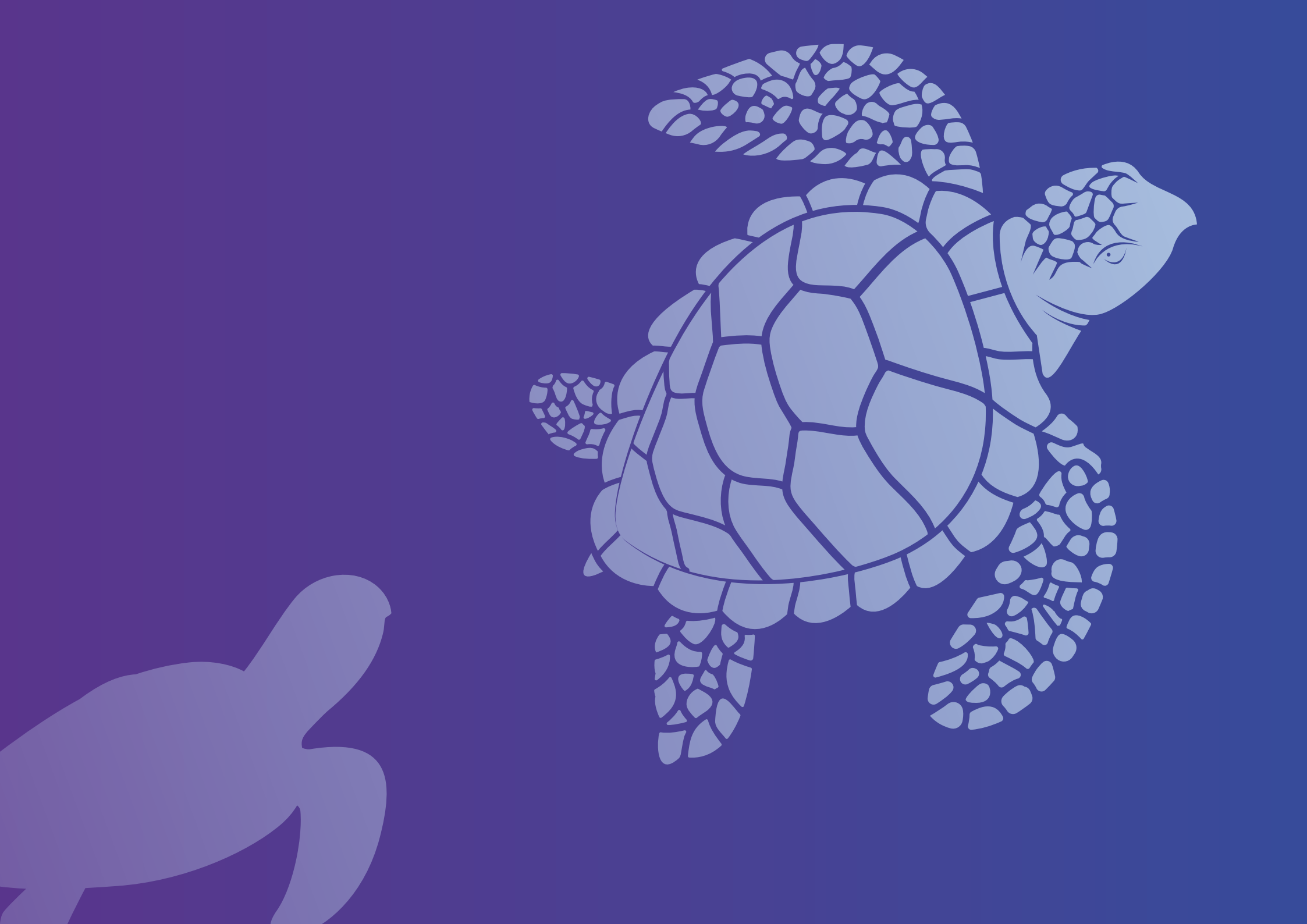
KPMG | CYBER SECURITY COALITION.be

Cybersecurity in Belgium 2026

Every link matters

KPMG. Make the Difference.

September 2026



Foreword KPMG

Sovereignty decides

Digital transformation opens up new opportunities for growth, innovation and efficiency. And so the turtle that graces our cover this year symbolically dives into the digital world, using agents for its propulsion. At the same time, the attack surface for companies is growing: cyberattacks today hit not only IT systems but business processes, supply chains, and our trust. Artificial intelligence (AI) acts as an accelerant; it enables new forms of automation but equally changes the dynamics between attack and defense. In parallel, digital sovereignty is moving into focus: those who cannot control core data, platforms, and dependencies lose their options for action when it matters most.

The second edition of our Cybersecurity in Belgium 2026 report, produced with the Belgian Cyber Security Coalition and with the support of Agoria, offers a practical framework for understanding how these three key themes, digitalization, AI, and digital sovereignty, fit within modern corporate governance.

Cybersecurity is a leadership task

For Belgian organizations this means one thing above all: cybersecurity must be firmly anchored in decisions, priorities, and governance structures. Cyberattacks are not an exceptional event but a permanent business risk, with consequences for availability, integrity, and confidentiality. The use of AI increases the speed and complexity with which risks evolve and at the same time places new demands on governance. Digital sovereignty adds to the question of how dependent we are on technologies, providers, and jurisdictions and which alternatives are realistically available in a crisis. What matters is not a flurry of initiatives, but the ability to demonstrate that the organization is in control.

Orientation instead of alarmism

This study is intended to help classify developments and sharpen the right questions for steering cybersecurity: Which critical processes must remain operational even under pressure? Where do new risks arise from AI-supported automation and from information that is difficult to verify? And how can digital sovereignty be shaped so that freedom of choice, compliance, and resilience exist not only on paper?

In the following chapters, you will find no alarmist rhetoric, but a structured basis for strategic discussions, prioritization, and effective implementation, with a focus on direction, responsibility, and long-term resilience.

A big thank-you goes to the many participants who took part in our survey and once again answered our questions this year, as well as to everyone who supported us in interviews. Only with your help is it possible to publish the cybersecurity study for Belgium in 2026 once again at this scale and quality!

We wish you a stimulating read and helpful impulses for the further strategic direction of your organization.

Benoit Watteyne
Partner
KPMG Cybersecurity Services

Benny Bogaerts
Partner
KPMG Cybersecurity Services

Our cooperation partners

We would like to thank our cooperation partners for their contribution to this study. The study was conducted in collaboration with the Belgian Cyber Security Coalition and with the support of the CCB and Agoria.

CYBER SECURITY COALITION.be

.AGORIA

CENTRE FOR CYBERSECURITY BELGIUM

Foreword Cyber Security Coalition

Cybersecurity is a business imperative

Cybersecurity is no longer a matter for specialists alone. It has become a defining factor in how organizations operate, innovate, and build trust in an increasingly interconnected world. The findings of this second edition of the Cybersecurity in Belgium study confirm that cyber risk is firmly established as a business risk that demands attention at every level of the organization, rather than being treated as an exceptional event. Rising professionalized attacks, growing supply chain dependencies, geopolitical tensions, evolving regulatory requirements, and the rapid adoption of artificial intelligence are reshaping the environment in which Belgian organizations operate and compete.

The results of this study are both encouraging and sobering. On the one hand, awareness continues to grow. More organizations are investing in cybersecurity, strengthening governance, improving incident reporting, and taking concrete steps to enhance resilience. On the other hand, significant challenges remain. Supplier risk has become a major concern, digital sovereignty has emerged as a strategic issue, and many organizations are still working to translate regulatory obligations into sustainable operational practices. Perhaps most strikingly, almost one in five respondents experienced a successful cyberattack causing disruption or damage over the past year.

Resilience is a collective endeavor

One of the clearest messages emerging from this year's survey is that resilience cannot be achieved in isolation. The security of an individual organization increasingly depends on the security of its suppliers, partners, and wider ecosystem. Collaboration, information sharing, and collective preparedness are therefore more important than ever. This conviction has guided the Cyber Security Coalition since its creation and remains at the heart of our mission.

The study demonstrates that Belgian organizations recognize the value of cooperation. Whether managing supply chain risk, implementing NIS2 requirements, responding to cyber incidents, navigating the opportunities and risks of artificial intelligence, or countering the growing impact of mis- and disinformation, success depends on strong partnerships between industry, government, academia, and the wider cybersecurity community.

Building Belgium's cyber future together

We would like to sincerely thank all organizations and professionals who participated in the survey and shared their experiences, insights, and concerns. Their contributions make this study possible and create a valuable benchmark for Belgium's cybersecurity maturity, challenges, and priorities.

We hope this report will stimulate meaningful discussions, support informed decision-making, and encourage stronger cooperation across our community. Cyber resilience is not a destination but a continuous journey. By learning from each other, sharing expertise, and working together across sectors, we can strengthen Belgium's collective resilience and build a safer, more trusted digital future for all.

Karine Goris
President of the Cyber Security Coalition

Contents

Introduction

The illusion of calm

A trend that has emerged in recent months and will presumably continue into the future is the change in how cyberattacks are carried out and the signals with which they appear. Whereas in the past an attack was relatively loud (e.g. ransomware that very quickly brought the organization to a standstill), cyberattacks are now becoming increasingly quiet. But quiet is not a sign of relaxation; rather, it is a clear indication that cyberattacks are becoming increasingly professionalized, sophisticated, intense, and complex.

Quiet attacks underline once more that we are no longer dealing exclusively with classic organized crime. We are experiencing phenomena that occur in combination, such as state or state-sponsored actors working with intelligence or secret services. Perpetrators today act strategically through espionage and information gathering against research, public, and industrial institutions, but also with disinformation campaigns designed to undermine our trust in institutions and information.

They all have one thing in common: they work more quietly, more patiently, and with a longer horizon. Their success is measured not primarily by quick ransom payment, but by lasting, persistent access. Especially when we think of export-oriented countries like Belgium, with a strong industrial base, high innovation density, and tightly interwoven supply chains, this is no longer an abstract threat. It is a threat that affects competitiveness, challenges the attractiveness of the business location, and at its core raises the question: what remains reliable when systems, data, and decisions come under the pressure of cyberattacks?

More efficient, better, faster?

The past 12 months have shown us that no area has been left untouched when it comes to cybersecurity and technological development. AI has driven rapid change which, on the one hand, has brought significant benefits by enabling us to automate tasks and perform them more efficiently and given us much more freedom in how we handle them. On the other hand, it has also shown us how quickly we are at the mercy of attackers. In the long term, AI tools may make the world safer, but in the short term the currently available models create a "Wild West" scenario. The Zero-Day Clock vividly shows the time it takes from the discovery of a vulnerability to its exploitation. In 2025 it was still 23.2 days; in May 2026 we were at 10 hours.

This factor (one fifty-sixth) means we have arrived in a new reality. A reality we have consciously created for ourselves because it makes us faster, more efficient, and more capable. Yet it is precisely this reality that exposes us.

Handing over the helm

Beyond that, we have also decided to surrender our decision-making competence further and further. We let the machine decide for us, including all the consequences that come with it. We are seeing that hallucinations remain the order of the day and that autonomous systems cause ever more headaches when they delete our data and information. But at least they remain polite about it and apologize afterwards for having done so.

This is exactly the world we have created. A world in which we have shown attackers how quickly we are vulnerable today. In the race against cybercriminals, we have fallen back many places and the momentum clearly lies with the attackers.

Defeating automation with automation

Autonomous systems can already carry out attacks independently and completely. While this is currently confined to laboratory environments, and such environments do not fully reflect the realities of a company with all its dependencies and complexities, the recent Hugging Face incident has shown that autonomous hacking is already a reality today.

What does that mean for us? We must counter automation with automation and automate tasks that are still performed manually or require significant coordination. Is that always easy? No. But this shift in thinking is necessary for organizations. Seemingly unremarkable measures, such as maintaining good cyber hygiene across the infrastructure, become a lifeline. Organizations must be able to respond more quickly to potential cyberattacks, not only to meet regulatory reporting obligations. Automated responses to cyber incidents should also become standard practice.

Too late, too slow, too comfortable?

Automation and AI are not the answers to all

problems; they are solutions but can also create problems at the same time. This rethinking must take place not only among companies but also among manufacturers. At present, security is very often tied to manufacturers' specifications to meet guarantee and warranty requirements, which permit only certain software version levels. Given the current dynamics, this is no longer viable in the long run. In other words, cooperation is therefore needed on all sides to find a solution. Speed is the top priority for everyone.

Attacks succeed where defense is too late, too slow, or too comfortable. That is no reason for alarmism, but a good reason for cybersecurity to mature. In the end it is as it so often is: those who play for time in the face of such developments, will eventually be overtaken by the pace. The threat is not new. What is new is the speed at which we now have to explain why it has once again been underestimated.

Trust becomes a decision criterion

Finally, greater trust in AI is needed, especially when it comes to the integrity and immutability of information. We will have to conduct this integrity debate more intensively than ever over the next twelve months because, despite the advantages AI offers for making autonomous decisions, it can on the flip side also alter existing information.

At this point, the appeal is this: we should not always regard AI as the miracle tool par excellence. Notwithstanding its many strengths, at the end of the day these are simple algorithms and processes that we already know from the past and that are now, dressed up with a new ribbon, presented as promising cure-alls. Even the most conventional medicines have side effects, for which one must consult the package leaflet, doctor or pharmacist.

Exactly the same is necessary in the field of AI. Agent-based systems can completely undermine a well-intentioned network segmentation at a stroke, throwing us back into flat structures and thereby disabling our existing cybersecurity and risk management measures.

Digital sovereignty put to the test

We have arrived in an age in which establishing who is on the other side is becoming increasingly difficult. AI, in the form of deepfakes, is making a significant contribution to this trend. At the same time, new vulnerabilities are being identified in systems that were previously unknown. In other words, the exclusive targeting of humans as the entry point is shifting; instead, technological vulnerabilities in both hardware and software are coming into the crosshairs.

Technology is also moving to center stage at another level, as technological progress requires innovation, competencies and sovereignty in the digital domain. It is precisely this sovereignty, or the lack of it, that challenges us. The power-projection capabilities of technology companies and platform operators, whether from East or West, hold up a mirror to Europe's digital position: Belgium and Europe remain significantly dependent on technologies and ecosystems that are increasingly influenced by geopolitical developments.

In a tight spot

In cybersecurity we recognize three fundamental protection objectives: confidentiality, which concerns keeping information inaccessible to third parties; integrity, which refers to the accuracy, immutability, and trustworthiness of data and is coming under increasing pressure, particularly from AI; and availability of information, which is gaining renewed importance in the context of digital sovereignty.

At first glance, digital sovereignty may appear to be primarily a technology-policy topic. On closer inspection, however, it becomes clear that it has a direct impact on cybersecurity, in particular on the protection objective of availability. If services, platforms and cloud solutions become unavailable from one day to the next, companies face significant operational and existential challenges.

Such unavailability may result from technical failures, but it can also be used as an instrument of geopolitical influence or power projection. Recent examples in Europe have demonstrated how quickly personal displeasure can lead to individuals or entire institutions being completely denied access to technologies. The same effect may also occur through economic means, for instance when license or subscription costs for individual regions or countries are significantly increased, often in connection with political pressure. And switching to an alternative provider is not something companies can accomplish overnight. Digital sovereignty is therefore more than a pure technology topic. It is a topic of resilience, of security and of the long-term viability of Belgian organizations.

> "Cybersecurity is the conscious decision to put reliability above convenience, traceability above mere speed and responsibility above technological novelty."

Stormy seas

As a society, we are learning that the operating environment is becoming increasingly challenging as a result of technological innovation and the constantly evolving nature of cyberattacks. To strengthen resilience and limit the impact on society, value chains, and supply chains, legislators and regulators are responding with a growing body of regulation. This is reflected in the Cybersecurity Act (and its future evolution as CSA2), DORA for the financial sector, NIS2 for essential and important entities, the Cyber Resilience Act (CRA) for product manufacturers, the Critical Entities Resilience Directive (CER), and the AI Act. Together, these initiatives aim to enhance resilience, improve security, and foster trust in digital technologies among organizations and the public.

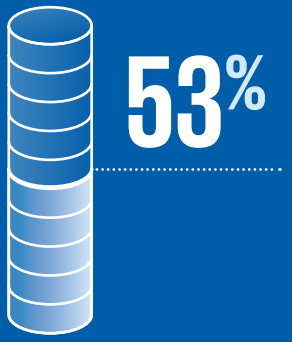
For some organizations, meeting these requirements is a substantial undertaking. It is nonetheless the logical consequence of a digital economy in which local instability can propagate rapidly and a single dependency can disrupt an entire chain. Regulation exists to contain that propagation. It becomes effective only when organizations understand what is expected of them and when regulators apply the rules in a proportionate and pragmatic manner. With these requirements, cybersecurity moves from a technical discipline governed by standards to a legal obligation governed by supervisory authorities.

Trust, reliability and sovereignty

One thing is clear: the requirements imposed by regulation are demanding. However, they are requirements that companies can and must fulfil and they remain far removed from any excessive demands (the often overused "gold-plating"). Rather, the aim is to enable the proper, secure and stable operation of digital network and information systems and of critical (digital) infrastructures. The fact that shortcomings from the past, often referred to as "digital debt", cannot be resolved overnight and may at times conflict with the digitalization initiatives that organizations pursue with agility and an innovative mindset, is beyond dispute.

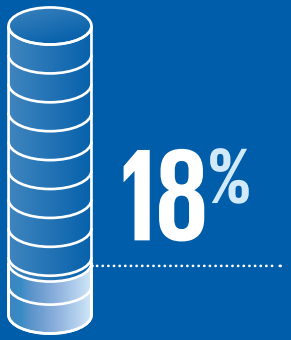
Perhaps that is the real lesson of this era: not every crisis announces itself loudly. Some emerge quietly, in small shifts, in dwindling reliability, in decisions that still appear plausible even though their foundation has long since become fragile. A digital society rarely fails because of what it cannot do, but because of what it has relied on too carelessly for too long. That is precisely why cybersecurity today is more than protection against attacks. It is the conscious decision to put reliability above convenience, traceability above mere speed and responsibility above technological novelty.

Key findings 2026



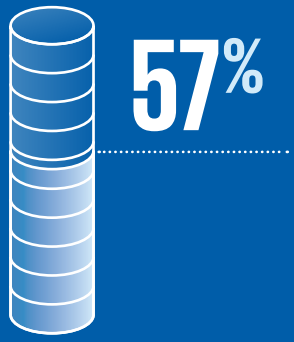
53%

report that cyberattacks against them increased over the past twelve months, marking the second consecutive year in which this figure reached 50% or more.



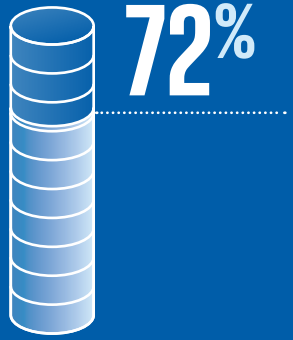
18%

roughly every sixth organization, suffered at least one successful cyberattack causing disruption or damage.



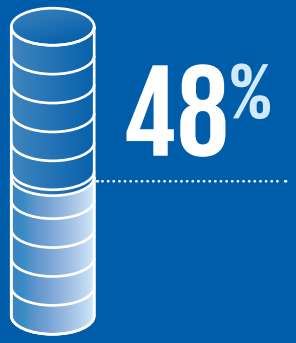
57%

saw a service provider or supplier fall victim to a cyberattack, or suspected it; supply chain attacks jumped from #11 to #3 in the cyber-risk ranking.



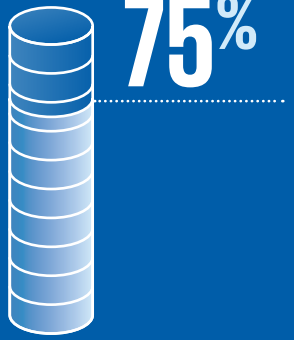
72%

of NIS2-scoped organizations describe their implementation as at least advanced, yet only 3% call it complete, down from 13% last year.



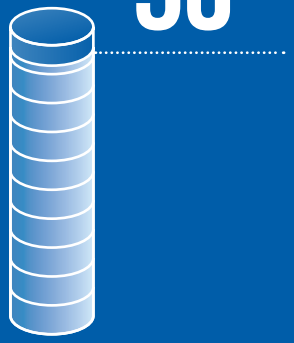
48%

lack a transparent cybersecurity budget: 22% of organizations report having no dedicated cybersecurity budget, while a further 26% are unable to state what their budget is.



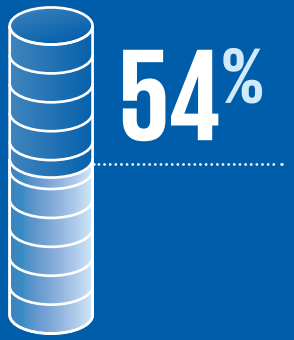
75%

source their cybersecurity applications from abroad, one of the two most import-dependent technology categories.



93%

agree that AI makes it easier to carry out cyberattacks, while 62% expect AI to markedly improve their own defense in the coming twelve months.



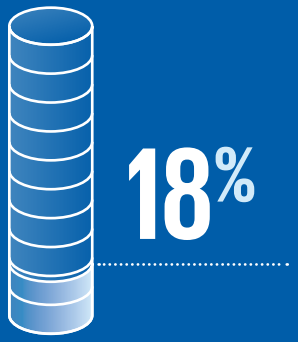
54%

believe their business activities can be influenced by online disinformation campaigns, up 22 points in one year.

01

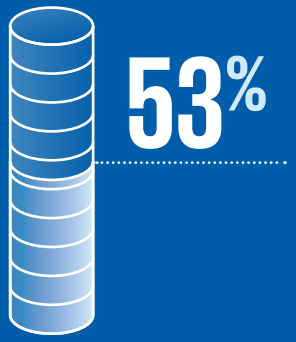
Review of the current threat landscape

At the center of cyberattacks on Belgian organizations this year are the increasing frequency of attacks and the speed at which they evolve. Alongside artificial intelligence, geopolitical conflicts are key drivers. Companies' ability to detect incidents is more important than ever before – because without the awareness that an attack has taken place at all, it is impossible to respond appropriately to it.



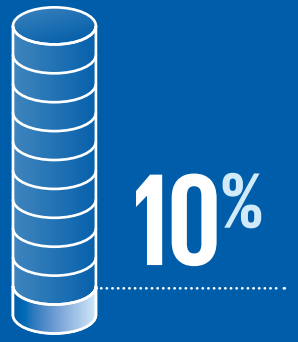
18%

have experienced a successful cyberattack in the past 12 months that resulted in a disruption or damage.



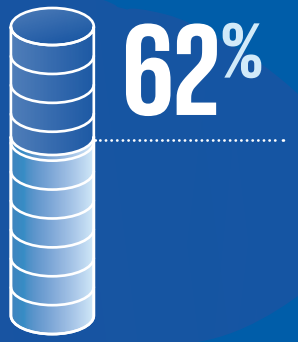
53%

report an increase in cyber attacks, the second year above fifty percent; barely 2% report a decline.



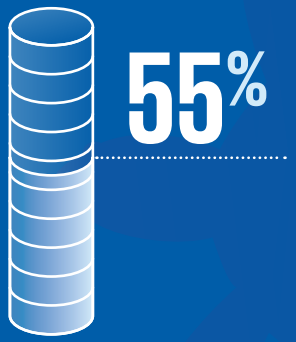
10%

do not know whether they suffered successful attacks.



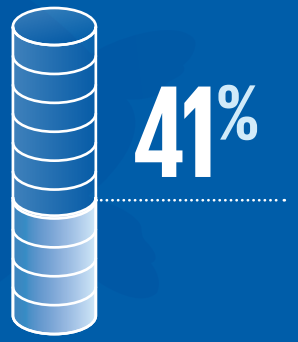
62%

of affected organizations report incidents to CERT.be/CCB, double last year; only 15% file no report at all.



55%

could not determine where attacks came from.



41%

attribute attacks to organized crime, and 27% name their own suppliers as the actors

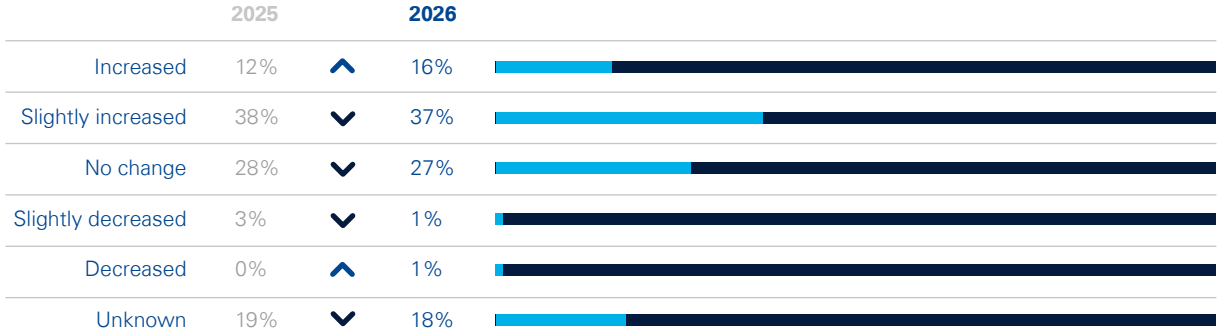
Review of the current threat landscape

Development of cyberattacks

Cyberattacks on Belgian organizations have again increased significantly over the past 12 months, even though they were already at a high level. More than half of the respondents say that cyberattacks on their company have increased strongly or somewhat. For 27 percent the number of cyberattacks has remained constant. Interestingly, almost one in five (18 percent) cannot assess the development compared with last year. The responsible units and people lack comparative figures or insight into the previous year's cyberattacks, or any current risk and situational picture of cyberattacks at all. This frequently points to gaps in measurement and detection capability (e.g. logging, monitoring, defined security events).

The time has long since come for companies to engage in depth with the well-known attack vectors such as malware via email attachments, identity theft and social engineering, but also with vulnerability management, penetration testing, OT-specific challenges and reporting and training. And we must not forget that all these attack vectors will gain a new dynamic over the coming 12 months through the use of AI.

Fig. 1: Change in attacks, 2025–2026.



Reasons for the change in cyberattacks

The geopolitical situation is still one of the main reasons for the change in cyberattacks compared with the previous year. Another reason appears to be the changing threat landscape for companies. At the same time, we see that AI is regarded as a driving force lifting attacks to a new level, above all through better scaling and higher quality of social engineering campaigns (e.g. (spear) phishing, multilingual and context-rich), identity impersonation (e.g. deepfake voice) and automation of reconnaissance/OSINT. This phenomenon is connected with changing phishing attacks, new forms of business email compromise, but also with attacks on the supply chain.

Attempted cyberattacks on Belgian organizations

Almost three quarters of respondents reported that they had not experienced a successful cyberattack resulting in disruption or damage. By contrast, 18 percent indicated that their organization had suffered damage from a successful cyberattack, compared with 16 percent in the previous year. While this represents only a slight increase, it means that almost one in five organizations experienced a successful attack in 2026, keeping the overall level relatively high.

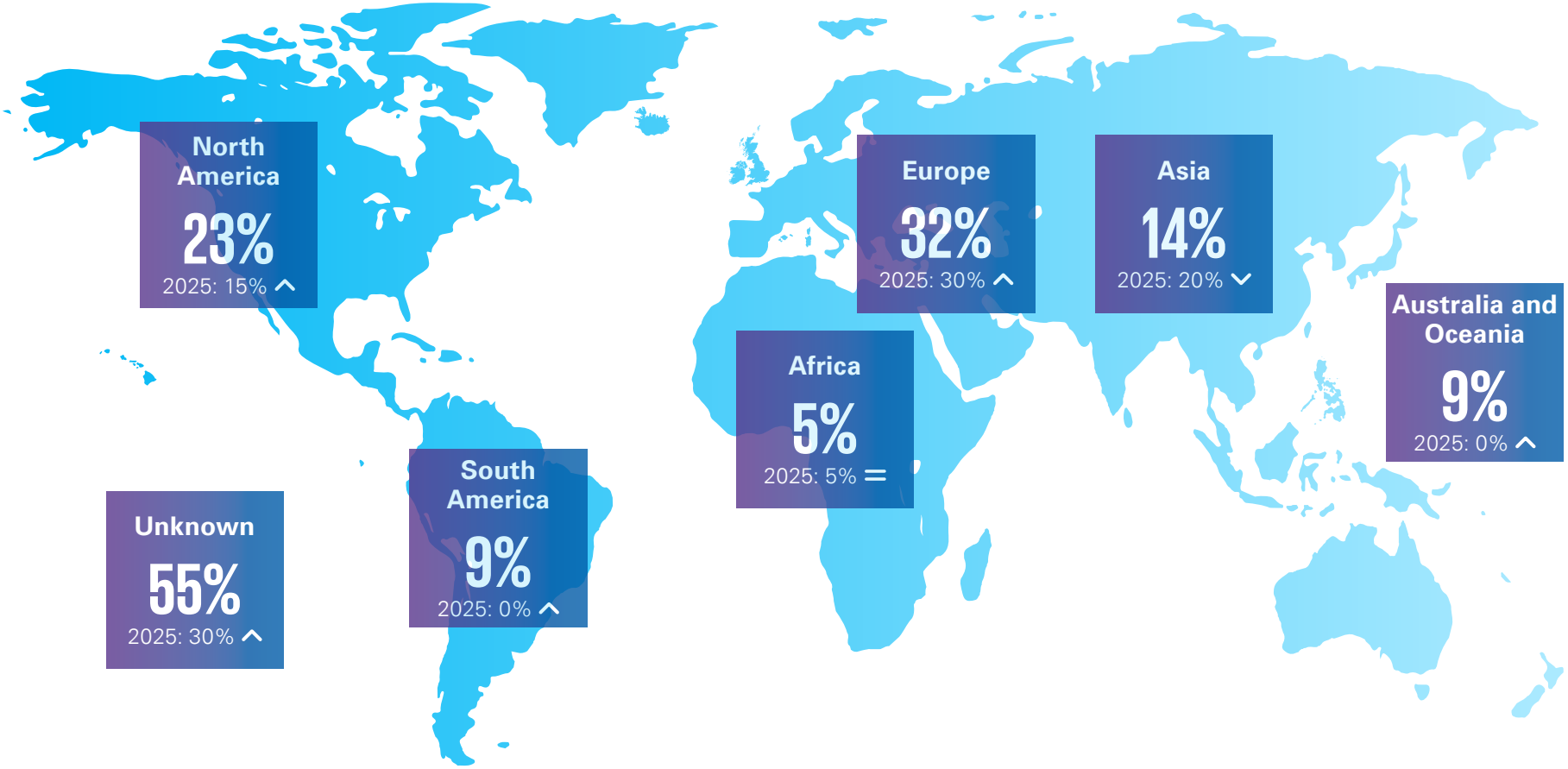
A further 10 percent do not know whether harmful attacks on their company occurred. This grey area has decreased slightly compared with last year but is still alarming: those who do not know whether attacks are being carried out against their own company can hardly protect themselves against them. Typically, core foundations are then missing, such as complete logging, central analysis/correlation and a clearly defined incident response process.

