



.AGORIA



Cybersecurity in Operational Technology - State of Belgian industry in 2026

Cyber Made in Belgium

September 2026

Table of contents

1. Foreword	3
2. Key takeaways	4
3. Why OT cybersecurity matters now?	5
3.1 The factory is connected	5
3.2 Attackers and regulators arrive at the same time	6
3.3 The same picture worldwide	7
4. Key survey findings	8
4.1 OT environment and exposure	8
4.2. Governance, culture and policies	11
4.3. Regulatory readiness	15
4.4. Resilience in practice	19
5. The leading pack	23
5.1 Are budget, size or region differentiators?	23
5.2 Leaders finish where the others start	23
5.3 Leaders can see what happens on the OT network	24
5.4 Leaders govern OT explicitly and use the industrial standard	24
5.5 Ability to recover is the clearest differentiator	25
Ten insights from the OT leaders	26
6. Evolution over the last 5 years	27
6.1 The six common KPIs that moved	27
6.2 The new catalyst that improved the OT resilience	28
6.3 Where the progress is factual	28
6.4 Where the progress is less addressed	29
7. Conclusion	30
8. Acknowledgment	31
9. Methodology	33
References	35
Sponsors	36
About the authors	38

1. Foreword

The first edition of the cybersecurity in manufacturing study was published in 2021, when cybersecurity in a factory was a question of good practice, not of compliance. **Five years later, factories are connected, attackers have understood that production is the weakest point and European regulations reach the production floor.**

We focus on manufacturing because the consequences become physical: a compromised control system can stop a line, damage equipment or put an operator in danger. **OT cybersecurity is therefore not IT cybersecurity applied to machines.**

Belgian Defence has made this a national priority. Europe is rearming, Belgian industry is taking part, and Belgium hosts NATO Headquarters and SHAPE. Being part of a defence supply chain can make a company a target for state-linked attackers.

OT Cybersecurity is becoming a requirement for doing business: prime contractors increasingly ask suppliers to prove that their factories, systems and equipment's are properly secured.

This edition is embedded in a global dynamic. The same topic appeared across the Belgian cyber ecosystem:

- CMiB4ICS/OT, the ICS and OT focus group of Cyber Made in Belgium within Agoria
- CyberActive, led by Sirris with Howest, UCLouvain and VUB
- The ICS/OT Security focus group of the Belgium's Cyber Security Coalition

What was missing is the level of cybersecurity maturity in Belgian manufacturing. This report provides key indicators about this maturity level. The study is based on 82 Belgian companies operating in OT environments.

Education is following: Howest, along with its Cyber 3 Lab OT cybersecurity research projects, offers a Bachelor including OT Cybersecurity; Belgian Defence provides Cyber Defense Factories; the inter-university Master joins ULB, UCLouvain, UNamur, HE2B and the Royal Military Academy; Hénallux trains automation and systems security. Hopefully a new generation will reach the production floor already familiar with OT.

The Network and Information Security Directive 2 (NIS2) extends its scope from 7 sectors to 18, of which 11 are new, in which 10 are closely related to the industrial world (Operational Technology). Meaning many manufacturers are facing these obligations for the first time. The Cyber Resilience Act (CRA) adds cybersecurity requirements for digital products with elements since 11 September 2026. The Machinery Regulation for machinery itself from 20 January 2027, without expected transition period.

The Centre for Cybersecurity Belgium (CCB), our national cybersecurity authority, makes them workable through its CyberFundamentals (CyFun®) framework, a proportionate way to **assess a company's cybersecurity maturity.**

The purpose of this study is to assess the current state of Belgian industry with regard to the cybersecurity of Operational Technology (OT) environments.

We thank the 82 companies that answered, our sponsors and the members of the CMiB business group.

Note that the Agoria's 10-Page guide, **"Cyber Security in Operational Technology (OT)"** (Agoria, 2026) provides leadership audiences with an overview of applicable European regulations, key OT cybersecurity risks, key counter-measures and on top some guidance on selecting the appropriate cybersecurity framework for different situations.

The 10-pager together with this document forms the program of the Agoria Cyber Business Group (Cyber made in Belgium - CMiB).

The overall picture of this study is encouraging: the difference between the best-in-class companies in OT cybersecurity and the rest is more driven by organisation than by budget, which means the gap can be closed.



Eric Van Cangh
*Senior Business Group
Leader Digital,
Agoria*

+32 492 23 24 34
Eric.vancangh@agoria.be

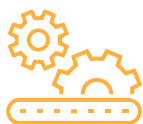


Alain Wayenberg
*Business Group Leader
Manufacturing & Process Systems,
Agoria*

Alain.wayenberg@agoria.be

2. Key takeaways

40%



of the respondents have a complete^(*) and current OT asset inventory.

The inventory is the dividing line. Companies that understand their OT environment thanks to a comprehensive inventory can protect it effectively; those that don't remain exposed, regardless of their size or budget.

19%



of the respondents have a dedicated OT CISO or equivalent.

The budget moves, but the ownership does not. Belgian industry is investing in OT cybersecurity, accountability appears to be unclear. Without a clear owner, the policy applies primarily within the IT boundaries, the training stays generic, and the budget allocations appear to lack clear strategic decisions.

20%



of the respondents combine a governance framework with IEC 62443

Manufacturers need guidance on which rules apply to them.

Belgian industry is engaging with the regulations, but many companies still do not know which ones cover them, or how to proceed. Attention goes to NIS2, where the deadline has already passed and the CCB has defined how late entities are expected to catch up, while the Cyber Resilience Act and the Machinery Regulation are still ahead, on fixed dates. The frameworks exist — CyberFundamentals or ISO 27001 for the organisation and IEC 62443 for the production floor — but only few combine them.

38%



of the respondents declare that they are confident that they would detect an attack on their OT within hours, while 34% have no technical detection capability at all.

Confidence is not verified. Belgian industry approaches OT resilience with a confidence that is not really verified - Incident Response and Business Continuity Plans are mainly limited to the IT environment, and backups and detection are not regularly tested.

88%



of the leading pack validate their OT backups through recovery testing, against 23% of the others.

The leading pack finishes what the others start.

The leading companies are not larger, better funded or better staffed than the rest. They are the ones that completed what the others started and that they can demonstrate their resilience controls are tested.

65%



of the respondents use or consider at least one cybersecurity framework, against 34% in 2021.

Five years of progress have mainly stayed within the IT boundary. Since 2021, buying practices, supplier follow-up and the use of frameworks are clearly better. Detection, testing and the way companies judge their own cyber risks have not changed.

^(*) Subject to the quality of the inventories. Asset inventories are difficult to keep complete and up to date. This note applies throughout the document

3. Why OT cybersecurity matters now?

3.1 The factory is connected

Operational Technology (OT) is the new cyber security battlefield environment.

This environment is made of hardware and software that runs physical processes: Programmable logic controllers (PLC), human-machine interfaces (HMI), supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), the wider family of industrial control systems (ICS), and the industrial internet of things (IIoT).

In the past, these systems were built during another age: they were isolated, they used their own proprietary protocol, and they were expected to run for twenty years without any change. A large part of that equipment is still on the production floor today.

What has changed is connectivity. Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) integration, predictive maintenance, energy monitoring, cloud platforms, remote support by machine builders and integrators — Most of them requires a connection between the plant and the outside world.

This is what we call IT–OT convergence. The business benefits are real, but the problem is that **the attack surface grows faster than the cybersecurity controls that surround it.**

Moreover, the attack rarely starts where one would expect it. **Most OT incidents begin in IT and then spread into the operational environment because IT and OT networks are not adequately separated** (Dragos, 2024). The entry point is IT, nevertheless the consequence is felt in OT production.

This is also why OT security is not IT security applied to machines. The order of priority is reversed around: in OT, safety and availability are more important than confidentiality. Patching may be impossible, and an active vulnerability scan could stop a PLC.



Gregorio Matias

CEO - Cybersecurity Consultant, MCG
VP CMiB4ICS/OT Focus group, Agoria

“Securing OT connected to IT requires a deep understanding of the mutual challenges that can no longer be separated nowadays.”

The good news is that nothing needs to be invented.

More specifically:

- ISO 27001 standard and CyberFundamentals (CyFun®) framework cover the organisation like how the risk is managed, who is responsible and how an incident is reported.
- IEC 62443 covers the plant: zones, security levels, secure development, and the duties of the asset owner, the integrator and the equipment supplier.

The two are complementary, and neither one replaces the other. A security framework alone is mainly limited to the IT boundaries while IEC 62443 alone has almost no management system behind it.

Combining them is what makes a company more resilient on the production floor.

Sections 4 and 5 of this report show how far Belgian manufacturers have come on that path.

3.2 Attackers and regulators arrive at the same time

Two forces are reaching industrial companies at the same time. **Attackers have understood that production is the single point of failure, and Europe has written rules that directly affect industrial operations.**

On the threat side, five patterns dominate:

- **Ransomware** has moved from encrypting file servers to stopping production lines. Downtime creates a stronger negotiating position than stolen data.
- **The supply chain** has become a preferred entry route. On 19 September 2025 Brussels Airport was paralysed — not because the airport was attacked, but due to one of their luggage suppliers (Reuters, 2025). One compromised check-in platform cascaded across several European airports.
- **Remote connections** remain one of the most exploited entry points. Almost every industrial site depends on external parties: machine builders, integrators, maintenance partners, software suppliers, and staff working from home.
- **State-aligned actors** are no longer only collecting intelligence. For example, Russia-linked groups have shown destructive intent, including against Polish energy infrastructure in December 2025 (Chancellery of the Prime Minister of Poland, 2026).
- **The tempo has changed. Exploitation of a new vulnerability** took about a **year in 2021** and is **now counted in days**, most of it on or before the day of disclosure (TXOne Networks, 2026). AI agents already execute parts of an attack campaign on their own (MITRE ATT&CK, 2026), while an industrial **remediation cycle is still counted in months**.

Belgium is at risk. NATO Headquarters and SHAPE, the European Union institutions, the port of Antwerp and the chemical and pharmaceutical clusters place the country on the target list, on top of a dense industrial base that still operate a lot of legacy equipment's.

The regulatory answer arrives as a wave.

The regulatory answer can be perceived not as wave but more as a tsunami:

- NIS2 governs how an organisation manages cyber risks and reports incidents, and the Belgian NIS2 law has entered into force since **18 October 2024**.
- The Cyber Resilience Act (CRA) governs every connected digital component product placed on the EU market, with reporting obligations from **11 September 2026**.
- The Machinery Regulation 2023/1230 governs every machine placed on the EU market from **20 January 2027, with no transition period**.
- Alongside these, one also finds the CER Directive, the AI Act and the Radio Equipment Directive (RED-DA).
- ...

For some Belgian manufacturers **these regulations may overlap**. The same company can be an operator, a manufacturer of connected equipment and an integrator. **A company that work on the three separate compliance projects will pay a high price.**

Even companies outside the direct scope of those regulations will feel the pressure. **Companies in scope must secure their supply chain** and require their suppliers to meet the same level of security expectations.

The Agoria publication “Cyber Security in Operational Technology (OT)” describes each of these texts in detail — NIS2, the Cyber Resilience Act and the Machinery Regulation — with the applicable dates and the obligations per role: operator, manufacturer, importer, integrator (Agoria, 2026, chapters 2, 3 and 10).

3.3 The same picture worldwide

Belgian manufacturers are not facing a local problem. The gap, they see in their own plants, reflects the shift in the global cyber-risk landscape.

The Global Cybersecurity Outlook 2026 of the World Economic Forum (WEF, 2026) shows the perceptions of Cyber risks by executive is changing.

Artificial intelligence has become the dominant concern:

- 94% of respondents see AI as the main driver of change in cybersecurity, while 87% identify AI-related vulnerabilities as the fastest-growing cyber risk of the past year.
- Geopolitics is also shaping security decisions more directly than before, with 64% of organisations taking geopolitical considerations into account when determining their protection measures.

At the same time, confidence in national cybersecurity readiness is declining gradually. Nearly one-third of respondents — 31% — have low confidence in their country's ability to respond to a major cyber incident, up from 26% a year earlier. The report also points to a widening resilience gap between organisations that can absorb a major disruption and those that cannot, with smaller companies increasingly exposed.

The SANS State of ICS/OT Security survey (SANS, 2025) provides the operational counterpart to this picture. **In 2025, 22% of organisations reported an incident affecting their ICS/OT environment.** Of these incidents, **40% disrupted operations**, and almost **20% required more than a month for full remediation.** Unauthorised external access accounted for roughly half of the incidents, with ransomware close behind. The exposure described in the previous section is therefore very real.

Two findings of the SANS Institute survey are particularly important.

