

RESILIENT COMPANIES BUILD A RESILIENT SOCIETY

06/2026



RESILIENCE CENTER DENMARK

CONTENT

RESILIENT COMPANIES BUILD A RESILIENT SOCIETY	3
EXECUTIVE SUMMARY	3
A NEW REALITY AND A NEW OPPORTUNITY	4
RESILIENCE AS A DRIVER OF INNOVATION AND COMPETITIVENESS	5
WHAT MIGHT THIS LOOK LIKE IN A DANISH CONTEXT?	6
WHAT ACCELERATION REQUIRES	7
WHERE CAN A DANISH COMPANY START TODAY?	8
AN INVITATION TO COLLABORATION AND DIALOGUE	9

About the publisher: This white paper is published by Resilience Center Denmark¹, a national collaboration between the seven existing Danish GTS institutes². The GTS system has a statutory mandate to support Danish companies, especially SMEs, through technological advisory services, testing, and applied research. The paper is written from an expert technological perspective on how resilience, as a strategic direction, can be applied in practice while strengthening Danish competitiveness. It contains practical observations that can strengthen Danish companies and whole-of-society preparedness across industries and sectors, as well as proposals for what individual companies can do to contribute in the short term. This white paper is intended for Danish companies, especially SMEs, as well as industry associations and authorities working with resilience and whole-of-society preparedness.

Jasmin Skøtt, Troels Behrenthz Andersen, Thuvarakai Kandasamy, Jorge Ivan Contreras-Cardeno, Luis Campos Roman & Lone Borg

Translation note: This English version of the June 2026 white paper was AI-assisted and reviewed by co-author Jorge Ivan Contreras-Cardeno for terminology and clarity.

¹ Read more about the Resilience Center Denmark at this [link](#).

² Read more about the RTO institutes from Denmark (Called GTS in Danish) in this [link](#).

RESILIENT COMPANIES BUILD A RESILIENT SOCIETY

How Danish companies can navigate a new geopolitical reality, and how technical expertise and Resilience Center Denmark can accelerate the development of resilient business and society.

EXECUTIVE SUMMARY

The new geopolitical reality - war in Europe, hybrid attacks, disrupted supply chains, and climate extremes - has made resilience a competitive parameter on a par with efficiency. Customers, insurers, and authorities increasingly demand documented ability to deliver under pressure, and with the EU's Preparedness Union Strategy, published in March 2025, a European market for tested resilience solutions has emerged. Danish companies are strongly positioned, but the necessary solutions do not yet exist as finished products. They must be developed, tested, and validated at a pace that keeps pace with the threat landscape. This requires four things: research translated more quickly into practice; development across sectors; test environments under realistic conditions; and independent validation. The technical expertise and capacity already exist in Denmark, within the Danish GTS institutes and across the field of resilience and are gathered at Resilience Center Denmark. This white paper describes how that capacity can be put to work and where individual companies can begin today.

A NEW REALITY AND A NEW OPPORTUNITY

The globalised economy's long period of stable value chains is over. War on the European continent, hybrid attacks against NATO, subsea cables cut in the Baltic Sea, cyberattacks against critical infrastructure, climate extremes, and a trade order being reshaped together constitute the most serious threat landscape in decades. This is the reality behind the Danish government's decision to establish integrated whole-of-society preparedness. The decision rests on the recognition that societal resilience cannot be delivered by authorities alone. It requires Danish companies, large and small, to contribute the capacities that make the difference in a crisis.

But companies are not only being asked to contribute. The same conditions that create the need are also changing the business logic. As the surrounding world grows more unstable, the ability to continue delivering under pressure is becoming part of what customers and financial actors are willing to pay for. Efficiency alone no longer captures the full picture of competitiveness. Capacity, redundancy, documented continuity, and the ability to deliver under pressure are becoming standalone parameters in the assessments made by customers, insurers, banks, and authorities. NHO's³ Report: *The Road to Growth*⁴ states that, in the new geopolitical reality, security and preparedness are fundamental prerequisites for competitiveness, not additional costs. In other words, a new business field has emerged.

Denmark's business structure has a good start in this field. The close connection between large global companies and a broad, specialised SME base is exactly what a modern resilience effort requires, and it is precisely the structure that enables rapid transition. For smaller companies, size is a double-edged sword. They have fewer buffers, but they are fast, flexible, and close to operations. With the right framework, agility becomes what makes them winners.