The actors behind the attacks

The phenomenon of organized crime (41 percent) dominates compared with last year when it comes to the question of which actors the attacks originate from (+13 percent). We also see a professionalization of attackers in disguising their identity: a third of affected organizations (32 percent) were unable to identify them (-1 percent). It is also interesting that state or state-sponsored actors have hardly been identified this year (–28 percent). Instead, 27 percent of affected organizations name their own suppliers as the actors behind the attacks they suffered. Whether as compromised attack vectors or as the source of the incident itself, the third party has moved from the risk register into the actor list. However, these findings are often based on initial indicators rather than definitive evidence, as robust attribution generally requires telemetry, threat intelligence, and forensic analysis.

The prevailing attack vectors will gain a new dynamic over the coming 12 months through the use of AI.

Fig. 2: Origin of the attacks, with year-on-year trend.

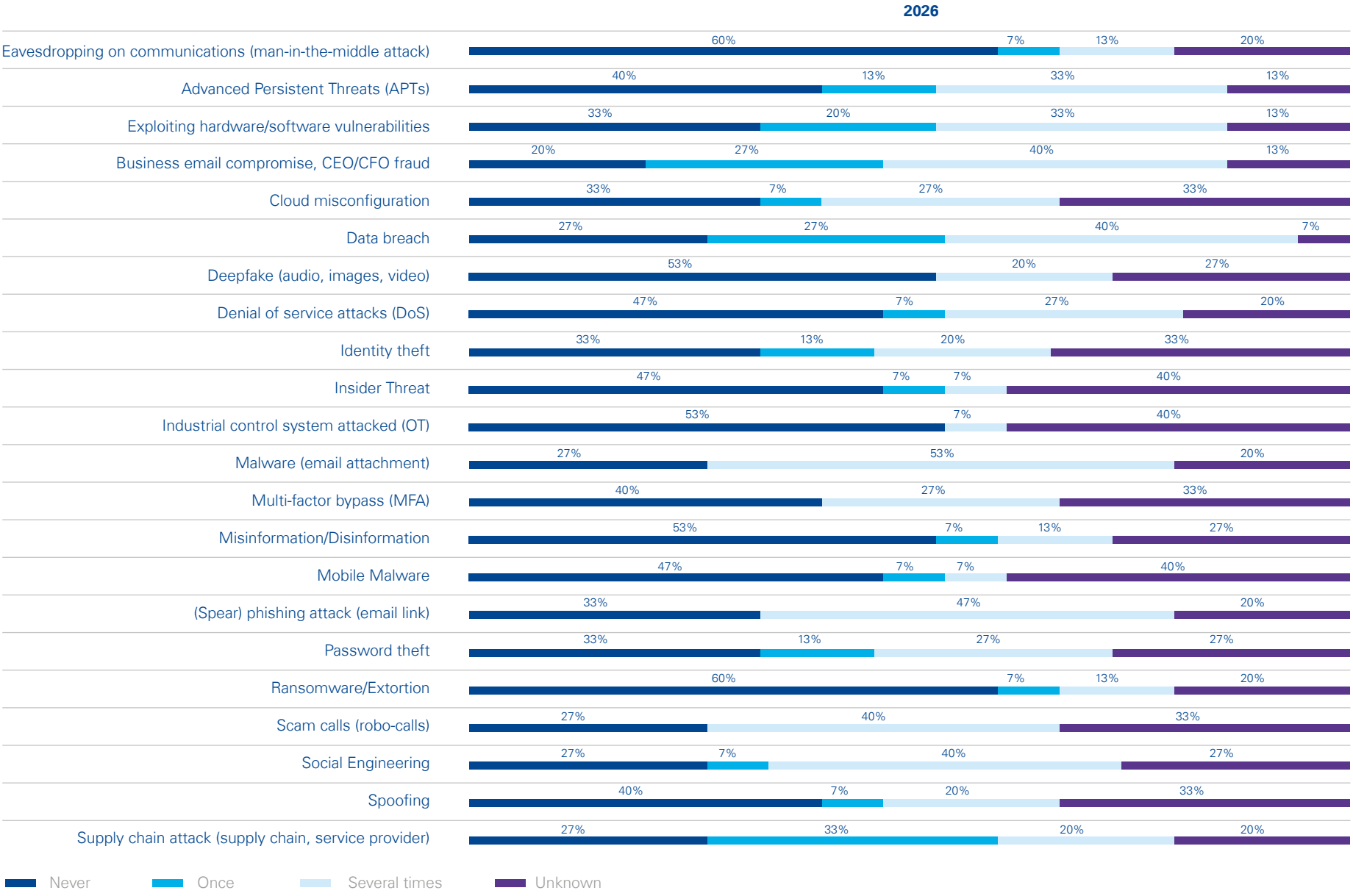


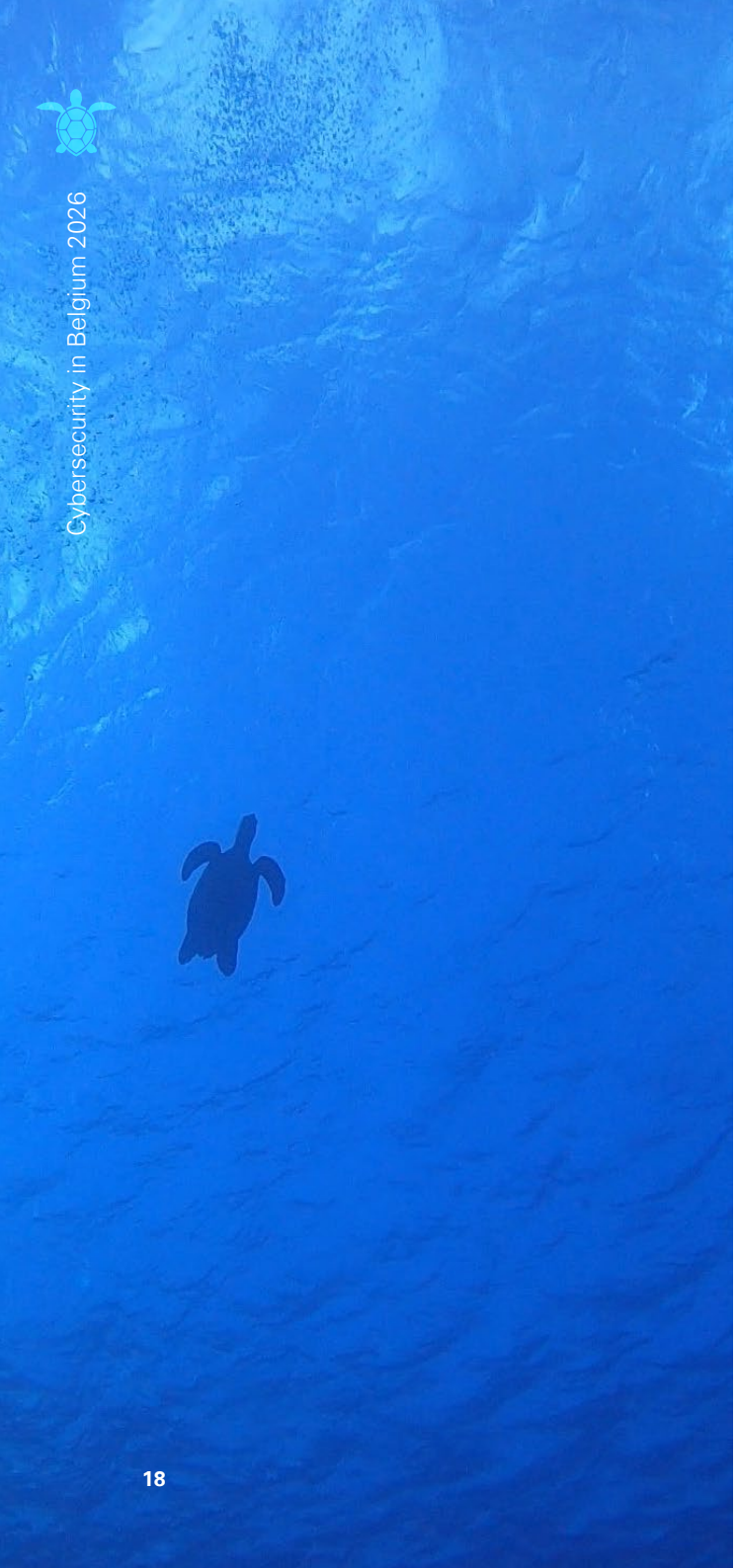
2025 and 2026 use different measurement bases; rank movements are indicative and the values are not directly comparable.

The origin of the perpetrators

Two trends are emerging regarding the origin of the perpetrators. Importantly, the reported "origin" in many cases describes the location of the attack infrastructure used (e.g. botnet nodes, proxy servers, rented cloud systems) and not necessarily the actual origin of the perpetrators. At 32 percent, attacks from the European region are perceived most strongly (+2 percent). 23 percent of attacks come from North America (+8 percent). 14 percent come from Asia (–6 percent). A striking finding is that more than half of respondents were unable to determine the perpetrators' country of origin. This highlights the continuing challenge of attribution in today's threat landscape, where attackers increasingly rely on distributed infrastructure and anonymization techniques to conceal their location and identity.

Fig. 3: Frequency of attack types over the last 12 months, 2026.





Dominant threat picture 2026: data breaches and business email compromise

Comparing this year's results with our first edition, the most reliable signal of change comes not from incident counts but from how organizations rank their risks and there the movement is unmistakable. Data breaches and business email compromise hold the top two positions for the second year running, confirming that data and payment fraud remain the risks survey respondents fear most. Underneath that stable top, the map has reorganized: supply chain attacks, ranked eleventh in 2025, jump to third place in 2026, the largest movement in the ranking, while denial of service attacks fall from sixth to tenth. The loud, disruptive attack is fading from the risk picture; the quiet compromise via a trusted third party has taken its place.

The reported attack experience points in the same direction. Among the organizations that detailed the attacks they suffered, business email compromise and data breaches were the most widespread, each experienced by two thirds. Supply chain attacks, malware via email and the exploitation of software vulnerabilities follow, each affecting more than half, with phishing, social engineering and advanced persistent threats close behind. Notably, the attack types that dominate the experience data are the same ones rising in the risk ranking, indicating a strong alignment between perceived and observed risks.

Shifts versus 2025: less "loud", more "targeted"

The practical conclusion is unchanged from last year but sharper: when the threat shifts from noisy disruption to targeted compromise of identities, configurations and suppliers, access controls, configuration hygiene and continuous monitoring become the decisive levers. This year's findings also show that these measures must extend beyond the organization's own perimeter to the third parties on which it depends.

Recurrence as a core finding of 2026: "several times" as the normal case

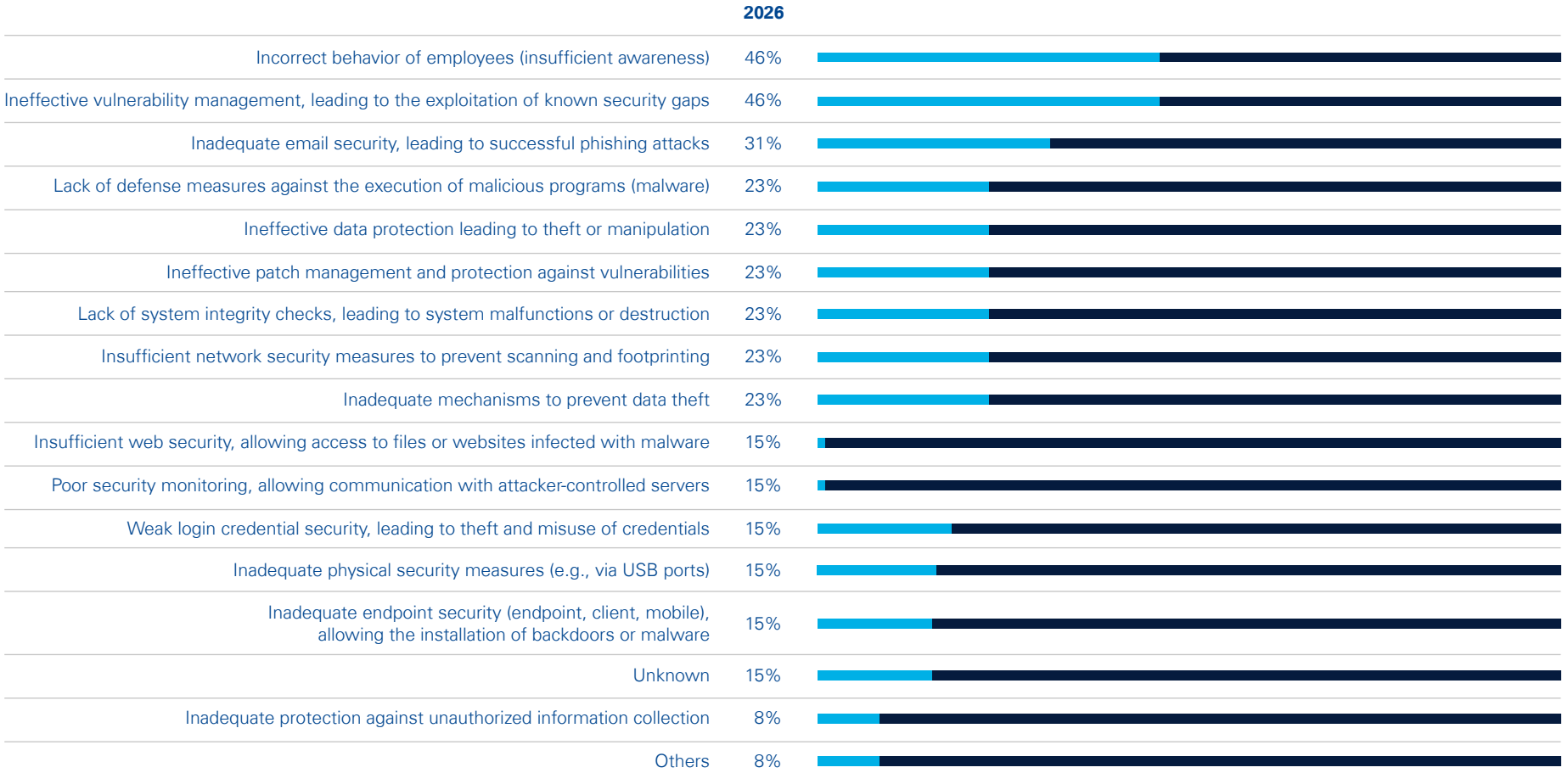
The survey also shows that "several times" is a frequent pattern in several categories (including scam calls, phishing and malware). Companies should therefore plan for recurring serial attacks and scale their capabilities for detection, response and restart (incident readiness and recovery) accordingly.

Classification and implications for 2026

For practice, the survey results point above all to the following priorities: (1) Email and social engineering remain the largest attack surface: awareness, technical email protection mechanisms and clear anti-fraud processes should be implemented as a package. (2) Expand identity protection: harden IAM, priorities phishing-resistant MFA and risk-based access controls (including device/session controls). (3) Secure cloud operations: establish binding baselines, continuous configuration and entitlement controls (e.g. CSPM/CIEM) and end-to-end logging/monitoring. (4) Design for recurrence: set up detection and response (SOC use cases, automation) and recovery processes so that serial attacks remain operationally manageable.

In summary, 2026 is not a year of simply more attacks, but one of professionalization: more exploitation of real vulnerabilities, greater focus on identities and cloud environments, and a more campaign-driven character, while attribution continues to decline. This can only be managed effectively as an integrated program: continuous exposure management, identity-first security, cloud guardrails and well-rehearsed recovery and crisis exercises.

Fig. 4: Causes of successful attacks.



High success rate

Two causes share first place. Incorrect behavior of employees, insufficient awareness, typically exploited through social engineering, and ineffective vulnerability management, leading to the exploitation of known security gaps, are each cited by 46 percent of affected organizations. The human factor thus remains central, but in Belgium it is far from the only issue. Just as often, the door was already open: a known vulnerability that had been identified but was never prioritized based on its exploitability or remediated. Adequate transparency about one's own exposure is indispensable and the lack of such visibility can be just as significant a cause of compromise as a well-crafted phishing mail.

Inadequate email security follows at 31 percent, providing continuity with last year, when it topped the list. Behind it sits a broad middle tier: patch management, defenses against malicious code, network security, system integrity checks and data protection, each named by roughly a quarter.

One movement deserves attention despite the small bases: weak login credential security, the second most cited cause in 2025, has dropped to the bottom tier this year. While it would be premature to celebrate, this development is consistent with the broader findings of this study: multi-factor authentication has become standard practice, and attackers have adapted accordingly. As a result, the circumvention of MFA now ranks among the most significant perceived cyber risks. The credential itself is no longer the weakest link; increasingly, the battleground lies in the mechanisms designed to protect it.

The conclusion for defenders is straightforward: invest in people and in vulnerability management with equal seriousness. Awareness programs help address the first cause; transparency over exposed systems, prioritization by exploitability and disciplined remediation address the second. Organizations that neglect either area leave themselves exposed to a significant share of successful attacks.

Employees as the most important asset for attack detection

How are cyberattacks detected within organizations? Employees have become the leading detection channel, at 46 percent against 27 percent a year ago, while internal security systems fell from 40 to 23 percent: in nearly half of all incidents (46 percent), it was an employee who first noticed that something was wrong. This highlights the importance of human awareness and the ability to recognize unusual activity. At the same time, it may indicate that technical detection capabilities, such as endpoint, email, and network monitoring, are not yet consistently identifying threats at an earlier stage.

Irregularities in processes rank second at 31 percent. In third place are internal security systems. Surprisingly – and a positive tendency – suppliers and external service providers stand out: in 23 and 15 percent of cases respectively it was they who helped detect the attacks.

Reporting of cyberattacks

One of the most encouraging findings in this year's study concerns incident reporting. The proportion of organizations that did not report a cybersecurity incident to any party fell from 31% in 2025 to 15% in 2026, halving within a single year. This suggests a significant shift in reporting behavior across Belgium.

The center of gravity is unambiguous. CERT.be, operated by the Centre for Cybersecurity Belgium (CCB), is the first port of call for 62 percent of affected organizations, double last year's 31 percent. The police follow at 38 percent (+23 percentage points), the Data Protection Authority at 23 percent (+8 percent) and 23 percent informed their customers (+15 percent). The specialized national institutions are clearly regarded as the reliable points of contact and the CCB's growing visibility, through Safeonweb, sector outreach and its role as NIS2 authority, is plausibly a direct driver of the improvement.

Regulation is the other driver. With the Belgian NIS2 law in force since October 2024, notification within 24 and 72 hours is no longer good practice but a legal duty for a substantial part of the economy. The behavioral shift is visible; the operational readiness is not yet keeping pace. As chapter 3 shows, only 28 percent of NIS2-scoped organizations have a fully defined and tested notification process. Reporting more is not the same as being ready to report well, closing that gap is the obvious next step.

Types of damage

What does a successful attack cost? For Belgian organizations, the greatest impact is often not the technical incident itself, but its consequences for customers. Half of affected organizations (50%) reported costs related to informing customers and meeting data protection obligations, ahead of investigation and remediation costs (40%), reputational damage (30%), and the failure, theft, or damage of systems (20%).

In a GDPR-driven environment, the response to a breach can be as costly as the breach itself. Notification requirements, customer communication, and the effort needed to maintain trust often represent a substantial part of the overall impact.

Encouragingly, only 10% of organizations were unable to determine the damage caused by an incident, indicating that visibility and understanding of cyber risk continue to improve.

High financial damage

Estimating the financial impact of cyber incidents remains a challenge, which is why the results should be interpreted as indicative. In 2025, a third of affected organizations could not quantify their losses at all. Mid-range losses between roughly EUR 1,000 and 50,000 were the most common quantified band (24 percent), with 8 percent reporting losses between EUR 100,000 and one million. The 2026 answers spread across the same ranges and include one organization reporting damage above EUR 1 million. The distribution matters less than the persistent finding behind it: most organizations cannot translate cyber risk into financial exposure and either. For budgeting, insurance and board-level risk appetite, that quantification gap is itself the risk.

Business interruptions were the consequence

On recovery duration, the positive finding is consistent across both waves: among organizations that experienced disruption, the largest share restored operations within 24 hours (44 percent this year, compared with 69 percent of incidents resolved within a day in 2025). Yet the long tail remains significant. Some interruptions lasted several days or even up to two weeks, and in a services-based economy, the difference between a one-day disruption and a one-week standstill can be existential. Ultimately, business impact analysis, regularly tested recovery capabilities, and a realistic understanding of operational tolerance thresholds are the disciplines that determine which side of that divide an organization ends up on.

Measures against cyberattacks

What do survey respondents do after an attack? First and foremost: they turn inward. Updating identity and access management is the number-one post-incident measure for the second consecutive year (60 percent, up from 50 percent in 2025): accounts, privileges and authorizations are reviewed and tightened before anything else. Half of affected organizations (50 percent) additionally report a stronger internal shift of security responsibility after an incident: ownership moves up and in, not out.

The second tier is tooling and exposure reduction: additional security tools, modernization of SIEM capabilities and a systematic search for further vulnerabilities each follow at 40 percent. External help from specialized consultants and service providers, by contrast, is cited by 30 percent, down from 40 percent in 2025.

We interpret the Belgian pattern as a sign of maturity rather than self-reliance for its own sake. Organizations increasingly treat incidents first and foremost as identity events, reflecting the reality of modern attacks, which often exploit compromised credentials and privileged access. They also use incidents as opportunities to strengthen capabilities and resilience. The share restoring operations within 24 hours fell from 69 to 44 percent, a 25-point deterioration on a small base rather than a one-off response to a particular year's threat environment. It also points directly to the technology priorities explored in Chapter 6, where identity and access management once again emerges as a top-tier investment and risk management focus.

Effectiveness testing

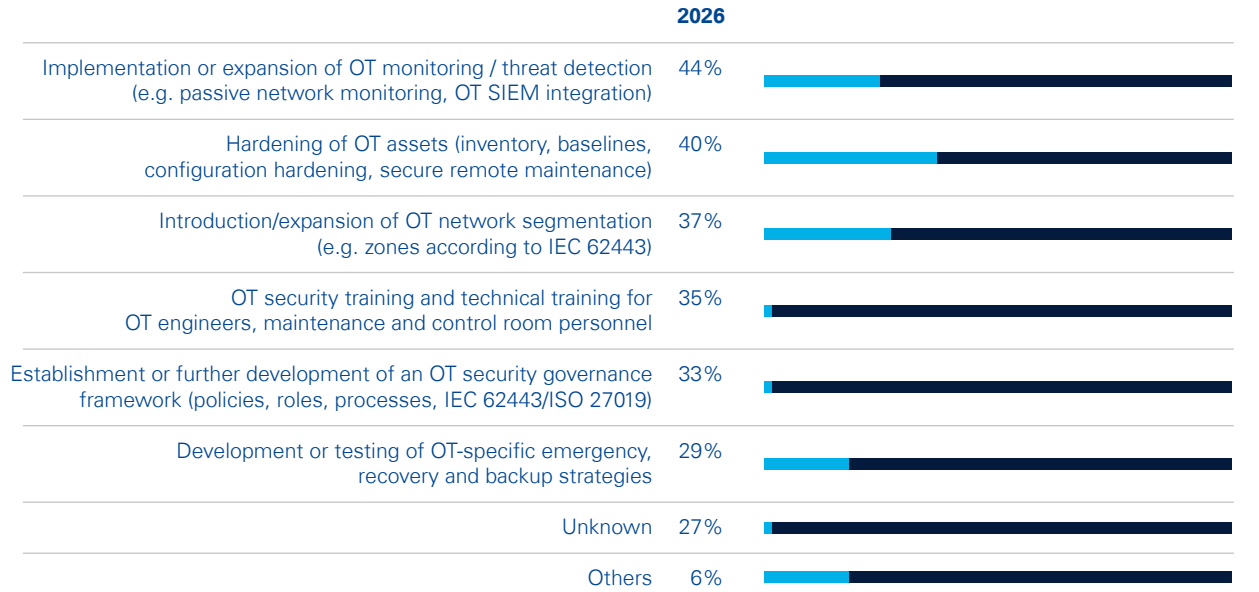
Classic penetration testing remains widespread at 60 percent, but it is no longer the clear frontrunner it was in 2025 (73 percent). More revealing is what gained ground in its place: KPI reporting to management and governance jumped from 41 to 60 percent, external gap analyses and audits from 53 to 60 percent and structured, threat-led attack simulation (TLPT) doubled within a single year, from 25 to 50 percent.

Half of respondents now plan intelligence-led attack

simulations of the kind pioneered in the financial sector under TIBER-BE and mandated for significant financial entities under DORA. That a testing discipline designed for banks and market infrastructures has spread this far this fast suggests a genuine trickle-down of regulatory good practice: threat-led testing is becoming the benchmark for what "assured" means, well beyond the regulated perimeter. Red teaming (40 percent, up from 32 percent in 2025) reinforces this preference for realistic, end-to-end validation.

The countertrend deserves equal attention: uptake of tabletop exercises fell from 52 percent to 40 percent. Yet simulated crisis decision-making remains one of the most cost-effective resilience tests an organization can conduct and the one most directly aligned to the notification and escalation readiness discussed above. As organizations expand their use of technical simulations, they should take care not to let tabletop exercises fall by the wayside. Cyber resilience depends as much on decisions, coordination and communication under pressure as it does on technical response capabilities.

Fig. 5: OT security measures over the next 12 to 24 months.



OT Plans

Operational technology has traditionally been a blind spot in cybersecurity strategies. The Belgian data suggests that this is changing. Asked about their OT security plans for the next twelve months, respondents answer with unusual decisiveness: passive network monitoring and OT threat detection lead at 44 percent, followed by hardening of OT assets (40 percent), network segmentation in line with IEC 62443 (37 percent), OT-specific security training (35 percent) and OT governance frameworks (33 percent). Only 27 percent do not yet know their plans. The Belgian OT agenda exists and it is sensibly sequenced: see first, harden second, segment third.

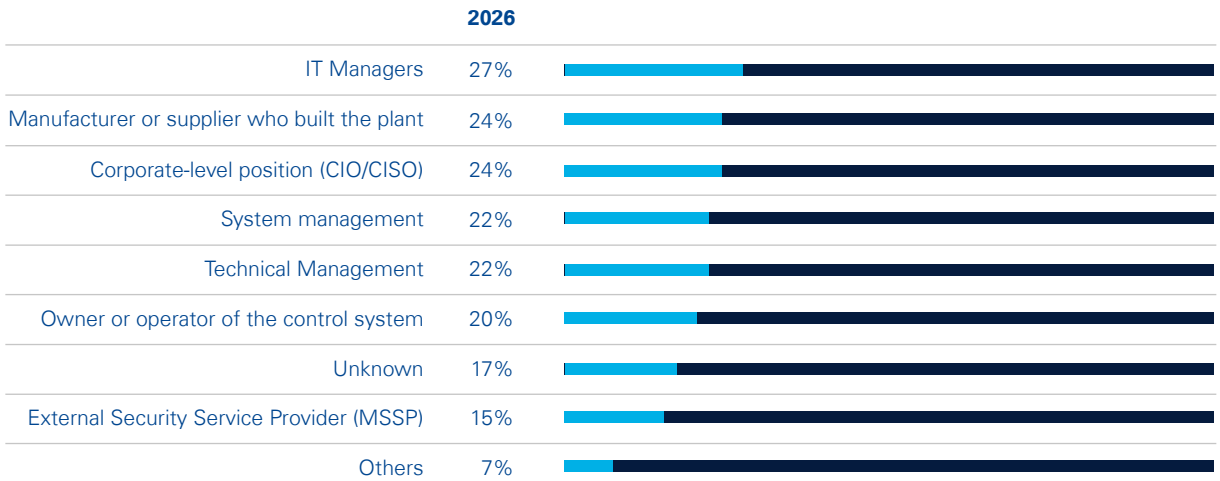
OT challenges

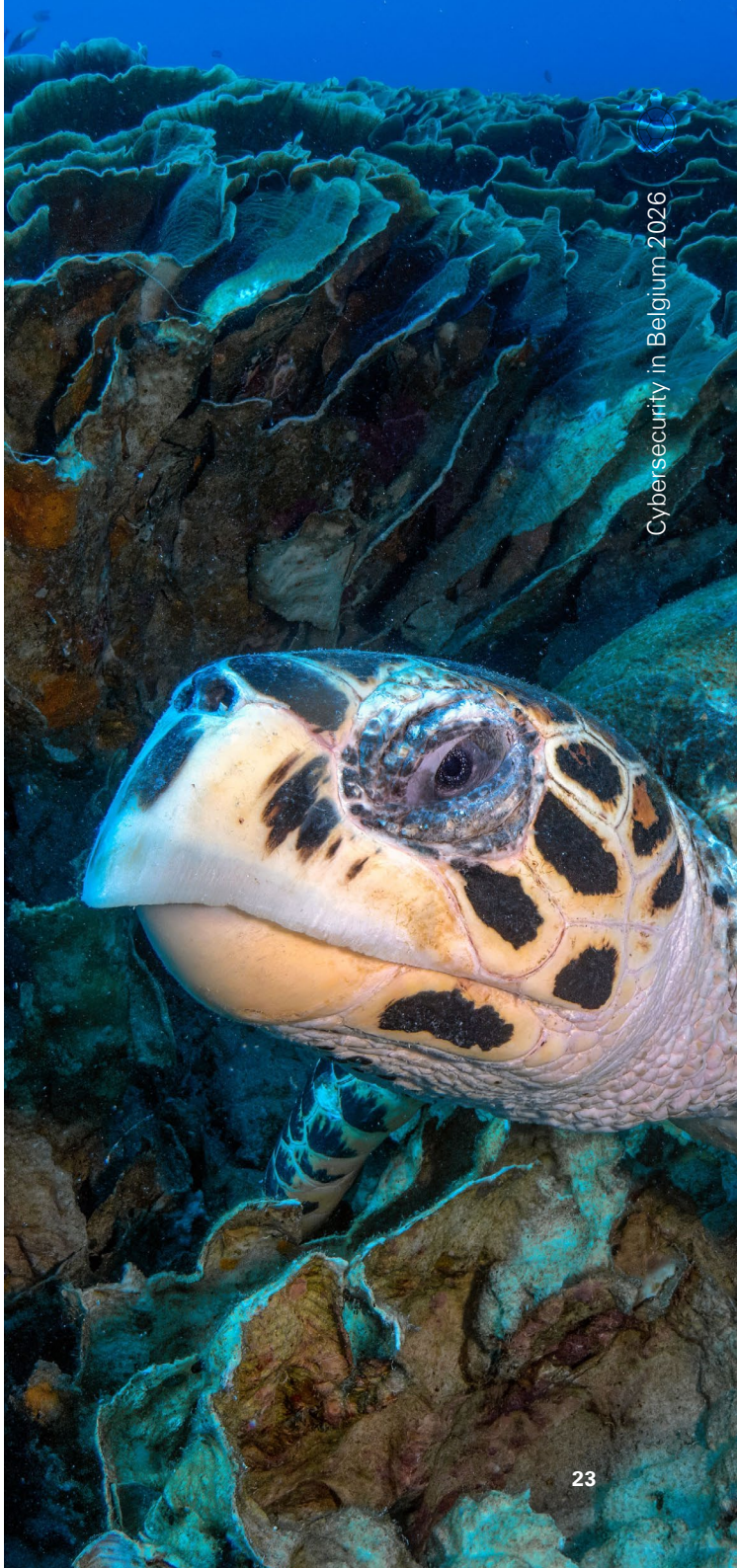
The obstacles are just as clear. The technical integration of legacy OT with modern IT systems dominates (54 percent), followed by insufficient staff to implement existing measures (37 percent) and a quarter of respondents concede that their IT personnel do not understand OT operational requirements, while a similar share finds conventional IT security technology unsuited to control systems. The IT/OT convergence problem, in other words, is as much cultural and human as it is technical. At the same time, AI is penetrating ever more deeply into OT systems, industrial plants and process automation and creating corresponding vulnerabilities – although risks usually arise not from AI as such but from increasing complexity, additional interfaces/connectivity, new dependencies (e.g. cloud/remote services) and potentially insecure data and model pipelines. The differing speeds of system development make outdated technology a challenge.

