motion sensor provides another. A power monitor, door contact, water leak detector, or camera adds a different perspective. Security policies help protect the devices and systems operating on the network.

Not every business needs every available capability. The goal is to select the right combination for the problem we're trying to solve.

This is also why I don't think of VigiLynx simply as a backup system.

For a business starting from scratch, it can provide a foundation for secure networking, connected monitoring, and cameras from the beginning. For a business with existing systems, compatible capabilities can be added to improve visibility or provide independent measurements of important conditions.

You may already have a refrigeration monitoring system that works well. That's fine. Keep it, and consider whether independent temperature monitoring would provide additional protection. You may already have cameras or internet connectivity. The question is whether those existing investments can be complemented or brought into a more useful operating environment.

And the benefits extend beyond cybersecurity. The same monitoring that helps recognize a potential cyber-related incident can also reveal ordinary operating problems, such as a failing compressor, a refrigerator door left open, a water leak, or unexpected activity after hours.

These don't have to be malicious events to become expensive problems.

The business still benefits from knowing about them sooner.

From one location to an entire business

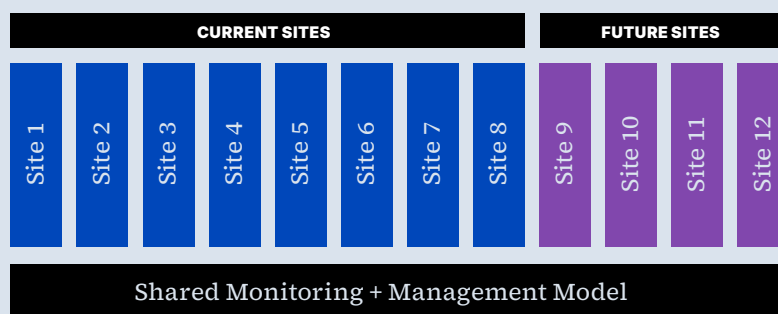
Now imagine you're not responsible for one supermarket, but fifty.

You can't personally inspect every refrigerator, review every camera, or walk through every stockroom. You need a way to maintain visibility across locations without treating each store as an entirely separate technology project.

Veeva's platform supports centralized management of connected sites, allowing operators and service providers to manage network policies, review site status, and support distributed locations. With appropriate monitoring configurations, businesses can establish more consistent operating practices, monitoring rules, and incident workflows across their sites.

FIELD NOTE

*One method.
Many locations.*



Repeat monitoring patterns without treating each site as a separate project.

The same principles that help protect one critical asset can become a repeatable model for protecting many.

That creates a different opportunity for businesses and the service providers supporting them. Instead of delivering a router, installing a camera, and walking away, we can think about the location as an environment that needs to remain connected, protected, monitored, and operational over time.

The technology becomes part of an ongoing service, one that can evolve as the business grows and its needs change.

The lesson from France goes far beyond cybersecurity

When most people hear the word cyberattack, they think about stolen passwords, ransomware, compromised accounts, or customer data being exposed. Those are serious problems, but the attacks in France illustrate something that deserves equal attention.

Today, software and networks increasingly control physical equipment. Refrigeration systems, heating and cooling, industrial machinery, building systems, and other essential infrastructure are connected in ways that make them easier to operate and manage.

That also means a cyberattack doesn't have to steal a single customer record to create devastating consequences. It can interrupt production, damage equipment, destroy inventory, or prevent a business from operating normally.

The financial implications can be especially complicated. [Reuters reported on October 15](#) that physical inventory losses associated with the French attacks may not be covered by conventional cyber insurance policies. Coverage varies by contract, but the exposure is real. Imagine dealing with destroyed inventory, disrupted operations, and damaged equipment, only to discover that the insurance protection you expected may not apply.

This is why I believe cybersecurity and operational monitoring should be considered together. One is focused on protecting access to systems and preventing unauthorized activity. The other helps us understand the physical conditions those systems are responsible for maintaining.

Neither replaces the other.

We cannot say that SecureConnect and VigiLynx would certainly have prevented the French attacks or saved a particular store's inventory. The result of any deployment depends on the attack path, the installed equipment, the configuration of the monitoring system, and how quickly people respond.

But we can say that a business with properly designed security controls, independent physical monitoring, and reliable notification paths has more opportunities to recognize and address developing problems.

A business should have more than one opportunity to notice trouble before the only remaining task is calculating the loss.

That, to me, is the real lesson of what happened in France.

Don't wait for the five in the morning phone call

I keep thinking about that supermarket director in Normandy.

His employees arrived expecting another ordinary day. Instead, they were dealing with damaged equipment, spoiled inventory, and the difficult process of recovering from something they never expected to happen.

More than \$100,000 worth of food was lost. But the consequences weren't limited to inventory. There were employees trying to respond, customers who depended on the store, suppliers, technicians, and an entire business operation suddenly interrupted.

And I keep coming back to the same question that started this article.

What if they had known sooner?

We can't promise that an earlier warning would have saved everything. Sometimes equipment fails quickly, and sometimes the damage happens before anyone can intervene. But there is an enormous difference between being aware that something is going wrong and discovering the consequences hours later.

That's ultimately what we're trying to accomplish with Veeva SecureConnect and VigiLynx.

We're not simply connecting devices, securing networks, or installing sensors and cameras. We're helping businesses understand what's happening within their operations, recognize conditions that require attention, and give people a better opportunity to act.

You don't need to become an expert in cybersecurity, edge computing, or wireless technology to understand the value. You only need to know what matters to your business and what it would cost you to lose it. Maybe that's a refrigerator full of inventory. Maybe it's a pharmacy's medication storage, a restaurant's walk-in freezer, a warehouse, or an important piece of equipment. Whatever it is, the question is the same:

If something started going wrong inside your business tonight, would you know before you opened the doors tomorrow morning?

*Put us
to the test.*

Here's my challenge: Show us what your business can't afford to lose. Give us the opportunity to demonstrate how we'd protect and monitor it.

Bring us one real problem, one critical asset, or one location. We'll walk through the risks with you, identify what needs to be measured and protected, and demonstrate how Veeva's security, independent sensors, cameras, and connectivity can work together in a properly configured solution.

We'll put the technology in front of you and show you what it does. Where your particular use case needs a different sensor, additional integration, or a deployment step that has not yet been validated, we'll say so. A real demonstration should prove the capability, not ask you to imagine it.

Don't just take our word for it. Put us to the test.

Because the goal isn't to sell you a collection of devices you don't understand. It's to show you something that makes you say, "Why haven't we been doing this already?"

Know what's happening. Protect what matters.

Explore [SecureConnect](#) and [VigiLynx](#) or contact Veeva or an authorized provider to request a demonstration.



Intelligently Connected™



Veeva Inc. 164 E 83rd Street | New York, NY, 10028

sales@veeva.com

© 2018 - 2026 Veeva Inc. All Rights Reserved. Specifications subject to change without notice.
Veeva and VeevaHub are trademarks of Veeva Inc. All other trademarks and tradenames are the property of their respective owners.