Acronis

WHITE PAPER

Why European manufacturers need an enterprise resilience plan

Reduce downtime, strengthen NIS 2 readiness and improve cyber insurance eligibility

Executive summary

European manufacturers face a confluence of challenges:

Unplanned downtime is one of the most significant threats to manufacturing performance across the continent.

The continually evolving NIS 2 Directive has elevated business continuity and disaster recovery to an executive level of accountability.

At the same time, cyber insurers are demanding stronger proof of resilience before granting policies.

The challenge is that those pressures are no longer separate. A single cybersecurity incident or disaster now directly impacts operations, compliance and financial recovery. In response, manufacturers must move beyond fragmented backup strategies for their operational technology (OT) environments and adopt a true enterprise resilience plan focused on recoverable production.

The leadership challenge: One incident, three impacts

Many organizations still manage backup, compliance and insurance separately. In theory, they converge during an incident. But what happens when they don't?

If a manufacturer can't restore production in a controlled and documented way, it faces three immediate consequences:

- Production disruption and missed delivery commitments.
- Regulatory exposure under NIS 2.
- Increased risk of disputed or reduced insurance claims.

A weak recovery posture therefore creates a compounded business risk, not just a technical issue.

Copyright © 2003–2026 Acronis International GmbH.

European threat landscape and regional insights

Cyber incidents are already disrupting manufacturing operations across Europe, with ransomware remaining the primary threat to industrial environments. European manufacturers face converging risks. Ransomware gangs are targeting the manufacturing sector, increasing the number of serious incidents and expanding vulnerability exposure. At the same time, many small and medium-size enterprises (SMEs), including manufacturers, do not have mature cybersecurity strategies and are therefore vulnerable to attack. Industry 4.0-driven initiatives have also expanded the attack surface in OT environments, and many manufacturers haven't taken adequate measures to protect their data.

Recovering from a cyberattack is expensive. Globally, the average data breach in an industrial environment cost $5.0 million in 2025, according to IBM.[1] As ransomware and other attacks rise in number and severity across Europe, manufacturers, like other SMEs, need to develop an effective strategy for protection and recovery. Numbers suggest that the situation is getting worse, not better.

For instance:

Europe: According to the ENISA Threat Landscape 2025 report, nearly 15% of ransomware attacks analyzed in the report were aimed at manufacturing, which was the fifth-most targeted sector out of nearly 20 studied in the report.[2]

United Kingdom: The U.K. National Cyber Security Centre (NCSC) reports that manufacturing is among the sectors most frequently targeted by ransomware.[3]

Germany: Any.run reported in 2026 that because German manufacturers had integrated Industry 4.0 technologies, IoT sensors, operational OT and cloud-integrated production systems, attacks extended beyond data loss to cause potential operational shutdown, physical equipment damage and supply chain disruption. Since staff members on the plant floor were rarely tried in cybersecurity, social engineering attacks were particularly effective.[4]

France: The French cybersecurity agency (ANSSI) said in a 2026 report that French manufacturers had become major targets for both state-sponsored disruptions and ransomware attacks. The report specified that smaller manufacturers were particularly vulnerable to digital sabotage.[5]

Italy: A Telecom Italia cybersecurity report found in 2025 that Italian manufacturing companies were the target of roughly 26% of ransomware attacks in the country from 2022–2024.[6]

Nordic countries: Mordor Intelligence reports that Industry 4.0 programs that expand OT attack surfaces are driving investment in cybersecurity solutions in Nordic countries at an impressive combined annual growth rate (CAGR) of more than 8% per year. Manufacturers are responding to risks by converging IT and OT defenses.[7]

While OT-specific statistics remain limited, available national data highlights a broader escalation of cyber risk across manufacturing environments, including industrial systems and SMEs.

[1] IBM, Cost of a Data Breach Report 2025: The AI Oversight Gap, research conducted by Ponemon Institute, published 2025, based on analysis of 600 organizations across 16 countries between March 2024 and February 2025.

[2] ENISA Threat Landscape 2025, version 1.2, European Union Agency for Cybersecurity, January 2026.

[3] National Cyber Security Centre. (2024). NCSC annual review 2024. GCHQ.