OT responsibilities

Responsibility for OT security is becoming more concentrated, but it is not yet fully settled. IT managers are the most frequently identified owners (27 percent), yet nearly a quarter of organizations assign responsibility to the manufacturer or supplier that designed or maintains the installation, extending this study's broader supply-chain theme directly into the plant environment. Most often, that responsibility is exercised through maintenance and support contracts. More concerningly, 17 percent of respondents do not know who is responsible at all. In environments where availability, reliability and physical safety are critical, an unowned control system represents a risk waiting to materialize. Establishing clear ownership, backed by appropriate authority and resources, may be the simplest and most cost-effective security improvement identified in this year's findings.

Fig. 6: Who is responsible for implementing OT security measures?





Data theft

How does data leave the company? The small number of organizations able to provide detail on exfiltration incidents point to two recurring causes: software vulnerabilities and theft at the service provider. Even at this baseline level, the second finding resonates: the same third-party channel that dominates this study's risk landscape is present at the moment data leaves the organization. The data lost is spread evenly across communication data, customer data, employee data and passwords.

Ransomware

On ransomware, this year's wave cannot report on payment behavior, as too few affected organizations reached the relevant survey question. The professional guidance, however, remains unchanged and bears repeating: paying a ransom offers no guarantee of decryption, identifies the victim as a willing target for future extortion, may create legal or sanctions-related risks, and helps finance future attacks. Organizations that want a genuine alternative to paying must build it in advance through offline backups, tested recovery capabilities, and a rehearsed decision-making framework agreed at board level before the clock starts ticking.

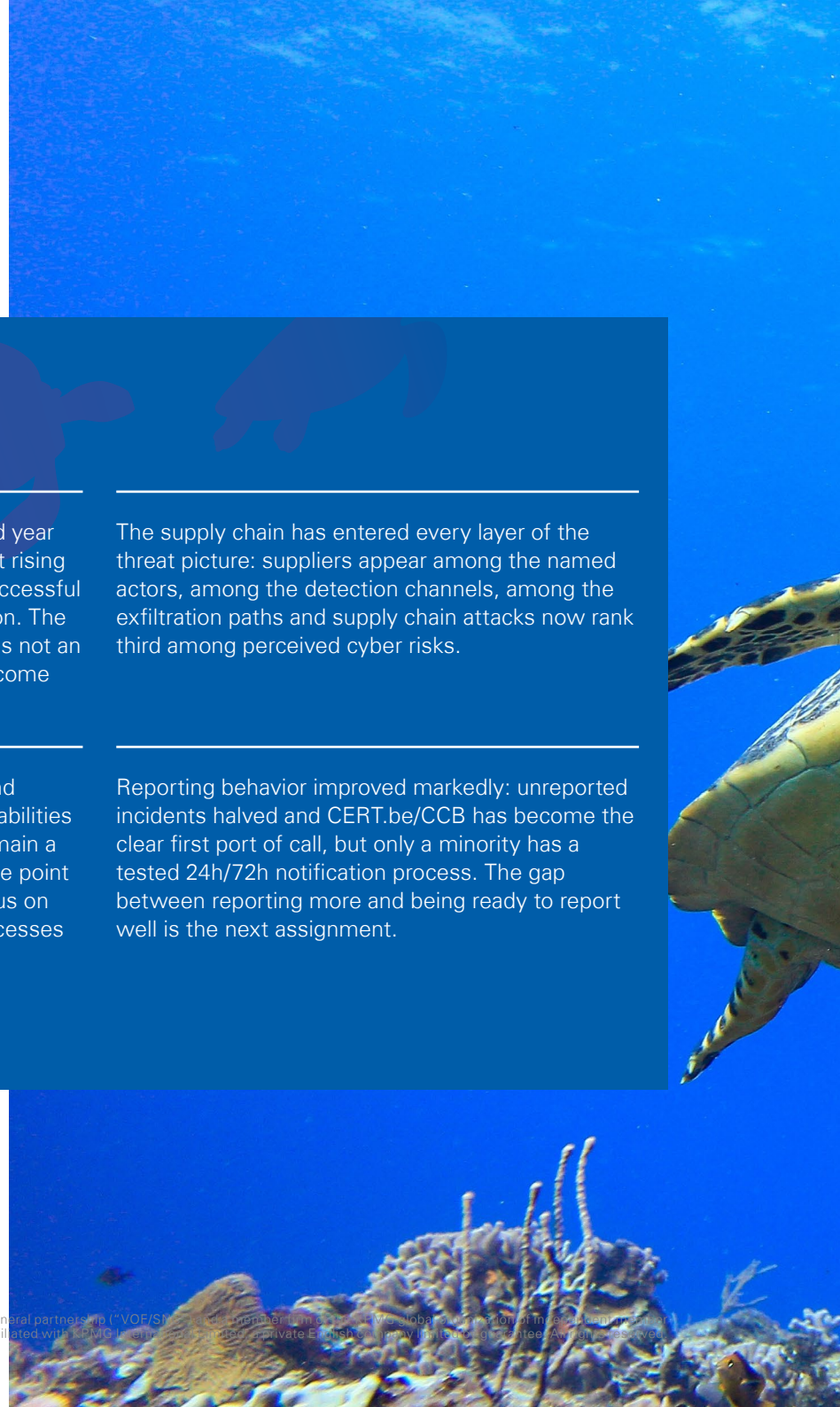
Chapter takeaways

The pressure is structural: for the second year running, a majority of respondents report rising attacks. Almost one in five suffered a successful attack and repeat victimization is common. The threat environment observed in 2025 was not an anomaly or a temporary surge. It has become the baseline.

The supply chain has entered every layer of the threat picture: suppliers appear among the named actors, among the detection channels, among the exfiltration paths and supply chain attacks now rank third among perceived cyber risks.

Attacks succeed through human error and through known but unremediated vulnerabilities in almost equal measure. Credentials remain a key target, but they are no longer the sole point of weakness. Increasingly, attackers focus on bypassing or exploiting the controls, processes and systems that surround them.

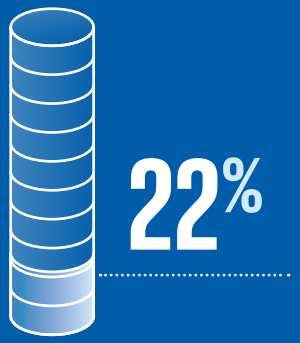
Reporting behavior improved markedly: unreported incidents halved and CERT.be/CCB has become the clear first port of call, but only a minority has a tested 24h/72h notification process. The gap between reporting more and being ready to report well is the next assignment.



02 Cybersecurity governance

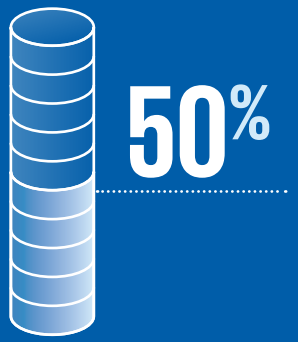
Cybersecurity has become a core leadership responsibility. The focus is on investment decisions, the assignment of responsibilities, risk transparency, and the ability to remain resilient and capable of action in an emergency.

This chapter examines how organizations govern and steer cybersecurity, covering budgets and staffing, perceptions of the most significant cyber risks, and the ongoing tension between security priorities and day-to-day business demands. Taken together, these findings provide a clear view of whether cybersecurity is embedded as a strategic management responsibility or addressed primarily as an operational and reactive function.



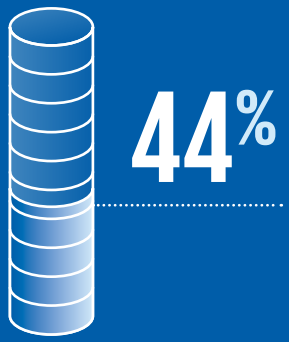
22%

have no dedicated cybersecurity budget.



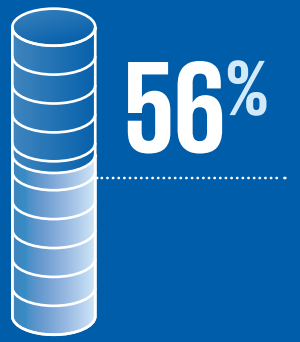
50%

point to regulation and the threat situation as the joint top budget drivers.



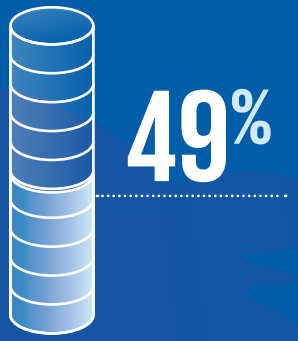
44%

rate the likelihood of damage as (rather) high, up from 35%.



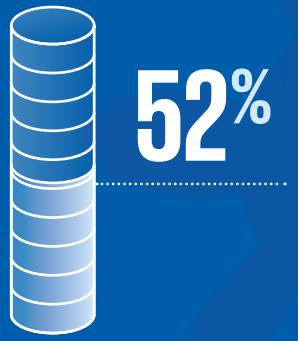
56%

place data theft and data breaches in their top five cyber risks, the most frequently selected risk for the second year.



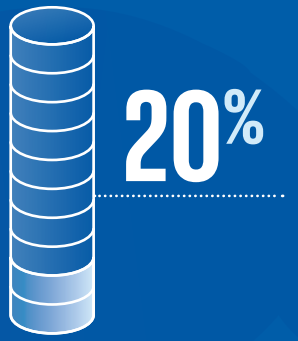
49%

place business email compromise and CEO fraud second: fraud remains the way intrusions get monetized.



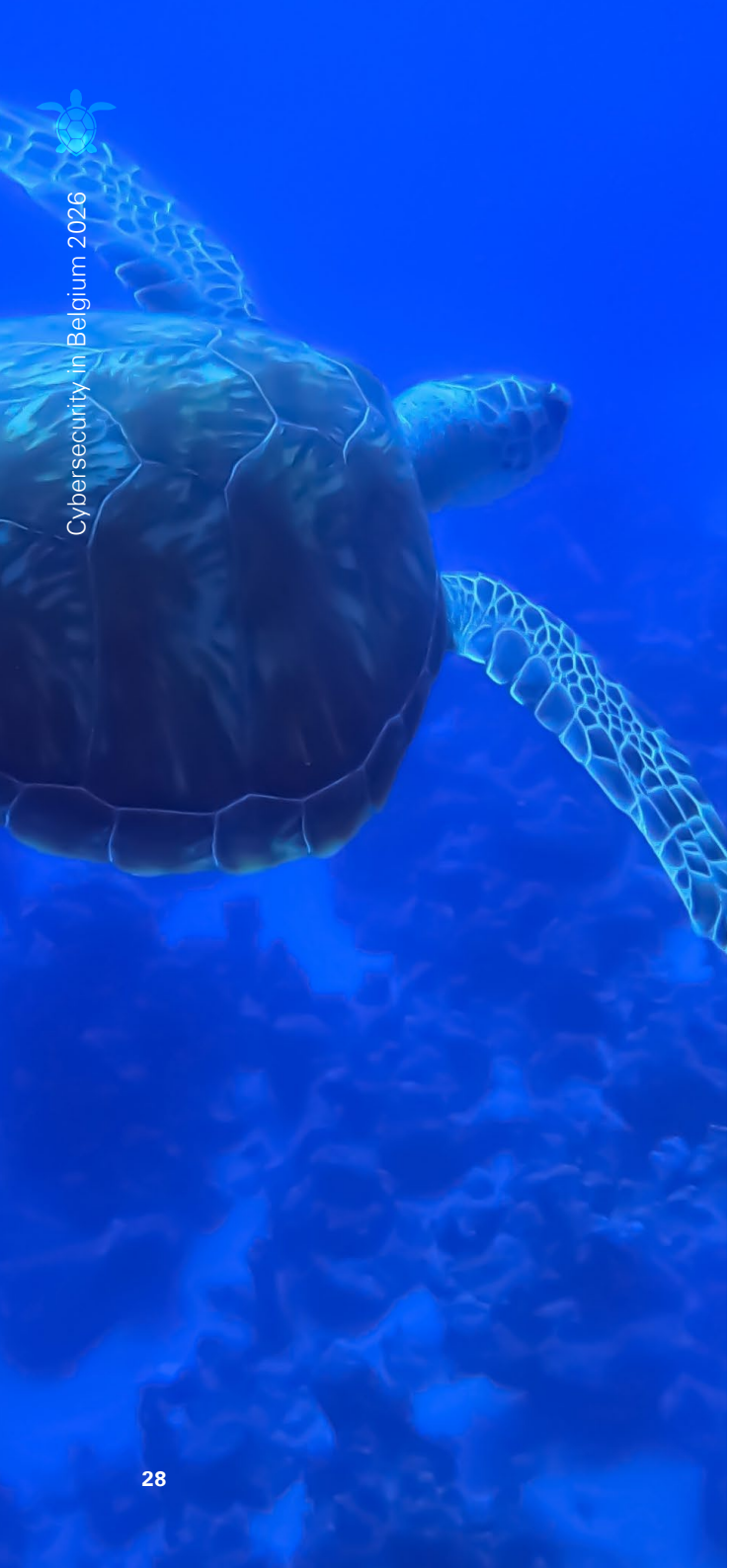
52%

know how they would react to a major attack; a quarter concede they do not.



20%

One in five cybersecurity teams counts no women, down from 32% in 2025.



Cybersecurity governance

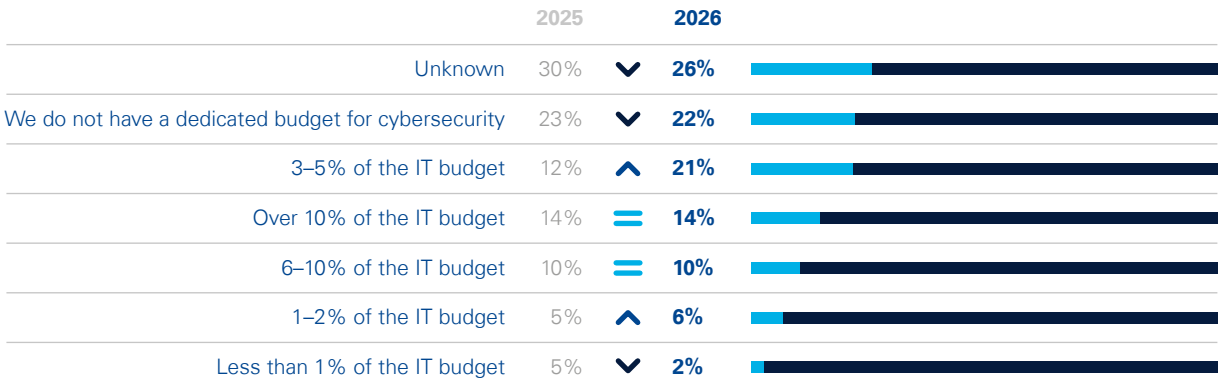
How much companies spend on cybersecurity

The budget basis for cybersecurity is heterogeneous and, in many organizations, only partially transparent. 22 percent state that they have no explicitly designated cybersecurity budget, almost unchanged from 23 percent in 2025. A further 26 percent cannot say whether such a budget exists, against 30 percent a year ago. Taken together, 48 percent of respondents cannot locate their cybersecurity spend in the books.

Where a budget is designated, the levels are respectable. 45 percent of respondents allocate at least 3 percent of the IT budget to cybersecurity: 21 percent spend between 3 and 5 percent, 10 percent between 6 and 10 percent and 14 percent more than 10 percent. Only 8 percent sit below the 3 percent mark. Of roughly half of the market that can point to a cybersecurity budget at all, then, the large majority funds it at a defensible level. The Belgian issue is not the size of the cybersecurity budget so much as the number of organizations that have no budget line to size.

From an expert perspective, the share without an explicit budget is a maturity indicator. Where cybersecurity spending simply runs along inside project or IT budgets, transparency and steerability decline. Risks cannot be prioritized against cost, effectiveness cannot be measured and operating costs cannot be planned. For CISOs and management this raises the pressure to run cybersecurity as a steerable program with clear objectives, cost centers and suitable effectiveness metrics. An organization that cannot say what it spends will struggle to demonstrate that its measures are appropriate to the risk.

Fig. 7: Cybersecurity budget 2025–2026.



Reasons for the budget change

Looking at the overall trend, this year's answers point predominantly upward. Two drivers share the top spot and have done so across both survey waves: a new or changed threat situation and official or regulatory requirements, each named by 50 percent of respondents in 2026, against 58 and 56 percent respectively a year earlier. Corporate strategy follows at 38 percent, level with economic necessity, also at 38 percent. New markets and expansion are cited by 25 percent, up from 9 percent.

The most significant finding is not that these two factors rank highest this year, but that they have remained the leading drivers across both survey waves. This consistency is unlikely to be a coincidence. The Belgian NIS2 law has been in force since October 2024. The registration deadlines, the CyFun-based assurance route and the first supervisory contacts all fall within the period this survey covers. Regulation drives investment through minimum requirements, evidence and auditability, while the threat situation drives it through the need for protection and crisis resistance. Between them, they push cybersecurity investment into the category of a mandatory program for keeping business processes stable and away from the category of a transformation or growth initiative.

Strategy and threat situation interlock in practice. New forms of attack, geopolitically motivated activity or a wave of extortion campaigns feed into strategic decisions on supply chain security, cloud use or new digital services. Conversely, strategic moves such as growth, internationalization, or outsourcing enlarge the attack surface and trigger additional security investment. The rise in expansion as a stated reason fits that logic, since new markets bring new partners, new IT and cloud dependencies and new exposure with them.

Staff in the cybersecurity team

Belgian cybersecurity teams remain lean where execution matters most. 36 percent of respondents manage cybersecurity with one or two people, while a further 14 percent do so with three to five. That concentration at the bottom of the scale is sharper than in 2025, when 22 percent had one or two people and 2 percent had nobody.

That spread matters more for governance than any average would. A large share of respondents manage cybersecurity with at most two people and the constraint is visible throughout this study. A lack of internal resources is the most frequently cited obstacle to NIS2 implementation, mentioned by 61 percent of respondents in Chapter 3. This explains why external assurance and managed services recur throughout the answers on effectiveness testing. It is also the backdrop against which the automation findings below should be read.

Fig. 8: Reasons for the cybersecurity budget change.

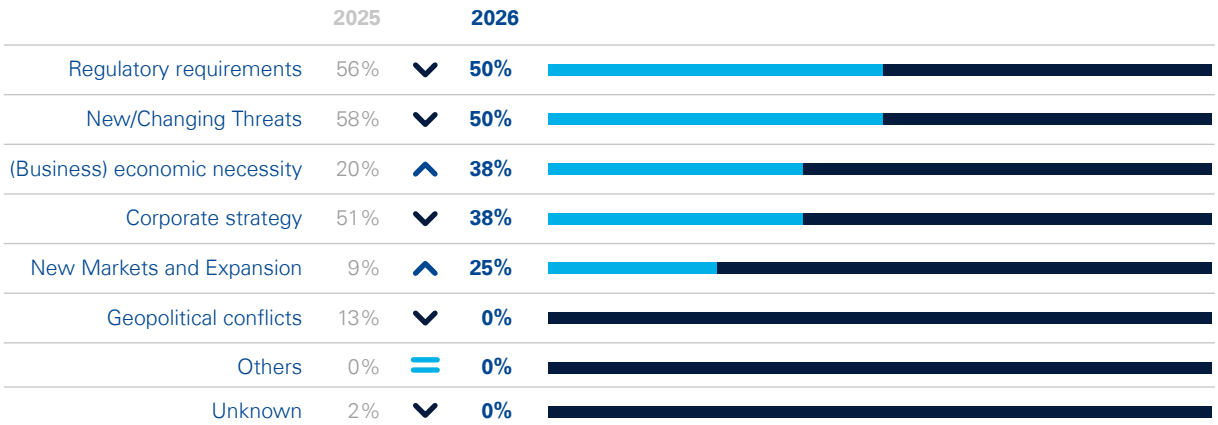
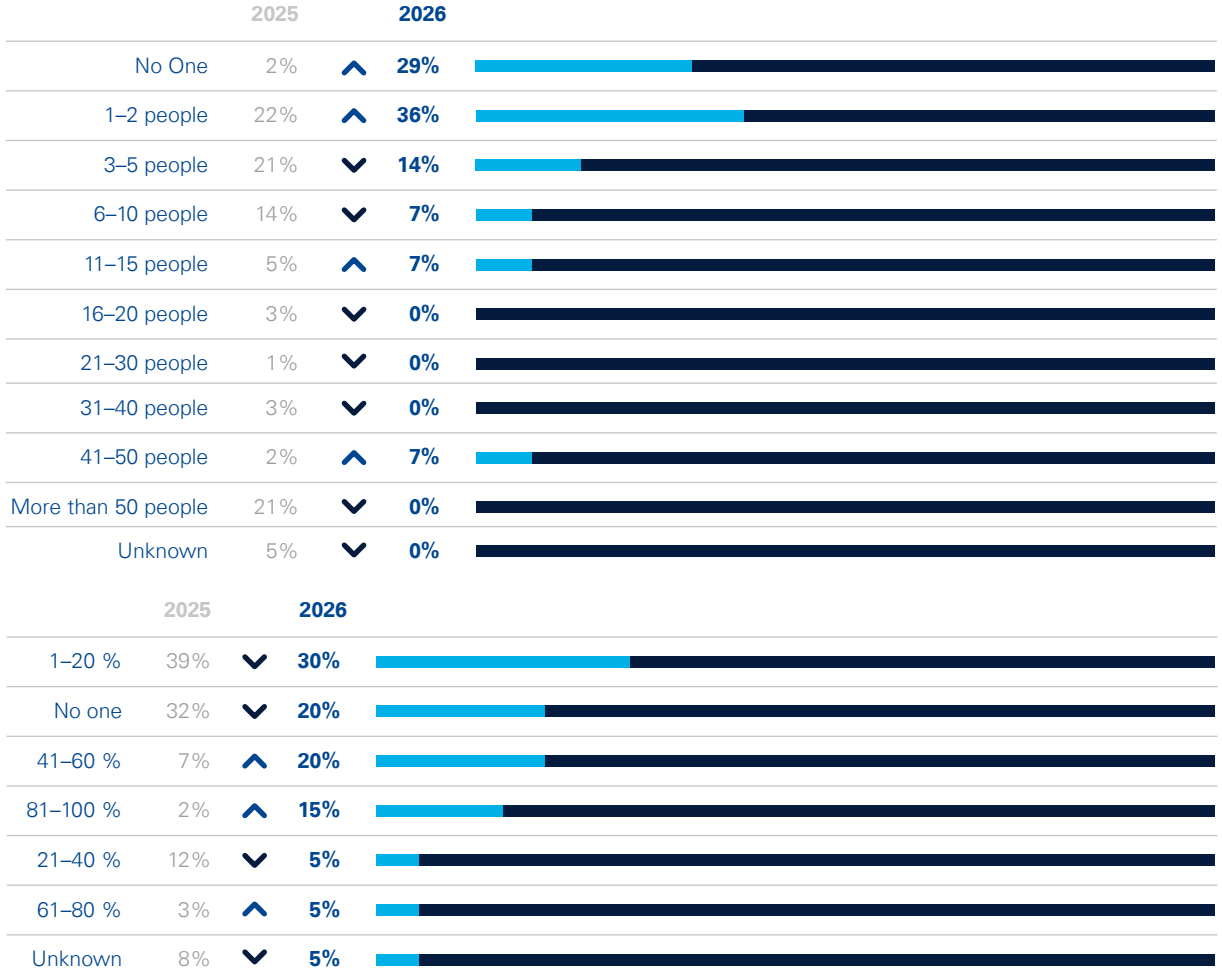


Fig. 9: Share of staff in the cybersecurity team incl. change versus previous year.



Automation instead of headcount

If teams cannot grow, capability must come from somewhere else and respondents are clear about where they are looking. 60 percent agree that generative AI improves their defensive capability. 37 percent state that they are already using AI to improve cybersecurity, and a further 35 percent describe it as an option in principle. Only 8 percent regard the topic as not relevant to them.

Opportunities concentrate where automation scales best. User behavior analytics leads at 75 percent, ahead of threat intelligence at 70 percent, with vulnerability management the biggest mover, up from 42 to 65 percent, which is the clearest movement among these findings and a sensible one given that ineffective vulnerability management was among the two leading causes of successful attacks in Chapter 1. Security monitoring and SIEM follow at 58 percent, against 53 percent a year ago. Both are domains in which the work is high-volume, repetitive, and previously rationed by staff availability.

The conclusion for Belgium is therefore not that automation is shrinking security teams, but that automation is the answer being adopted by teams that are structurally thin. That is a defensible strategy provided two conditions hold. First, automation has to reduce workload rather than relocate it, since an AI-assisted triage process still needs someone competent to act on what it surfaces. Second, the governance around AI use has to be built at the same time as the capability: model and data provenance, access to sensitive telemetry, human decision points for containment actions, and a clear position on what the tools may not do autonomously. Efficiency gains bought at the cost of competence gaps are borrowed rather than earned.

Top 5 cyber risks

When asked to select the five cyber risks that matter most to them, respondents name data breach and data theft first, at 56 percent. Business email compromise and CEO fraud follow at 49 percent, supply chain attacks at 48 percent, ransomware and extortion at 44 percent, and malware at 40 percent. Just outside the top five sit phishing and spear phishing via email links at 39 percent, the circumvention of multi-factor authentication and identity theft at 28 percent each, and cloud misconfiguration at 24 percent.

The risk map is stable at the top but evolving beneath the surface. Data breach and business email compromise have held the first two places across both waves. The loss of data and the manipulation of payment and approval processes remain the risks our respondents fear most and there is no sign of that changing. Beneath them, the ranking has shifted considerably. Supply chain attacks have risen from eleventh place in 2025 to third place in 2026, the largest single shift in the ranking. Denial-of-service attacks have fallen from sixth to tenth place, while ransomware has slipped from third to fourth despite maintaining a similar level of concern in absolute terms.

Taken together, these movements suggest a shift in focus from visible disruption to trusted compromise. Attacks that take websites offline appear to be losing prominence, while compromises delivered through a supplier, systems integrator, or software update are moving up the agenda. This shift is corroborated elsewhere in the study. Suppliers appear among the named attackers in Chapter 1, third-party risk features prominently in Chapter 3, and third-party risk management tops the technology agenda in Chapter 6. Viewed together, these findings suggest a substantive change in risk perception rather than a short-term response to media attention or recent incidents.

One result stands out. The fraudulent use of AI and machine learning is selected by only 12 percent as a top-five risk, having ranked last in 2025. Yet the same respondents place the AI cluster at the very top of the particular challenges discussed later in this chapter. The tension is instructive rather than contradictory. AI-driven attacks are perceived as difficult, unfamiliar and hard to counter, but not yet as the most likely thing to cause damage in the coming year. Respondents, on this evidence, are worried about AI without yet budgeting against it.

For security programs, the practical consequence is reinforced rather than changed. The dominant risks in the Belgian top five are impact risks rather than entry vectors: data leaving the organization, payments being misdirected, operations being encrypted, trust in a third party being abused. Organizations that control identity through phishing-resistant multi-factor authentication and privileged access management, control data flows through classification, egress monitoring, and data loss prevention, and maintain tested backup and recovery capabilities reduce the effectiveness of all five at once. Increasingly they must extend the same controls to the suppliers who now rank third.

Fig. 10: Top 5 cybersecurity risks, 2026.

		2026
1	Data breach	56%
2	Business email compromise, CEO/CFO fraud	49%
3	Supply chain attack	48%
4	Ransomware/Extortion	44%
5	Malware (email attachment)	40%
	(Spear) phishing attack (email link)	39%
	Bypassing multi-factor authentication	28%
	Identity theft	28%
	Cloud misconfiguration	24%
	Denial of service attacks (DoS)	22%
	Advanced Persistent Threats (APTs)	21%
	Social Engineering	17%
	Industrial control system compromise (OT)	12%
	Insider Threat	12%
	AI/ML fraudulently used	12%
	Eavesdropping on communications (man-in-the-middle attack)	10%
	Deepfake (audio, images, video)	9%
	Password theft	9%
	Spoofing	7%
	Unwanted, automated calls	4%
	Espionage	2%
	Mobile Malware	1%
	Other types of attack	1%

2025 and 2026 use different measurement bases; rank movements are indicative and the values are not directly comparable.

Assessment of cyber risk and likelihood of occurrence

Belgian risk perception has risen sharply. 44 percent of respondents now rate the likelihood that the named types of attack will actually cause damage in their own organization as high or rather high, made up of 21 percent high and 23 percent rather high. In 2025 the equivalent figure was 35 percent. 45 percent rate the likelihood as average, down from 55 percent, and only 11 percent consider it low or rather low, with 9 percent rather low and 2 percent low.

The interesting part of that movement is where it came from. The share of respondents rating cyber risk as low or rather low has not meaningfully changed. What has shrunk is the middle: ten points have moved out of the average band and into the upper half of the scale. Last year's reading, namely that cyber risk was normalizing into an ordinary mid-range business risk, is giving way to something more pointed. A substantial part of the Belgian market now expects to be damaged, not merely attacked.