- First, detection has improved, but recovery has not kept the pace. Half of the incidents were detected within 24 hours, and most were contained within 48 hours, yet full remediation still often takes weeks. Detection speed is therefore no longer the only constraint. **The harder challenge to restore production safely, confidently and rapidly.**
- Second, external access remains both the leading entry route and **one of the least mature areas of protection.** Only 13% of the organisations report that they have fully implemented advanced controls such as session recording or OT access management.

This helps explain why only 14% of respondents consider their organisation fully prepared for the threats ahead.



Erik De Nert
Head of spotit OT,
Spotit

“In almost every customer conversation over the past year, one need keeps coming up: secure remote access to OT environments. It is no longer optional. Taking control of who can access which assets, when and how is one of the first and most effective steps towards stronger OT resilience.”

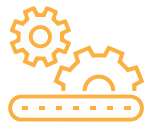
There is, however, one encouraging finding. Organisations operating under mandatory compliance requirements experienced approximately the same number of incidents as other organisations but suffered roughly half the financial losses and safety impacts. Regulation does not necessarily prevent incidents, but when controls are implemented effectively, it appears to reduce their consequences.

The following section examines how Belgian manufacturers compare with this global picture.

4. Key survey findings

4.1 OT environment and exposure

This section examines the technical exposure of the surveyed OT environments: what companies operate, how they protect it, and how well they control the access to it.



40%

of the respondents have a complete^(*) and current OT asset inventory



17%

of the respondents have an OT asset inventory, an OT network segmentation, an OT access policy and a secure remote access to OT



18%

of the respondents report uncontrolled supplier remote access



58%

of the respondents systematically consider cybersecurity features when buying equipment

4.1.1. Individual controls look reasonable; combined coverage does not

Taken one by one, **3 foundational controls** appear moderately implemented:

- IT/OT network segmentation
- Secure remote access
- A formal OT access credential policy

Segmentation and secure remote access are fully in place for 56% of respondents, and a formal OT password and access policy for 47%.

Taken together, the picture changes: **Only 25% have all three fully in place**, while 21% have none of the three.

Looking at each control separately gives a more positive impression than looking at the three controls together.

The exposure is determined by the combination these measures, and on that basis only 25% of the companies have a complete foundation.

^(*) Subject to the quality of the inventories. Asset inventories are difficult to keep complete and up to date. This note applies throughout the document

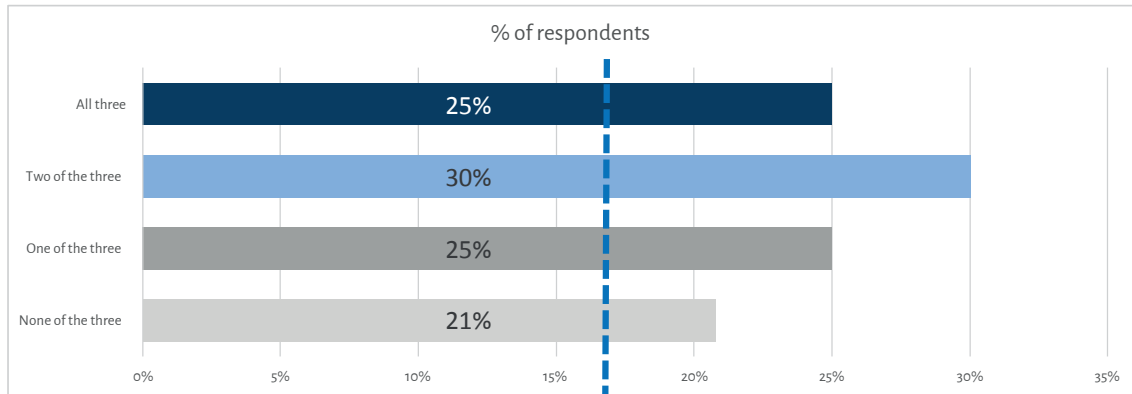


Fig. 1: Combined existence of fundamental controls: IT/OT network segmentation, secure remote access and a formal OT access credential policy.

17% with the three controls AND a complete inventory

It is interesting to note that adding a complete asset inventory, on top of the 3 fundamental controls, reduces this group to 17%. This leads us to the next finding.



Pierre Ciparisse
General-Major,
Belgian Cyber Force

“By silently prepositioning themselves within OT environments, attackers gain the opportunity to disrupt industries, supply chains, and critical infrastructure at the moment of their choosing. Only continuous detection and proactive threat hunting can deny them that advantage and protect our country.”

4.1.2. Asset inventory is the dividing line

Among the respondents with a complete and current OT inventory, 83% have full IT/OT segmentation, none report segmentation as absent, 69% apply a formal access policy in full and 92% report that supplier remote access is managed by their own IT or OT team.

Among the respondents with no inventory at all, only 31% are fully segmented, 46% have no access policy whatsoever and 54% describe supplier remote access as vendor-owned, uncontrolled or unknown.

We can reasonably say **there is a correlation between the actual existence of a complete inventory and the companies which are in control of their environment.** This is a **more robust criteria** than the company size or the region to leverage the control maturity of their cyber resilience.

OT asset inventory	Full IT/OT segmentation	Fully secured remote access	Fully applied access policy	"Supplier remote access managed by IT or OT"
Complete inventory	83%	69%	69%	92%
Partial inventory	41%	56%	35%	90%
No inventory	31%	23%	23%	46%

Fig. 2: Control maturity status by inventory status.

4.1.3. Legacy exposure is widespread and is not compensated

Legacy is one of the major issues in the OT world.

End-of-life operating systems remain common in production: **almost half of the respondents (47%) still run at least one unsupported Windows version**, and 31% run Windows 2000, XP or CE.

Two thirds report that **their oldest OT device is at least 10 years old, and one third at least 20 years!**

The relevant finding is, not the presence of legacy technology, which is inherent to industrial life cycles, but the **absence of any mitigation measures around this major issue**. 58% of the respondents running Windows 2000, XP or CE lack full segmentation, fully secured remote access or both.

4.1.4. Uncontrolled supplier access is concentrated in small OT environments

18% of the respondents describe remote access to their OT equipment as vendor-owned and not governed by them, as possibly running over 4G gateways that they do not control, or as simply unknown.

Amongst those 18% suffering from lack of control:

- 92% operate small OT environments, while none of the respondents running a large OT environment report this situation.
- Moreover, 83% of these companies have no complete asset inventory which confirms the finding of the previous point.

The two weaknesses mean that these companies neither know what they operate nor control who connects to it.

4.1.5. Security is specified at purchase but not followed up during operation

Procurement practice is comparatively mature: 58% of respondents systematically consider the cybersecurity features of new industrial equipment, although only 48% systematically consider the applicable regulations and frameworks.

Amongst the companies that systematically consider the cybersecurity features, the **operational follow-up remains rather weak:** 51% of the respondents do not systematically apply the guidance that they subsequently receive, while 49% do systematically apply the cybersecurity recommendations issued by their equipment manufacturers.

		Manufacturer recommendations applied systematically	
		Systematic	No
Equipment security features considered systematically in procurement	Yes	49%	51%
	No/ Not systematically	29%	71%

Fig. 3: Procurement intention versus operational follow-up.

The capability to specify security requirements is therefore present in most request for proposals; **what is missing is the process to act on manufacturer guidance once the equipment is installed and is in production.**

Key Takeaways

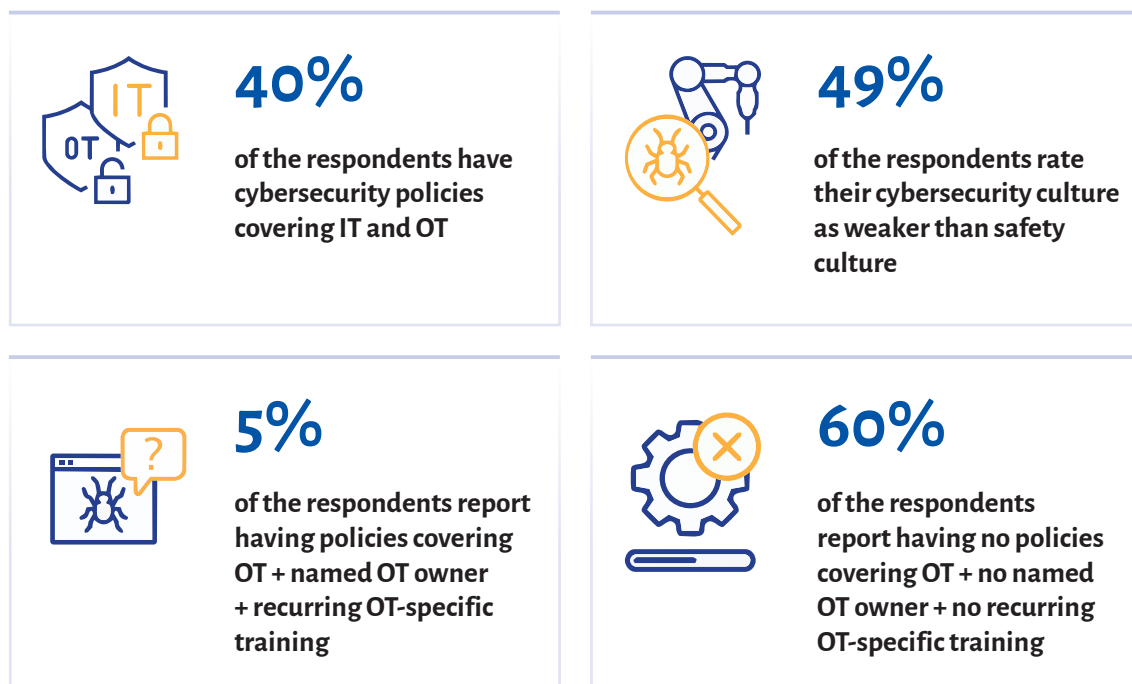
- Companies that understand their OT environment thanks to a complete inventory can protect it effectively; those that don't remain exposed, regardless of their size or budget.
- The legacy is a major issue in the OT world: some OT devices are more than 20 years old ...
- Supplier access requires stronger control.

4.2 Governance, culture and policies

This section examines how OT cybersecurity is organised rather than how it is implemented technically.

It covers:

- The scope of the cybersecurity policy,
- The assignment of responsibility,
- The awareness training,
- The way resources and budget are provided, and
- **The relationship between the cybersecurity culture and the safety culture.**



4.2.1. OT governance is all or nothing: the policy is the decisive element

For the whole base, **only 19% of the respondents have an OT CISO or equivalent**, while 63% do not have one and 18% do not know.

Concerning the existence of cybersecurity policies:

- 40% of the respondents have a cybersecurity policy covering both IT and OT,
- 53% have a policy for IT
- and fortunately, only 5% have no policy at all.

These figures are not surprising in themselves, but they predict the rest of the governance picture very closely, especially when they are cross-analysed with the following 3 aspects:

- The presence of a dedicated OT CISO or equivalent,
- The existence of recurring OT-specific training, and
- The systematic application of the manufacturer guidance.

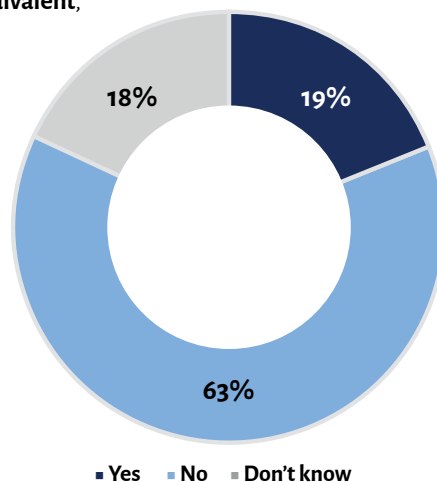


Fig. 4: Presence of a dedicated OT CISO or equivalent.

