KPMG

Europe at a crossroads

A resilience strategy without contextual knowledge doesn't make sense

Kees Dekker

February 2026

A resilience strategy without contextual knowledge doesn't make sense

Even a non-functioning label printer can undermine whole operations" Kees Dekker, CFO Royal Koopmans

Kees Dekker is the CFO of Royal Koopmans, a Dutch company with a rich history dating back to 1846, specialising in the processing of grain into flour and related products. The company began as a buckwheat mill founded by Uilke Klazes Koopmans and has since grown into a modern producer of flour, finely ground grain, food coatings, and other ingredients for professional bakers and the wider food industry.

It is still a family-owned business and was granted the Royal designation in 1976. After selling its consumer baking mixes every Dutchmen knows from 'oliebollen' and pancakes in 2000, Koopmans shifted its focus entirely to B2B operations, emphasising sustainability, locally sourced grains (Nedertarwe), and continuous technological modernisation of its production facilities in Leeuwarden. Kees Dekker shares practical advice on the resilience strategy. "Even a non-functioning label printer can undermine whole operations."

When is cyber resilience vital for you as a board member? When discussing the topic, it's easy to imagine the topic for high-tech companies or critical infrastructure giants. Yet, the reality is far broader. Even organisations that might not see themselves as prime cyber targets are, in fact, vital links in national and international supply chains. Their resilience or lack thereof can have ripple effects far beyond their own premises. Dekker knows that all too well and points out how the NIS2 directive, a European regulation aimed at improving resilience, has accelerated his thinking.

"The introduction of the NIS2 directive was a turning point. NIS2 didn't set our entire agenda, but it did push cyber resilience higher up the priority list. The directive introduced a compliance imperative: resilience wasn't just good business sense; it was a legal requirement. This external pressure proved to be a catalyst. It gave us the nudge we needed. Without it, I doubt we'd have been able to justify bringing in a team to help us with readiness assessments and all the steps that followed."

Can you elaborate a bit on why it is important for Royal Koopmans?

"We operate two factories on a single site, with limited storage capacity and a just-in-time supply chain. It means the operations are vulnerable in case of disturbance. In fact, we don't only need to warrant just-in-time processes, but we also need to keep the concept of just-in-case top of mind. If something goes wrong, an explosion, a fire, a cyberattack, the factory stops, and we have an immediate problem. Some risks are visible and tangible, like a compressor fire. Others less so. With IT, you can't see or smell the problem, but the impact is just as real. If the ERP system goes down, the whole production process can grind to a halt. Even something as minor as a label printer malfunction can stop trucks from leaving the site, causing a cascade of delays."

Sounds logical. How do you translate this into complying with NIS2 in an approach that goes beyond checking the box exercises?

Viewpoint
Koos Wolters

Context makes resilience work

Cyber resilience is only effective when it aligns with the specific dynamics of an organisation. Regulatory frameworks like NIS2 show that resilience is not one-size fits all: requirements differ by sector, criticality, dependencies, and governance responsibilities. Without contextual knowledge, of critical services, IT OT interdependencies, threat exposure, third party reliance, and organisational decision-making structures, resilience efforts remain abstract and risk-based measures cannot be effectively prioritised.

When resilience strategies are determined by these concrete circumstances, organisations can design targeted controls, meet regulatory expectations, and prepare for disruption in a way that reflects how their business really works. Context transforms resilience from compliance into capability: it ensures incident response timelines are realistic, controls are targeted, governance is accountable, and investments go where disruption would truly hurt. This approach enables resilience efforts that are practical, proportionate, and capable of withstanding real-world threats.

"The NIS2 framework, while less prescriptive than some earlier other regulations, provided enough structure to drive action without stifling practical adaptation. But it is vital to have an approach where you use contextual knowledge, with understanding of your business dynamics. Practical experiences also help. In recent past, we have been indirectly affected by a ransomware attack on a key logistics partner. This transporter was hit hard. While their systems were offline the wheels of their trucks kept turning due to paper-based workarounds, but it was a stark reminder of how much we are depending on our partners. It took a year to get rid of the administrative headaches caused by this. These experiences have shaped a pragmatic approach to resilience. We realised that it's not just about preventing incidents, but foremost about how quickly we can resume operations when something does go wrong."

These experiences also help to get the resilience plan beyond the proverbial paper tiger?

"Indeed. We didn't want a paper tiger, a plan that looks good on the shelf but doesn't work in practice. Therefore, we involved key process owners from across the business in its creation, ensuring the plan reflected real operational realities. One of the most tangible steps was establishing agreements with competitors to ensure supply continuity in case of a major disruption. If our factory goes down, we have arrangements to source from competitors so we can keep serving our customers. It sounds simple, but it's critical. If you can't deliver, your customers will find alternatives, and your business could be finished. The plan also identifies specific scenarios, such as cyberattacks, explosions, supply chain failures, including rare but high-impact scenarios such as the Elfstedentocht, a major national ice-skating event that can disrupt logistics, and outlines clear actions for each.

Sounds like you are ready for any scenario?

"Our crisis team is ready to mobilise, and responsibilities are clearly defined. We've learned that you need to plan for the unthinkable, and you need to make sure everyone knows their role when it happens. Testing and maintaining the plan is just as important as writing it. We make sure the plan is physically available, not just on a server that might be inaccessible during an incident. We also have someone from our Continuous Improvement team responsible for ensuring we actually use the plan during a crisis, instead of just improvising."

How do you ensure that the whole organisation is aware?

"Technology and process are only part of the equation to become resilient and human error is often the weakest link. Internal communication is key. We use a tool that send weekly challenges to everyone, creating a bit of competition and making security awareness part of the culture. It's not the most exciting topic, but we try to make it engaging."

Do you have a final word of advice to peers?

'Perhaps the most important lesson is the need for context. A resilience plan has to fit your business. You can't just copy a cybersecurity specialist's template and expect it to work. We made sure the people who know our processes best were the ones writing the plan, with external advisors facilitating rather than dictating.'

Viewpoint
Meret Keeris

The relevance of contextual knowledge for cyber resilience

It's always a great pleasure to work for companies with a very tangible product. In the case of Royal Koopmans, we discovered while talking about the great Nedertarwe-initiative, that the local bakery our family buys bread is one of Koopmans' clients. This brings the topic of resilience very close to home: if Koopmans fails to get their product to the local bakeries, there's no bread available when I'm at the bakery on Saturday morning. Koopmans is a very practical organisation and challenged us rightfully to make things as practical as possible. So, I totally agree with Kees' remark about making sure resilience processes are not paper tigers: it's very important to have a practical approach to resilience and people know what to do in case of an issue. On the other hand, with NIS2, showing and proving resilience is sufficiently addressed is important too. Especially for internal and external stakeholders and the public.