From this perspective, resilience is a strategic discipline, not merely a matter of an emergency management planning document. A company that maps its dependencies often identifies new suppliers, new markets, and new products. A company that takes data security seriously earns the trust of customers and other stakeholders who increasingly demand documented resilience. A company that trains its organisation through scenarios discovers bottlenecks that would otherwise surface during a busy period. Business interests and corporate social responsibility point in the same direction.

For many companies, and for entire industries, the situation is also an opportunity to rethink themselves. Working with resilience is a strategic review of the business: an opportunity to step back and examine how value and resilience are actually created in a new world. In recent decades, business has moved at a pace where growth has absorbed most attention, leaving little time for this kind of review. But right now, when the framework has to be reconsidered in any case, there is a clear opportunity to pause and identify new, and perhaps better, ways of doing things.

³ NHO stands for Næringslivets Hovedorganisasjon, which translates to the Confederation of Norwegian Enterprises. It is Norway's largest employers' and business organization.

⁴ Find NHO's report "The Road to Growth – What Now Norway?" in this [link](#).

RESILIENCE AS A DRIVER OF INNOVATION AND COMPETITIVENESS

When the full breadth of Danish business is to be included, it is not enough for each company to see the advantage. The framework must be designed to strengthen societal resilience while opening business opportunities for companies: new products and services in response to growing demand for resilience; new market access for companies that document capacity; and export potential in a situation where all EU countries face the same requirements. With the EU's *new Preparedness Union Strategy*⁵, preparedness and resilience have, for the first time, become a consolidated political agenda alongside competitiveness and the green transition. This opens a European market for Danish resilience solutions that have been tested and documented nationally. We do not have to start from scratch. Our Nordic neighbours have worked with whole-of-society preparedness for decades, and although it is not our role as a technical body to determine which model Denmark should choose, we can uncover recurring patterns.

What can we learn from the Nordic countries?

Finland, Norway, and Sweden have chosen different paths to whole-of-society preparedness. Finland has a collaborative model in which the state, business, and civil society address the task together through established networks. Norway builds on a combination of functional preparedness and shared values such as trust and local community. Sweden has chosen a more centrally governed model with close links between civil and military preparedness. Across all three, the same basic principle applies: those responsible for a function in normal times remain responsible when that function is put to the test⁶.

Two points stand out. First, Danish business and civil society have historically engaged through associations, not directly through the state⁷. This means that industry associations are the natural channel to the full breadth of business, especially to small and medium-sized enterprises. Second, models that last over time rest on an independent technical body that validates methods, performs measurements, and provides documentation.

The invisible infrastructure of trust

The second point mentioned deserves attention because it is the part of resilience that often slips under the radar. In everyday life, we take a remarkable amount of trust for granted: that the fire alarm activates at the right thresholds; that medical equipment delivers the precise dose; that water quality is measured correctly. No one thinks about it, and that is exactly the point. Every day, trust works because it rests on an invisible network of measurement bodies, test facilities, standards, and controls. That network is part of what the GTS system maintains every day, in companies and laboratories. It is the technological infrastructure of trust.

This capacity becomes critical in whole-of-society preparedness. At a time of increasing digitalisation, complex global supply chains, and hybrid threats, the ability to say with technical authority, "we have tested it, we have measured it, and we can stand behind it," is the prerequisite for companies, authorities, and citizens to act quickly and in coordination during a crisis. If the technical foundation is solid, the rest of the system can be built faster. If it is not, even the best models become paperwork. This network already exists in Denmark, and Resilience Center Denmark has gathered it across the field of resilience.

That is the resource we want to bring into play.

⁵ Find the EU's preparedness union strategy at this [link](#).

⁶ Find access to the article at the following [link](#).

⁷ This draws on Nordic resilience research on whole-of-society approaches, including Björnsson and Dahlberg (2025), who point out that models must be translated into a national context rather than transplanted.

WHAT MIGHT THIS LOOK LIKE IN A DANISH CONTEXT?

The following examples show how such an approach can unfold in practice.