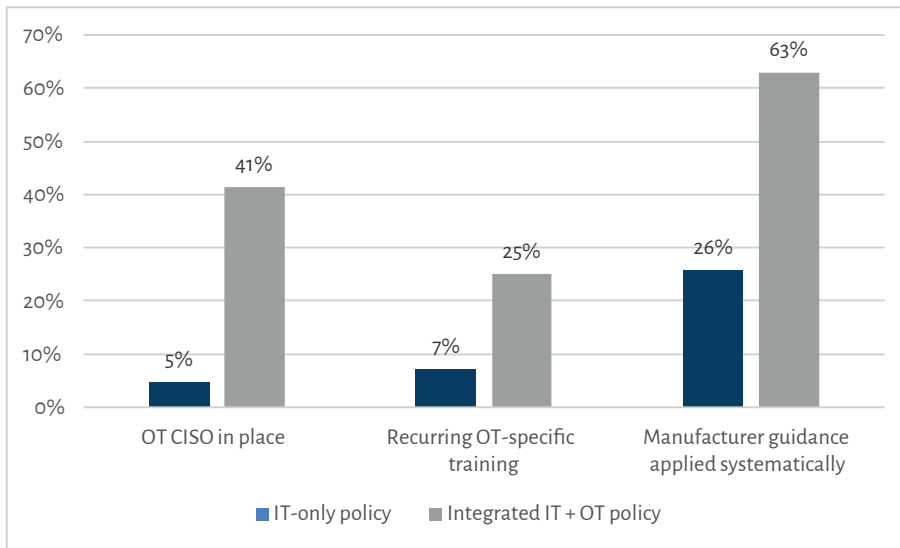
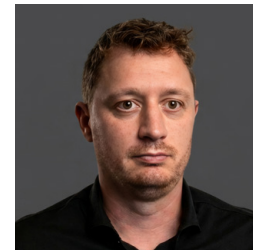


Fig. 5: Company maturity related to integrated IT and OT policies.

There is no gradual middle position. Companies either extend their governance to OT across all three dimensions (OT CISO, OT training and manufacturer guidance applied), or they leave all three outside it.

“OT Security is successful when implemented by design rather than by assumption. The same structure that governs IT must be extended to cover OT. This ensures that OT Security starts from the same risk-based program that has its origin in your business strategy.”



Jasper Hooft

Head of Organisational security, Toreon
Co-Chairman CMiB4ICS/OT Focus group, Agoria

4.2.2. The OT cybersecurity budget is moving while ownership is missing

43% of the respondents report that their OT cybersecurity budget has increased in recent years. However, 63% have no OT CISO or equivalent, or do not know whether they have one. **It seems that this budget is released without anyone being formally responsible for managing it.**

Most of the companies that have no identified owner for OT security cannot describe the budget trend at all. The absence of a clearly identified OT security owner is closely associated with a lack of visibility over the OT cybersecurity budget.

4.2.3. The company size does not explain the governance maturity, but the region partly does

When focusing on the maturity of the policies, the OT ownership and the existence of an OT-specific awareness programme, **the company size doesn't show any significant variance**, that is a valuable finding in itself.

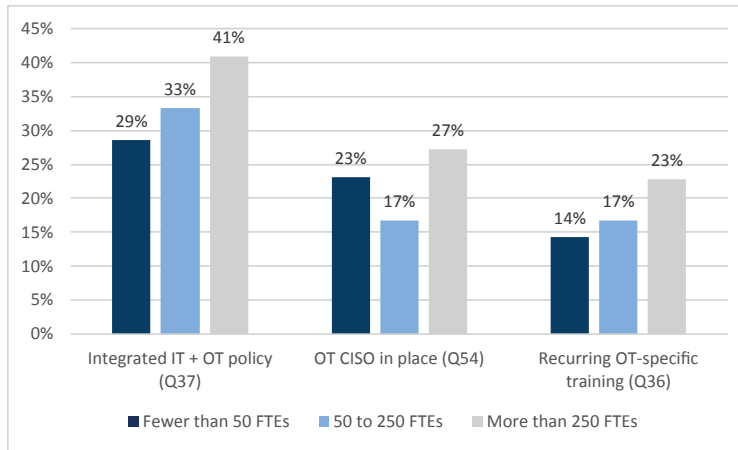


Fig. 6: OT maturity by company size.

Larger companies are slightly better in terms of integrated policies, but the OT ownership and the education levels remain virtually identical. **Large companies are not better governed.** They are only better informed about their own OT cybersecurity budget.

This supports the observation made later in the study that **the leading companies in cybersecurity maturity are not necessarily the largest ones.**

The region separates the sample much more clearly than the size. The integrated IT + OT policy reaches 50% in the Brussels-Capital Region against 44% in Flanders and 19% in Wallonia, OT-specific training 20% for the Brussels-Capital Region against 15% for Flanders and 6% for Wallonia, and respectively an increasing budget of 60%, 47% and 25%.

However, the difference disappears on two indicators: the presence of an OT CISO (18% against 19%) and the culture assessment (50% against 44% rating cybersecurity below safety).

Flanders seems to be further ahead in translating cybersecurity into formal policies and budgets, which possibly reflects an adequate supported ecosystem funded by VLAIO and delivered by Sirris.

4.2.4. The companies with low OT cybersecurity hygiene miss ownership and do not seem to be looking for talents

18% of the respondents have no OT cybersecurity resource at all. Some answers state a clear “NO”, and others say that it still requires implementation.

None of these companies has an OT CISO or equivalent, and the concern about hiring or retaining OT cybersecurity expertise does not exist either.

Respondents working with an external provider or with combined internal and external resources are clearly more concerned (60%) than those relying on internal staff only or having no OT staff dedicated at all (36%).

The concern for OT sourcing therefore reflects an effective contact with the labour market rather than the absence of capability. **Companies that are looking for OT security expertise have discovered that talents are rare, while companies that have never looked report no problem.**

The overall concern for 49% of the respondents confirms **the talent gap challenge however it seems underestimated due to the fact that many companies are not even looking for resources!**

4.2.5. The self-assessment culture is credible, and safety is an enabler for OT cybersecurity

Nearly half of industrial companies (49%) rate their cybersecurity culture as weaker compared with their safety culture, and more than half (57%) already run mandatory, recurring security awareness training.

Yet only 15% include any cyber-OT-specific content in their training:

- 43% train recurrently on generic IT topics only,
- 22% limit the training to onboarding or one-off sessions, and
- 21% provide no training at all

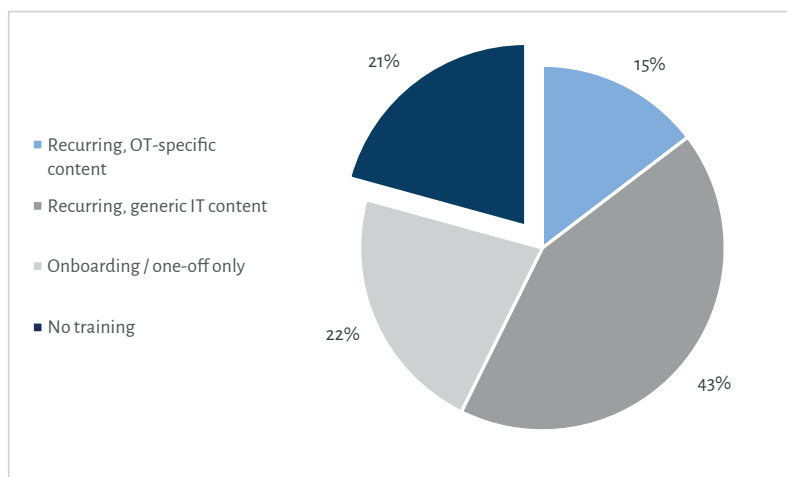


Fig. 7: OT awareness training.

The main issue is not awareness or the lack of a training culture — both already exist.

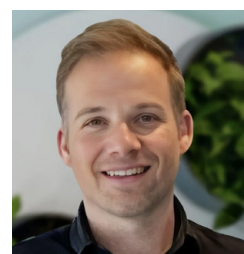
What is missing is specific OT cybersecurity content covering the key areas within the mandatory and recurring awareness programmes already in place. Adding a ready-to-use OT training module is therefore much more realistic than trying to build a new awareness culture from scratch.

This content already exists.

For example, **Agoria's 10-pager guide, "Cyber Security in Operational Technology (OT)"**, explains the behaviors expected from field operators, control engineers, IT and security staff, and plant management (Agoria, 2026, Chapter 6).

It can therefore be used directly as the OT component of an existing awareness program.

“OT Risk perception hasn't moved because risk is still written in technical language. A plant manager doesn't act on a vulnerability count. He acts on three things: which line stops, how long it takes to restart, and which customer deliveries slip. That translation is the work.”



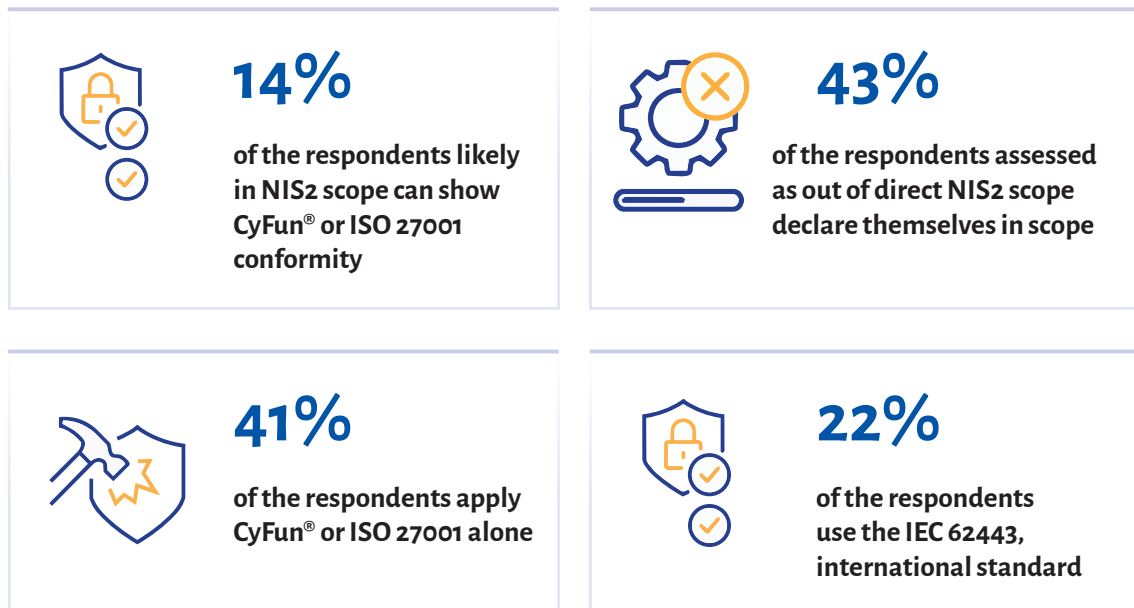
Nick Peeters
Managing Partner,
Soterics

Key Takeaways

- Belgian industry is investing in OT cybersecurity, accountability appears to be unclear. Without a clear owner, the policy applies primarily within the IT boundaries, the training stays generic, and the budget allocations appear to lack clear strategic decisions.

4.3 Regulatory readiness

This section looks at how prepared the respondents are for the European regulations that apply to their activity, and which standards they use to meet them. The analysis is based on the respondents that are probably in scope of NIS2, the Cyber Resilience Act (CRA) and the Machinery Regulation. That scoping uses the sector, the size and the role in the OT value chain declared by the respondent. The scoping is a research segmentation and not a legal determination: the scope follows from the NIS2 law and is confirmed through registration and classification with the Center for Cybersecurity Belgium (CCB), our national cybersecurity authority. The comparison between what a company probably is and what it believes it is remain the most useful outcome of this section.



4.3.1. Companies do not know which regulations apply to them

Companies do not know whether NIS2 applies to them, and the error goes both ways: some declare themselves in scope when they probably are not, others assume they are out of scope when they probably are not in scope.

Out of the respondents probably not in the direct scope of NIS2, 43% declare themselves in scope. At the same time, 28% of the respondents assessed as likely, according to the criteria defined in the Belgian NIS 2 law (26 April 2024) in scope declare that they are not subject to it, or do not know.

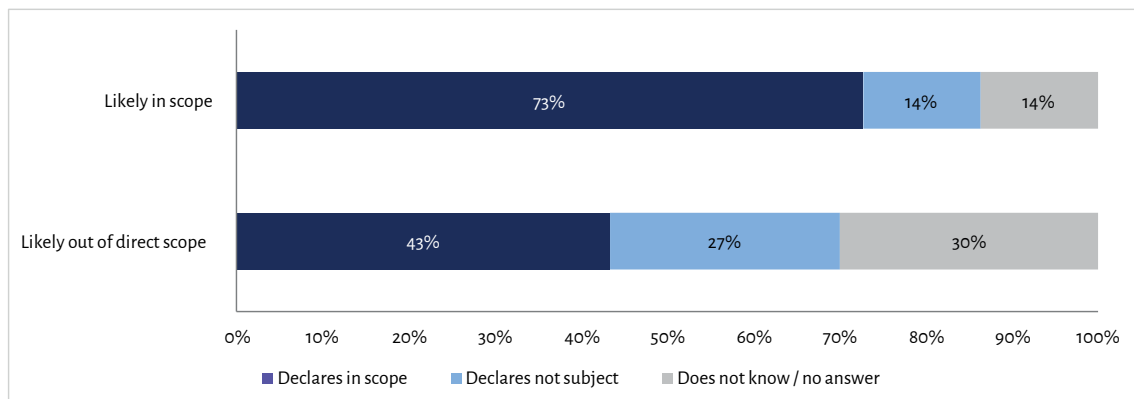


Fig. 8: Companies do not know which regulations apply to them.