That expectation is well founded. Roughly one organization in six suffered a successful attack in the past twelve months, repeat victimization is common, and the attack types rising in the risk ranking are the same ones dominating the incident data. Cyber risk is accordingly better understood as a permanent business risk with a relevant likelihood of occurrence rather than as an exceptional event. Cybersecurity programs should reflect that by combining prevention with demonstrable resilience, meaning containment, recovery capability, rehearsed crisis processes, and clear decision-making and communication paths.

Reaction to a cyberattack

Are survey respondents prepared for an emergency? 52 percent agree or rather agree that a plan exists and that it

is fundamentally known how to proceed. 25 percent do not. In 2025 the figures were 59 and 18 percent respectively, so the share who feel prepared has fallen by seven points over the year.

A plan on paper is in any case not the measure that counts. What decides the outcome of an incident is whether roles are clear across IT, security, management, legal, and communications, whether reporting channels are defined and rehearsed, whether external support such as forensics is contractually secured in advance, and whether the whole arrangement has been exercised recently enough for people to act without improvising. On each of those points the Belgian data gives more reason for concern than for comfort. Tabletop exercises fell from 52 to 40 percent over the year, and only 28 percent of organizations in scope of NIS2 have a fully defined and tested notification process, as Chapter 3 sets out. Respondents report incidents far better than they did a year ago. They are not yet demonstrably ready to handle them well.

Threats: day-to-day business versus specific challenges

A clear maturity dividing line runs through the 2026 results. One group of threats is classified by most organizations as normal day-to-day business, meaning events for which established controls, clear escalation paths, and rehearsed procedures are in place. In parallel, a second group persists as a particular challenge, covering scenarios in which organizations recognize the risk but do not yet have the combination of technology, processes, roles, and governance needed to respond consistently and effectively. Reading the two dimensions side by side shows where Belgian capability has matured and where it has not.

Particular challenges for Belgian organizations

The challenge dimension is headed by state actors and artificial intelligence together. State-sponsored and state-supported attacks are named as a particular challenge by 54 percent, the highest value in the list, with espionage close behind at 48 percent. Three threats share second place at 51 percent each: AI-assisted attacks, the poisoning of AI models, and ransomware and extortion. AI data poisoning follows at 45 percent, deepfake attacks at 43 percent, and zero-day attacks at 42 percent.

The composition of that cluster points to a specific gap rather than a general anxiety. Data poisoning, deepfakes, and AI-assisted attacks are all, at bottom, attacks on integrity: on the trustworthiness of the data an organization trains and makes decisions on, on the authenticity of the voice or face approving a payment, and on the reliability of the signals a defender is reading. Espionage and the circumvention of multi-factor authentication complete the picture, since both work by turning legitimate trust, whether an insider position or a valid session, against its owner.

Classic perimeter controls have little purchase here. What does have purchase is provenance and verification: knowing where data and models come from, verifying consequential instructions out of band, applying the four-eyes principle to payment and approval processes, and hardening authentication against relay and fatigue techniques rather than merely deploying it.

Perfectly normal day-to-day business

The day-to-day dimension shows which threats our respondents have managed to turn into routine, and the spread across this category is wide. Phishing is classified as day-to-day business by 72 percent, malware by 71 percent, password theft by 67 percent and scam calls by 65 percent and social engineering by 52 percent. Mis- and disinformation reaches 38 percent. Ransomware and extortion sit at 29 percent.

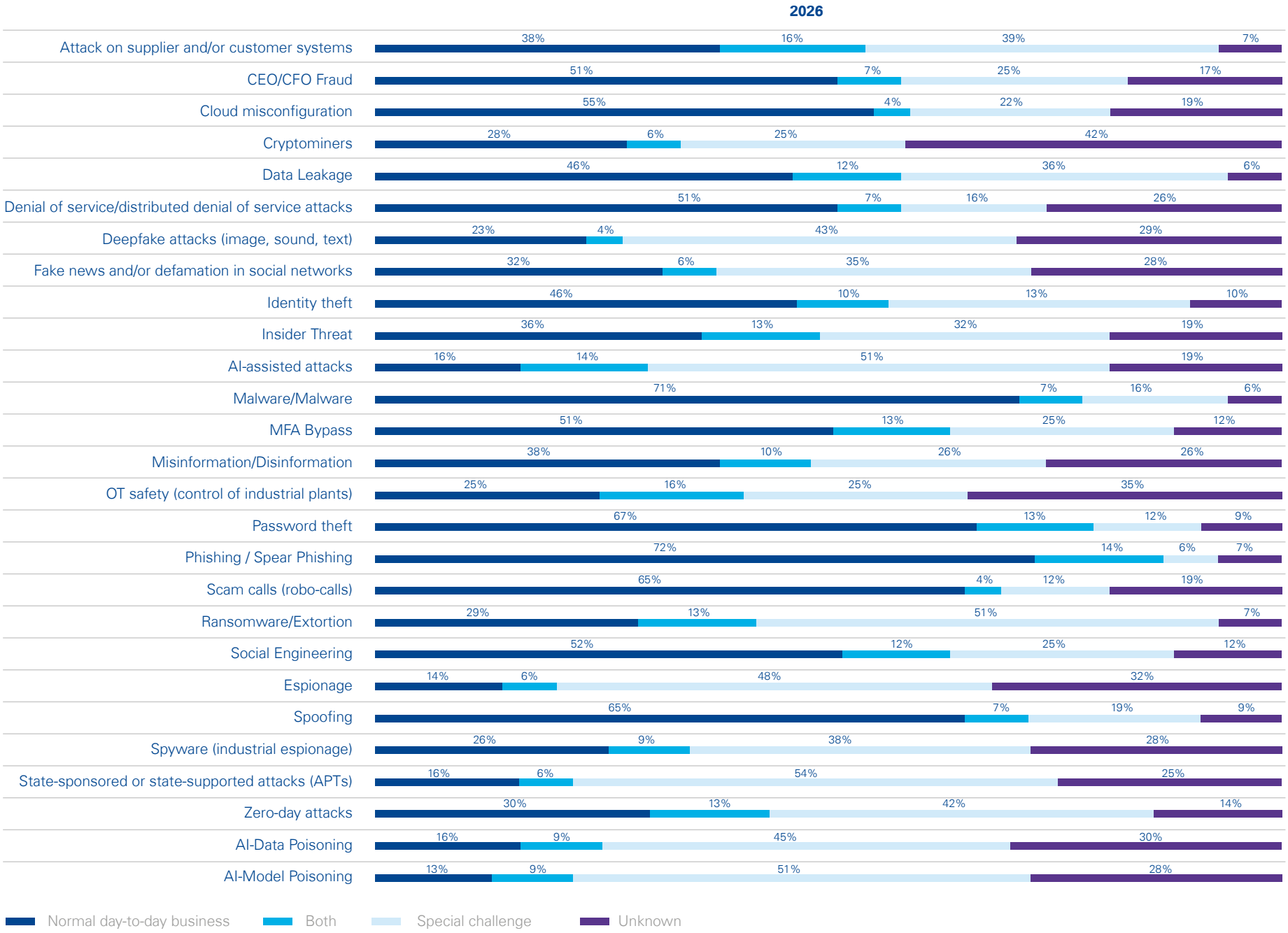
The ransomware figure is the sharpest finding in this battery because it points in the opposite direction to the challenge dimension. Fewer than three organizations in ten treat ransomware as routine, while more than half classify it as a particular challenge. That is a striking finding for a threat that no Belgian organization is encountering for the first time. Ransomware is the most frequently ranked risk, named in the top five by 44 percent, though only a minority of affected organizations experienced it, 44 percent rank it among their top five risks, and organizations know exactly what they are dealing with. Yet familiarity has not translated into confidence: they still do not feel they have a settled answer to it.

The reason is visible elsewhere in this study. Handling ransomware well depends on tested backup and recovery, rehearsed crisis decision-making, and a clear position on payment. Chapter 1 records tabletop exercises falling from 52 to 40 percent over the year. The capability that would make ransomware routine is the capability survey respondents have been practicing less.

Mis- and disinformation, at 38 percent, sits awkwardly for a different reason. Chapter 5 shows the perceived threat from disinformation rising faster than any other theme in this survey, yet fewer than two organizations in five regard handling it as ordinary business. That fits the wider picture, in which disinformation falls between communications, legal, and security, without a clear owner.

The wording of this dimension is worth clarifying. Day-to-day business does not mean harmless. It means manageable: detectable, containable, and recoverable. The risk lies in complacency. Controls that are considered settled stop being tested, and the disciplines that made scam calls and social engineering manageable in the first place are often the first to lapse.

Fig. 11: Specific challenges vs. day-to-day business, 2026.



Day-to-day business vs. specific challenges as separate tasks

From an expert perspective, the decisive conclusion is to manage day-to-day capabilities and specific challenges capabilities separately. “Day-to-day business“ requires robust standardization (playbooks, automation, repeated rehearsal). “Specific challenges“, by contrast, require targeted capability-building programs, particularly in the fields of identity security (phishing-resistant MFA, PAM, session controls), data control (classification, egress monitoring, DLP/DDR), detection & response (EDR/XDR coverage, use-case hardening, threat hunting), and fraud-resistant communication and approval processes (call-back mechanisms, four-eyes principle, out-of-band verification, deepfake awareness).

For management, a clear steering logic follows: success metrics should not primarily hang on “incidents“ but on demonstrable effectiveness and resilience. Practicable KPI brackets are (1) exposure reduction (patching pace, attack-surface trends), (2) identity robustness (MFA resistance, privilege hygiene), (3) detection and response performance (MTTD/MTTR, containment time), and (4) restart capability (RTO/RPO fulfilment, recovery tests).

Precisely in an environment in which threats increasingly operate via trust and identity, what matters is not the existence of individual tools but the consistent ability to make decisions quickly and securely – under uncertainty, time pressure, and potentially manipulated communication channels.

Cyberattacks are not an exceptional event but a permanent business risk, with consequences for availability, integrity, and confidentiality.

Chapter takeaways

Nearly half of the survey respondents cannot identify their cybersecurity spend at all, though where a budget does exist it is funded at a defensible level. The Belgian budget problem is one of transparency and steerability rather than of generosity.

Security capability is constrained by people rather than money, with a market running on two very different staffing models under identical obligations. Automation is the answer being adopted, particularly in vulnerability management and security monitoring.

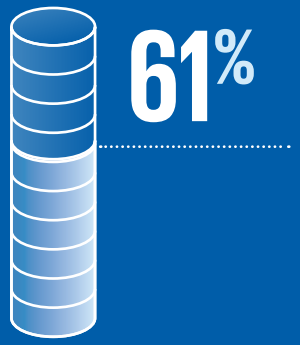
The risk map is stable at the top and shifting underneath, with supply chain attacks climbing sharply while denial-of-service falls away. The quiet compromise through a trusted third party has displaced the loud, disruptive attack.

Cyber risk is no longer perceived as a mid-range possibility, yet confidence in knowing how to react has softened and exercises have declined. Perception has moved faster than preparedness.

03

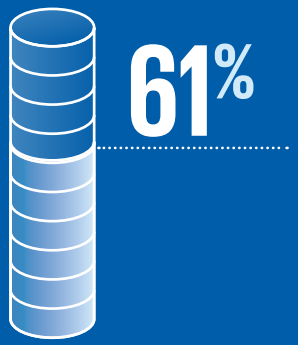
Cyber regulation and NIS2 implementation in Belgium

Which cyber regulations shape the pressure on Belgian organizations to act, and what concrete requirements for governance, processes, and demonstrability follow from them? For most organizations, the work now centers on NIS2 and its Belgian transposition, alongside DORA, the Cyber Resilience Act, the AI Act, and the CER law of 19 December 2025. Two years after the Belgian NIS2 law entered into application, the question is no longer whether the rules apply. It is whether the measures behind them work and whether that can be shown.



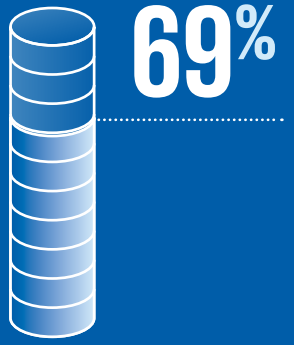
61%

of respondents are affected by NIS2.



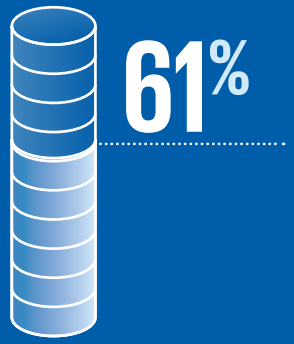
61%

comply through CyberFundamentals, compared with 36% through ISO 27001.



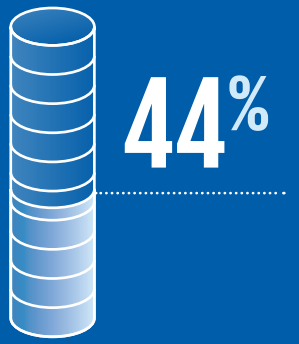
69%

say they are on track for the Belgian NIS2 deadlines.



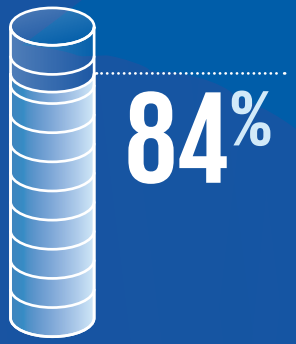
61%

name lack of internal resources as their number one implementation obstacle.



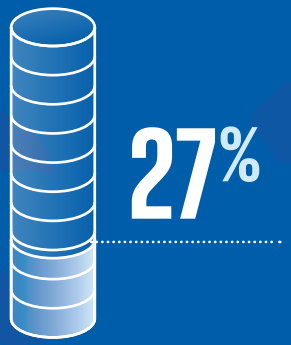
44%

saw a supplier fall victim to a cyberattack.



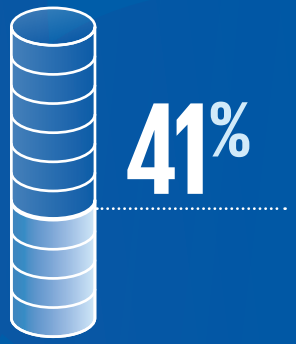
84%

are concerned that attacks on their service providers will hit them, identical to last year.



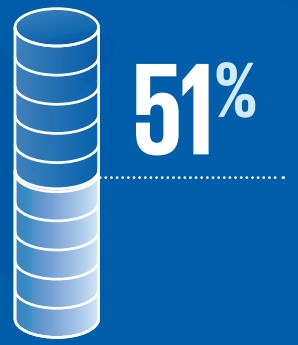
27%

suffered a service interruption from a supplier incident; only 7% experienced a follow-on attack.



41%

concede their organization lacks awareness of supply chain attack risks, up from 31%



51%

request security certifications from suppliers.

Cyber regulation and NIS2 implementation in Belgium

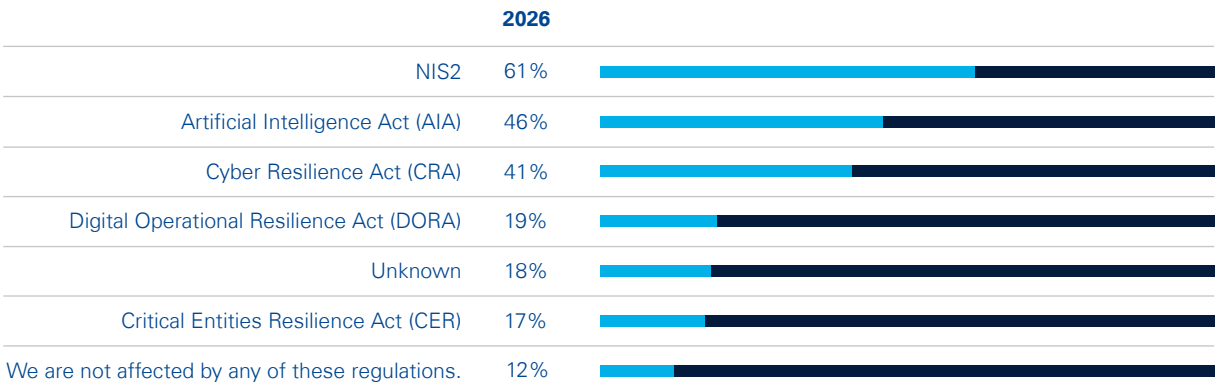
Cyber regulations

The European regulatory wave has fully arrived in Belgian boardrooms. 61 percent of surveyed organizations state that they are affected by NIS2, against 64 percent a year ago, making it by far the broadest instrument. The AI Act follows at 46 percent, up from 42 percent, and the Cyber Resilience Act, which sets a minimum level of cybersecurity for products with digital elements, at 41 percent, against 40 percent. DORA is named by 19 percent, down from 30 percent, reflecting the smaller financial-sector share in this year's sample rather than any narrowing of the regulation. The CER law of 19 December 2025 is named by 17 percent, and 20 percent of respondents report a formal designation as critical infrastructure under it.

Only 12 percent see no applicability at all, against 11 percent last year, while 18 percent cannot yet judge. Applicability under the CER regime differs in logic from NIS2 because it rests on a formal determination by the authorities. Affected organizations are explicitly identified and informed, which increases legal clarity for those concerned and removes the self-assessment problem that NIS2 creates.

The picture is stable year-on-year and that stability is itself the finding. Regulation has moved from an emerging concern to an established operational reality for Belgian organizations. The advisory question has shifted accordingly. For the large majority, the task is no longer to establish whether the rules apply but to integrate overlapping obligations from NIS2, CyFun, DORA, the AI Act, and the GDPR into one coherent control framework, rather than running them as parallel compliance exercises with duplicated evidence, audits, and effort. For the 18 percent who still cannot judge their position, and for the group that does not know its NIS2 designation, a structured applicability and gap analysis remains overdue rather than optional. Supervision is hardening, and the deadlines do not wait for the analysis.

Fig. 12: Regulations – share of companies affected.



Belgium's head start and what it demands

Belgium transposed NIS2 through the Law of 26 April 2024, which entered into force on 18 October 2024. The Centre for Cybersecurity Belgium (CCB) acts as the national cybersecurity authority. Organizations may use CyberFundamentals or ISO/IEC 27001 certification as recognized assurance and conformity assessment mechanisms that can support a presumption of conformity, subject to the applicable scope and assessment conditions.

The CCB has clarified its supervisory approach for the mandatory conformity assessment of NIS2 essential entities due by 18 April 2027. Entities that cannot demonstrate cybersecurity measures equivalent to the CyFun Essential assurance level by that date will be asked to submit a remediation plan evidencing at least Important-level measures and setting out how they will reach the Essential level by 18 April 2028. This applies to all three assessment routes: CyFun certification or verification, ISO/IEC 27001 certification, and assessment by the CCB's Inspection Service. It is not an extension of the legal deadline and no remediation plan is required where the entity demonstrates Essential-equivalent measures or justifies a lower level based on its risk analysis.

Among organizations within NIS2 scope, 50 percent are designated Essential and 31 percent Important, while 19 percent do not know their designation. A year ago, the CyFun assurance levels reported within scope were 44 percent Essential, 42 percent Important, and 9 percent Basic. The share that cannot state its own designation deserves attention, because designation determines the supervisory regime, the intensity of obligations, and ultimately the liability position of the management body. A lack of awareness is not without consequence.

CyFun is consolidating as the Belgian route of choice. 61 percent pursue compliance via CyberFundamentals against 36 percent via ISO 27001 certification. A year ago, the figures were 49 percent for CyFun and 28 percent certified, with a further 15 percent aligned but not certified. The declared assurance levels are Important for 41 percent, Essential for 27 percent, and Basic for 18 percent, markedly lower than last year, when 44 percent reported Essential. The fall of 17 points may reflect more realistic self-assessment as organizations engage with the framework, but it is a decline and should be read as one. As organizations engage seriously with the framework and see what evidence each level actually demands, self-assessments become more honest rather than more ambitious.

One finding deserves particular attention. Almost one in five organizations that consider themselves in scope of NIS2 are unable to identify whether they are classified as an Essential or Important entity. Given that entity designation determines supervisory expectations, assurance requirements, and reporting obligations, this suggests that regulatory understanding remains uneven despite generally high implementation progress.

Implementation progress: further along, more sober

72 percent of NIS2-scoped organizations describe their implementation as at least advanced, made up of 50 percent advanced, 19 percent very advanced, and 3 percent complete, up from 63 percent a year ago. 14 percent have recently started, and 6 percent describe themselves as still at the beginning. On timing, 69 percent believe they are on track for the Belgian deadlines, against 73 percent last year, while 19 percent say they are not. Expected time to full compliance is under six months for 25 percent, six to twelve months for 39 percent, twelve to eighteen months for 11 percent, and more than eighteen months for 17 percent.

The most revealing movement is one that looks at first glance like regression. Claimed completion fell from 13 percent to 3 percent, even as the share at least at an advanced stage rose. Read together, the

two movements describe maturation rather than backsliding. Last year's completion claims often rested on an assumed equivalence between an existing ISO 27001 certification and NIS2 conformity, a position the 2025 edition already flagged as challengeable in an audit. A year closer to supervision and with the first CyFun assessments behind them, organizations are recalibrating what "done" means. Fewer now claim to be finished, and those that do may have stronger grounds for doing so.

That recalibration should extend to the confidence figures themselves. Being on track is a perception; readiness is a state. The organizations that will fare best under the first supervisory contacts are those whose confidence rests on something external, such as a readiness assessment, a gap analysis against the applicable assurance level, or a governance checkpoint with a documented outcome, rather than on an internal sense that things are going reasonably well.

The notification test

The sharpest single indicator of operational readiness in the Belgian regime is the incident notification duty: an early warning within 24 hours, an incident notification within 72 hours, intermediate reporting where required, and a final report generally within one month.

It is the one obligation that has to be executed under pressure, at speed, on a day nobody chooses.

Only 28 percent of scoped organizations have a fully defined and tested notification process. 44 percent have defined one but never tested it, 22 percent hold no more than a draft, and 6 percent have no process at all. Seven organizations in ten have therefore never rehearsed a process that may attract significant supervisory attention due to the strict reporting timelines involved. A notification process that has never been exercised is a plan on paper and the first serious incident is the wrong moment for a first rehearsal, particularly given that the 24-hour clock starts running from awareness rather than from certainty.

There is a genuinely encouraging counterpoint and it comes from Chapter 1. Actual reporting behavior has improved sharply. The share of organizations reporting an incident to nobody at all halved from 31 to 15 percent, and reporting to CERT.be and the CCB doubled from 31 to 62 percent. Survey respondents are reporting far more than they were. What they have not yet built is the ability to report well, meaning completely, accurately, and within the deadline. Closing the gap between the two is the most concrete assignment this chapter produces and also among the cheapest, since a rehearsed notification path requires an exercise rather than a program.

Notification readiness remains one of the clearest operational gaps identified in the survey. While most respondents report substantial implementation progress, only 28 percent indicate that their incident notification process has been fully defined and tested. More than seven out of ten organizations are therefore relying on either untested, incomplete, or non-existent notification procedures.

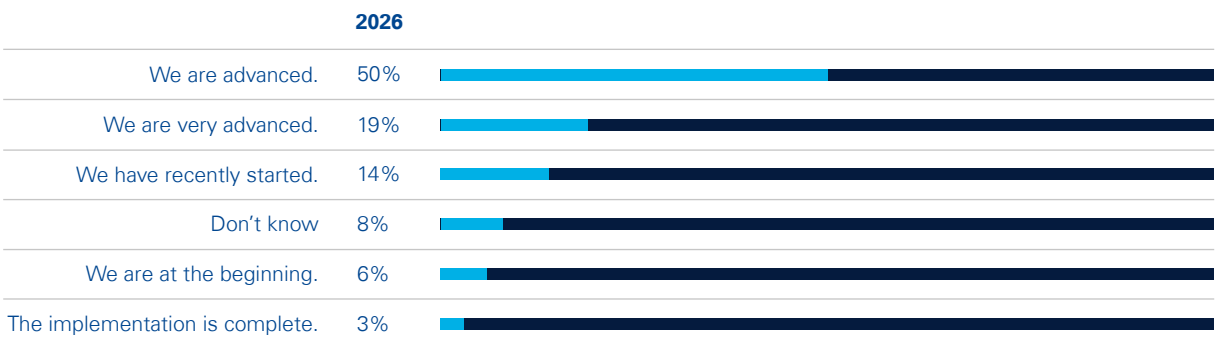
Where implementation hurts

Asked about the biggest obstacles to NIS2 implementation, organizations point first to people rather than technology. Lack of internal resources leads at 61 percent, ahead of supplier dependencies at 42 percent, budget constraints at 39 percent, a lack of management buy-in at 28 percent, and legacy integration and unclear roles at 25 percent each. The ranking matters because the top two obstacles are capacity and third parties, and neither can be bought as a product.

This is the same constraint Chapter 2 described from the other side. A large share of our respondents run cybersecurity with at most two people, and NIS2 does not scale its obligations to the size of the security team. Where capacity is the binding constraint, the realistic answers are prioritization, reuse, and outside help: sequencing measures by risk rather than by chapter order, building evidence once and using it across several frameworks, and buying assurance capability where it is uneconomic to build it internally. Attempting full coverage with a two-person team is how implementation programs stall quickly.

The named challenge areas point in a consistent direction. Supply chain security leads at 25 percent, ahead of governance and documentation at 19 percent, asset management at 17 percent, and identity and privileged access management at 11 percent. Monitoring and logging, secure development, and backup and recovery each register at 6 percent, and vulnerability management at 3 percent. The pattern is instructive. The technical control domains are largely not perceived as the bottleneck. What organizations find hard is knowing what they have, governing and evidencing it, and extending both beyond their own perimeter, which is precisely what a principles-based regulation demands and what no product delivers on its own.

Fig. 13: Implementation status of NIS2 risk management measures among in-scope respondents.



The results reveal an interesting maturity paradox. While nearly seven in ten respondents describe themselves as advanced or very advanced in their implementation journey, only three percent consider implementation complete. This may indicate that organizations increasingly recognize the effort required not only to implement controls, but also to evidence, test, and sustain them over time.

Recurring hurdles: from requirement to operating model

Behind the individual obstacles sits a single, larger challenge: translating regulatory requirements into a viable target operating model. Governance, roles and responsibilities, risk and decision-making processes, and control mechanisms have to be designed so that cybersecurity is anchored as an organization-wide task rather than remaining an isolated IT undertaking. The recurring hurdles are consistent across the responses. They include clear support from top management, the consistent involvement of business units in protection-needs assessment, risk ownership and business continuity, and mastering complex responsibility structures in hybrid and historically grown environments.

The effort is not primarily in writing the documents. It is in transferring policies, an information security management system, and the accompanying measures into ongoing operations and monitoring them regularly. This is where the difference between a compliance project and a compliance capability becomes visible and where the legal expectation bites hardest. Measures must be effective on a continuing basis and that effectiveness must be demonstrable when the occasion arises, whether that is an inspection, an audit, or an incident.

> The regulatory environment is intended to promote stability and resilience against cyberattacks. It only becomes effective when organizations translate it into lived practice rather than documentation.

Interestingly, respondents do not primarily associate NIS2 implementation difficulties with technical security controls. Governance and documentation, asset visibility, and third-party dependencies rank considerably higher than traditional security domains such as vulnerability management, incident response, or monitoring. The challenge appears increasingly organizational rather than technological.

Across multiple questions, a consistent theme emerges: organizations no longer appear to struggle primarily with understanding NIS2 requirements. Instead, implementation capacity has become the dominant challenge. Despite high levels of reported implementation progress, a majority continue to cite internal resource limitations, supplier dependencies, and budget constraints as significant barriers.

Voices from the field

The open answers in this year's survey add context that the percentages alone cannot provide, and several themes recur often enough to be worth reporting.

The documentation burden comes first, coupled with a shortage of usable templates. Organizations describe spending disproportionate effort producing artefacts rather than improving security. Several respondents raise the dominance of CyFun itself, which they perceive as strongly promoted while practical alternatives feel thin on the ground. It is a fair concern, though one that must be weighed against the coherence a single national framework buys. Organizations operating across several EU member states describe the difficulty of running one framework through several national transpositions, each with its own registration mechanics, deadlines, and supervisory habits. Questions about auditor consistency appear repeatedly, since two assessors reaching different conclusions on the same control set limits the value of the assessment for everyone. Sector-specific financing gaps are raised sharply by hospitals, where the funding mechanism is described as insufficient for the cyber investment the regulation requires. A number of responses return to accountability, noting that NIS2 places responsibility at board level and that this has not everywhere translated into board-level attention.

These themes echo last year's central conclusion, which the quantitative data has now reinforced: self-assessment tends to outpace reality, and the first supervisory audits will define what good practice actually looks like in Belgium. Organizations that would rather learn that from a readiness assessment than from a supervisor still have time to choose.

Breadth first, then depth

For the implementation work still ahead, a two-stage logic holds. First, stabilize breadth, bringing measures consistently from partially to largely implemented and transferring them into standardized operations. Then increase depth, with the focus on controls that are not merely implemented but demonstrably effective. For CISOs that means standardizing controls, generating defined evidence, and anchoring testing and review as a recurring cycle. For management it means aligning priorities and resources so that what emerges is not a completed implementation project but a permanent, audit-ready control operation.

The survey data suggest the market is well into the first stage and has barely begun the second. Design is largely done; testing and evidence are not. The notification figures make the point most starkly, with 44 percent having a defined process they have never tried, and the same gap appears wherever the survey asks about verification rather than intention. Investment should therefore flow into control operations, measurability, tests and exercises, and management reporting, not exclusively into one-off implementation programs.

For the management body, steerable implementation requires clear target states per measure, quarterly milestones, and unambiguous owners, supported by compact recurring reporting built on a few key figures covering maturity, coverage, and evidence of effectiveness. On this year's data, the priority fields are supply chain security, effectiveness testing, and the notification process.

Attacks on the supply chain

Supply chain attacks allow attackers to circumvent security measures by going through a third party, and at central service providers, they can trigger cascade effects along many customer relationships at once. In Belgium, this has moved from a theoretical concern to a measured and rising exposure.

44 percent of respondents state that a service provider or supplier fell victim to a cyberattack within the last 12 months, up from 38 percent. A further 13 percent report at least a suspicion that this happened, against 12 percent a year ago. Taken together, 57 percent of our respondents either know or suspect that a supplier in their ecosystem was hit during the year, against 50 percent a year ago.

The visibility story alongside it is the more encouraging one. The share of organizations unable to say whether their suppliers had been attacked fell from 29 to 16 percent, close to a halving in a single year. Third-party incidents are becoming visible to the organizations they affect, which is exactly what maturing supplier management and improving notification practice should deliver. A remaining one in six still cannot answer the question, and in risk terms, an unanswerable question about a supplier is indistinguishable from an unknown exposure.