[4] ANY.RUN. (April 1, 2026). Major cyberattacks in March 2026: OAuth phishing, SVG smuggling, Magecart, and more.

[5] Agence nationale de la sécurité des systèmes d'information. (March 11, 2026). Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002). ANSSI.

[6] Telecom Italia (TIM), & Cyber Security Foundation. (2025, June 12). Cyber security report 2025. TIM Group.

[7] Mordor Intelligence, Nordics cybersecurity market size and share analysis: growth trends and forecasts (2026–2031), estimating market size at $14.92 billion in 2026 growing to $22.25 billion by 2031 (8.36% CAGR), published 2026.

Copyright © 2003-2026 Acronis International GmbH.

Real-world cyberattacks on manufacturing in Europe

Across Europe, cyber incidents in OT environments are no longer isolated IT events. They are production events that can severely disrupt operations and lead to extended downtime. Recent examples include:

- **Jaguar Land Rover:** A now infamous 2025 cyberattack on Jaguar Land Rover disrupted U.K. production for several weeks at a cost of at least £50 million per week,[8] according to estimates, and leading to job losses. The attack demonstrated how enterprise IT disruption can directly impact factory operations.
- **Volkswagen Group France:** In October 2025, Volkswagen Group France suffered an attack by the Qilin ransomware group that led to the exfiltration of about 2,000 files and 150GB of sensitive data.[9]
- **Dodd Group:** In 2025, U.K. defense contractor the Dodd Group suffered a cyberattack that led to a leak of sensitive U.K. Ministry of Defense files with information on air force and navy bases.[10]

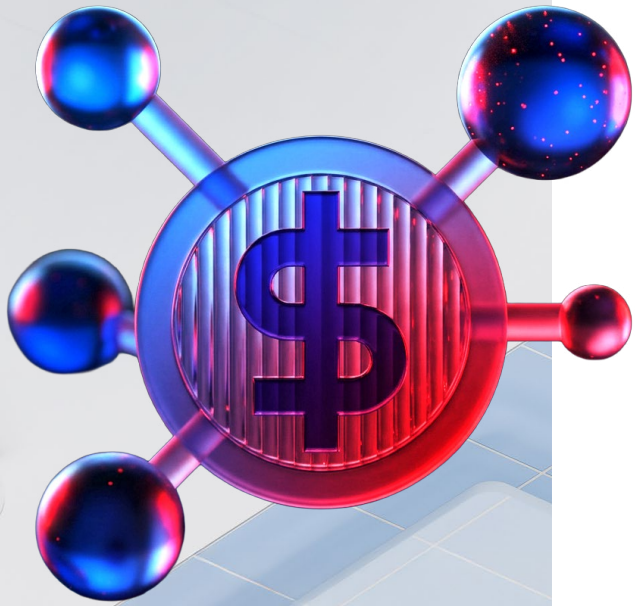
What NIS 2 requires in practice

Compliance remains a major issue in OT environments, where potential financial penalties can compound the cost of unplanned downtime. NIS 2 introduces a fundamental shift from prevention to demonstrable resilience.

Under Article 21, organizations must be able to prove that they can continue operations and recover effectively. This includes:

- Business continuity and disaster recovery planning.
- Backup management aligned to operational needs.
- Crisis management and governance structures.

The critical change is accountability: organizations must demonstrate that recovery works in practice, not just on paper. So, recovery capability is now a compliance requirement, not a mere operational preference.



[8] BBC News, Jaguar Land Rover cyber-attack disrupts production and supply chain, published September 2025.

[9] Cybernews. (October 16, 2025). Volkswagen France hit by ransomware, Qilin gang claims.

[10] Security Affairs. (October 20, 2025). Russian Lynk group leaks sensitive U.K. MoD files, including info on eight military bases.

Copyright © 2003–2026 Acronis International GmbH.