Drinking water supply as an example. Denmark has around 2,500 waterworks, the vast majority of which are small or medium-sized. The sector is critical infrastructure and subject to both NIS2⁸ and CER⁹, which impose stricter requirements for continuity, physical security, and documentation. But what actually happens if the control system of a local waterworks is hit by a cyberattack, or if a main connection is interrupted? For an individual waterworks, building an internal emergency response organisation capable of answering that question is unrealistic. By contrast, it is realistic for the sector, together with technical actors, to develop practical solutions. These may include hydraulic models that simulate how a supply network reacts during attacks or outages. They may include sensor-based monitoring systems that detect abnormal patterns in real time. They may also include tested emergency procedures for the most likely scenarios and a qualification scheme through which small waterworks can document compliance with NIS2 and CER without having to build a compliance function from scratch. This increases the capacity of the Danish sector and, at the same time, provides Danish water technology companies with an exportable product. The Danish water sector already has a strong international position, and a resilient water supply under increasing climate and security pressures is exactly what the European market demands.

IT and cloud providers, as an example. The Danish market has a broad ecosystem of specialised IT and cloud providers serving both larger private customers and the public sector. NIS2 directly requires documented resilience from a large part of the segment, while CER affects the largest designated actors in digital infrastructure. But the real pressure is increasingly coming from supply chains. Large customers in regulated sectors such as energy, finance, healthcare, and transport are beginning to place requirements on their IT and cloud providers because they themselves need to document continuity across the entire chain. For a smaller Danish provider, this means resilience becomes a market-entry requirement for the largest customers, regardless of whether the company itself is directly subject to the directives. But how does a smaller Danish cloud provider actually document that it can continue operating during an advanced cyberattack, or that its data centers can maintain operations during a prolonged power outage? For an individual SME provider, it is unrealistic to build the internal compliance and testing capacity needed to answer that question. By contrast, it is realistic for the industry, together with technical actors, to develop practical solutions: tested reference architectures for secure operations; independent penetration and continuity testing; sector-specific threat monitoring adapted to SMEs; and a multi-Tier qualification scheme through which a provider can document resilience at a recognised level. This opens the door to public tenders, to larger customers with supplier requirements, and to the European market, where smaller cloud and IT providers face exactly the same challenge as their Danish counterparts.

Cross-cutting dependencies as an example. The previous examples have one thing in common: no sector fails in isolation. A water utility, a data center, and a cold chain each depend on stable power, digital control systems, and the functioning of the others. A prolonged power outage affects not only the energy sector but also drinking water, data centers, and food production, and the effects reinforce each

⁸ NIS2 (Network and Information Security Directive 2), the EU directive on a high common level of cybersecurity in network and information systems.

⁹ CER (Critical Entities Resilience Directive), the EU directive on the resilience of critical entities.

other across sectors. But while each sector has strong specialists in its own field, no one naturally bears responsibility for their interaction. The energy sector tests energy supply, the water sector tests water supply, and the IT sector tests IT. The cascade effect that emerges between them falls through the cracks. This is not something one sector can or should solve alone, because it requires an impartial actor outside the interests of the individual sectors, able to connect them around common scenarios, test processes, and a shared data foundation. That is precisely the role Resilience Center Denmark can fulfill: not as another specialist in one sector, but as the neutral place where cross-sector dependencies can be modeled, tested, and documented as a whole. At the same time, this creates a market for resilience providers delivering models, testing, and monitoring, because their services can be independently validated and recognised across sectors rather than having to be validated anew in each industry.

WHAT ACCELERATION REQUIRES

The solutions we have outlined for the water and IT sectors, as well as cross-sector dependencies, do not yet exist as fully developed off-the-shelf products. They must be developed, tested, and matured, and this must happen at a pace that matches the threat landscape. This places specific demands on the technical infrastructure supporting companies.

First, research must be translated more quickly into practice. Universities and research institutes are currently producing new knowledge about cyber threats, hybrid attacks, climate resilience, materials, sensor technology, and critical infrastructure. That knowledge is often not immediately ready for business use. It must be translated, adapted, and tested before it becomes a solution that a company can apply. This is precisely one of the tasks the GTS institutes were established to solve. They are where existing knowledge is synthesised with practical capacity that works.

Second, development must take place in collaboration, not in isolation. Resilient drinking water, secure cloud services, or documented continuity in a supply chain are not things that a single company can solve alone. The technical questions cut across sectors, and solutions are best developed when industry associations, companies, research institutes, and authorities work together in specific projects with shared test facilities and a shared data foundation. This kind of collaboration is not new, but the scale must increase if the pace is to keep up. This is precisely where Resilience Center Denmark can play a role as the facilitator that connects sectors, disciplines, and institutions around shared test facilities and a shared data foundation.