The survey consistently identifies supply-chain security as the practical face of NIS2 implementation. It ranks as the most frequently cited implementation challenge, one of the largest

organizational obstacles and a significant source of concern among respondents. The findings suggest that extending governance, assurance, and resilience practices to suppliers is proving more difficult than implementing internal security controls.

The impact on our respondents

Where a supplier was hit, what followed? For 27 percent of the organizations concerned it was a service interruption in their own operations, against 11 percent reporting business interruption a year ago. 16 percent report reputational damage, up from 3 percent, and 9 percent report supply bottlenecks, down from 15 percent. 7 percent report that the supplier incident was connected to an attack on their own organization, essentially unchanged from 6 percent. 47 percent record no impact on themselves.

The transmission channel from a supplier incident to its customers is therefore mainly operational rather than intrusive. The typical consequence is not that the attacker arrives next; it is that something stops working. That distinction matters for where defensive effort belongs. Guarding the connection to a supplier, by segmenting it, limiting its privileges, and monitoring it, addresses the 7 percent case. It does nothing for the 27 percent case, which is answered instead by continuity planning: knowing which suppliers are single points of failure, what the tolerable outage is for each, and what the fallback is. On this evidence, third-party risk management in Belgium is at least as much a business continuity discipline as a security one.

One further movement deserves a sentence of its own. A year ago, 53 percent of organizations could not say what impact a supplier incident had had on them. This year, that share has all but disappeared, at 2 percent. Visibility into third-party incidents has improved dramatically, which is exactly what maturing supplier risk management should produce, and it means that part of the apparent rise in operational consequences reflects better sight of what was already happening.

> More than half of our respondents saw a supplier hit, or suspected it, in the last 12 months, with the share rising to 57 percent from 50 percent a year ago. For more than one in four of those, the result was a service interruption in their own operations.

A multitude of impairments

Asked about further consequences, companies emphasized considerable internal effort: laborious analyses to remediate or restore the affected/stolen data, as well as additional effort for incident handling, documentation, reviews, and follow-up. There were also operational impairments such as disrupted payment transactions with the affected supplier, delayed order processing, and necessary access blocks.

Third-party risk

The concern matches the exposure. 84 percent of respondents are concerned or rather concerned that cyberattacks against their service providers will also affect their own organization, comprising 44 percent concerned and 40 percent rather concerned. The figure is identical to last year's 84 percent, then composed of 41 percent and 43 percent. Near-universal agreement, held stable across two waves and two different samples, makes this one of the strongest and most reliable results in the entire study.

Awareness is not the binding constraint in Belgian third-party risk. Whatever is holding the discipline back, it is not that organizations have failed to notice the exposure.

Effectiveness of security measures at service providers

To verify the effectiveness of security measures at their service providers, our respondents use several instruments. Requesting certificates or attestations is the most common, named by 51 percent, identical to last year. Self-declaration questionnaires follow at 44 percent, up from 33 percent. Third-party audits are used by 29 percent, down from 36 percent, independent audits at the service provider by 24 percent against 25 percent, and external security ratings by 22 percent, unchanged. 23 percent do not know to what extent such verification is carried out, where a year ago 9 percent did not know. Two observations follow. The first is positive: verification is now near universal in principle, and the share unable to say what their organization does has risen, from 9 to 23 percent. The second is less comfortable. The instrument that grew fastest is the weakest one. Self-declaration questionnaires rose by eleven points while third-party audits fell by seven, which means supplier assurance is becoming broader and shallower at the same time. A self-declaration provides limited assurance unless it is complemented by evidence-based audits, monitoring, or contractually anchored audit and reporting rights. It documents that a question was asked. It does not establish that the answer was true.

From a governance and liability perspective, the remaining share that cannot say is the more serious issue. Where an organization cannot explain how it verifies its critical suppliers, it can neither steer third-party risk nor demonstrate the due diligence that NIS2 expects, particularly given that supplier dependencies are in this same survey the second-largest obstacle to NIS2 implementation.

What effective supplier assurance looks like

Given the regulatory requirements and the maturity gaps discussed in this chapter, the key components of an effective program are clear. For critical suppliers, these include risk-based assessment and qualification before onboarding; contractual minimum requirements, including audit and notification rights; concrete evidence rather than simple claims, with the level of evidence matched to the criticality of the service; and continuous monitoring instead of relying on an annual questionnaire. They also include organizational controls for managing the supplier relationship, such as the four-eyes principle, out-of-band confirmation for sensitive changes such as bank details, least-privilege access, and strict separation of access. For the most important suppliers, organizations should also conduct joint continuity and crisis exercises and deliberately develop alternatives, such as second suppliers or alternative data exchange routes. The purpose of all these measures is the same: to ensure that the arrangement works effectively during an incident and can withstand an audit afterwards.

Software supply chain

In software development the supply chain is a central risk driver in its own right. It co-determines whether products are developed securely or whether vulnerabilities enter the organization's own software supply chain through third-party components, build tools, and dependencies. The development pipeline offers attackers a scalable lever, since one compromise is distributed automatically to everyone downstream.

61 percent of organizations surveyed now rate attacks against the development pipeline as a major risk, made up of 29 percent who agree and 32 percent who rather agree. A year ago, the figure was 42 percent. That is a rise of nearly twenty points in twelve months and one of the sharpest escalations anywhere in this study. It is grounded in experience rather than speculation, since among the free-text answers on attackers one respondent names a specific software supply-chain campaign as the source of an incident.

The escalation sits comfortably alongside the wider picture. Tool and dependency complexity keeps growing, cloud services multiply the number of parties with a hand in the build, and AI-based assistance and code generation are entering development processes faster than the governance around them. A pipeline that pulls in generated code, third-party packages, and managed build infrastructure has a supply chain of its own and few organizations map it as such. Securing it through provenance of components, integrity of the build, and control of what may reach production strengthens both product security and the integrity of the data the products process.

> In software development, the supply chain co-determines whether products are secure. Organizations that secure their software supply chain raise not only product security but the integrity of the data they process.

Security standards of suppliers

Concern about suppliers not meeting the same information security standards fell (24 percent vs 51 percent in 2025) while incidents involving suppliers rose. That tension needs an explanation rather than a headline and there are at least three plausible ones. Risk perception may have re-anchored, with the specific worry about standards absorbed into a broader and better-articulated third-party risk as supply chain attacks climbed to third place in the overall risk ranking. Prioritization may have shifted, with attention moving from supplier hygiene to the operational consequences of supplier failure. Or maturity may genuinely have improved for some, with better assurance producing better-founded confidence. The countervailing evidence argues against reading it as evidence that complacency has been resolved. 41 percent concede that their organization lacks awareness of supply-chain attack risks, up sharply from 31 percent a year ago. Self-awareness of the gap is growing even as the specific concern falls, which is not the profile of an organization that has solved the problem.

The operational figures settle the question. Only 27 percent have an emergency plan or incident and continuity playbook for security incidents in the supply chain, down from 36 percent. 27 percent regularly coordinate and evaluate the risk of attacks within the supply chain together with their suppliers and service providers, level with 27 percent a year ago, while 24 percent at least conduct regular supplier security assessments.

Set those numbers beside the 84 percent who are concerned about supplier attacks affecting them, and the story becomes clear. Concern is near-universal, practice is thin, and the gap between the two widened this year rather than narrowing. One organization in four maintains a regular risk dialogue with the suppliers it depends on. Just over one in four could follow a plan if one of them failed. For a discipline that respondents themselves rank as their leading NIS2 challenge area and their second-largest implementation obstacle, that is a striking shortfall and, given that the operational impact of supplier incidents is now measurable at 27 percent, an expensive one.

Chapter takeaways

Regulation has become the operating environment rather than an approaching event. The real work has shifted from determining applicability to integrating NIS2, CyFun, DORA, the AI Act, and the GDPR into one control framework instead of several parallel compliance exercises.

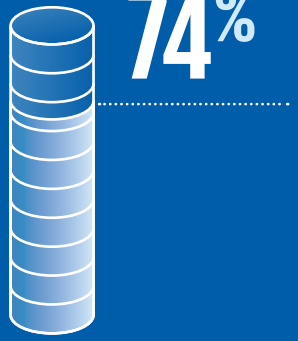
Progress is real but recalibrating, with more organizations well advanced in their NIS2 implementation journey, while far fewer now claim to be finished. That suggests they are learning what "done" requires rather than losing ground, and CyFun is emerging as the established Belgian route.

Design has outrun assurance. Most organizations have a notification process they have never tested and the binding constraint is capacity rather than conviction.

Third-party risk is where the gap between concern and practice is widest. Supply chain security is simultaneously the leading NIS2 challenge area and the least operationalized discipline in this study.

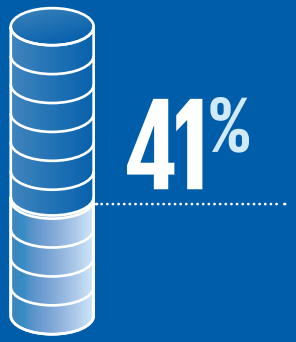
04 Digital sovereignty

Digital sovereignty has evolved from a mere political buzzword into a central strategic question for business, the state, and society. The geopolitical tensions of recent years, increasing trade conflicts, and the technological dominance of a few global providers have clearly exposed Europe's vulnerability.



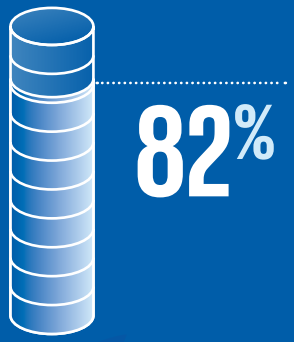
74%

describe themselves as (very) dependent on digital technologies and services from abroad.



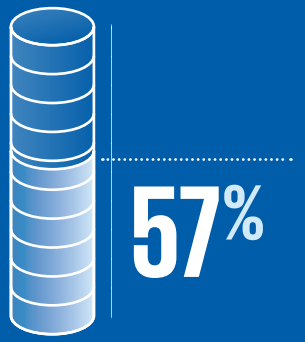
41%

do not know how long they could operate without foreign technology; of those who do, 56% say three months at most.



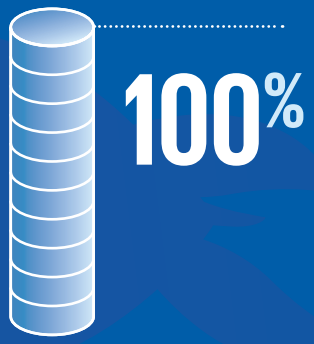
82%

see Belgium as (very) dependent on IT component imports.



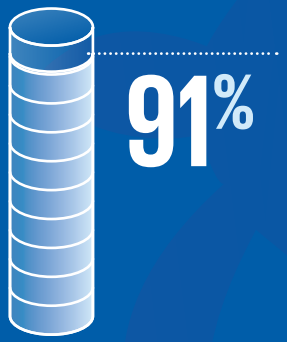
57%

expect Belgium's import dependence to increase over the next five years.



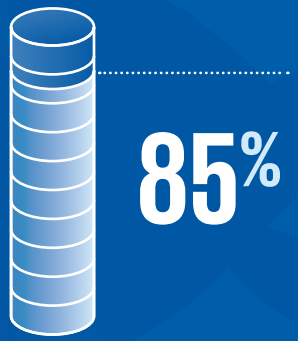
100%

place the European Union among their five most trusted locations for business relationships.



91%

want politics to prioritize digital sovereignty, with zero disagreement.



85%

want Belgium to invest more in key technologies.

Digital sovereignty

Belgium is dependent on non-European providers for large parts of its digital infrastructure, its cloud services, and its security-critical technologies, often without sufficient transparency about data flows, access rights, or legal means of influence.

These dependencies grew historically and for good reasons. Efficiency, economies of scale, and innovation speed meant that digital solutions were selected primarily on economic grounds, while questions of jurisdiction, control, and strategic resilience played a secondary role. In a globalized and stable world, that division of labor makes obvious sense. Under today's geopolitical and regulatory conditions, it is increasingly a risk. Digital infrastructures have long since become critical infrastructure, and their control helps determine economic stability and the state's capacity to act.

For cybersecurity specifically, digital sovereignty is decisive. Security does not end with technical protection measures. It begins with control over systems, data, and access. Where central components sit outside an organization's own sphere of influence, additional risks follow, including limited transparency, potential third-party access, and reduced ability to respond during an incident. Without digital sovereignty, cybersecurity is structurally limited. This chapter examines the state of digital sovereignty in Belgium and the areas for action that emerge from it.

> Technological progress requires innovation, competencies, and sovereignty in the digital domain.

Digital technologies from abroad

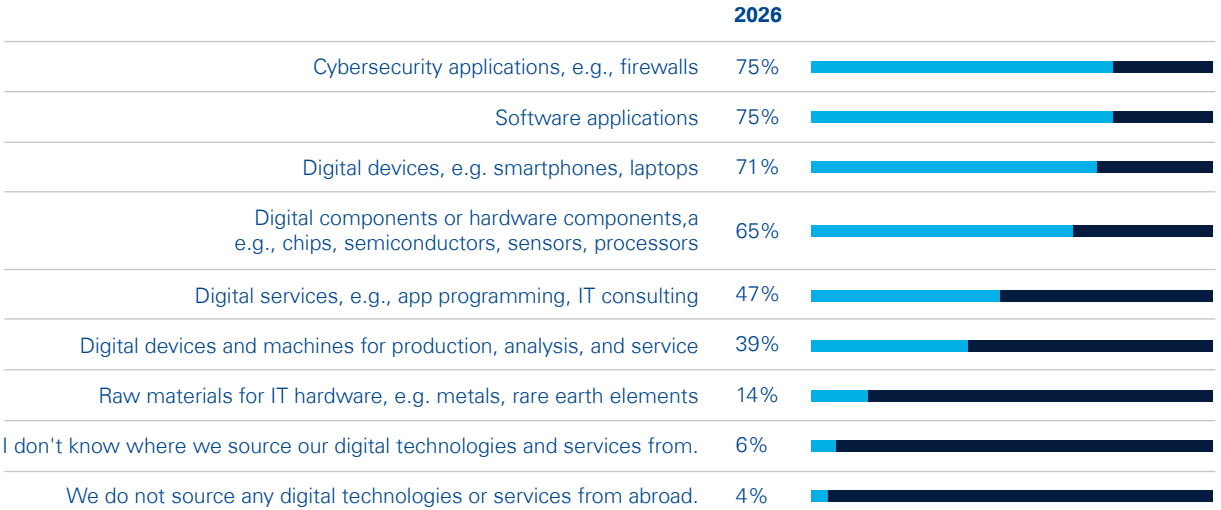
Respondents report sourcing most of the digital technologies they use from abroad, and the ordering of what they import is worth pausing on. Cybersecurity applications, meaning firewalls and other security-relevant components, are sourced from abroad by 75 percent, jointly the highest category alongside software applications, also at 75 percent. Digital end devices such as smartphones and laptops follow at 71 percent, and hardware components including chips, sensors, and processors at 65 percent. Only 4 percent of respondents state that they source no digital technologies or services from abroad at all.

The security implication deserves to be stated directly. The tools organizations rely on to protect themselves are, on this evidence, alongside software applications, their most import-dependent technology category. This creates, in addition to the traditional confidentiality concerns regarding who

can access the data and where telemetry data is stored, a new availability risk. This risk stems from growing geopolitical uncertainty and the potential impact it may have on the continuity and resilience of cybersecurity and software solutions provided to Belgian companies.

This is not an argument against foreign security tooling, which is often the best available and, in several categories, the only realistic option. It is an argument for treating the security stack as a sovereignty question in its own right, which means asking where its data resides, what happens to support and updates if the commercial or political relationship changes, and what the fallback looks like. Chapter 6 shows the market reaching the same conclusion from the demand side, with 69 percent now paying attention to a provider's country of origin when procuring cybersecurity solutions and 61 percent saying they would prefer Belgian solutions where these exist.

Fig. 14: Digital technologies from abroad.

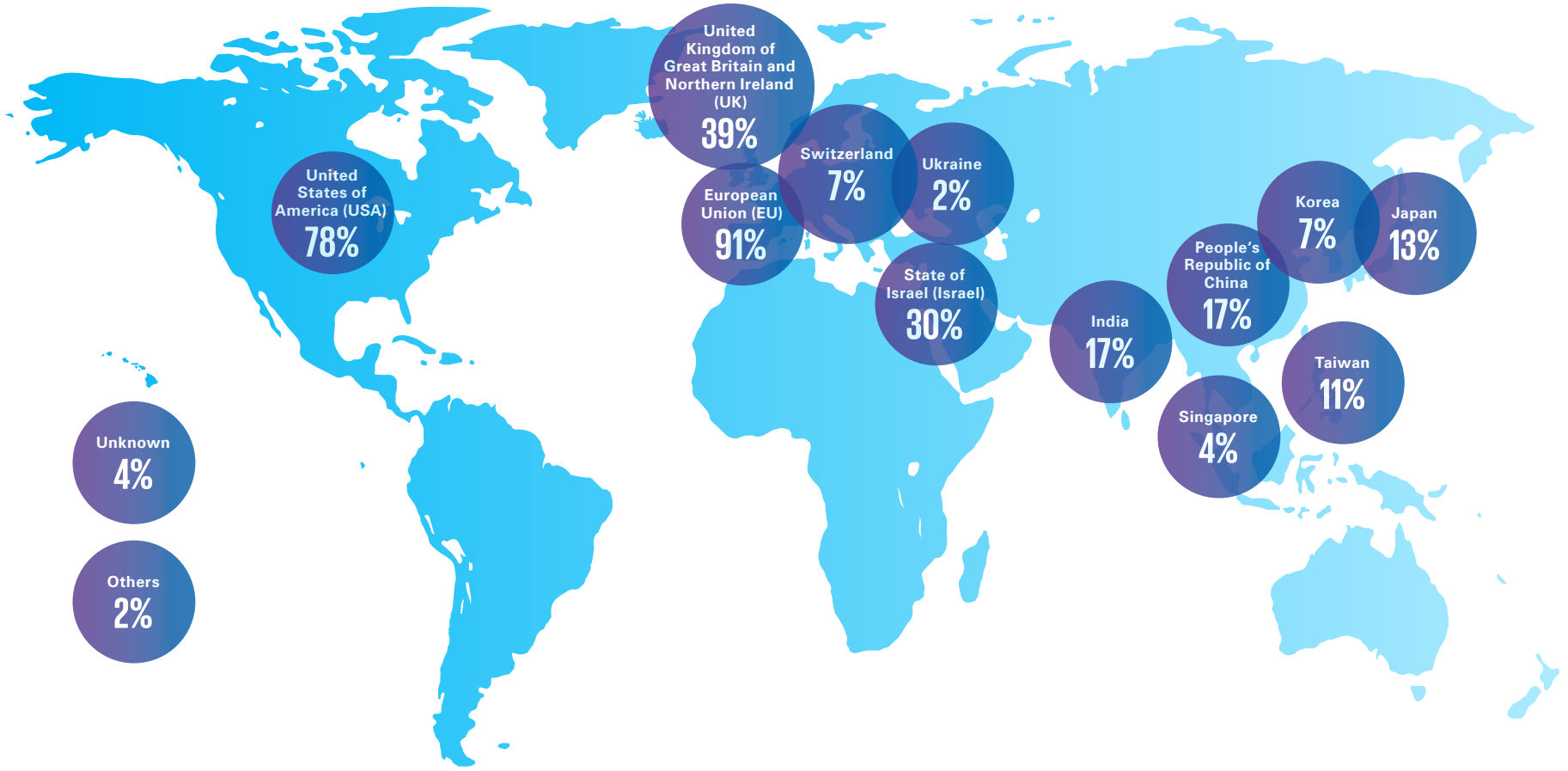


Regions from which digital technologies are sourced

Asked where their digital technologies come from, respondents name the European Union first, at 91 percent, followed by the United States at 78 percent, and the United Kingdom at 39 percent. Israel follows at 30 percent, then India and China at 17 percent each. Taiwan is named by 11 percent of the respondents.

Taiwan's low direct share should not be mistaken for low dependence. Few respondents buy directly from Taiwan, yet almost all of them depend on what Taiwan produces. Respondents recognize this themselves, with 69 percent regarding Belgium as very or rather dependent on semiconductor imports. The distance between 11 percent direct sourcing and 69 percent acknowledged dependence illustrates why sovereignty analysis cannot stop at the first tier of suppliers. The dependencies that matter most are usually the ones that never appear on an invoice.

Fig. 15: Regions from which digital technologies are sourced.



Companies in dependence

Three quarters of surveyed organizations describe themselves as dependent on digital technologies and services from other countries: 39 percent very dependent and 35 percent rather dependent, 74 percent together. Only 16 percent consider themselves independent. That places the supply chain questions of Chapter 3 in a wider frame, because an interruption need not be malicious to be damaging, and the same dependence that produces efficiency in normal conditions produces fragility in abnormal ones.

The biggest risk is not knowing

The question that turns dependence into a business risk is how long an organization could keep working if foreign digital technologies and services became unavailable. The most striking result here is not an answer but its absence: 41 percent do not know.

For an organization to be resilient under geopolitical uncertainty, knowledge of its own dependencies is the foundation everything else rests on. It makes planning possible, allows alternatives to be worked out in advance, and converts an abstract worry into decisions about which systems to duplicate, which contracts to renegotiate, and which risks to accept knowingly. The organizations that cannot answer the question are not necessarily worse prepared than the rest. They simply have no way of knowing whether they are.

Fig. 16: How dependent is your company on digital technologies and services of other countries?

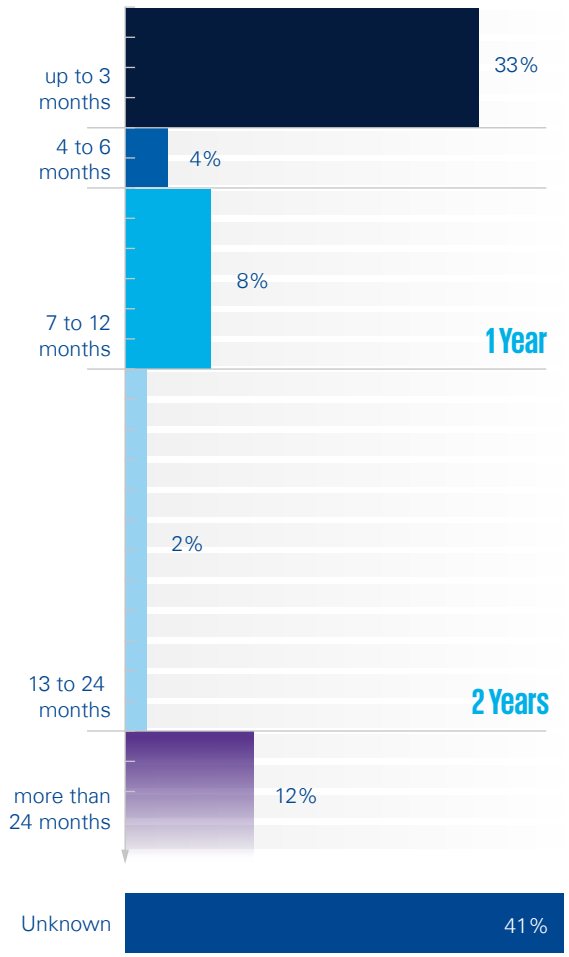
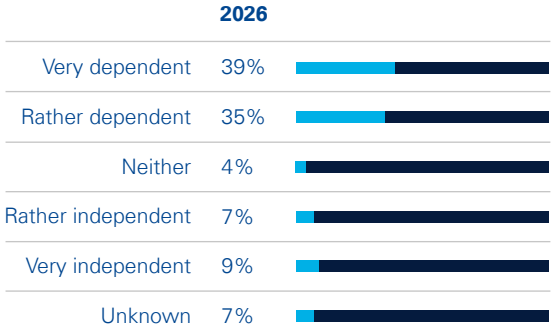


Fig. 17: Time to standstill if foreign digital services fail.

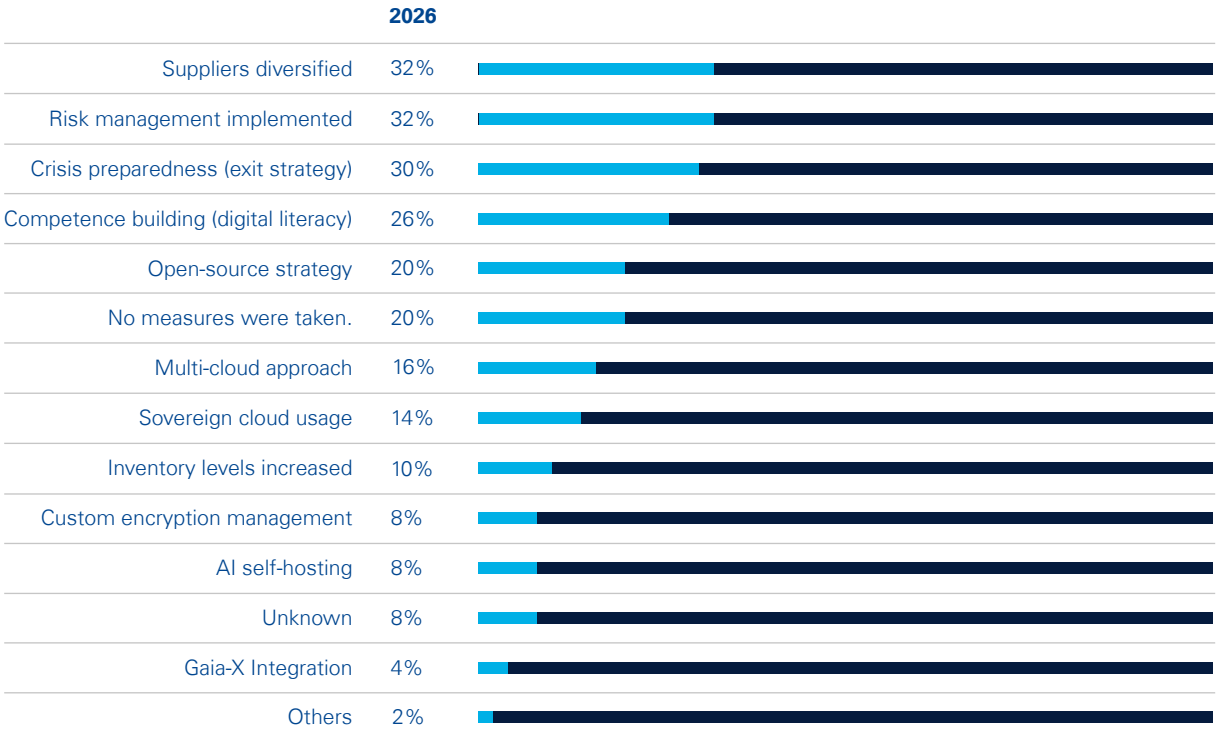


Taking precautions

What are respondents doing about it? Two measures share first place. Implementing risk management measures and diversifying suppliers are each named by 32 percent. Crisis preparedness in the form of an exit strategy follows at 30 percent and building internal competence at 26 percent. The more architectural responses sit further down the list, with an open-source strategy at 20 percent, multi-cloud at 16 percent, and sovereign cloud at 14 percent. 20 percent have taken no precautions at all and 8 percent do not know what their organization has done.

Two things stand out. First, most survey respondents know what they have done and what they have not. Second, Belgian respondents mostly focus on practical, short- to medium-term actions to understand and reduce risk. The most common measures are governance-related, such as assessing risks, preparing an exit strategy, and diversifying suppliers. Longer-term architectural solutions, such as open source, multi-cloud, or sovereign cloud are less prioritized because they require more effort, time, and investment.

Fig. 18: Precautionary measures and provisions to minimize digital dependencies.



Pressure from foreign partners

Resilience means responsiveness and the availability of alternative courses of action. The current geopolitical situation shows repeatedly that technology is being used as an instrument of pressure between economic blocs and survey respondents feel the resulting powerlessness. 66 percent state that they have hardly any means of responding to political or economic pressure from foreign partners or governments.

That is not a problem individual organizations can procure their way out of, which is why the appeal running through this chapter is directed at policy as much as at management. A joint European strategy for avoiding geopolitical dependencies is the only mechanism through which most of the respondents could acquire any room for maneuver at all.

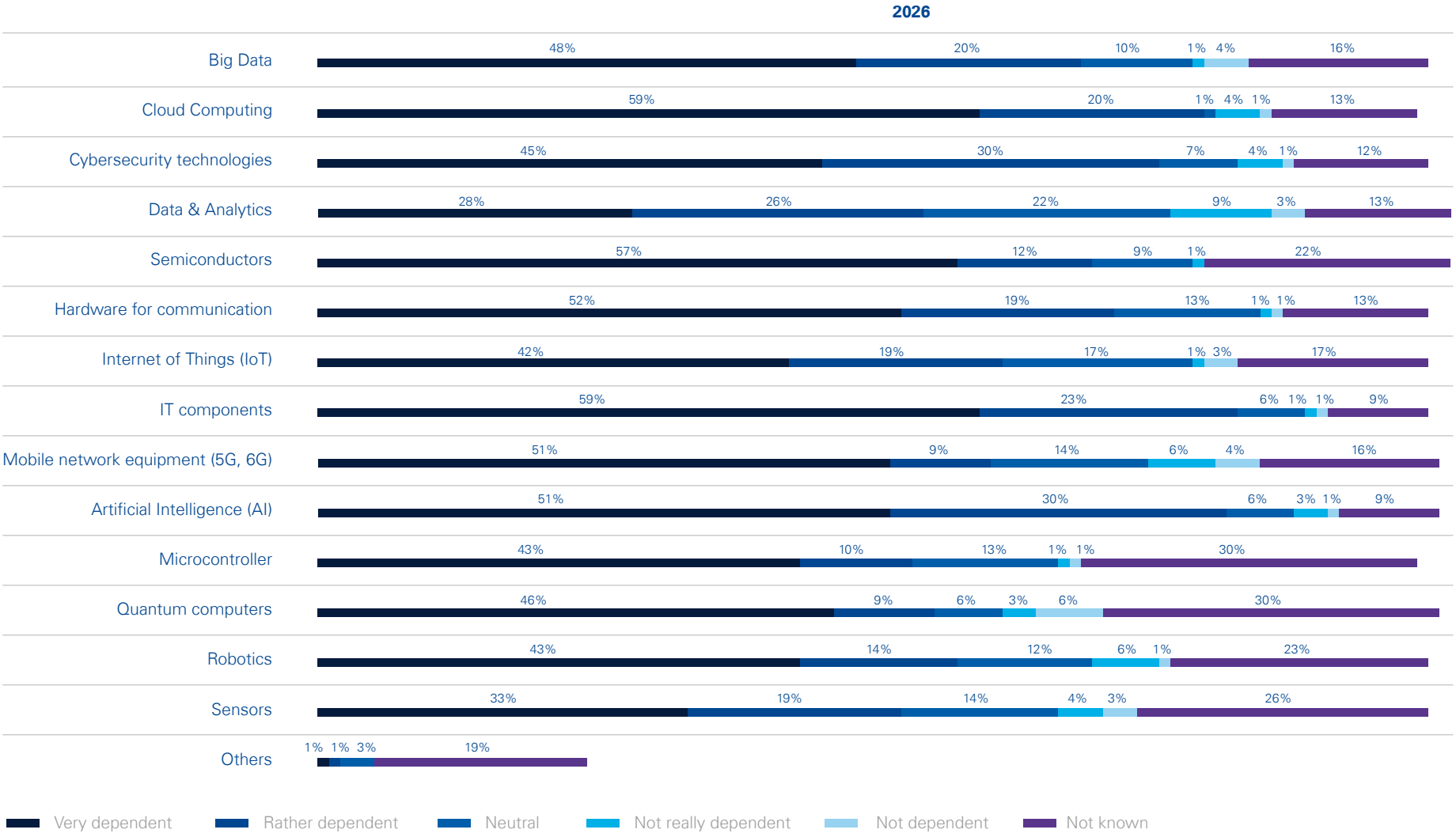
Dependence on technology imports

When asked about perceived dependency, the responses give a broader picture of how dependent our respondents believe they are in different categories. IT components lead at 82 percent, followed closely by artificial intelligence at 81 percent and cloud computing at 79 percent. Cybersecurity technologies follow at 75 percent, communications hardware at 71 percent and semiconductors at 69 percent.