“The overlapping waves of NIS2, CRA, and the Machinery Regulation are placing immense pressure on industrial supply chains. Companies attempting to solve these in silos will pay a high price.”

Gerrit Neyrinck
Cybersecurity Architect IT/OT, Easi
Secretary CMiB4ICS/OT Focus group, Agoria

The over-declaration (43%) is probably not a mistake. NIS2 entities must manage the security of their supply chain and require their suppliers to demonstrate their level of cybersecurity maturity. A company active in a sector not covered by NIS2 that answers “in scope” as a subcontractor is very likely describing a customer or contractual requirement rather than a legal obligation.

The practical consequence is the same in both cases: **the declared status in the survey results cannot be used to measure who is regulated.**

4.3.2. A majority has started, but few can show formal evidence yet

The survey was carried out after 18 April 2026. By that date, essential entities had to be able to prove their cybersecurity level. The two main routes are either a CyFun® verification statement at level Basic or Important issued by an accredited body, or an ISO 27001 certificate. An entity that had a signed agreement with an accredited body and was actively in the process of being verified was also considered to have taken the step. The results show how far the population stands from that requirement.

Amongst the companies likely in the NIS2 scope, 14% of the respondents report either CyFun® or ISO 27001 conformity, and 23% use neither framework.

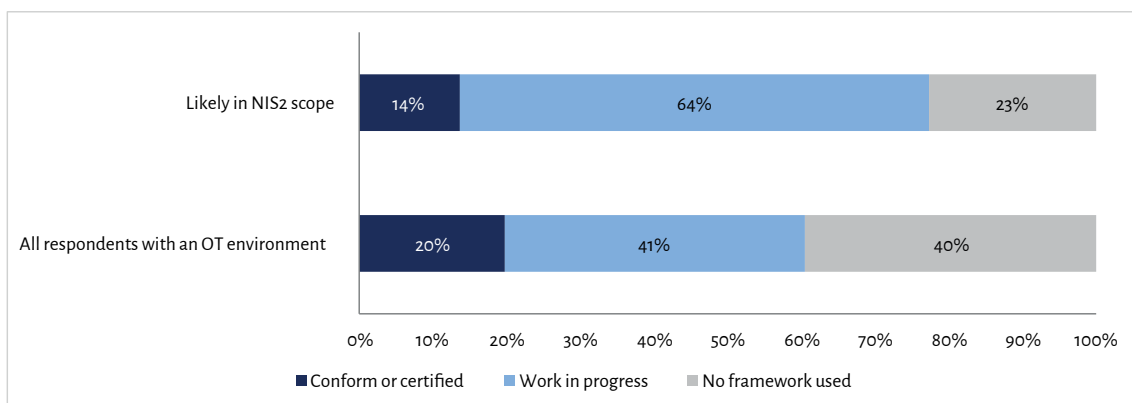


Fig. 9: A majority has started, but few can yet show formal evidence.

“NIS2 puts IT and OT in scope together. In our assessments we keep seeing the same gaps: OT run as an island, understaffed OT security, and no demonstrable IEC 62443 knowledge. With the CRA and Machinery Regulation coming, that is no longer a compliance detail.”



Patrick Coomans
Global Strategy and M&A for Trust in Digital,
Vinçotte, part of Kiwa Group

4.3.3. The NIS2 deadlines have not moved - only a remediation route is defined

The 18 April 2026 **deadline** for essential entities to demonstrate their conformity **has not been extended**. For those who could not meet it, the CCB has formulated the preferred remediation routes, in execution of the NIS2 law: a remediation plan, measures equivalent to CyFun® Important by 18 April 2027, and CyFun® Essential by 18 April 2028.

In the survey, out of the 22 respondents who are probably in scope, 17 declare that they are in progress and 3 declare that they are compliant.

There is a risk that companies read these remediation routes as a sign of greater flexibility. It is not the case. An entity that was not conform on 18 April 2026 is late, stays under supervision, and is expected to show a credible plan.

The arithmetic of the remediation calendar also deserves attention.

Reaching the CyFun® Basic assurance level can reasonably be estimated in quarters, and the Important assurance level in years. **A company that is under the cyber poverty line today is therefore already outside a realistic window for April 2027.** The year that separates the two remediation milestones only covers the step towards the Essential assurance level.

Concerning the Cyber Resilience Act (CRA), the reporting obligations apply from 11 September 2026, **and this date has not changed**. Out of the 28 respondents who are probably in the scope, only 4 make use of IEC 62443 international standard.

The Machinery Regulation becomes applicable on 20 January 2027, **with no transition period foreseen at this stage**. Out of the 30 respondents who are probably in the scope, 13 respondents answer that they are not concerned or that they do not know.



Philippe Massonet
Scientific Coordinator,
CETIC Research Center

“Integrating third-party components makes you a legal manufacturer; you can no longer delegate accountability down the supply chain. Compliance is not a static milestone, but a continuous operational muscle covering design, full-lifecycle patch management, and strict incident response. To survive to all OT this regulatory shift (NIS 2.0 / CRA / Machineryo...), integrators must transform from simple assemblers into fully proactive, lifecycle-long product stewards.”



4.3.4. Combination of cybersecurity OT frameworks is key

78% of the respondents do not use IEC 62443 international standard or do not know it. Only a few are compliant. Only 20% apply the combination between **CyFun®** or **ISO 27001 framework** and **IEC 62443**, while 41% apply the CyFun® or ISO 27001 framework alone and 38% have neither.

The gap is largest where the standard matters most: 20% of the respondents likely in scope for the Machinery Regulation use IEC 62443 international standard, and 14% of those likely in scope for the CRA.

The substitution runs in one direction only, since 68% of the companies use CyFun® without IEC 62443 international standard while only 29% do the opposite.

This is a missed opportunity as CyFun® (version updated in 2025) is better aligned with IEC 62443 among other references, but adoption probably focuses mainly on the IT layer.

The choice between the right standard and frameworks is a challenge for every company.

The Agoria 10-pager publication “Cyber Security in Operational Technology (OT)” compares ISO 27001, CyberFundamentals and IEC 62443 side by side and indicates which combination fits which situation, including the case of the mixed IT and OT production companies (Agoria, 2026, chapter 8).

Note that the CCB has published correspondence tables linking each CyFun® 2025 requirement to its equivalent in ISO/IEC 27001, ISO/IEC 27002 and IEC 62443 (CCB, 2026).

Key Takeaways

- Belgian industry is engaging with the regulations. Still manufacturers need more guidance to know if they fall under which regulation and how to proceed while combination of standards is key



Geoffroy Moens
Senior Principal Cybersecurity Architect,
Schneider Electric

“At Schneider Electric, we have invested a lot in the development and adoption of IEC62443 because it is applicable to vendors, integrators, and asset owners. Currently, we are very actively involved in the development of CRA standards to bring consistency between regulations and IEC 62443.”

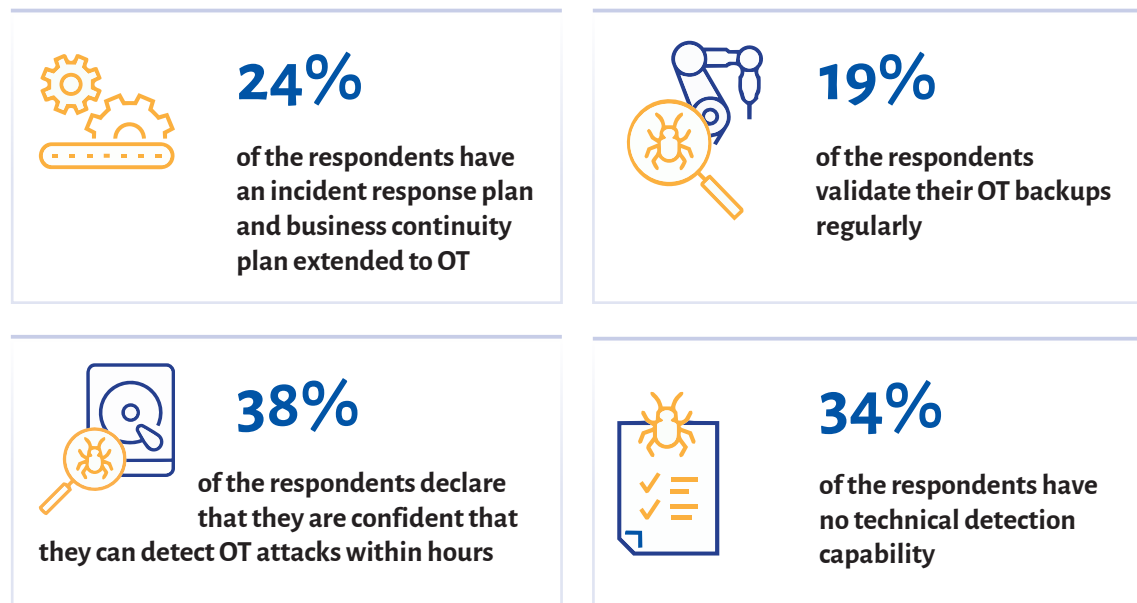


4.4 Resilience in practice

This section looks at what happens when prevention fails.

It covers 4 elements:

- The plans that organise the response,
- The capabilities that allow an attack to be detected,
- The testing practices that verify those capabilities,
- And the backup validation that determines how quickly production can restart.



4.4.1. Resilience plans exist but mainly limited to the IT boundary

Most respondents have an incident response plan and a business continuity plan: 73% have an incident response plan and 58% have a business continuity or disaster recovery plan.

Among the existing plans, unfortunately:

- 70% of Incident Response Plans (IRPs) cover IT only.
- 67% of Business Continuity plans (BCPs) cover IT only.

This is a missed opportunity, as many companies already have these plans in place but have not yet extended them to the OT environment.

Only 24% of respondents have extended both plans to OT.

Company size does not explain this result:

- Respondents with more than 250 employees are not more likely to include OT in their resilience plans than the smaller ones.
- **The size of the OT environment does explain it.** 67% of the respondents with a very large OT environment include OT in their incident response plan, against 14% of those with smaller OT environments.

Based on the self-declarations, this gap is not perceived. Among the respondents whose plan covers IT only, 66% rate the maturity of that plan as average or high. **They assess the plan that they have and not the coverage they do not have.**

“Before you buy anything, count the accounts. Not the people - the accounts: every supplier login, every service account, every machine and application credential that can reach something in the plant. Most organisations can produce some kind of asset list within a week. Almost none can produce that account list, and the ones who try are usually surprised by both the number and the age of what they find. An account nobody can name is an entrance nobody is watching. It costs a query and one uncomfortable afternoon.”



Samir El Makrini
Sales Director,
Proximus NXT

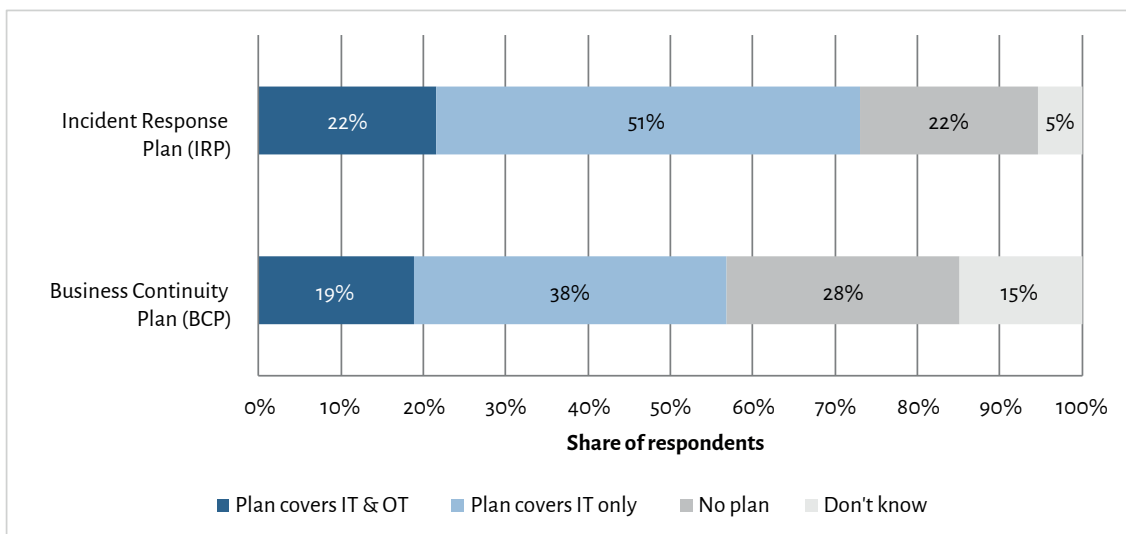


Fig. 10: Scope of the Incident Response Plan (IRP) and of the Business Continuity Plan (BCP).