Third, there must be places where new solutions can be tested under realistic conditions before they are deployed. This applies whether the solution is a new sensor-based monitoring method for a waterworks or a new reference architecture for a cloud provider. Without test environments that can validate performance under pressure, solutions become either too cautious or too risky. Both are barriers to putting new resilience capacity to work across Danish business.

Fourth, validation must be independent. When a company says, "We are resilient," this must be documented by someone who has not sold the solution themselves. This is the role the GTS system already plays across a wide range of areas, and it is the role that will be decisive when resilience must be demonstrated in the European market.

The four prerequisites are interconnected. Research translated into practice, collaboration across sectors, test facilities under realistic conditions, and independent validation form the technical foundation. This already exists in Denmark, brought together across the resilience field by Resilience Center Denmark. The question is therefore not whether the capacity exists. It is whether we put it to work at the pace reality demands.

WHERE CAN A DANISH COMPANY START TODAY?

This development takes time, both the technical maturation and the collaboration among industries, companies, and research that are required. But companies do not have to wait for everything to be in place. Just as on an aircraft, where you put on your own oxygen mask before helping others, each company can usefully begin with itself. Resilience is not a project that gets completed. It is a continuing practice, effort, and discipline that the company builds and maintains over time because the threat landscape never stands still.

Here are three steps every company can take today:

- **Map the five critical dependencies in your value chain.** This is not a full risk assessment, but a simple consideration: what five things does the company rely on most in order to deliver next week? Energy, a specific supplier, an IT platform, a key person, a transport route? For each one, ask: what happens if it fails for 24 hours, one week, or one month? The review can be completed in one day and often uncovers three or four things that surprise management. The solutions generated are often innovative and can sometimes be initiated immediately, without a crisis necessarily being underway.
- **Run one scenario exercise per year and train your resilience muscle.** Not another preparedness document, but an exercise. A few hours in which the full management team jointly works through a realistic scenario, such as a 48-hour power outage, ransomware in the ERP system, bankruptcy of the main supplier, or a crisis affecting the largest customer, using a simple structure: what do we do in the first hour, the first day, and the first week? Learning lies in the exercise itself.
- **Join at least one network that strengthens your resilience over the long term.** Industry association network groups, the Business Forum for Societal Security and Preparedness, the Confederation of Danish Industry's preparedness reference group, Falck's Corporate Emergency Response Team, the Danish Home Guard's Infrastructure Home Guard, and InterForce's supporting business scheme are different entry points depending on the type of company. The actual capacity to handle an incident lies in relationships, and they cannot be established overnight when a crisis hits. Resilience Center Denmark also runs a network group as part of its work, and companies and other actors are welcome to participate.

These steps are not dramatic, and they do not cost much. But they set in motion the continuing discipline that enables the company to be resilient regardless of what the future brings, while also opening a strategic dialogue about building resilience.

AN INVITATION TO COLLABORATION AND DIALOGUE

Denmark is at a historic moment for its societal resilience and whole-of-society preparedness. The political momentum is there. Resources are beginning to arrive. The institutional framework is being built. The next task is to translate the framework into operational practice that includes the entire breadth of Danish business.

This is a task that no actor can solve alone. It requires collaboration among authorities, industry associations, companies, and an independent technical capacity that can translate research, requirements, and experience into methods, tools, and standards that the entire business community can use.

For the individual company, this landscape is currently fragmented and difficult to navigate. New directives, new requirements, new initiatives, and new actors create noise, and that noise costs time, especially for smaller companies that lack a compliance function to lean on. Resilience Center Denmark is the joint response of the seven GTS institutes to this challenge. Resilience is an interdisciplinary discipline that draws on competencies from across the GTS system, from testing materials and products to cybersecurity, supply chains, standards, and certification. We have gathered these competencies in one place so that companies, industry associations, and authorities have a cross-cutting entry point to the combined technical capacity when it comes to resilience. Resilience Center Denmark can coordinate work in this field, and assignments are carried out in collaboration with the institute or institutes that have the relevant technical expertise. The ambition is to create a platform where research, testing, modeling, and technology development can work together on cross-sector resilience. This connection is a natural fit for the GTS institutes, which already act as a bridge among sectors, companies, and research, and therefore already possess the necessary bridging capabilities.

We invite SMEs, large companies, authorities, and industry associations to work with us on concrete issues. Those issues may concern sector-specific challenges that need shared solutions. They may concern testing and documentation of new products and services. They may concern translating research and international experience into Danish conditions. Right now, we are further defining the specific initiatives, and the dialogue is open.



RESILIENCE CENTER DENMARK