Artificial intelligence in second place is the entry that should give pause. AI capability has been procured at scale for roughly two years and has already reached the top of the dependency table, with foundation models and the infrastructure they run on being sourced predominantly from outside Europe. As chapter 5 shows, the same organizations are pushing AI into their security operations at speed. Dependency is being created faster than can be governed.

Semiconductors at 69 percent complete the picture from the other direction. This is the dependency almost nobody buys directly, as the regional data showed. For a Belgian economy with strong industries such as logistics, chemicals, pharmaceuticals and precision manufacturing, it reaches well beyond the IT department and into the production floor.

Fig. 19: Belgium's dependence on the import of digital technologies from abroad.



Selection of business partners

Digital sovereignty requires organizations to rethink their strategic orientation and to identify their dependencies deliberately. Reliability and stability now weigh heavily in that assessment, with 70 percent stating that trust in the political stability and reliability of the partner country is a decisive factor when selecting global business partners.

Diversification is the standard answer to concentration risk, but for many of these technologies it is barely available. 62 percent of respondents state that only a few foreign providers exist for the technologies they use and 73 percent say that dependence on foreign business partners cannot currently be avoided at all.

This highlights the central tension of the chapter. Diversifying suppliers is one of the two most frequently named precautions, at 32 percent, yet only 22 percent actually take care to spread their suppliers across different countries or world regions and 37 percent state that distribution across regions is not a necessary element of diversification at all. Diversification is at once the preferred remedy and the one respondents themselves say the market cannot supply. Where alternatives do not exist, diversification quietly degrades into buying from two resellers of the same dependency.

Political developments are nonetheless changing behavior at the margin. Some organizations are selectively reshaping international relationships, while others continue to accept political reliability risks where alternatives are limited or the business case for change is weak. On the broader question of value chains, 49 percent hold that globally networked value chains should be oriented more regionally, moving from going global towards going regional or local, while 17 percent do not regard realignment as relevant to them.

Taken together, these figures describe an economy that has understood the problem, accepts that it is currently exposed and is adjusting where adjustment is possible. Realignment is happening at the edges, in partner selection, risk acceptance and regional preference, but the harder question sits in the technology stack itself. Many organizations rely on SaaS platforms and security tools that are deeply embedded in their operating model, so changing provider often means changing processes, integrations and user habits as well. Alternatives may exist, but they are not always equivalent in quality, maturity or ease of use. The real sovereignty question is therefore not simply whether organizations can switch, but whether they are willing to trade some performance, familiarity or convenience for lower dependency risk.

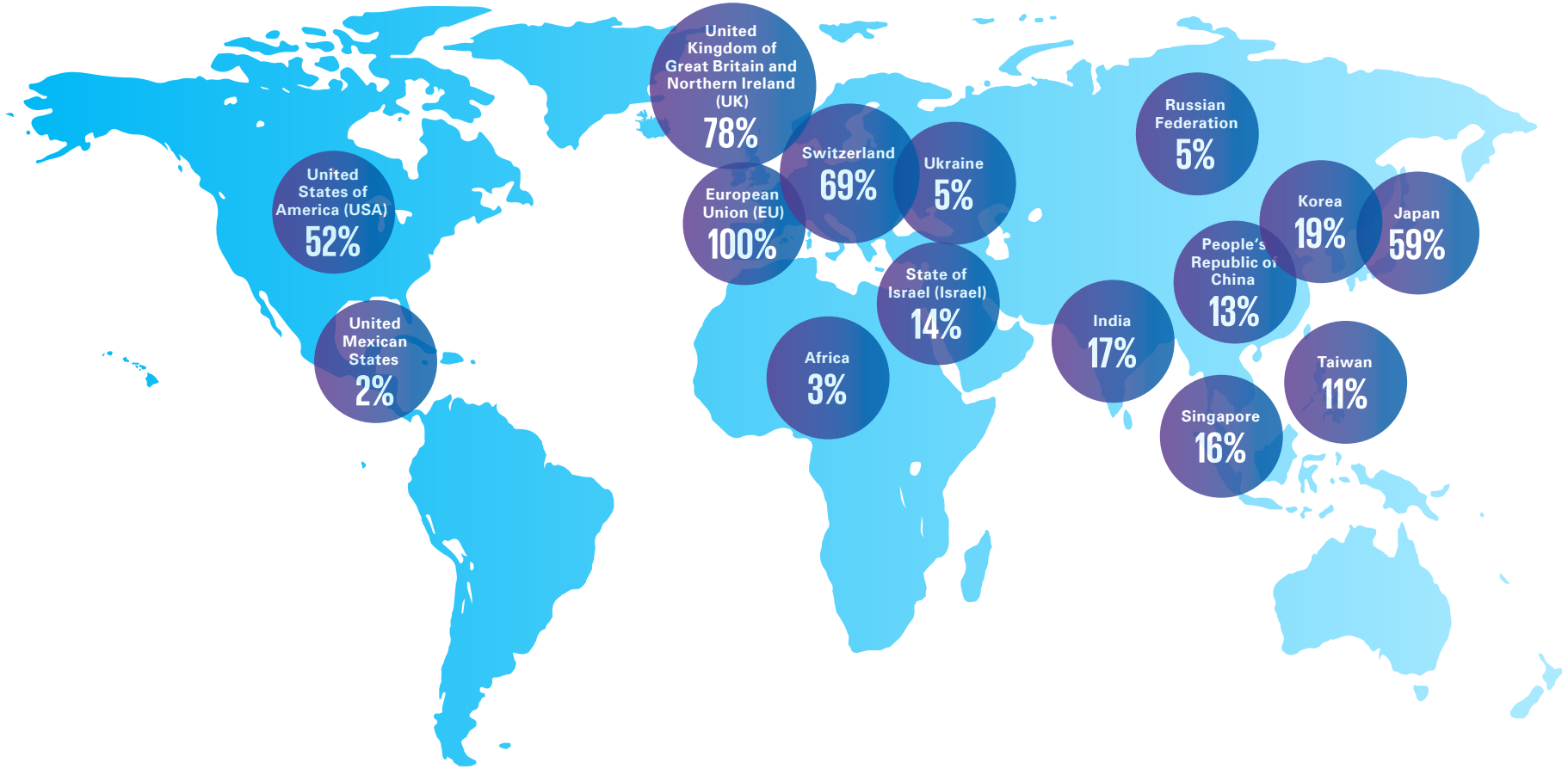
Geopolitical conflicts and dependencies

Geopolitical conflict has become a measurable business factor. The clearest Belgian result concerns the Middle East, where 60 percent of respondents report a negative impact on their own business, made up of 18 percent who agree and 42 percent who rather agree, while only 17 percent see none. As the survey fieldwork concluded in June 2026, these responses reflect business sentiment after the latest escalation in the region, when disruption to trade, shipping routes and supply chains was already being felt.

For Belgium this is a real concern. An economy organized around the port of Antwerp-Bruges, chemical and pharmaceutical supply chains and a logistics sector serving the wider European hinterland feels maritime route disruption early and broadly. The digital dimension follows the physical one, since hardware, components and devices travel the same routes and a shipping disruption becomes a technology availability problem some weeks later.

The war in Ukraine is judged to have a negative effect on their own business by 47 percent, with only 15 percent identifying no effects. 42 percent are concerned about the economic consequences of an escalating conflict between China and Taiwan, which is lower than the Middle East figure but concerns a scenario that has not yet occurred rather than one already under way. Set beside the 69 percent who acknowledge semiconductor dependence, it suggests that the Taiwan scenario is understood as serious in principle but has not yet been translated into concrete planning.

Fig. 20: Countries by trust as a location for business relationships.



Strengthening digital sovereignty as a political priority

91 percent of respondents state that politics should prioritize strengthening digital sovereignty in order to create suitable framework conditions for Belgian organizations, made up of 69 percent who agree and 22 percent who rather agree. Not a single respondent disagreed.

Unanimity of this kind is rare in survey research. Whatever else respondents disagree about, they are of one mind that digital sovereignty is a matter for public policy rather than something the market will resolve on its own. The quality labels "Made in Belgium" and "Made in Europe" must regain weight if the domestic location is to be secured, particularly in key technologies for digital elements but equally for IT systems. Chapter 6 records the same conviction in a more concrete form, with 79 percent saying Belgian security companies should receive targeted political support.

Trust in individual economic regions

Trust in economic regions largely mirrors the places survey respondents consider realistic and relevant for business. The European Union stands out, named by all respondents, confirming it as the natural anchor for trusted business relationships.

The United Kingdom follows at 78 percent and Switzerland at 69 percent, reflecting proximity, familiarity and perceived institutional stability rather than technological leadership alone. In a more uncertain geopolitical environment, political and economic reliability has become a location criterion in its own right. For comparison, Japan sits at 59 percent and the United States at 52 percent.

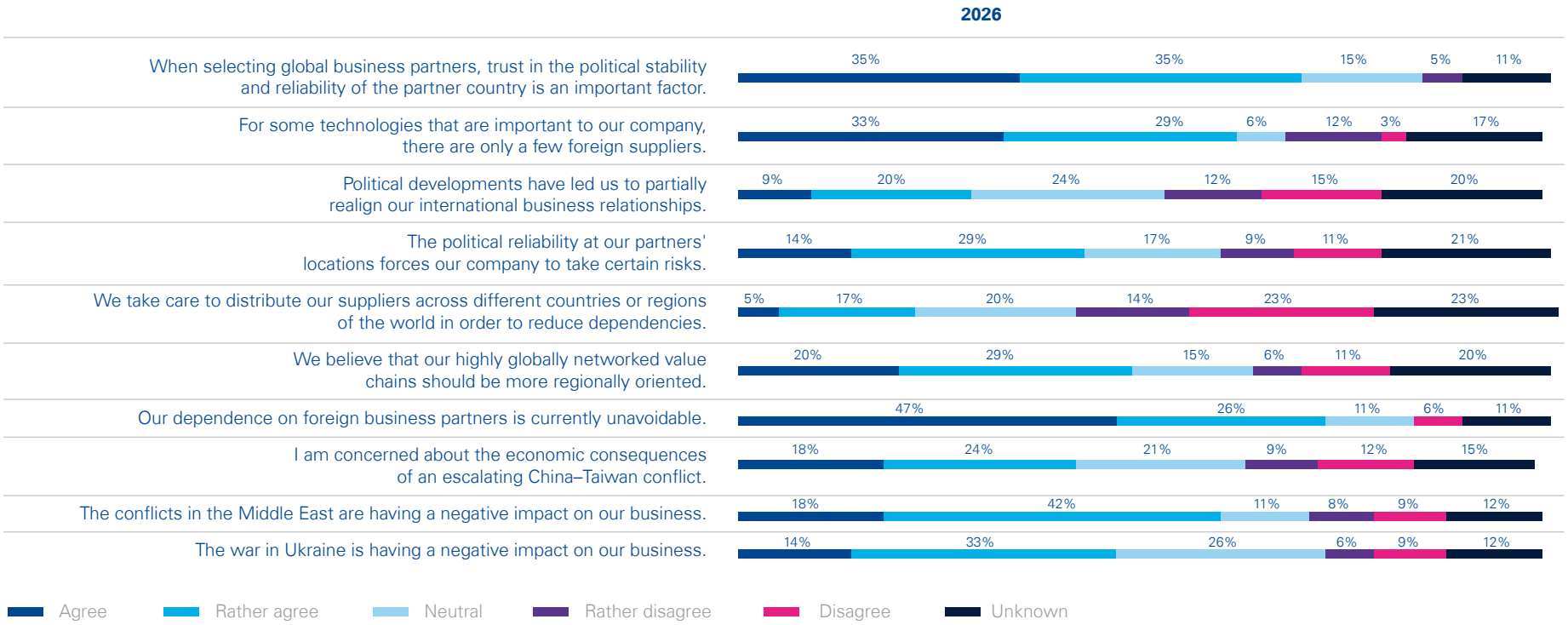
The United States illustrates the central dependency tension in the Belgian data. It is the second most common source of digital technology, cited by 78 percent of respondents, yet it ranks lowest among the top five trusted partner regions, at 52 percent. Respondents therefore rely heavily on a market they trust less than other regular partners. This mismatch helps explain why 66 percent say they have limited means to respond to external political or economic pressure. Reducing the gap would require either credible alternatives that are not yet available at scale, or a level of geopolitical trust that organizations cannot create on their own.

Belgium's investment in key technologies

Establishing key technologies and strengthening the domestic location are economic-policy tasks, which makes the appeal from our respondents worth hearing clearly. 85 percent consider it necessary for Belgium to invest more in key technologies to reduce dependencies.

Read alongside the 91 percent calling for political prioritization and the unanimous agreement on the EU as a trusted location, the message from Belgian business is consistent. Organizations accept that they cannot solve structural dependency individually, they regard the European framework as the right level at which to address it and they are asking for investment rather than merely for regulation. What this chapter cannot say is how much of that appeal reflects a willingness to pay a premium for sovereign alternatives when they eventually appear. That question is worth asking in the next wave.

Fig. 21: Digital sovereignty in the context of companies' business activity and strategic orientation.

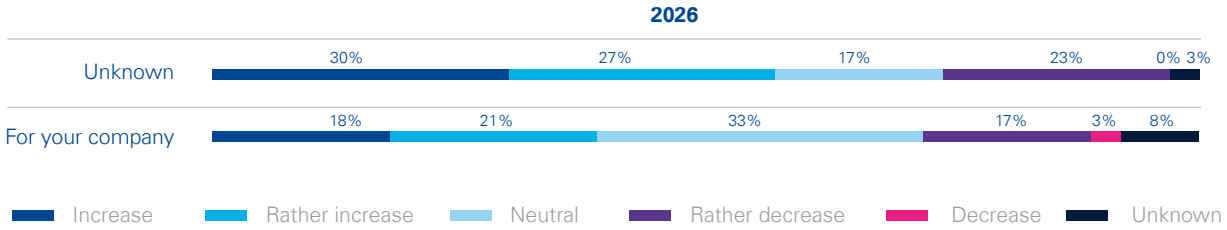


Future development of dependence

Looking ahead five years, Belgian respondents are concerned but not fatalistic. 57 percent expect national dependence on imported digital technologies, services and expertise to increase, while 23 percent expect it to decrease. That is a less pessimistic outlook than the debate around digital sovereignty often assumes, and it reflects the visibility of European sovereignty initiatives at the time of the survey.

Asked about their own organization rather than the country, respondents are less concerned. 39 percent expect their own dependence to increase and 20 percent expect it to fall. The gap between the national and the organizational view is consistent across both questions since organizations believe they have more room for maneuver over their own architecture than they have over the country's. Another way to look at it is to see the country's dependency simply as the aggregate of everybody's own. Both perspectives can be true at the same time. Individual organizations genuinely can reduce specific dependencies, while the structural dependence of a medium-sized open economy on imported technology remains beyond their collective reach.

Fig. 22: Dependence on the import of digital technologies for Belgium and for one's own company.



Chapter takeaways

Geopolitical tensions have turned digital sovereignty into a core part of effective cybersecurity. In Belgium, "the protective layer itself is among the most import-dependent technology categories, which transforms cybersecurity from a procurement question into a business continuity issue.

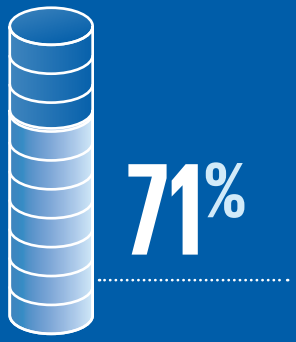
Dependence is widely acknowledged but also goes largely unmeasured, with many organizations unable to say how long they could keep operating without foreign technology.

Survey respondents are taking pragmatic precautions, but these mainly help them understand and manage dependency rather than remove it. Risk management, exit planning and supplier diversification are the most common responses, yet real diversification is difficult as good alternatives are limited.

Respondents see the European level as the right place to create viable alternatives, manage structural dependencies and strengthen digital sovereignty. Preparedness today remains mostly operational, while the structural answer depends on broader European capability-building.

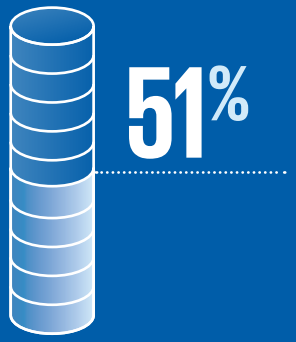
05 AI and mis-/disinformation

Artificial intelligence has long ceased to be a mere tool and is increasingly becoming an independent factor of influence in the digital risk landscape. Within a very short time, the way information is generated, distributed and interpreted has fundamentally changed.



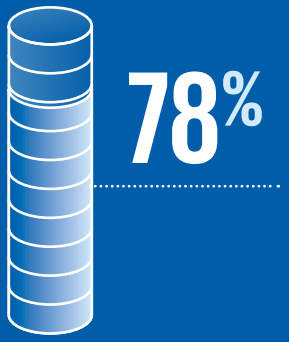
71%

see AI as an opportunity; risk perception doubled from 5% to 11%.



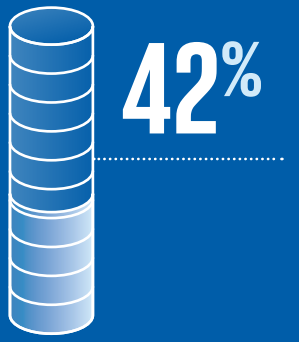
51%

see increased AI use in attacks against them.



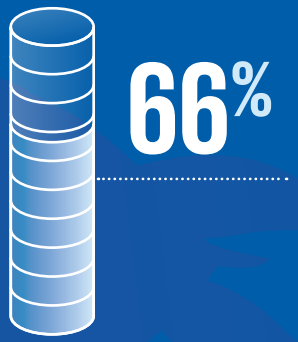
78%

name data protection violations as the top AI risk, and every risk category grew this year.



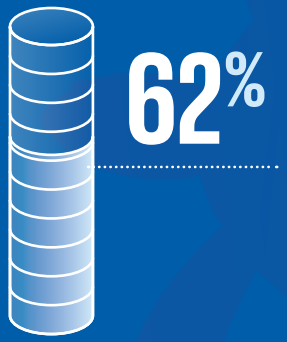
42%

say AI improved their cybersecurity over the past twelve months, up from 30%.



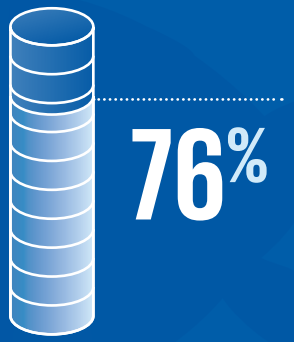
66%

attach high importance to the sovereignty of AI security solutions; EU AI Act compliance leads its aspects at 83%.



62%

view individual criminals as the main source of disinformation.



76%

believe disinformation undermines societal resilience, up from 65%.

AI and mis-/disinformation

AI systems can generate high-quality content at almost unlimited scale, reinforcing existing narratives or creating new ones. This shifts the threat landscape, because beyond systems and data, perception, context and trust are on the line.

For organizations, decisions increasingly rest on information of which the origin and integrity cannot always be traced. AI-generated content can be deployed deliberately to create uncertainty, influence reputation or disrupt operational processes indirectly. The challenge lies less in any individual piece of false information than in the systematic manipulation of the information spaces in which organizations operate.

At the same time, AI is changing the dynamic between attack and defense. The ability to automate, personalize and continuously adapt attacks lifts the scalability and efficiency of threat actors to a new level, while classic defensive mechanisms, built for a more stable and more verifiable information base, reach their limits. AI is thus becoming the central arena of cybersecurity: it's a tool, an attack surface and a defensive instrument all at once. Organizations face the task of further developing their technical protections, and of sharpening their ability to assess information flows critically, detect anomalies and actively manage trust.

That raises asymmetry: attackers need no sprint planning and no change advisory board, so their improvement cycle is basically instantaneous. The defense has the same technology available, but its release process was never designed for that speed or that volume. The survey results below should be read in that context.

How companies view AI

71 percent of respondents regard AI as an "opportunity" or "rather an opportunity", made up of 25 and 46 percent respectively. A year ago, the figure was 76 percent. In parallel, the share regarding AI more as a risk has doubled, from 5 percent to 11 percent.

The opportunities still clearly outweigh the risks and respondents remain fundamentally positive about the technology. But companies start looking at AI in a different way. After the first playful steps, the initial hype is fading, risks are becoming more visible and organizations are beginning to assess AI in a more realistic light. A doubling of skepticism in a single year, from a very low base, is not a rejection of AI, it's a sign that the technology is being taken seriously.

Fig. 23: How companies classify AI — opportunity or risk (2026 vs 2025)

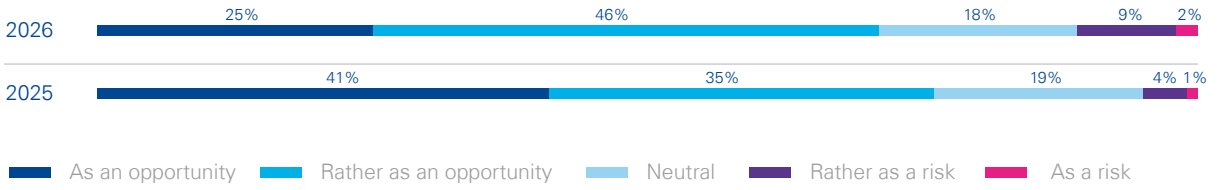
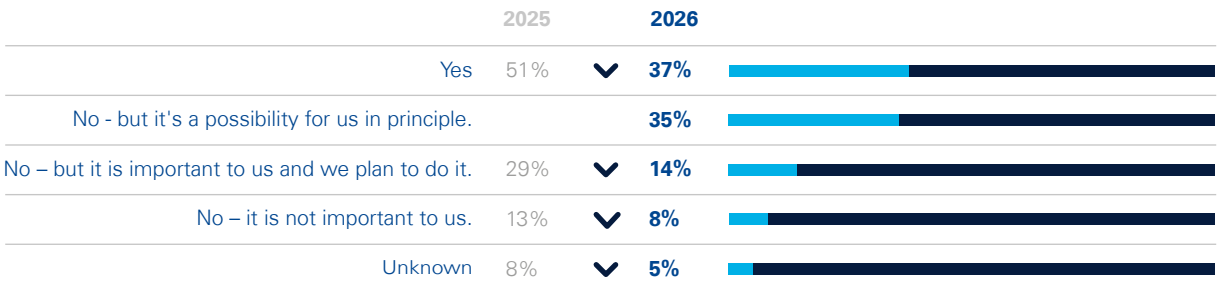


Fig. 24: Has your company already engaged with the use of AI to improve cybersecurity?



Engaging with AI to improve cybersecurity

The use cases for AI run from text generation and search to the creation of images, audio and video, and the possibilities within cybersecurity keep multiplying. 37 percent of respondents state that they have already used AI to improve their cybersecurity, down from 51 percent a year ago. A further 35 percent have not done so yet but regard it as an option, 14 percent have not used it but consider the topic important and 8 percent regard AI for cybersecurity as not relevant to them, down from 33 percent a year ago.

Roughly seven out of ten organizations are therefore either already working with AI for defense or explicitly open to it, and the group that dismisses the question outright has shrunk to a small minority. Whatever else is uncertain, Belgian security teams are no longer indifferent about AI.

AI deployment and its risks

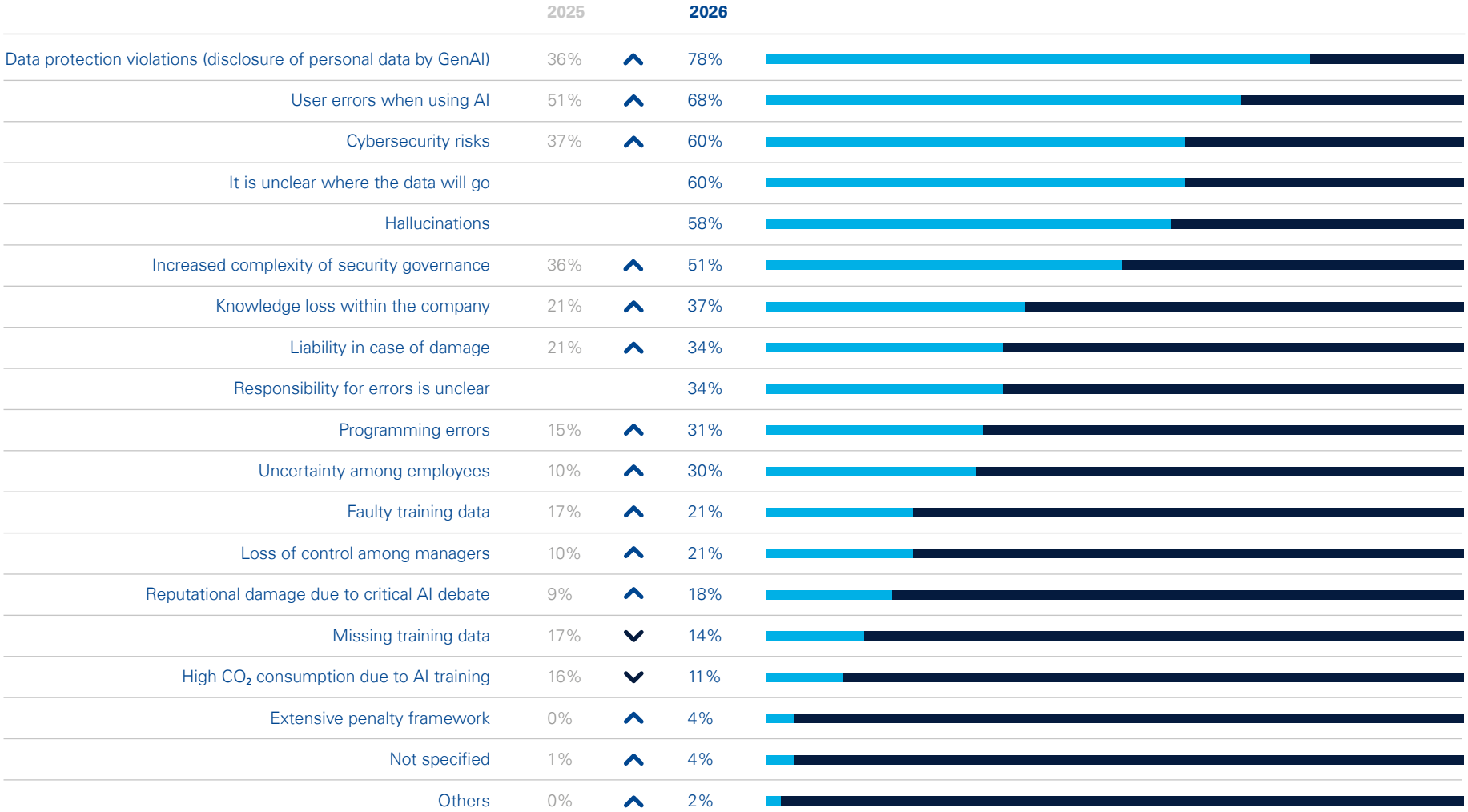
Where do respondents see the risks of using AI themselves? Data protection breaches lead with 78 percent, in particular the disclosure of personal data through generative AI, up from 70 percent a year ago. User errors in the use of AI follows at 68 percent, a sharp rise from 51 percent. Access possibilities and data transfer, meaning uncertainty about where data actually goes, and cybersecurity risks, share third place at 60 percent each, with the cybersecurity figure rising steeply from 37 percent. Hallucinations follow at 58 percent.

Striking about this result is that almost every category rose year-on-year and several rose steeply, while faulty training data, missing training data and CO2 consumption each fell slightly. Governance complexity climbed from 36 to 51 percent, the loss of internal knowledge from 21 to 37 percent and liability questions from 21 to 34 percent. This signals broad-based AI risk awareness across the board.

Governance complexity stands out: it jumped fifteen points, in the same year that AI moved into second place among the most import-dependent technology categories in chapter 4. This points at a specific problem. Capability is being adopted faster than the rules for using it can be written. The organizations answering here are not saying AI is dangerous per definition. They are saying they are not yet sure who decides what it may do, on which data, with what evidence trail, which is precisely the question a supervisor under the AI Act will eventually ask.

The top two risks tell a consistent story with the rest of this study. Data protection breaches and user errors are both, in essence, questions of what people do with a powerful tool rather than of what the tool does by itself.

Fig. 25: AI deployment and its risks — multi-year comparison 2025/2026.



The race between attack and defense

AI is available to attackers and defenders alike. 60 percent of respondents say the spread of generative AI will improve cybersecurity because it can be used to fend off attacks, made up of 22 percent who agree and 38 percent who rather agree. A year ago the figure was 67 percent. At the same time, 77 percent still say the spread of generative AI will impair cybersecurity because criminals can use it, down from 84 percent.

Both figures dropped. It reveals a pattern of a market putting away its most sweeping statements about AI while becoming considerably more specific about what it actually worries about. A year ago the question was whether AI would transform cybersecurity for better or worse. This year, fewer respondents will sign either grand claim, while far more can name data protection exposure, user error, governance gaps and hallucination risk as concrete problems.

The underlying contest has not slowed. Attackers still improve their tooling without a change process, deepfake imitation of voice and image is available through chat, telephony and video calls and phishing has been professionalized through tailor-made messages at scale. What has changed is that respondents increasingly discuss this in operational rather than existential terms.