4.4.2. Confidence in detection is higher than the capability to detect

5 detection capabilities across the respondents are unevenly deployed:

- 49% have network monitoring or intrusion detection on the OT network (IDS, NDR, OT-specific)
- 39% have endpoint detection on OT workstations (EDR or antivirus with a central console)
- 29% have 24/7 monitoring (in-house SOC, external MSSP or equivalent)
- 26% have centralised log collection from OT systems (SIEM or equivalent)
- 10% have anomaly detection on PLC or controller behaviour

The capabilities that already exist in IT and can be extended towards the OT network are the most common. The one written specifically for industrial protocols is the rarest. **90% of the companies have no means of noticing that a controller is behaving differently from the way it was programmed.**

38% of the respondents are confident that they would detect an attack on their OT environment within hours. That figure deserves to be analysed.

Within this confident group,

- 42% have three technical detection capabilities or more in place.
- **48% of respondents who expect to detect an attack within HOURS cannot point to any related detection capability that would produce the alert.**

Confidence in detection is therefore, for a significant part of the group, a judgement rather than a measurement.

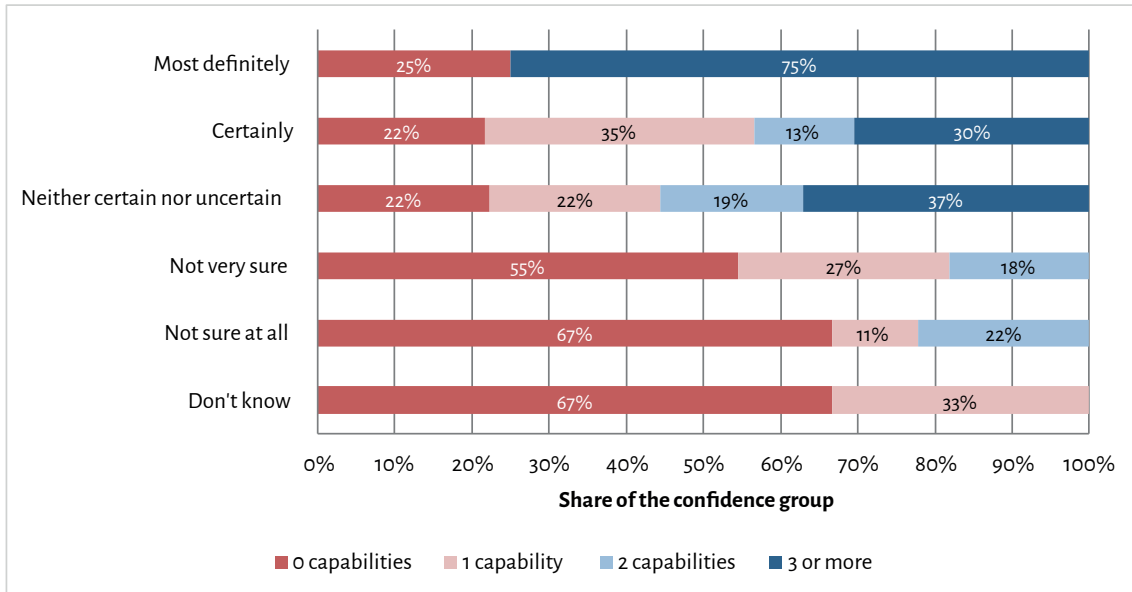
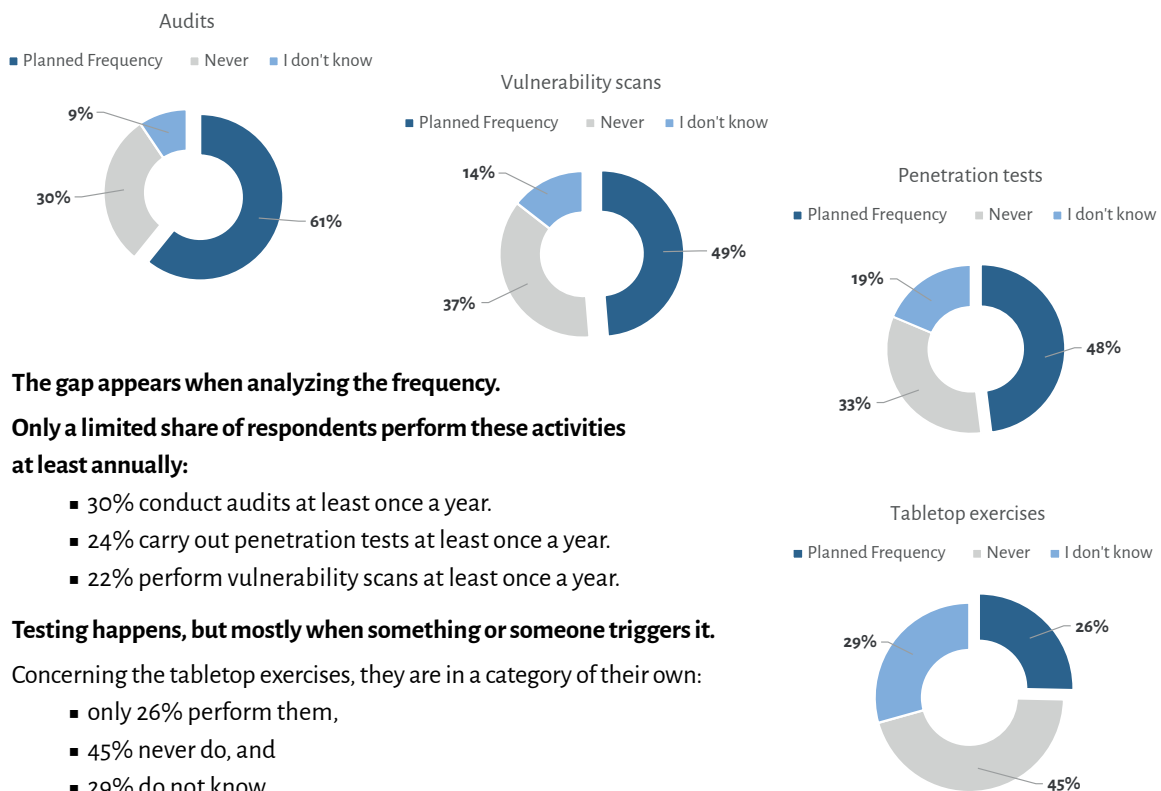


Fig. 11: Number of detection capabilities in place, compared with the declared confidence in detecting an attack within hours.

4.4.3. Testing is rare, and exercises are almost absent

Most respondents do test their OT environment in some form:

- 61% run audits,
- 49% run vulnerability scans, and
- 48% run penetration tests.



The gap appears when analyzing the frequency.

Only a limited share of respondents perform these activities at least annually:

- 30% conduct audits at least once a year.
- 24% carry out penetration tests at least once a year.
- 22% perform vulnerability scans at least once a year.

Testing happens, but mostly when something or someone triggers it.

Concerning the tabletop exercises, they are in a category of their own:

- only 26% perform them,
- 45% never do, and
- 29% do not know.

When almost 30% of the respondents cannot say whether one took place, the honest reading is that it did not.

Fig. 12: Frequency of the four testing activities

4.4.4. Backups are assumed rather than proven

Only 31% of respondents regularly or partially validate their OT backups through recovery testing. By contrast, 57% do not test them at all or rarely and 12% do not know.

This creates a clear paradox: **81% rank safety or availability as their top OT priority, yet most do not regularly verify that they can recover their systems.**

A backup that has never been successfully restored is not a proven safeguard for availability. Another 12% do not know whether their backups are tested. Their actual recovery capability is therefore uncertain.

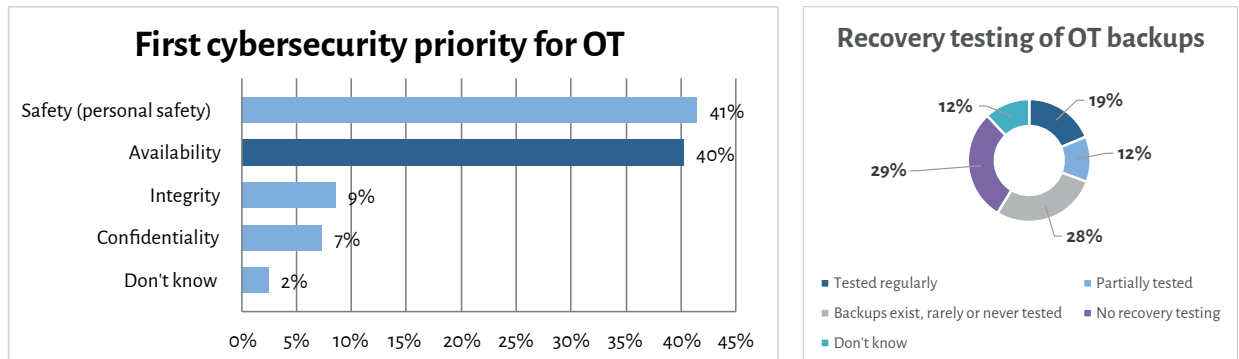


Fig. 13: Backup recovery testing, compared with the first OT priority declared by the respondents.



Laurent Deheyer
Chief Delivery Officer,
Approach Cyber

“A recovery plan that has never been tested is not a security control—it is an assumption. Until your backups and recovery procedures have been validated under real-world conditions, your resilience remains theoretical. Otherwise, when an incident happens, all that is left is hope... and lighting a candle.”

4.4.5. The transparency is key for incident reporting visibility

9% of the respondents report an OT incident during the last 12 months. **52% of the respondents consider an attack on their OT unlikely, or do not expect one at all.**

These findings should be considered as minimum estimates:

- 10% of the respondents reported that they **are not allowed to answer** which creates a lack of transparency, and
- a third of the population has no detection capability. **A company that cannot detect cannot report.**

The number of incidents reported describes what the respondents were able to see and were allowed to disclose. **It does not describe the real frequency of incidents in Belgian industry.**

Key Takeaways

- Belgian industry approaches OT resilience with a confidence that is not really verified: incident and continuity plans often stop at the IT boundary, backups and detection are not regularly tested, while four companies out of ten still expect to detect an attack within a few hours.

5. The leading pack

Based on the survey results, we identified a leading group of respondents. Each company operating an OT environment was scored across 7 maturity domains, elaborated in the methodology section. Top 10% of respondents form the “leading pack”. The comparison below shows how this group differs from the remaining 90%.

This analysis highlights a clear pattern among leading companies.

5.1 Are budget, size or region differentiators?

The short answer is no:

- 60% of the leading pack report an increasing OT cybersecurity budget, against 63% of the rest — no significant difference.
- The concern about hiring or retaining OT cybersecurity people is lower in the leading group, but not significantly.
- Recurring OT-specific awareness training reaches only a quarter of the leading pack, which remains low in absolute terms, even at the top of the field.
- The leading companies span all size bands, from fewer than 50 employees to more than 500.
- They cover all OT environment sizes and all the different categories in the OT chain, from asset owner to machine builder.
- Six are based in Flanders, which broadly matches the sample.

Maturity in this survey is a question of organisation rather than of resources or scale.

5.2 Leaders finish where the others start

The leading pack does not use different preventive controls than the others.

- 100% have an IT/OT network segmentation fully in place
- 88% have secure remote access to OT fully in place and 12% have it partially in place
- 75% have a formal password & access policy applied to OT and 15% have it partially in place
- 88% have a complete asset inventory in place and 12% have it partially in place

While, the situation is radically different for the rest of the pack

- 51% have an IT/OT network segmentation fully in place
- 52% secure remote access to OT fully in place
- 43% have a formal password & access policy applied to OT in place
- 35% have a full asset inventory in place

The difference increases as soon as the 4 preventive controls are combined:

- 63% of the leading pack have segmentation, secure remote access, a formal OT access policy and a complete inventory all fully in place,
- against 20% of the rest.

The rest of the industry has started many initiatives, but few are fully completed.