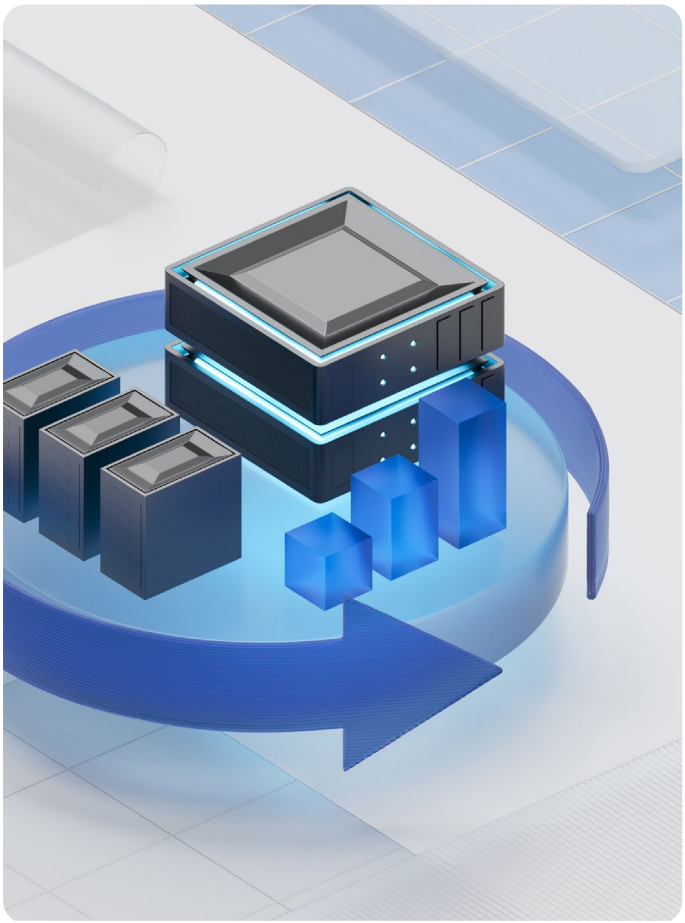
Why OT recovery is different

OT environments introduce complexities that traditional IT recovery approaches do not fully address, including legacy systems, tightly coupled production processes and strict restart conditions that make recovery sequencing critical.

As a result, resilience in manufacturing depends on restoring production capability, not just systems or data.

From backup to enterprise resilience

An enterprise resilience plan involves much more than just backup — it connects operational continuity, compliance and recovery into a single framework.



At a minimum, organizations should establish:

- Clear governance across sites and functions.
- OT-aware recovery capabilities.
- Regular validation of recovery processes.

The objective is not simply data recovery but ensuring that manufacturers can rapidly restore production in a controlled and predictable way.

Cyber insurance and defensibility

Cyber insurance providers are increasing scrutiny on manufacturing organizations, particularly around business interruption risk. Claims outcomes are increasingly influenced by an organization's ability to demonstrate preparedness and recovery execution.

Key expectations now include:

- Evidence of defined continuity and recovery processes.
- Documented recovery timelines and actions.
- Alignment between policy commitments and operational capability.

Without those elements, organizations risk entering a claims gray zone where coverage may be reduced or contested.

What manufacturing leaders should do next

Manufacturers must address resilience as a business priority rather than a technical project.

Leaders should focus on three immediate actions:

- Understand critical production dependencies and recovery risks.
- Align continuity planning with NIS 2 expectations.
- Establish a structured enterprise resilience plan.

This shift enables organizations to reduce downtime risk while strengthening both compliance and financial protection.

Copyright © 2003–2026 Acronis International GmbH.

How Acronis supports OT resilience

With Acronis Cyber Protect for OT, systems can be restored with a single action, without requiring deep IT expertise. In air-gapped environments in particular, One-Click Recovery is an essential capability. Manufacturers can minimize downtime and maximize speed of recovery without intervention or disruptions.

Acronis Cyber Protect for OT enables manufacturers to strengthen resilience across complex environments. It supports organizations in meeting the confluence of challenges:

- Protecting critical systems from unwanted downtime.
- Validating recovery processes and other elements essential for compliance.
- Generating the evidence required for cyber insurance.

A component of the natively integrated Acronis Cyber Platform, which combines multiple cybersecurity functions into a single console and point of management, Acronis Cyber Protect for OT enables manufacturers to achieve improved uptime and reduce unwanted downtime, as well as enjoy faster recovery times and stronger alignment between operational resilience and business risk management.

LEARN MORE

Acronis

Learn more at acronis.com

Copyright © 2003-2026 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2026-05