Fig. 26: Impact of generative AI on cybersecurity — agreement vs rejection, 2025 vs 2026.

	Agree			Disagree		
	2025		2026	2025		2026
The spread of generative AI will improve cybersecurity	67%	▼	60%	8%	▲	20%
The spread of generative AI will negatively impact cybersecurity	84%	▼	77%	1%	▲	5%

Agree = Agree + Rather agree. Disagree = Rather disagree + Disagree. Neutral not shown. Base: 2025 n=88, 2026 n=60.

AI as a threat to the economy

77 percent of respondents say AI is aggravating the threat landscape for the economy through cyberattacks, against 81 percent a year ago. For the second year, roughly four organizations in five regard AI as a net aggravating factor for the economy as a whole, even as most of them regard it as an opportunity for their own organization. That combination of good for us and worse for everyone is a familiar result in survey research and it usually indicates a risk that is understood collectively but managed individually.

Lower hurdles for cyberattacks

On one point respondents are almost unanimous. 93 percent say that the low-threshold availability and ease of use of AI mean cyberattacks are increasingly being directed against organizations, made up of 68 percent who agree and 25 percent who rather agree, with no respondent disagreeing. A year ago the figure stood at 91 percent.

The reasoning behind that near-unanimity is not hard to follow. The technical prerequisites and skills once needed to conduct a cyberattack have shifted away from experts towards a broad base of actors. The pool of people capable of running a credible attack now extends from state-supported groups, who have used these tools for years, to opportunists who simply want to try. This is the mechanism behind several other findings in this study. It is why volume keeps rising, why repeat victimization has become normal and why detection capacity rather than perimeter strength is the binding constraint for most organizations.

The delivery gap is closing

Last year's edition of this study concluded that AI had not yet delivered the transformative improvements many had hoped for. This year, that judgement is visibly softening from both directions.

Looking back at the past twelve months, 42 percent of respondents believe AI has contributed to improving their cybersecurity, up from 30 percent. 18 percent deny that any improvement took place. Looking forward, 62 percent believe AI will bring a marked improvement in cybersecurity over the coming twelve months, made up of 20 percent who agree and 42 percent who rather agree while 7 percent disagree.

Both the backward-looking and the forward-looking figure rose by double digits, which is the more persuasive of the two combinations. Rising expectations alone would suggest optimism. Rising experience alongside them suggests that something is actually being delivered. AI for defense appears to be moving from promise to perceived practice in security operations. The caveat is that these are perceptions rather than measurements and the study contains no independent evidence that incidents decreased or detection improved as a result. The delivery gap is closing in the judgement of the people running these programs, which is worth knowing and is not the same as proof.

Fig. 27: Impact of artificial intelligence on cybersecurity — four statements, agreement vs rejection, 2025 vs 2026.

	Agree 2025	Agree 2026	Disagree 2025	Disagree 2026
AI is exacerbating the threat posed by cyberattacks to the economy	81%	77%	2%	5%
AI makes it easier to carry out cyberattacks	91%	93%	2%	0%
AI has significantly improved cybersecurity in the last 12 months	30%	42%	13%	18%
AI will bring a significant improvement in cybersecurity in the next 12 months	49%	62%	9%	7%

Agree = Agree + Rather agree. Disagree = Rather disagree + Disagree. Neutral not shown. Base: 2025 n=88, 2026 n=60.

Using AI in Cyber Security

AI finds its applications above all where large-scale analysis is required. User behavior analytics leads the Belgian ranking at 75 percent, up from 63 percent and has held first place across both waves. Threat intelligence follows at 70 percent, up from 59 percent and likewise stable in second place. Vulnerability management is the biggest mover, climbing from 42 to 65 percent and into third place. SIEM and security monitoring reach 58 percent against 53 percent a year ago and identity and access management 45 percent against 39 percent.

Two things characterize this picture. The ranking is stable while every category rises, which means the AI-for-defense agenda is broadening and deepening at the same time rather than churning from one fashionable use case to the next. The vulnerability management jump is the second. Chapter 1 identified ineffective vulnerability management as one of the two joint leading causes of successful attacks in Belgium and a twenty-three point rise in AI adoption for exactly that discipline is the most direct evidence in this study of organizations aiming their new capability at their known weakness.

Only 7 percent do not know where AI could be deployed to improve their cybersecurity, so use-case literacy is close to universal. The Belgian question is no longer whether teams can imagine what AI might do for them, but whether they have the governance and the capacity to run it, which returns to the staffing constraint of chapter 2 and the governance complexity concern above.

Fig. 28: Use of AI to improve cybersecurity (domains, 2025 vs 2026).

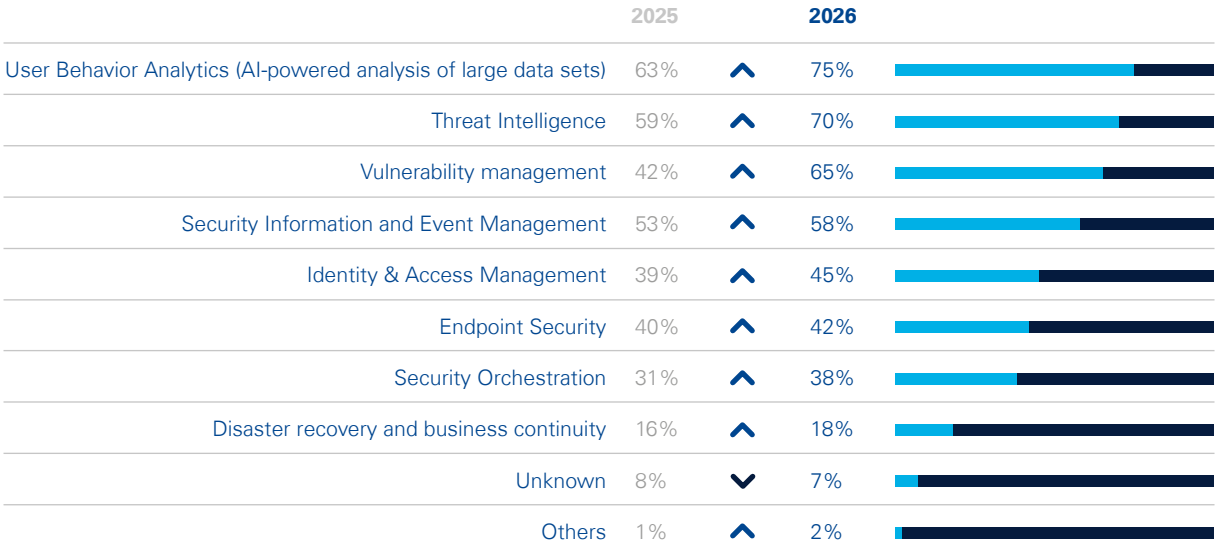
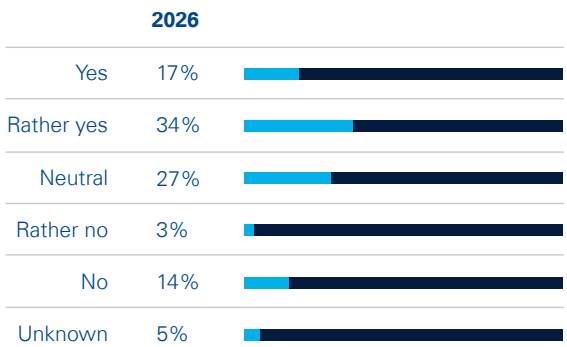


Fig. 29: Use of AI in cyberattacks against companies.



AI in cyberattacks

Just over half of respondents, 51 percent, comprising 17 percent yes and 34 percent rather yes, report that artificial intelligence is increasingly being used in attacks against them. This is most visible in phishing emails, but also in CEO and CFO fraud aimed at redirecting payments and in the well-documented cases where deepfake voice calls or impersonation in video conferences were used.

One respondent in two now perceives AI being used in attacks against their organization, on the respondents' own assessment. Set that beside the challenge dimension in chapter 2, where AI data poisoning, AI-assisted attacks and the circumvention of multi-factor authentication occupy the top of the list and the picture is coherent. AI-supported attack is no longer an emerging category to prepare for. It is the ordinary case.

Sovereignty of cybersecurity solutions

When AI is deployed defensively, what matters is that it is supplied with appropriate training data and that the integrity of the information is assured. For 66 percent of respondents, made up of 34 percent high and 32 percent rather high, the digital sovereignty of AI-based cybersecurity solutions has high importance in achieving the necessary reliability. Data residency within the EU, control over the models and control over the providers are treated as reliability questions rather than merely compliance ones.

Which sovereignty aspects matter

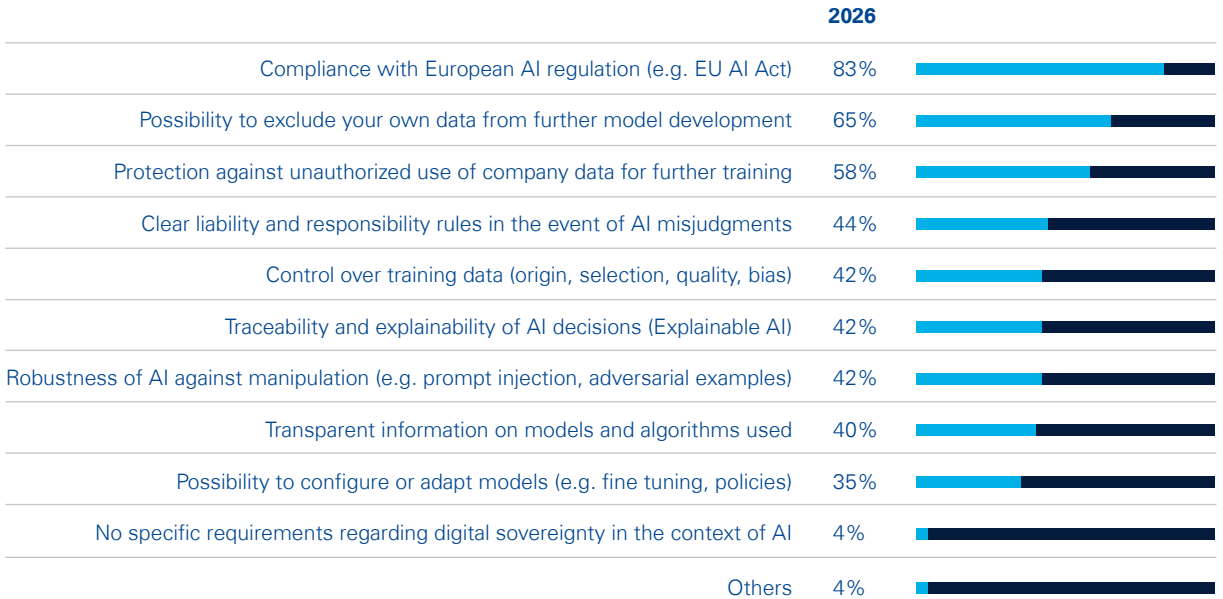
Asked which aspects of digital sovereignty matter in AI-supported cybersecurity solutions, respondents put compliance with European AI regulation such as the AI Act far out in front, at 83 percent. The ability to exclude their own data from model development follows in second place at 65 percent and protection of company data against unauthorized use for further training at 58 percent. Liability rules reach 44 percent. Robustness of AI against manipulation, meaning prompt injection and adversarial examples and the traceability and explainability of AI decisions each reach 42 percent.

The ordering is revealing and slightly uncomfortable. Respondents understand AI sovereignty primarily as a legal and data-control question: comply with the regulation, keep our data out of somebody else's model, control where it goes. The technical properties that determine whether an AI security

system can actually be trusted under attack, meaning resistance to manipulation and the ability to explain why it reached a conclusion, sit at the bottom of the list.

That is worth holding against a finding from chapter 2, where AI data poisoning was named among the leading particular challenges facing our respondents, at 45 percent. The same market that treats AI manipulation as a top-tier challenge puts the ability to configure or adapt models last among the properties it considers essential for sovereign AI, at 35 percent, with transparency about the models in use just above it at 40 percent. The ordering is understandable, since regulatory obligations are concrete and dated while control over model behavior is technical and hard to specify in a procurement document. It is a gap nonetheless. As AI moves further into detection and response, the ability to see inside a model and shape how it behaves will have to migrate from the bottom of this list towards the top.

Fig. 30: Aspects of digital sovereignty in AI-supported solutions.



Mis- and disinformation

If one theme escalated more than any other in this year's survey data, it is disinformation. 59 percent of respondents believe they could themselves fall victim to a cyberattack through which targeted influence is exerted on their organization, made up of 27 percent yes and 32 percent rather yes. A year ago the figure was 42 percent, of which only 10 percent was an unqualified yes. The overall share rose by seventeen points and the unqualified yes nearly tripled.

Last year's edition observed that awareness of influence operations was beginning to catch up with reality. That process has not merely continued, it has accelerated. Targeted influence has moved, within a single year, from something a minority considered plausible to something a clear majority expects could happen to them.

Affected business activities

54 percent of respondents now say their business activities can be influenced by online disinformation campaigns, made up of 16 percent yes and 38 percent rather yes, against 32 percent a year ago. A rise of twenty-two points is among the largest movements in this survey.

Disinformation has entered the corporate mainstream in Belgium. It is no longer filed as a political or societal phenomenon that occasionally brushes against business, since a majority of organizations now regard their own commercial activity as exposed to it. Belgium's position plausibly contributes to that. Brussels hosts the EU institutions and NATO, the country carries a dense concentration of international organizations, press and public affairs activity and the 2025 edition

already flagged this exposure as a distinguishing feature of the Belgian threat picture. What was flagged then as a structural characteristic is now showing up in what organizations say about their own operations.

The practical difficulty is that few organizations have a function that owns this risk. Disinformation sits between communications, security, legal and public affairs and it responds to none of the controls that work against intrusion. Monitoring the information environment, pre-agreeing who speaks in a manipulated-narrative scenario and rehearsing that alongside the technical crisis playbook are the measures that translate this rising concern into something operational. On the evidence of chapter 1, tabletop exercises are precisely what respondents have been doing less of.

Fig. 31: Disinformation actors.

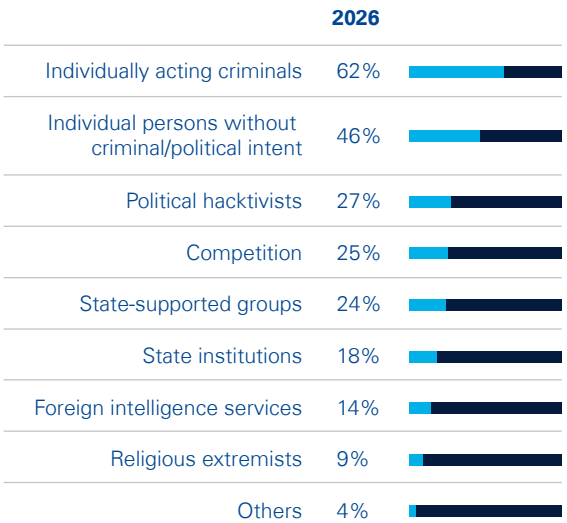
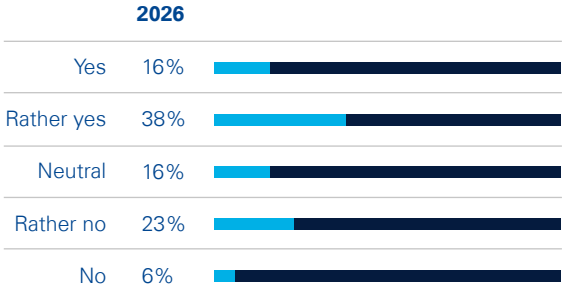


Fig. 32: Influence of disinformation campaigns on business activities



Disinformation actors

The ranking of who poses the greatest mis- and disinformation threat has changed significantly. Individually acting criminals lead at 62 percent. Individual persons acting without criminal or political intent follow in second place at 46 percent. Political hacktivists reach 27 percent, competitors 25 percent, state or state-supported groups 24 percent, state institutions 18 percent and foreign intelligence services 14 percent.

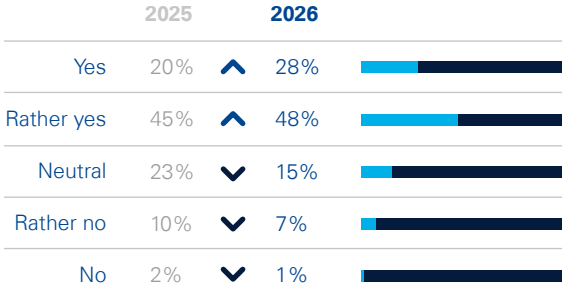
A year ago the Belgian ranking was led by political hacktivists, followed by state-supported groups, competitors and state institutions. The reordering therefore points in one direction. State-linked actors have been downgraded across the board and the perceived threat has shifted towards individuals. The picture has become more granular and, in a sense, more mundane. Organizations increasingly see themselves facing individually acting criminals whose affiliation is often unclear, operating as stand-ins for whoever benefits from the confusion they create.

Two entries in the list deserve separate attention. The first is the second-place finish of individuals with no criminal or political intent, at 46 percent. This is the unwitting amplifier, meaning the employee, customer or bystander who forwards a fabricated claim in good faith. It is a category no security control addresses and no attribution exercise resolves and its prominence explains why organizations increasingly treat disinformation as a communications and trust problem rather than a technical one.

The second is competitors at 25 percent, a continuity from last year's ranking where competition also featured prominently. Competitive disinformation remains a live concern and, unlike most entries on this list, it is one with existing legal remedies.

Societal resilience

Fig. 33: Influence of online disinformation campaigns on societal resilience (2025–2026).



Mis- and disinformation is not only an organizational concern but also a societal one. 76 percent of respondents say it can affect societal resilience, made up of 28 percent yes and 48 percent rather yes, up from 65 percent a year ago, while 8 percent do not believe such influence exists.

This increase is consistent with the broader findings in this chapter. Respondents report a higher

likelihood of being targeted themselves, greater exposure of their business activities, and a growing impact on the wider society in which they operate. Across all three areas, concern has risen significantly compared with last year.

For a phenomenon that was, until recently, largely viewed as a matter for governments and digital platforms, this represents a notable change in perception. The findings suggest that information integrity is increasingly regarded as a shared responsibility of businesses, public authorities, and the media.

> AI is becoming the central arena of cybersecurity: tool, attack surface and defensive instrument at once.

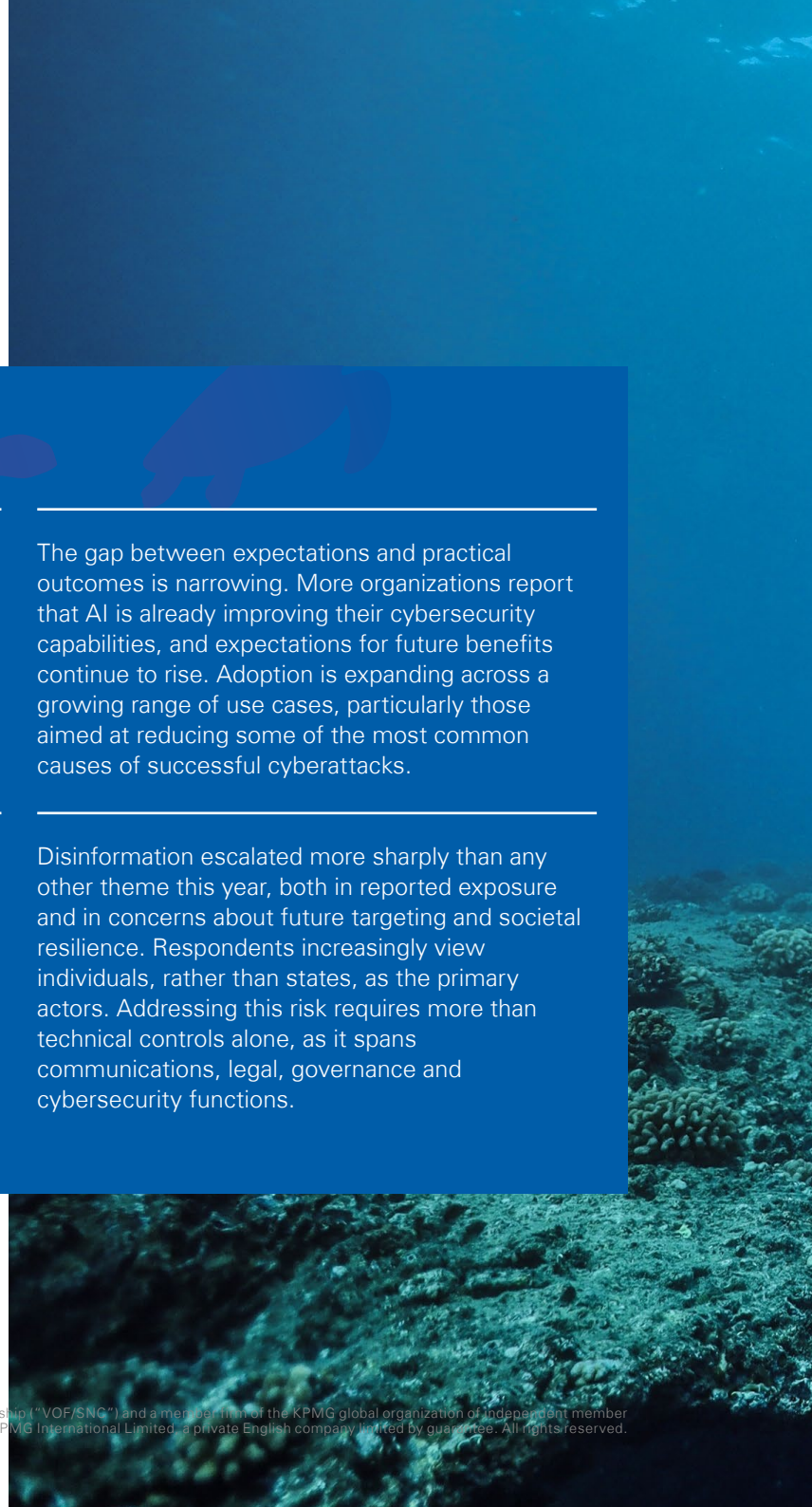
Chapter takeaways

Respondents are taking a more nuanced view of AI. While broad optimism and pessimism have both moderated, concern across specific AI risk categories has increased. The debate is becoming less ideological and more focused on practical risks and opportunities.

The gap between expectations and practical outcomes is narrowing. More organizations report that AI is already improving their cybersecurity capabilities, and expectations for future benefits continue to rise. Adoption is expanding across a growing range of use cases, particularly those aimed at reducing some of the most common causes of successful cyberattacks.

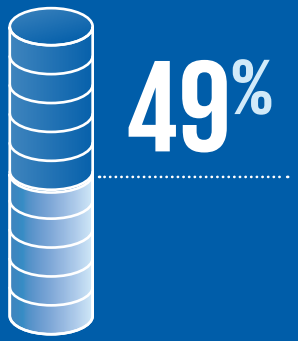
Organizations primarily view sovereignty in AI security tooling through a legal and compliance lens. Regulatory compliance and data control rank significantly higher than technical considerations such as robustness and explainability. Yet true sovereignty also requires trust in the technology itself: a model that remains vulnerable to manipulation or poisoning cannot be considered fully sovereign.

Disinformation escalated more sharply than any other theme this year, both in reported exposure and in concerns about future targeting and societal resilience. Respondents increasingly view individuals, rather than states, as the primary actors. Addressing this risk requires more than technical controls alone, as it spans communications, legal, governance and cybersecurity functions.



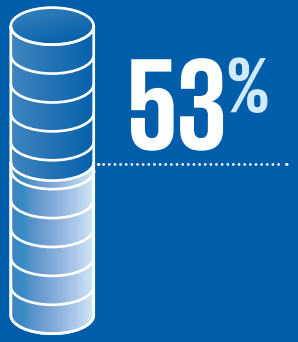
06
Outlook

Three large thematic blocks sit on the cybersecurity agenda of Belgian organizations and will continue to challenge us in the coming years: (i) dealing with rising cybercrime, (ii) the capability for effective cyber defense, and (iii) the question of digital sovereignty and industrial location policy.



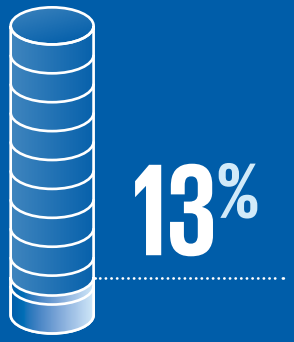
49%

Third-party risk management tops the technology agenda for the second year; AI/LLM security surged from twelfth to second.



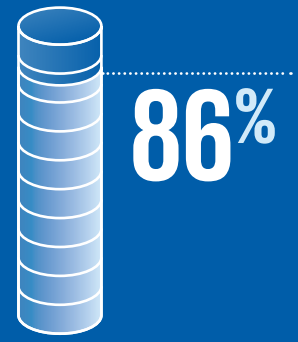
53%

say cyberattacks threaten their business existence, up from 44%.



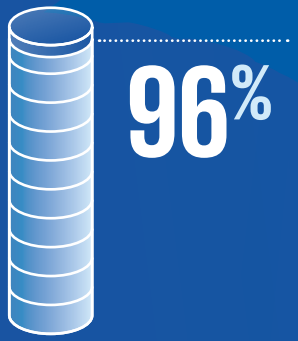
13%

are confident that Belgium is well prepared to respond to serious cyberattacks against critical infrastructure.



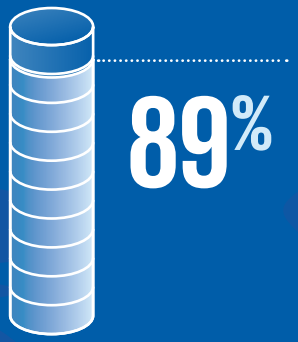
86%

want higher penalties for cybercrime.



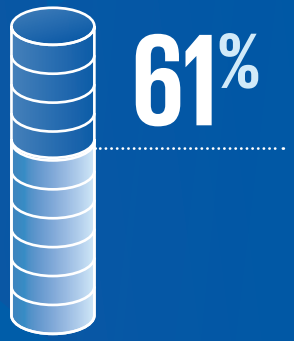
96%

call for stronger EU cooperation, the strongest consensus in the survey.



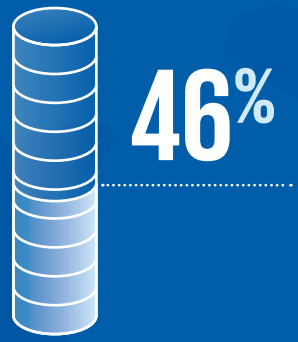
89%

say Belgium needs digital defense capability; 37% against 28% are open to offensive capability.



61%

would prefer Belgian security solutions, up from 46%.



46%

say politics neglects cybersecurity, up from 38%.

Outlook

Significant technologies and topics

The look ahead begins with a look back. Which technologies and topics gained particular importance for survey respondents over the past twelve months?

For the second year running, third-party risk management tops the technology agenda – named by 49 percent of respondents – and this year it has widened its lead. In second place is the security of AI and large language models at 37 percent, up from twelfth place a year ago. Application security follows at 25 percent, with identity and access management and business continuity management also ranking highly. Backup and recovery, which ranked second on last year's agenda, has slipped to 20 percent and end-user security and awareness now reaches 17 percent. Multi-factor authentication barely features at 10 percent.

This is a supply-chain-and-AI agenda and it is internally consistent with everything else in this study. Third-party risk management leads because supply chain attacks climbed from eleventh to third in the risk ranking in Chapter 2, because 84 percent fear that a supplier incident will reach them - 57 percent saw or suspected one this year - and because supplier dependencies are the second-largest obstacle to NIS2 implementation. The NIS2 and DORA supplier obligations pull in the same direction. When a topic holds first place across two waves and widens its margin, it has stopped being a trend and become a structural priority.

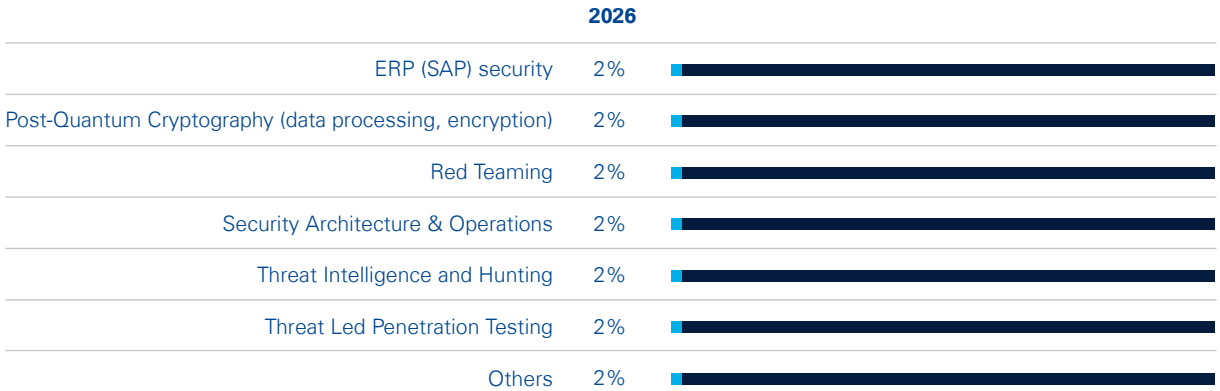
The AI security jump from twelfth place to second is the most notable shift and closely matches the risk data. AI data poisoning is among the leading challenges at 45 percent; every AI risk category rose year-on-year, and half of respondents now see AI in the attacks directed at them. What was a specialist curiosity twelve months ago is now the second most common concern that Belgian security functions say they worked on.

The descents of backup and recovery as well as multi-factor authentication are worth reading carefully. Backup and recovery slipping down the list does not mean organizations have stopped backing up. It means the discipline is largely built and no longer competes for attention. Multi-factor authentication at 10 percent points the same way, having become an assumed baseline rather than a project. The caution attached to both is the one this study keeps returning to. Capabilities that stop being priorities also stop being tested, and while 51 percent now treat the circumvention of multi-factor authentication as ordinary business, 28 percent still rank it among their top five risks against the 10 percent who treat it as a current priority. A control can be routine and worth attacking at the same time.

Fig. 34: Technologies and topics that gained importance for Belgian organizations over the past 12 months.