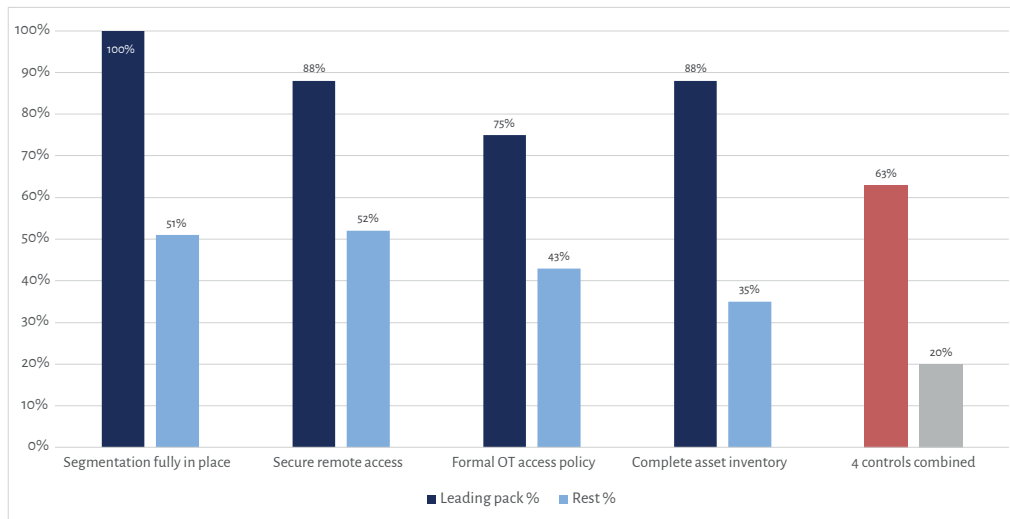


Fig. 14: Comparison of preventive measures implementation between leading companies and the rest of the pack.

5.3 Leaders can see what happens on the OT network

The leading pack reports 3 out of 5 detection capabilities on average (centralised log, network monitoring, endpoint detection, anomaly detection on PLC and 24/7 monitoring), against less than 2 for the rest, and 86% have at least three, against 27%.

The clearest single gap is passive monitoring of the OT network, present in 88% of the leading group and 45% of the others.

Their confidence is also better founded. Three quarters of the leading pack believe that they would **detect an attack within hours**, against 36% of the rest. The rest of the field is not only less able to detect an incident; it is also less accurate about its own ability.

“You cannot secure what you cannot see. That’s why we deployed our own OT monitoring device across several real-life operational environments. Passive visibility into asset inventories, protocol-level communication flows, and deviations from the intended security architecture is the starting point of operational OT cybersecurity—and it’s exactly the evidence base our research and education programs are built on.”



Johan Galle
Lecturer cybersecurity,
Howest

5.4 They govern OT explicitly and use the industrial standard

88% of the leading pack have a cybersecurity policy covering both IT and OT, against 34% of the rest.

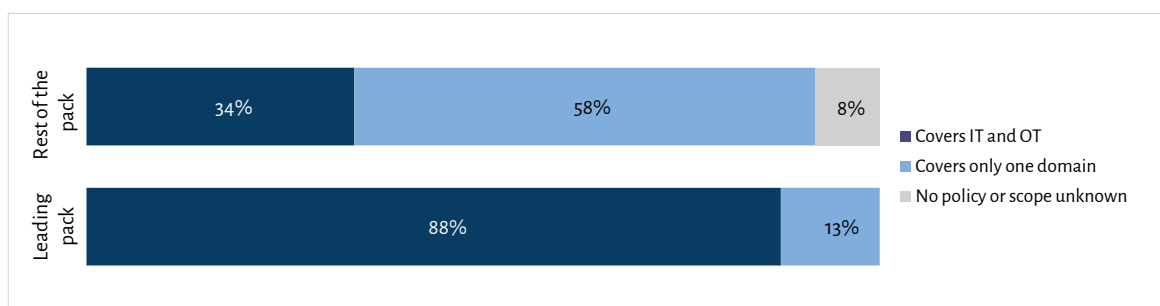


Fig. 15: Scope of the cybersecurity policy—leading pack versus the rest.

5.5 Ability to recover is the clearest differentiator

The sharpest difference in the entire survey is not in prevention but in the ability to recover:

- 88% of the leading pack validate their OT backups through recovery testing, against 23% of the rest.
- 80% have a business continuity or disaster recovery plan covering OT as well as IT, against 17%,
- 71% have an incident response plan that reaches the production floor, against 18%.

Taken together, 38% of the leading pack have all three, against 4% of the rest.

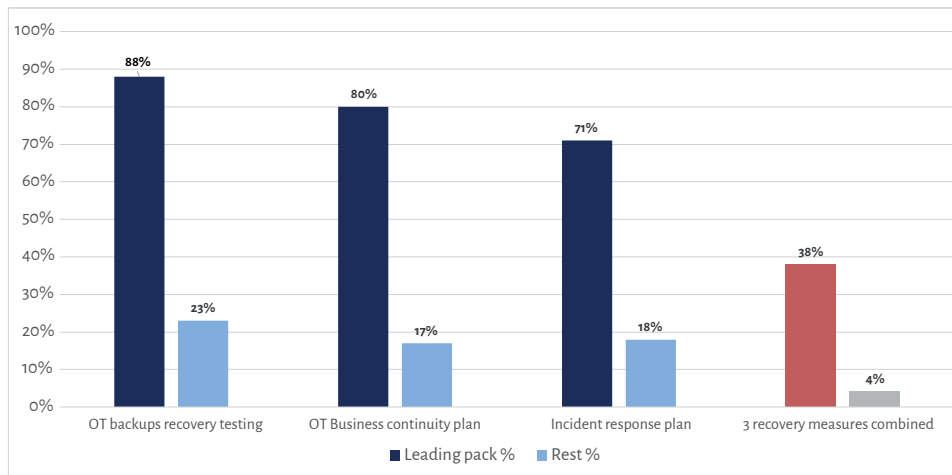


Fig. 16: Comparison of recovery control implementation between leading companies and the rest of the pack.

However, the most important figure is what remains on the other side:

- **77% of the companies outside the leading pack have none of the three recovery capabilities:** incident response, continuity planning and tested backups.
- **They may well prevent an incident, but they have not defined what happens on the day prevention fails.**

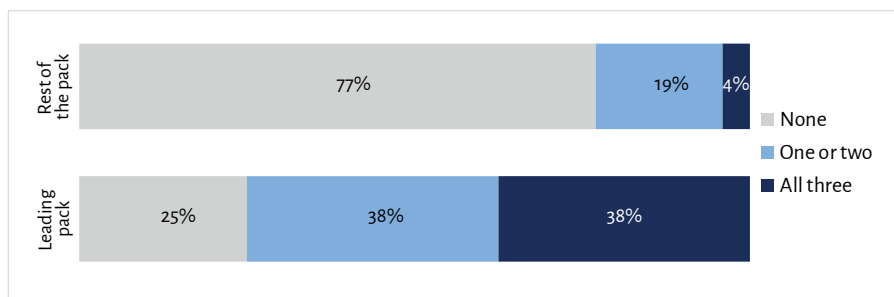


Fig. 17: Preparedness to respond and recover: Incident Response Plan (IRP), Business Continuity Plan (BCP) and tested backups.



Jurgen De Wever

Strategy & Innovation Manager, Siemens Digital Industries
Co-Chairman CMiB4ICS/OT Focus group, Agoria

“Cybersecurity is not just a technical feature, but a foundational prerequisite for successful digital transformation in the manufacturing space. Pillars towards OT cybersecurity excellence: understand the business impact of “Security by Demand”, embrace IEC62443-driven Defense-in-Depth concepts and apply “Security by Design” practices.”

Key Takeaways

- The leading companies are not larger, better funded or better staffed than the rest.
- They are the ones who completed the response and recovery measures that others only started.
- They have tested their detection capabilities, incident response and recovery plans.

Ten insights from the OT leaders

Opportunities for improvements

1. **Name someone.** OT cybersecurity ownership has to be attributed. Name a person with the authority to stop or isolate production when required.
2. **List your assets.** An up-to-date OT asset inventory is the essential starting point. Implement the approach incrementally, starting with one production line.
3. **Reduce the technical exposure.** Achieve the segmentation between IT and OT, identify known vulnerabilities and patch what can be patched or implement compensating controls.
4. **Take back control of supplier access.** Inventory all your suppliers having access to your IT and OT environments. Route every remote connection through your own IT or OT team, with individual accounts and logging. Minimize supplier-owned access solution and undocumented 4G gateway.
5. **Extend the cybersecurity policy to OT.** Most companies already have a policy. Adding OT scope is a revision, not a new project.
6. **Test backups.** Restore PLC configurations or engineering workstations from backup and test them. Untested backups are an assumption, not a control.
7. **Extend the incident response plan to the production floor.** Add who may stop production, how to bring back operations in a safe manner.
8. **Run one tabletop exercise a year.** Two hours around a table with production, maintenance, IT and management (best at lunch time!). This is the cheapest measure in this list and the rarest in the survey.
9. **Put OT traffic under observation.** Passive network monitoring on the OT network gives visibility without touching the process. It is the capability the leading group focuses on.
10. **Use IEC 62443 to structure the work.** IEC 62443 standard is an international reference for OT cybersecurity. The leading group typically combines it with other frameworks like CyFun® or ISO 27001.

“OT systems and how to protect them is one of the major unknown for most of the Security industry. But the technology is there, the standards are there, and NIS2 is very clear: we must, and we can, protect them. It is a matter of embracing new knowledge, and a new way of thinking. In OT systems, often it is more important to ensure continuity via backup and redundancy than to actually stop an attack. This requires a shift on the mind of security experts: this is clearly possible.”



Matteo Merialdo

Chief Technical Officer - Cyber,
Sopra Steria Group/Nexova Group

6. Evolution over the last 5 years

A first study covering Cybersecurity in manufacturing was published in 2021 (Agoria, 2021).

This section compares, between 2021 and today:

- where the Belgian industry has improved,
- where it has stood still, and
- what are the potential impacts of the new cybersecurity European regulations.

6.1 The six common KPIs that moved

The trends for the six common KPIs are presented below

	in 2021		in 2026	
 Cybersecurity taken into account when selecting industrial equipment	60%	➡	91%	++
 Manufacturer cybersecurity recommendations followed systematically or generally	55%	➡	75%	++
 Knows the age of its oldest OT equipment^(*)	69%	➡	94%	++
 Cybersecurity policy covering both IT and OT, whole base	34%	➡	40%	≈
 Uses or considers at least one cybersecurity framework	34%	➡	65%	+++
 Vulnerability scanning carried out	32%	➡	49%	+

(*) assuming that they have the full picture of their inventory

6.2 The new catalyst that improved the OT resilience

The 2021 respondents faced almost no binding obligation. NIS1 reached a handful of operators, CyFun® framework did not exist, and resilience in an industrial device was a commercial argument rather than a condition for placing it on the market.

Today, the same company could fall under three instruments at the same time:

- **NIS2** in effect since 18 October 2024,
- **CRA reporting from 11 September 2026**,
- **Machinery Regulation** on 20 January 2027 without any transition period

On top of CER Directive, AI Act and RED-DA which might also be relevant for some companies.

All of this, on a certain degree of magnitude, has certainly contributed to the shape of the progress.

The indicators that progressed are the ones a customer, an auditor or a certification body can be challenged:

- A purchasing specification,
- A supplier follow-up,
- A gap analysis,
- An equipment list,
- ...

The indicators that progressed less are the ones with less control:

- Internal knowledge or resources
- Vulnerability scanning
- Policy covering both IT and OT
- ...

6.3 Where the progress is factual

Progress is clearest among the companies that trust their own detection.

In 2021, that trust was largely unfounded. 58% of respondents were confident they could detect an OT cyberattack quickly, but 64% of them had a cybersecurity policy that covered IT only. They trusted their ability to protect OT, even though their cybersecurity controls were not effectively in place.

In 2026 the picture is reversed. Fewer companies claim that confidence — 38% — but now 68% of them have a policy that covers also OT.

Confidence has become rarer and much better founded.

The use of frameworks follows the same logic. Twice as many companies as in 2021 have started an OT cybersecurity journey and use at least one framework. The growth comes mainly from Cyberfundamental CyFun® and ISO 27001, the two routes recognised in Belgium under the NIS2 law.

Progress is clearest among the companies that trust their own detection.

6.4 Where the progress is less addressed

Today,

- **The cybersecurity compliance efforts are still mainly limited to the IT environment.** Few companies use a standard designed for OT, such as IEC 62443, and a large group have a limited knowledge of this international standard. This is exactly the layer where a manufacturer might have to demonstrate conformity under the CRA and the Machinery Regulation.
- **Detection capability remains an attention point.** A large part of the respondents has limited or no technical means to see what happens on their OT network. Tests and exercises remain rare, and many companies do not even know whether a test has ever taken place!
- The perception on the risk itself has not changed. In 2021, half of the companies did not expect a cyberattack on their OT in the coming year. Today, the share is the same. Five years of incidents and a full wave of European rules have not changed that belief.



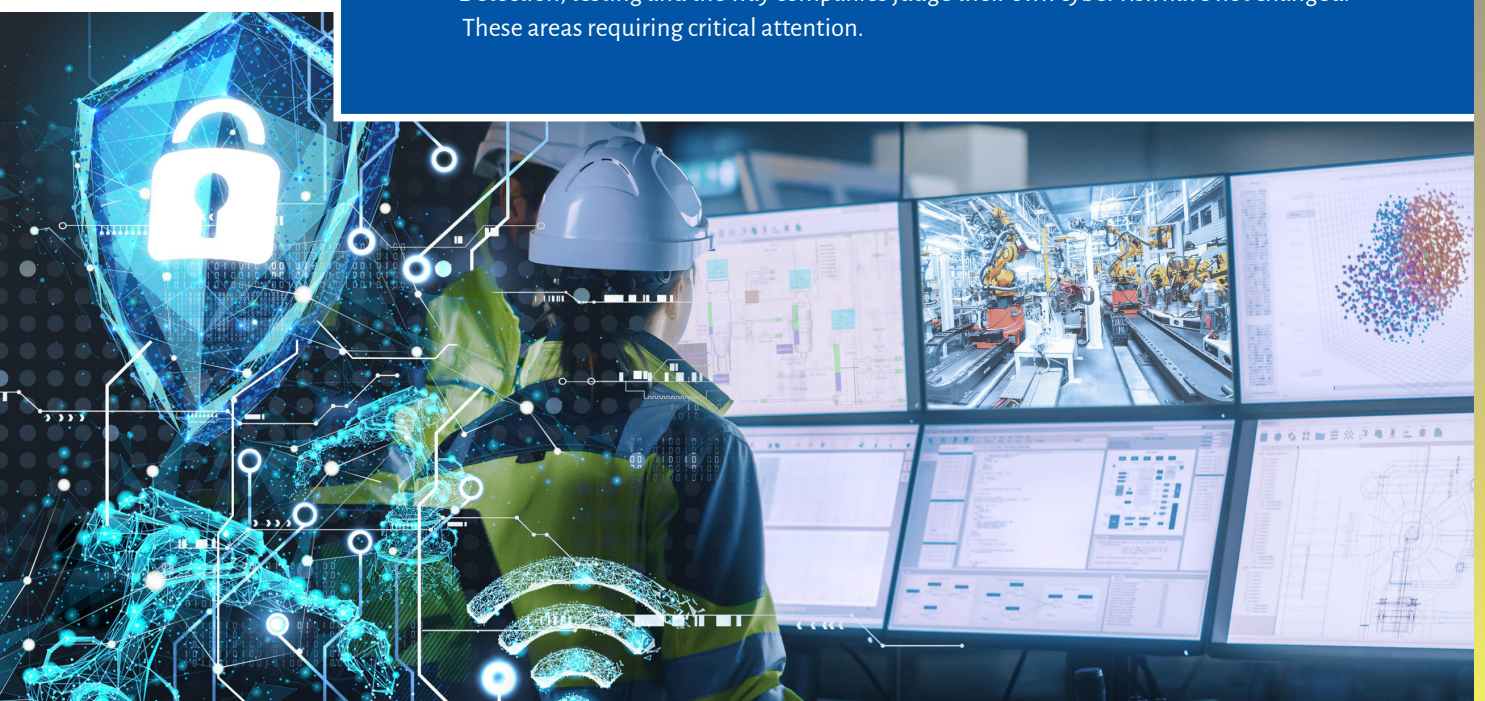
Tatiana Galibus

Cybersecurity ambassador,
Sirris

“We are at a unique moment: regulation has created both the mandate and the urgency to make our systems secure. But the biggest gap I see is not in technology or compliance—it is in risk assessment. Companies need to truly understand their systems, break down the silos between engineering, IT and cybersecurity, and embed risk assessment into the product lifecycle. That is how we move from compliance on paper to security by design”

Key Takeaways

- Since 2021, Belgian industry has improved on some aspects: buying practices, supplier follow-up and the use of frameworks are clearly better.
- Detection, testing and the way companies judge their own cyber risk have not changed. These areas requiring critical attention.



7. Conclusion

The Belgian industry has progressed on OT cybersecurity maturity since the first study covering cybersecurity in manufacturing was published in 2021 (Agoria, 2021).

Companies with OT now think about cybersecurity when they buy industrial equipment, they follow manufacturer guidance more often, and far more of them work with a recognised framework.

These are real improvements.

On the other hand, detection, testing and the way companies judge their own cyber risks is close to where they stood five years ago. Policies, plans and training usually are still mainly limited to the IT boundary. The production floor remains the least covered part of the business on a cybersecurity perspective.

One pattern runs through the whole survey.

Companies do not choose the wrong measures, but they often don't go all the way. Taken one by one, the cybersecurity controls look reasonable. Taken together, only a small group has a complete set of security measures.

The same is true for the cybersecurity governance aspect, where the budget grows while we observed a lack of ownership. For recovery, where plans exist however, they have not been often tested.

This is also what separates the best-of-class companies in OT cybersecurity from the rest.

- They are not larger, better funded or better staffed.
- They finish what the others start.
- They know what they operate, and
- They can show that their controls still work when production stops.

The gap for the rest of the pack is an organisational one, which means it can be closed without a bigger budget.

The regulatory calendar leaves less room than many companies assume:

- The NIS2 deadline has passed and has not been extended. Instead, the CCB, our national cybersecurity authority, has only defined how late entities are expected to catch up.
- The Cyber Resilience Act (CRA) and the Machinery Regulation arrive next, on dates that have not moved.

Many companies do not realise that the Cyber Resilience Act (CRA) or the Machinery Regulation applies to them. Most of them do not apply the industrial standards, despite the fact that the compliance deadline is fast approaching.

This is the most urgent finding of this report.

The way forward does not require new ideas. **It requires finishing the work that has already been initiated:**

- Naming someone who is responsible and testing at least once what you assume works.
- Knowing what you operate with a comprehensive asset inventory,
- Extending the existing policy and the existing plans to the OT environment,

In a nutshell, after consolidating all the data, **we are really pleased to observe a positive evolution of the OT cybersecurity maturity in the last 5 years.**



“As a partner for critical industries, we believe the convergence of IT and OT, combined with NIS2, introduces the need to bring security foundations to operational environments. This is a prerequisite for increasing both cyber resilience and regulatory compliance.”

Fabrice Wynants
VP Security & Networking,
Cegeka

8. Acknowledgment

We sincerely thank our executive partners, our financial sponsors and the AGORIA / CMiB members whose support made this research possible. Their commitment has enabled us to build a strong foundation for future growth and success in Operational Technology (OT) cybersecurity.

We are deeply grateful to the companies that participated in the survey. Their valuable insights allowed us to present an accurate picture of Belgium's cybersecurity in the industrial sector. **Trusted partnerships are critical**

We can thank and mention the valuable ongoing national trusted partnerships:

- With **CMiB4ICS/OT** board members for sharing their expertise and providing meaningful insights.
- With **CCB** about the opportunity to contribute to the national cybersecurity strategy and the Cyber Fundamental® 2025 especially in the field of OT.
- With **Belgian Defense Cyber Force** for their regular participation in CMiB activities, as well as their unwavering support and continued trust, particularly in the context of this study.
- Our partnership with the **Belgian Cyber Security Coalition** demonstrates the power of collaboration in strengthening Belgium's digital resilience. By combining Agoria's industry reach with the Coalition's cross-sector expertise, we amplify awareness, foster trust, and accelerate the adoption of best practices across businesses of all sizes.
- The **POD**, in particular Bernard Hansen and Nicolas Brixko, for hosting the survey team on their premises during the final crunch period.

By pooling our networks and expertise, we make it easier for organisations to learn fast, comply smartly and invest on cybersecurity where it matters.

Finally, we **warmly thank the colleagues** within **Agoria** who contributed to this study. Work of this kind is always done on top of daily responsibilities, and everyone contributed very generously.

Executive sponsors (In alphabetic order)

- Agoria/Cyber Made in Belgium (CMiB)
- Belgian Defense Cyber Force
- Belgian Cyber Security Coalition
- Centre for Cybersecurity Belgium
- Women4Cyber

Financial Sponsors

MCG, Schneider Electric, Cegeka, Proximus NXT, Siemens, Toreon, Soterics.

Surveyed companies (In alphabetic order)

ACB - Advanced Circuit Boards, Aisin Europe, Anglo Belgian Corporation, Aseptic Technologies, Ateliers Vlassenroot, Atlas Copco Airpower, AUMOVIO Benelux BV, Aurubis Beerse, Automatic Systems, Azorg, Bodycote Hot Isostatic Pressing, C-Energy, Cegelec Fire Solutions, CGK Group, ClozDloop, CMC - Compressor & Machine Controls, CNH Industrial Belgium, Com&Sens, Comet Technics, Coor Service Management, Cyber Praxis, D. Cloostermans-Huwaert, Daf Trucks Vlaanderen, Daikin Europe, De Meyer, Deprez Construct, Diarotech, E.D.&A., ECS Corporate NV, Ellimetal, Enovos Green Power, Equans, Erea Energy Engineering BV, FixSus, FN Herstal, Fomeco, Full Metal Services, Galva PowerGroup, Geldof (Engicon NV), GET - General Engineering & Technology, Heinen Doors Belgium, Heraeus Electro-Nite International, Hubert De Backer, ICsense, JAC, JSR Micro, KNDS Belgium, Kopal, Lasea, Laser Cladding Venture, Libeert SA, Louis Blockx, LVD Company, Menerga, Metalen Verhoestraete, Neoceram, Nyrstar Belgium, Orfit Industries, Packo Inox Limited, Penne, Picanol, PTS Machining srl, Roxell, SABCA - Société Anonyme Belge de Constructions Aéronautiques, Scalable Solutions, Sedac – Mecobel, Sisa, Soleras Advanced Coatings, Space Applications Services, SPIE Belgium, Spiromatic, Starion Technologies, Steeno, Stûv, Swarco Belgium, TE Connectivity Belgium, Terumo Europe, Thales Alenia Space Belgium, VDL Klima Belgium, VDL KTI, Volvo Car Belgium, ZF Wind Power Antwerpen

Contributors (In alphabetic order)

CMiB4ICS/OT board members

Patrick Coomans, Laurent Deheyer, Erik De Nert, Jurgen De Wever, Samir El Makrini, Tatiana Galibus, Jasper Hooft, Grégorio Matias, Geoffroy Moens, Nick Peeters and Gerrit Neyrinck.

At Agoria

Study Department, Marketing & Communications, Senior Management & Board of Directors.

And more specifically, (in alphabetical order) Amira Alieldin, Sybille Dechanmps, Jan Gatz, Cassylinne Mees, Vaishnu Balakrishnan Sugumaran, Ann Peeters, Stanislas Van Oost, Eric Van Canghai, Conny Vandeweyer, Christophe Vantongelen and Alain Wayenberg.

External support

Design - Manuel Gonzalez Peña – Kyrielle SCom



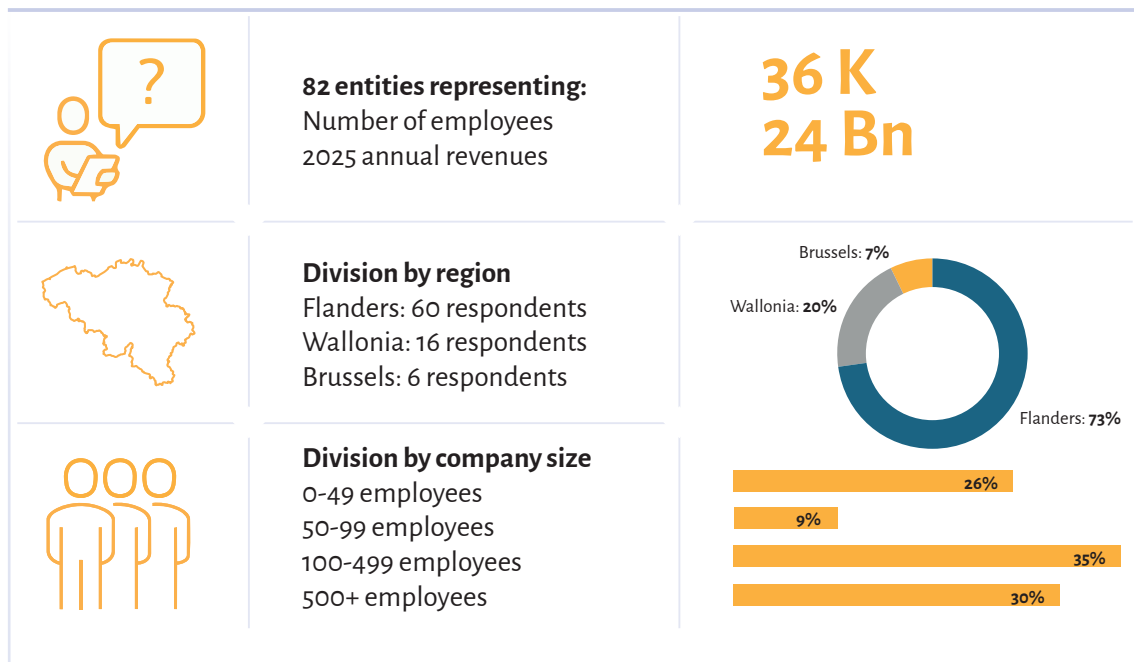
9. Methodology

To adequately represent the State of the Belgian industry concerning cybersecurity in Operation Technology (OT), we chose to create a quantitative survey to support our research. Most of the questions in the questionnaire are closed questions and few are open qualitative questions.