	2026		2026
3rd Party Risk Management	49%	OT Security (Industrial Control Systems)	10%
AI/LLM security	37%	Anti-fraud management	8%
Application Security	25%	Attack Surface Analysis	7%
Business Continuity Management	24%	CERT/CSIRT/SIRT (own)	7%
Identity & Access Management (IAM)	24%	Cloud Access Security Broker	7%
Backup and recovery	20%	Cloud Security Posture Management	7%
Data Leakage Prevention	20%	Cloud Threat Detection	7%
End-User Security & Awareness	17%	Denial of Services (D)DoS Protection	7%
Vulnerability Management	17%	Secure Software Development	7%
Governance issues (Security Regulations & Compliance)	15%	Security Information & Event Management (SIEM)	7%
Incident Response Management	15%	Crisis & Resilience Management	5%
IT and OT security convergence	15%	Hybrid threats (disinformation/misinformation)	5%
Penetration testing	14%	AI-supported protection mechanisms including forensics	5%
Security risk analysis and risk assessments	14%	Security Orchestration, Automation and Response (SOAR)	5%
Privileged Access Management (PAM)	12%	Security Operation Center (SOC - own)	5%
Security Operation Center (SOC - outsourced)	12%	Container security	3%
Zero Trust	12%	Next Generation Firewall	3%
Advanced Persistent Threat Engines	10%	Physical Information Security	3%
Endpoint Detection & Response (EDR)	10%	Security Monitoring	3%
Multi-factor authentication	10%	Security Testing	3%

2025 and 2026 use different measurement bases; rank movements are indicative and the values are not directly comparable.



Cybercrime: the emotional significance of cybersecurity

55 percent of respondents say the emotional significance of cybersecurity within their organization has changed as a result of current geopolitical conflicts, made up of 20 percent who agree and 35 percent who rather agree. The figure is identical to last year's 55 percent, a rare point of exact stability in a survey full of movement. For 23 percent the conflicts hold no significance for how cybersecurity is perceived internally.

Cyberattacks as question of survival

53 percent of respondents say cyberattacks threaten their entrepreneurial and business existence, made up of 23 percent who agree and 30 percent who rather agree, up from 44 percent a year ago. A nine-point rise in a single year means a majority of respondents now regard a cyberattack as capable of ending their business rather than merely as a cost.

That figure deserves to be read alongside Chapter 2, where 44 percent now rate the likelihood of damage as high or rather high, up from 35 percent. Both the perceived probability and the perceived severity rose in the same year. Risk, in the ordinary sense of likelihood multiplied by impact, has increased on both terms in the judgement of the people answering.

Higher penalties for cybercrime

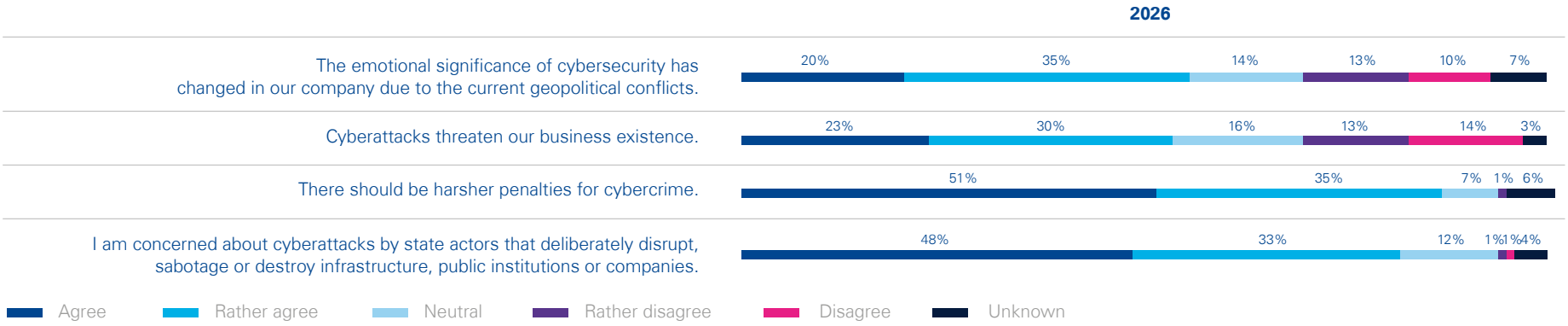
Offences in the digital space still carry sentencing ranges shaped in the early days of computing. 86 percent of respondents believe there should be higher penalties for cybercrime, made up of 51 percent who agree and 35 percent who rather agree, one of the strongest results in this chapter. As offences increasingly affect organizations and utilities, respondents evidently regard the current framework as calibrated to a different era of harm.

Concern about state actors

State actors in particular target critical infrastructure in attempts to destabilize other countries. 81 percent of respondents say they are worried by cyberattacks from state actors that deliberately disrupt infrastructure, public institutions, or organizations, made up of 48 percent who agree and 33 percent who rather agree.

The level is what matters. Four organizations in five are concerned about a category of attackers they can neither deter nor negotiate with and against which the practical response is the same set of detection, containment, and recovery capabilities that answer every other serious threat. Concern at this level argues for treating state activity as a standing feature of the operating environment rather than as an exceptional scenario requiring an exceptional plan.

Fig. 35: Outlook — cybercrime (four statements with agreement scales).



Cyber defense: attacks from abroad and identifying perpetrators

Threat is one side of the coin and law enforcement is the other. For 78 percent of respondents, it is frustrating that with attacks from abroad there is little prospect of identifying the perpetrators, up from 74 percent a year ago and not one respondent disagreed. Chapter 1 supplies the underlying experience, since attribution failed for roughly a third of the organizations that suffered an attack and more than half could not determine a country of origin at all.

Investigative powers

For such cases to be solved, law enforcement authorities need technical capabilities and legal powers. 78 percent of Belgian respondents say an expansion of the authorities' technical possibilities and powers is necessary if cyberattacks are to be solved - made up of 42 percent who agree and 36 percent who rather agree - up sharply from 60 percent a year ago. Only 3 percent believe no expansion is needed, down from 7 percent.

This is one of the clearest and fastest-moving consensuses in this year's data, with support rising by eighteen points while opposition fell to a rounding error. It should nonetheless be reported for what it is, namely the view of organizations that experience attribution failure directly and would like the state to be able to do something about it. It is not a judgement on where the limits should lie. Expanded investigative powers raise well-established questions of proportionality, judicial oversight, fundamental rights, and data protection, those questions belong to a democratic debate that this survey does not settle and in which the respondents to it are not the only stakeholders. The finding is that respondents have moved decisively to one side of that debate. Where the balance is ultimately struck is a matter for legislators, courts and civil society as much as for the organizations answering here.

Stronger EU-wide cooperation

Facing cyberattacks alone is rarely a winning strategy. 96 percent of Belgian respondents say stronger EU-wide cooperation on cybersecurity is needed if the effort is to succeed - made up of 74 percent who agree and 22 percent who rather agree - against 90 percent a year ago.

This is the strongest consensus in the entire Belgian survey and it completes a pattern. Chapter 4 recorded 100 percent naming the European Union as a location relevant to trust and 91 percent calling for digital sovereignty to be made a political priority, with no respondent disagreeing. Three separate questions, three near-unanimous answers, all pointing at the European level as the right scale for the problem. Whatever divides our respondents, the conviction that cybersecurity cannot be solved nationally is not among it.

Cyberattacks as military attacks

Language in this domain tends to escalate and the word war is reached for quickly. War is a form of conflict that brings human suffering, so when cyberattacks affect the lives of a civilian population, the question of when to use the term deserves care rather than reflex. Military conflict is conducted across domains: on land, at sea, in the air, in space,

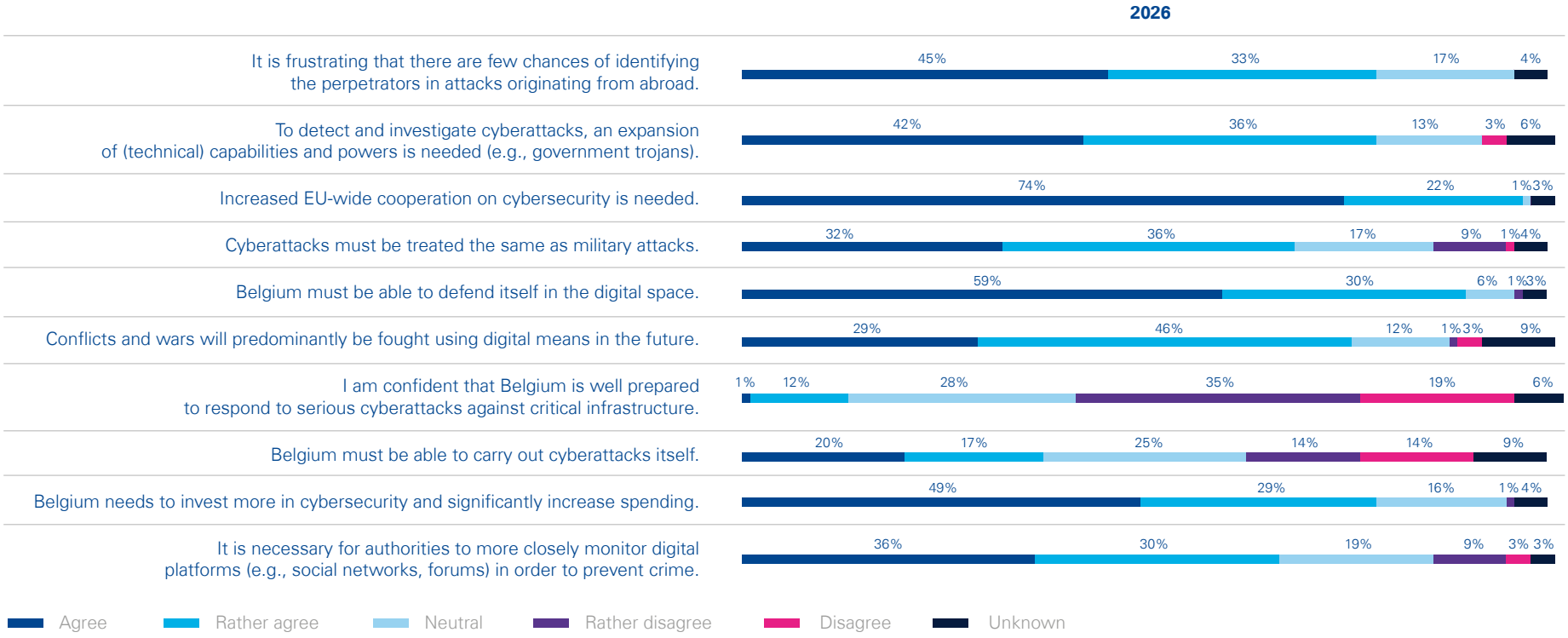
in the information space through mis- and disinformation and in cyberspace.

68 percent of Belgian respondents say cyberattacks must be treated the same as military attacks - made up of 32 percent who agree and 36 percent who rather agree. The consequences respondents have in mind are not abstract. Hospitals and infrastructure facilities brought to a standstill are the scenarios that move an offence out of the category of ordinary crime and into that of conflict between states.

Defending the country in the digital space

Resilience requires more than the ability to identify perpetrators. It also requires a deterrent effect, meaning capabilities substantial enough that an adversary does not begin. The Cold War analogy only travels so far, because in the cyber domain the effect of a given tool is largely unpredictable, which is what makes credible deterrence hard to construct. Effective deterrence nonetheless requires the competence to hold one's own digitally and 89 percent of Belgian respondents say the country needs the capability to defend itself in the digital space, made up of 59 percent who agree and 30 percent who rather agree.

Fig. 36: Outlook — cyber defense (ten statements with agreement scales).



Digital means of warfare

That defensive capability looks more necessary still given that 75 percent of respondents believe future conflicts and wars will be fought predominantly with digital means - made up of 29 percent who agree and 46 percent who rather agree. Preparation matters both from a state perspective, through the relevant security institutions and for organizations themselves, all the more where they form part of critical infrastructure and are expected, in a networked society, to supply stability and continuity to everyone else.

Confidence in national preparedness

Here the data produces its bleakest result. Only 13 percent of respondents are confident that the country is well prepared to respond to serious cyberattacks against critical infrastructure, made up of 1 percent who agree and 12 percent who rather agree. 54 percent disagree, with 35 percent rather disagreeing and 19 percent disagreeing outright. A year ago, 12 percent were confident and 45 percent were not. Confidence has not moved and disagreement has hardened.

What makes this striking is that it sits alongside evidence of an institution working well. Chapter 1 records reporting to CERT.be and the CCB doubling from 31 to 62 percent in a single year and chapter 3 shows CyFun consolidating as the compliance route of choice for 61 percent of NIS2-scoped organizations. Our respondents are using their national cybersecurity institutions more than ever and simultaneously telling us they do not believe the country is ready. That is a perception gap rather than a straightforward capability verdict and it is the more interesting finding for it.

Two readings follow and both are actionable. The first concerns communication. The means and options available for responding to a serious incident are not presented transparently enough, even allowing for the classification that necessarily surrounds parts of this work. An organization that cannot see the national response capability will assume it is absent. The second concerns involvement. The established models of public-private cooperation have not yet achieved the penetration that would be needed for organizations to feel part of a national posture rather than spectators to it. Belgium has the structures, including the CCB, the Cyber Security Coalition, the sector CSIRTs and the federation networks, so the question is one of reach rather than existence.

These figures read as an appeal to act. More intensive national cooperation and a closing of ranks on cybersecurity are becoming indispensable. Regulation can compel cooperation for those within its scope, but a large share of the Belgian economy - above all the smaller organizations that supply everyone else - falls outside it while remaining essential to it. For that group, models of voluntary exchange and mutual support are the only available mechanism, which makes developing them a priority rather than an accompaniment.

Conducting cyberattacks independently

Alongside defensive capability sits the offensive question, and it is the least settled item in this chapter. 37 percent of respondents say the country must be able to carry out cyberattacks, made up of 20 percent who agree and 17 percent who rather agree, while 28 percent reject the idea and around a quarter take no position.

Supporters therefore outnumber opponents, but neither group commands a majority and the neutral share is large. Cautious openness describes the position better than either endorsement or rejection. Our respondents are willing to consider an offensive capability without having settled what it would mean. The linkage to defense is what makes the question serious rather than rhetorical, since defending against a sustained attack does not consist only of isolating systems and can extend to neutralizing an attack far enough that its effect on the state's capacity to act is contained. Where exactly defense ends and offence begins is a question of law and mandate as much as of technology and the size of the neutral group suggests that debate has not yet reached the organizations this study surveys.

Investment in cybersecurity

Effective cybersecurity requires corresponding investment and 78 percent of Belgian respondents say the country must increase spending on cybersecurity at state level, made up of 49 percent who agree and 29 percent who rather agree. Read alongside the 13 percent who are confident in national preparedness, the message is coherent rather than merely demanding. Organizations do not believe the current level of national capability is sufficient, and they are prepared to say publicly that it should cost more.

Monitoring by the authorities

A defensive capability in the digital space depends on an up-to-date situational picture, which in turn depends on early information about perpetrator groups and quick recognition of their intentions. 66 percent of respondents say it is necessary for the authorities to monitor digital platforms such as social networks and forums more closely to prevent crime, made up of 36 percent who agree and 30 percent who rather agree. As with investigative powers above, these capabilities have to be reconciled with data protection and fundamental

rights requirements and the balance between an information advantage and the privacy of everyone observed in the process is a matter of law and public debate rather than one this survey resolves.

Location policy: security solutions from home

Cooperation extends to the technological level. Dependence on manufacturers outside Europe increasingly leaves survey respondents as bystanders in decisions taken elsewhere, which is why "Made in Belgium" and "Made in Europe" are gaining weight as procurement considerations rather than slogans. 61 percent of respondents say they would prefer to deploy security solutions from Belgian companies if these were available, made up of 36 percent who agree and 25 percent who rather agree, with 29 percent neutral. A year ago, the figure was 46 percent.

A rise of fifteen points in twelve months amounts to a sovereignty awakening in the procurement function. Last year's edition called for the development of a market for Belgian security solutions and the demand side of that market has now visibly shifted. The 29 percent neutral share is the group worth watching, since preference for domestic solutions is easy to express in the abstract and harder to act on when the domestic option is more expensive or less mature and this study cannot say how many of the 61 percent would pay a premium in practice.

Targeted political support

For such solutions to exist, the framework conditions must let organizations develop them here. 79 percent of Belgian respondents say Belgian security companies should receive targeted political support, made up of 43 percent who agree and 36 percent who rather agree, against 44 percent a year ago. That near-doubling is the largest single movement in this chapter and one of the largest in the study.

Targeted support is one element and creating the surrounding environment is another. Financing options beyond the familiar models are what determine whether a domestic security sector can reach the scale at which it competes internationally. Belgian security products can convince on quality and function. Whether they get the opportunity to do so at scale is a question of capital, procurement practice, and patience, rather than of engineering.

Provider country of origin

Procurement decisions themselves contribute to sovereignty and resilience. 69 percent of Belgian respondents say they pay attention to the provider's country of origin when procuring cybersecurity solutions - made up of 23 percent who agree and 46 percent who rather agree, up from 53 percent a year ago.

This sixteen-point increase is anything but marginal. Country of origin has moved within a single year from a consideration for the minority to a standard element of the majority's procurement assessment and it converts the sovereignty sentiment of chapter 4 into something that shows up in tender documents. Considerable ground remains to be made up and much of the constraint is supply rather than will. As Chapter 4 showed, 62 percent report that only a few foreign providers exist for the technologies they use, and cybersecurity & software applications are the most import-dependent category at 75 percent. While attention to origin is a necessary condition for a shift in sourcing, it is not by itself a sufficient one.

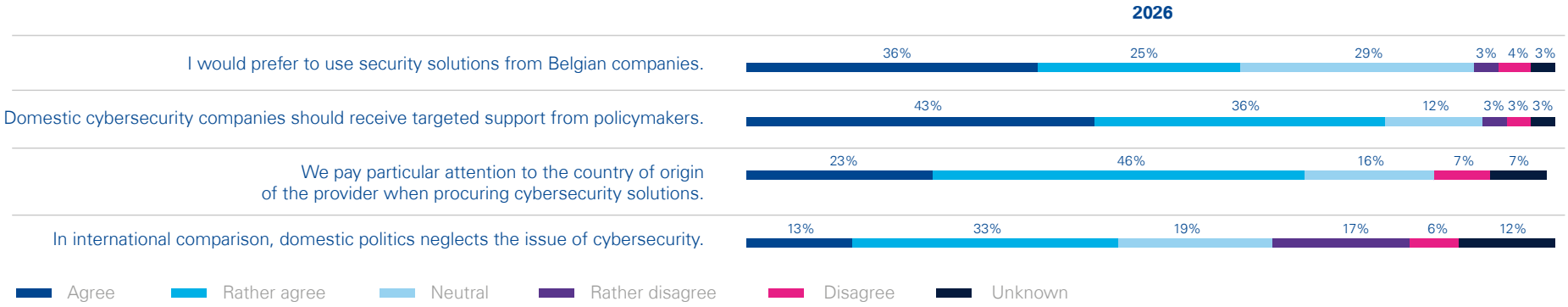
Political prioritization of cybersecurity

46 percent of Belgian respondents say that domestic politics neglects cybersecurity in international comparison - made up of 13 percent who agree and 33 percent who rather agree - while 23 percent disagree. A year ago, the figure stood at 38 percent, so perceived neglect has increased.

That movement runs against what an outside observer might expect from a year in which the state was unusually visible in this field, with NIS2 supervision beginning in earnest, CyFun adoption growing and reporting to the CCB doubling. The most plausible explanation is not that Belgian cybersecurity policy went backwards but that expectations of it rose faster than delivery could follow. The whole outlook section points the same way, with confidence in national preparedness flat at 13 percent, demand for state investment at 78 percent, and demand for political support of domestic vendors nearly doubling. Taken together, this chapter reads as an escalation of expectations of government rather than as dissatisfaction with a specific failure.

On balance, this is a healthier position than indifference and it comes with an obligation attached. Efforts must be pursued consistently enough to build a location in which cybersecurity carries appropriate weight and organizations can grow innovative solutions from it. Doing so secures existing employment and creates the kinds of role that will matter most in a labor market being reshaped by AI. It also requires the state to make its own work visible, since on this evidence survey respondents are not currently seeing it.

Fig. 37: Outlook — location policy (four statements with agreement scales).



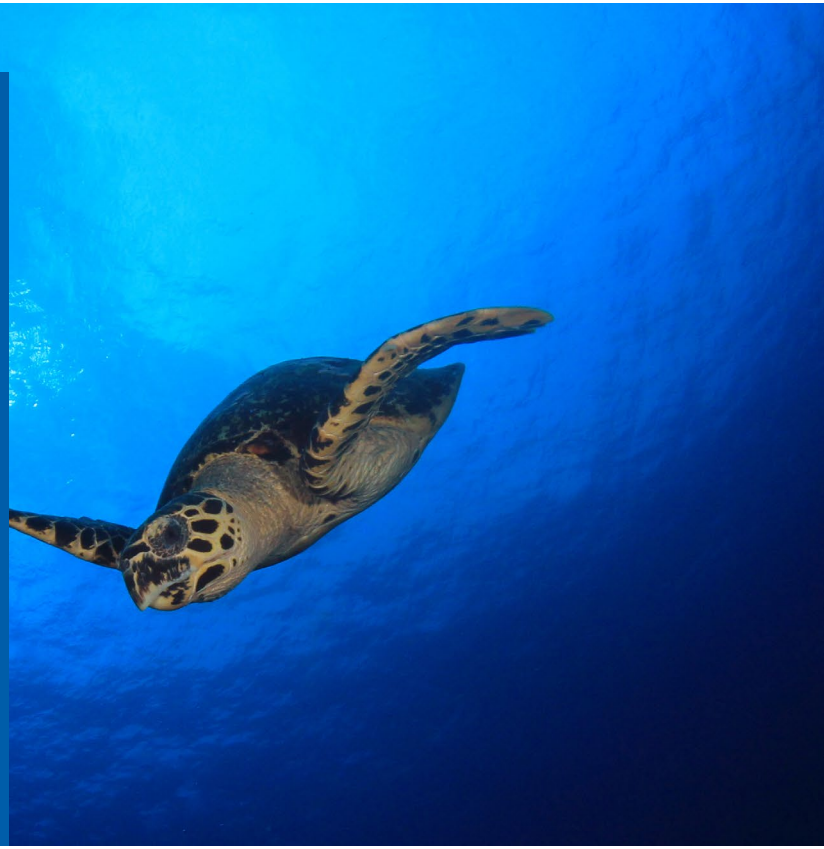
Chapter takeaways

The technology agenda is a supply-chain-and-AI agenda, with third-party risk leading for the second year running and AI security arriving from the periphery. Backup and multi-factor authentication have slipped down the list because they are largely built and capabilities that stop being priorities also stop being tested.

Geopolitics has been absorbed, with the emotional significance of cybersecurity unchanged while concern about state actors and about business survival both sit high. Both the perceived likelihood and the perceived severity of cyber risk rose in the same year.

The European level commands near-unanimous support and stronger EU-wide cooperation is the strongest consensus in the entire survey. Support for expanded investigative powers also rose sharply, leaving the proportionality and fundamental-rights questions to a wider debate than this survey.

Expectations of government are rising faster than confidence, in a year when the state was more visible than ever. The gap between institutional use and institutional confidence is this chapter's central finding and it is a communication and public-private engagement problem as much as a capability one.



07 Survey methodology

The KPMG study “Cybersecurity in Belgium“ examines how organizations respond to the growing threats of cybercrime and which security measures they take.

Survey methodology

Overview

KPMG in Belgium conducted this survey in the first half of 2026, with the data export closing on 28 June 2026. 302 respondents took part. The 2025 edition – published in October 2025 together with the Cyber Security Coalition and Agoria – drew on 266 respondents with fieldwork running from April to June 2025.

Respondents came from small, medium-sized, and large organizations across a wide range of sectors. The public sector accounts for 19 percent of the sample; the service sector for 18 percent; technology, media and telecommunications for 15 percent; financial services for 7 percent; and healthcare for 5 percent. A further 13 percent selected Other, with the remainder spread across construction, education, chemicals, energy, real estate, industry, consumer goods, tourism, and insurance.

Sample profile

Security professionals form the largest group among respondents. Chief security officers, CISOs, and security officers account for 29 percent; experts and employees for 28 percent; managing directors and owners for 20 percent; CDOs, CIOs, and IT management for 13 percent; department heads for 8 percent; and supervisory board members for 2 percent. 70 percent of respondents are male and 25 percent are female.

By location of Belgian headquarters, 53 percent of participating organizations are based in Flanders, 36 percent in the Brussels-Capital Region, and 11 percent in Wallonia. By size, 35 percent employ fewer than 50 people, 22 percent employ between 1,001 and 5,000 people, and 17 percent employ more than 5,000 people. Family businesses and start-ups or scale-ups each account for 10 percent of the sample. The most common legal forms are the BV or SRL at 34 percent and the NV or SA at 30 percent, with public sector bodies at 13 percent.

How to read the figures

Two points affect how the results in this report should be interpreted.

The base varies by question. Not every respondent answered every question, because the questionnaire routed participants according to their role and their organization's circumstances.

The sample is weighted towards security professionals. With 29 percent of respondents holding a CSO, CISO or security officer role, against 35 percent in 2025, the sample knows the subject better than a general business audience would. This plausibly raises scores on awareness and risk-perception questions relative to what a broader sample of survey respondents would produce and comparisons with general business surveys should take that into account.

Analysis

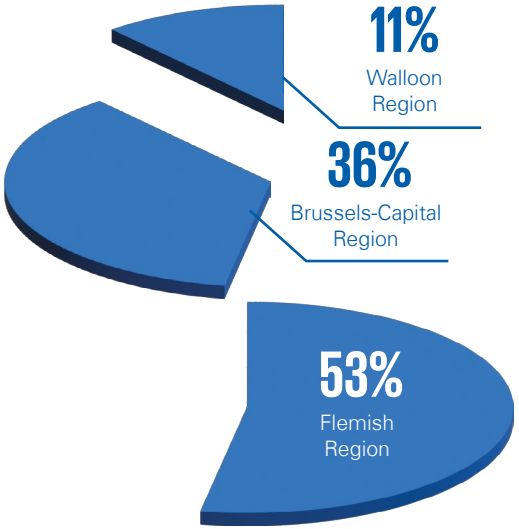
Each participant received an online questionnaire tailored to their role in the organization. Alongside quantitative questions based on a Likert scale,

qualitative questions gave respondents the opportunity to share additional impressions and comments in their own words. A team of KPMG cybersecurity experts from Cyber Security Services analyzed the results.

Respondent demographics — sector breakdown

	2026
Public Sector (Government/Public Sector)	19%
Service sector	18%
Technology, Media and Telecommunications	15%
Other	13%
Financial Services	7%
Healthcare	5%
Real estate industry	4%
Consumer goods	4%
Automotive industry	3%
Construction industry	3%
Industry	3%
Education	2%
Energy industry	2%
Chemical industry	1%
Groceries	1%
Tourism	1%
Insurance	1%

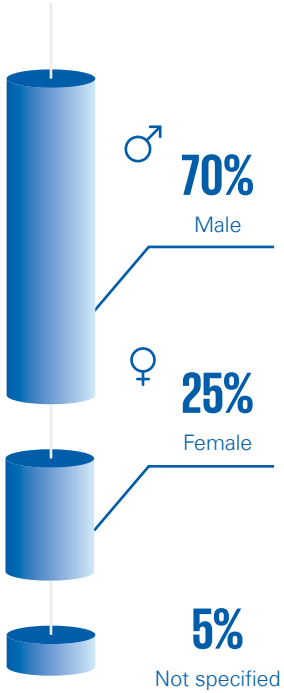
Region of Belgian headquarters



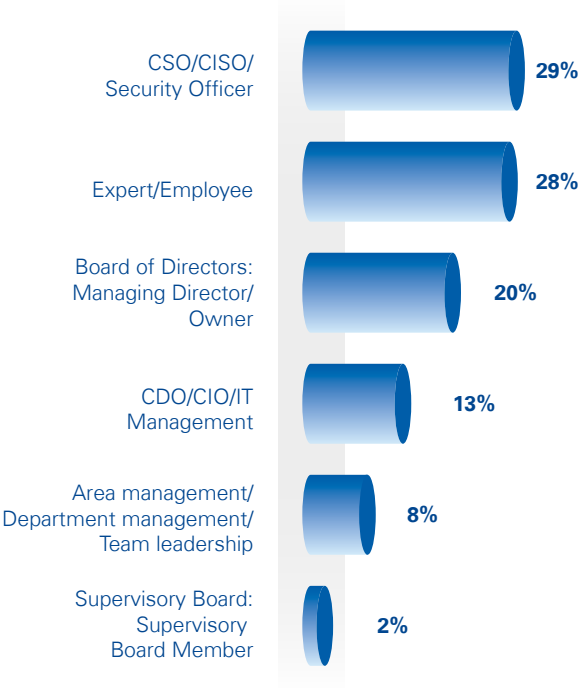
Organization size by number of employees

Fewer than 50 employees	35%
1,001–5,000 employees	22%
101–500 employees	11%
50–100 employees	10%
10,001–20,000 employees	7%
5,001–10,000 employees	5%
More than 20,000 employees	5%
501–1,000 employees	2%
Unknown	2%

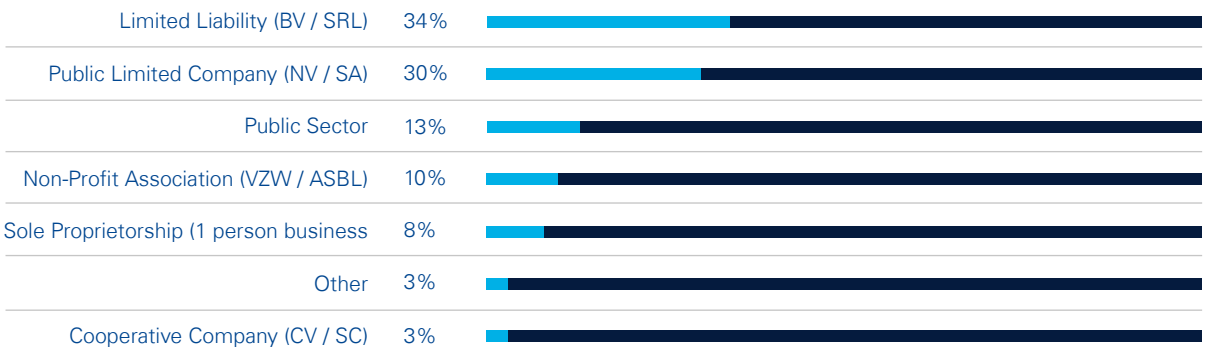
Gender of respondents



Role in the organization



Legal form of the organization



Contact

Benoit Watteyne
Partner
Cyber Security Services
KPMG Advisory

M: +32 (0)476 66 53 66
E: bwatteyne@kpmg.com

Benny Bogaerts
Partner
Cyber Security Services
KPMG Advisory

M: +32 (0)477 30 14 49
E: bbogaerts@kpmg.com

Henk Dujardin
CEO
Cyber Security Coalition

M: +32 (0)475 84 00 42
E: henk.dujardin@cybersecuritycoalition.be

kpmg.com/be