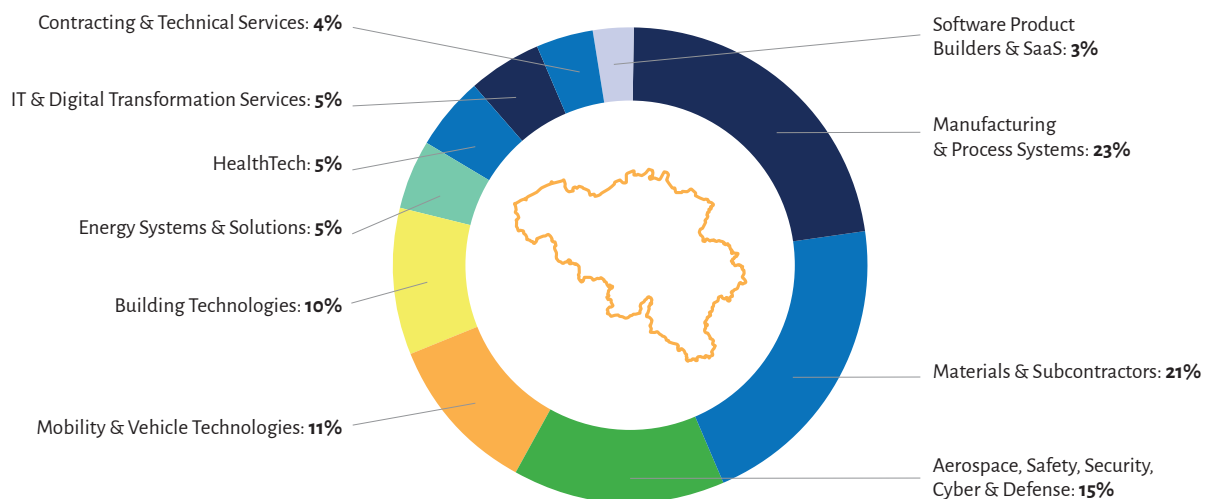
Survey

The questionnaire comprised **44 quantitative questions** that inquired about the role of respondent, the company, the equipment, the governance and the resilience status. The survey ran from 8 June to 17 July 2026.

Sample size



Sectors



Survey analysis process

The base used throughout the report. The survey collected 94 responses. **The analysis in this report is based on the 82 respondents who confirmed that they operate an OT environment.** Within these 82 respondents, not everybody answered every question. Each percentage in the report is therefore calculated based on the number of respondents who answered the specific question, which varies between 74 and 81. The base used is indicated with each figure.

Answers “Don’t know” are considered as not progressed and are not removed from the calculation. Removing them would artificially increase the positive results. When an indicator combines several controls, the result is calculated for each respondent: a company is counted only if all components are fully in place. This explains why combined figures are always lower than the individual figures.

Results for small subgroups, especially the regional **comparison, should be considered as an indication** of a trend rather than a confirmed difference because of the limited number of respondents. All answers are self-declared and were not independently verified.

Regulatory readiness.

For the regulatory sections, a separate scope analysis was made for each regulation. Based on the sector, company size and declared role in the OT value chain, each respondent received an estimated scope assessment for the Belgian NIS2 law, the Cyber Resilience Act (CRA) and Machinery Regulation.

This estimated assessment is then compared with the status declared by the respondent for the same regulation. The section reports the difference between these two views, and not only what the company declared.

When company size or role was not provided, the assessment is marked as “possible” instead of clearly in or out of scope. Company size is missing for 28 respondents and the role in the value chain for 30 respondents.

There are also some important limitations. Headcount is only one part of the EU company size criteria, while turnover and balance sheet information were not available in the survey. In addition, **this exercise is a research segmentation used to analyse the survey and should not be considered as a legal assessment.** For example, the final scope under NIS2 also depends on the registration and classification process with the CCB.

The leading pack - the best-in-class companies in OT cybersecurity.

The survey did not contain a predefined group of leading companies, so one was created for the analysis. Thirty survey questions were converted into a score between 0 and 1 and grouped into 7 maturity domains being:

- | | | |
|----------------------------------|--------------------------|-----------------------|
| ■ Protection controls | ■ Standards & frameworks | ■ Response & recovery |
| ■ Governance & culture | ■ Detection capability | |
| ■ Secure supply chain & patching | ■ Testing activities | |

Each domain score is the average of the available answers, and the overall score is the average of the available domains.

“Don’t know” and blank answers are excluded from the averages instead of being counted as zero. This avoids considering a lack of knowledge as automatically meaning that a control is not in place.

A respondent is included in the ranking only when there are at least 20 usable answers and at least 5 of the 7 domains are covered. In total, 68 of the 82 respondents meet these conditions. **The leading pack represents the top 10% of the OT base, meaning 8 companies selected from this ranked group.**

The two self-assessment questions about expected attacks and confidence in detection are not included in the score. This avoids giving a better score to companies simply because they are more confident about their capabilities.

Evolution over the last 5 years.

The following convention has been used for qualifying the evolution of the KPIs:

+++	Delta $\geq$ +30%
++	+20% $\leq$ Delta < +30%
+	+10% $\leq$ Delta < +20 %
$\approx$	-10% < Delta < +10%
-/--/---	mirror thresholds

References

- **Agoria. (2021) Cybersecurity in de maakindustrie - La sécurité industrielle dans l'industrie manufacturière**
<https://www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie>
<https://www.agoria.be/fr/etude-Cyber-securite-dans-industrie-manufacturiere>
- **Agoria. (2026) 10-Pager Cyber Security in Operational Technology (OT)**
<https://www.agoria.be/en/themes/industry-clusters/aerospace-safety-security-cybersecurity-defence/cyber-made-in-belgium-cmib/cybersecurity-for-icsot/cybersecurity-in-ot-a-practical-guide>
()See QR Code below*
- **Centre for Cybersecurity Belgium (CCB). (2026) CyberFundamentals Framework 2025 — mappings to ISO/IEC 27001, ISO/IEC 27002, IEC 62443, CIS Controls and NIST CSF 2.0**
<https://cyfun.eu/en/cyberfundamentals-framework-2025>
- **Chancellery of the Prime Minister of Poland. (2026) Poland Stops Cyberattacks on Energy Infrastructure**
<https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure>
- **Dragos. (2024) 6th Annual OT Cybersecurity Year in Review**
<https://www.dragos.com/resources/press-release/dragos-ot-cybersecurity-year-in-review-reports-rise-in-geopolitically-driven-attacks-ransomware-and-threat-groups>
- **MITRE ATT&CK (2026)— Anthropic AI-orchestrated Campaign (COO62)**
<https://attack.mitre.org/campaigns/COO62/>
- **Reuter. (2025) Collins Aerospace working on restoring software for airlines hit by cyberattack**
<https://www.reuters.com/business/aerospace-defense/collins-aerospace-working-restoring-software-airlines-hit-by-cyber-attack-2025-09-24/>
- **SANS. (2025) State of ICS/OT security 2025**
<https://www.sans.org/white-papers/state-of-ics-ot-security-2025>
- **TXOne Networks. (2026) 2026 Annual OT/ICS Cybersecurity Report**
<https://www.txone.com/security-reports/annual-ot-ics-cybersecurity-report-2026/>
- **WEF. (2026) Global Cybersecurity Outlook 2026**
<https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/executive-summary-6efae97d74/>



Sponsors

AGORIA



Cyber Made in Belgium executive partners



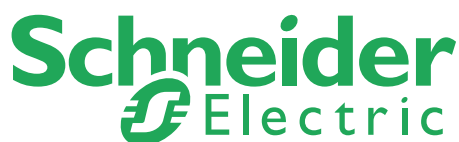
CENTRE FOR
CYBERSECURITY
BELGIUM



CYBER SECURITY
COALITION.be



Cyber Made in Belgium financial sponsors



Disclaimer

Agoria makes every effort to collect and share qualitative and up-to-date information, but cannot guarantee the full accuracy or completeness of the information provided. This information is in no way intended as personalised legal or other advice. Agoria disclaims any responsibility for the content of the report or the use that might be made of it. The reader or user is also aware that this information is subject to change without notice.

© Agoria 2026

About Agoria

Technology federation Agoria unites more than 2,250 Belgian businesses, 70% of which are SMEs. Together, they represent approximately 340,000 employees. They all have one ambition in common: strive for progress in the world, through the development or application of innovative technologies.

Agoria, which counts 200 employees, aims to connect all those inspired by technology and innovation, increase their success, and shape them in a sustainable way. Its service focuses on digitisation, the manufacturing industry of tomorrow, talent policy and training, market development, regulation, infrastructure, climate, environment and energy.

Find out more at agoria.be

About CMiB4ICS/OT

Cyber Made in Belgium for Industrial Control Systems and Operational Technology (CMiB4ICS/OT) is the focus group dedicated to industrial cybersecurity within Cyber Made in Belgium, the cybersecurity Business group / community of Agoria. It brings together solution providers, system integrators, machine builders, asset owners and experts who share one concern: the security of the systems that run physical production.

OT cybersecurity is not IT cybersecurity applied to machines. Availability and safety come first, equipment stays in service for twenty years, and conformity must be demonstrated on the production floor. CMiB4ICS/OT translates that reality into practical guidance for Belgian industry, in close collaboration with the Centre for Cybersecurity Belgium, Sirris, the Cybersecurity Coalition and the academic world.

Find out more at www.agoria.be/cmib

About the Centre for Cybersecurity Belgium

The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. Operating under the authority of the Prime Minister, it coordinates the national cybersecurity strategy, detects and responds to threats through the national CSIRT (CERT.be), and informs citizens and organisations through Safeonweb. It is also the authority that supervises the entities falling within the scope of the NIS2 directive in Belgium.

The CCB developed the CyberFundamentals Framework (CyFun®), which offers organisations a proportionate and measurable way to demonstrate their cyber resilience. Its 2025 edition comes with self-assessment tools, policy templates and correspondence tables between frameworks. That last element matters for industry: it lets a manufacturer build on the work already done instead of starting again for every obligation.

Find out more at www.ccb.belgium.be

About the Ministry of Defence

The Belgian Ministry of Defence has created the Belgian Cyber Force to defend military weapon systems and support operations against cyber threats. It constitutes a rapidly expanding civilian and military environment that creates close synergies with the public and private sectors, industries and academia. The Cyber Capacity houses experts in every cyber security domain imaginable, but also – and this is unique in Belgium – experts in offensive cyber operations.

Together with various national and international stakeholders and with the academic, industrial and non-profit sectors, the Belgian Cyber Force works every day to strengthen Belgium's national resilience.

Find out more at www.mil.be/en/about-belgian-defence/belgian-cyber-force/

About the authors



Eric Van Cangh

*Senior Business Group
Leader Digital*

+32 492 23 24 34
Eric.vancangh@agoria.be



Alain Wayenberg

*Business Group Leader Manufacturing
& Process Systems*

Alain.wayenberg@agoria.be



Stanislas Van Oost

*Senior Cyber
Security consultant*

Stanislas.vanoost.ext@agoria.be



Ann Peeters

Project Leader Studies Center

Ann.peeters1@agoria.be

Embracing technology
Embracing ambition

 **AGORIA**



Agoria means progress through technology. We are paving the way for all technology-inspired companies in Belgium pursuing progress internationally through the development or application of innovations and which, together, represent some 340,000 employees. We are proud that more than 2,250 member companies trust in the three pillars of our services: consulting, business development and the creation of an optimal business environment. Follow us on www.agoria.be and <https://X.com/agoriafr> or <https://X.com/agorianl>

www.agoria.be

© September 2026