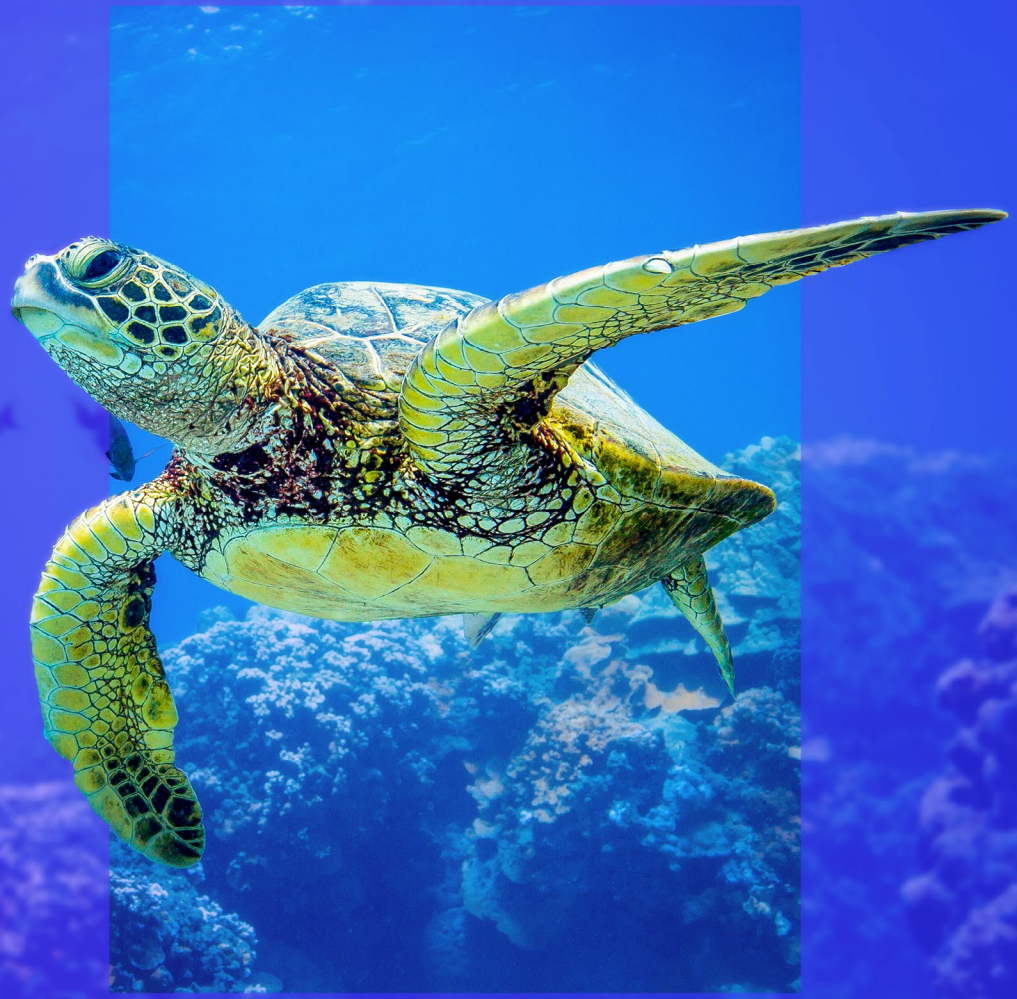
KPMG | CYBER SECURITY COALITION.be

Cybersecurity in Belgium



KPMG. Make the Difference.

October 2025

Content

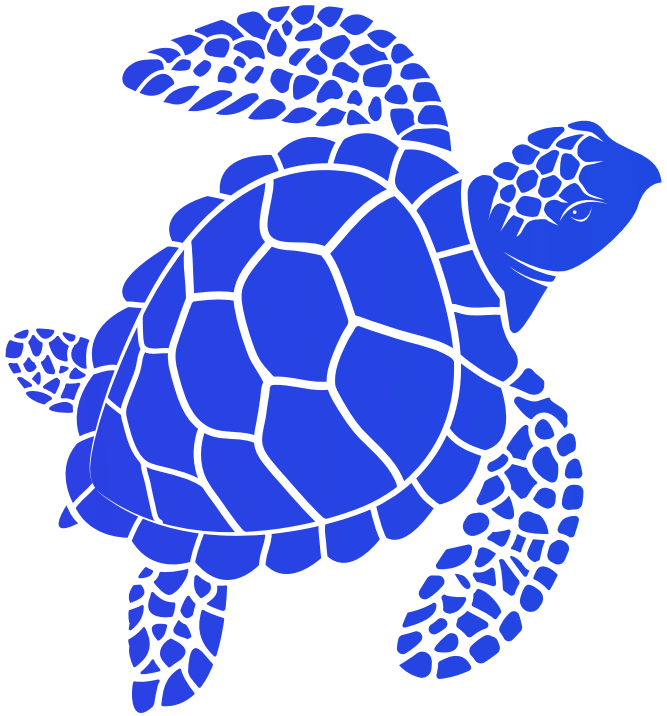
What do turtles have to do with cybersecurity?

We have chosen the turtle to be our companion in navigating the depths of cybersecurity. And it is hard to imagine a better guide—their history and way of life mirror many aspects of our cyber reality.

Turtles stand for wisdom and resilience—qualities essential for navigating the rough waters of the digital world. Like their shells, our protective measures must be both robust and adaptable.

Over millennia, turtles have had to adapt to dramatic changes in their environment, facing new threats to survival. In much the same way, organizations today confront an ever-shifting landscape of cyber threats, accelerated by digitalization and technological change.

At the end of the day, we face the same choice as the turtle: retreat into our shell and hide or keep swimming with resilience and stamina. Cybersecurity, like the turtle's journey, is about endurance, adaptability, and the strength to move forward despite the challenges.



Foreword

By the Chair of the Board, Cyber Security Coalition

In an era where digital transformation is reshaping every aspect of our society and economy, cybersecurity has become a defining challenge for Belgium and society at large. The Cyber Security Coalition, together with KPMG and Agoria, is proud to present the first comprehensive Cyber Survey Belgium 2025—a call to action for all stakeholders in our digital ecosystem.

This report provides, for the first time, a holistic view of the Belgian cybersecurity landscape, based on insights from nearly 270 organizations across all sectors. It reveals not only the scale and sophistication of the threats we face, but also the resilience and determination of Belgian organizations to meet these challenges.

Cyberattacks are evolving rapidly. No longer limited to data theft or disruption, they now aim to manipulate information, undermine processes, and erode trust. The boundaries between cybercrime, geopolitical conflict, and disinformation are blurring. Half of Belgian organizations reported an increase in attacks, and one in six suffered at least one disruptive cyberattack. The emergence of artificial intelligence is transforming both the threat landscape and our defences, while supply chain attacks have become a new Achilles' heel.

Despite technological advances, people remain at the heart of cybersecurity. Employees are both the first line of defence and, too often, the entry point for attackers.

Building resilience means investing not only in technology, but also in people—through training, awareness, and a strong security culture.

Cybersecurity is no longer a purely technical issue; it is a societal imperative. The complexity of today's threats demands cooperation between government, business, academia, and civil society. Belgium must strengthen its digital sovereignty, foster innovation, and prepare for hybrid threats that cross borders and sectors.

Absolute security may be unattainable, but resilience—the ability to withstand, adapt, and recover—must be our guiding principle. This report highlights where Belgian organizations are making progress, where challenges remain, and how regulation, technology, and people can work together to protect trust in our digital future.

Cybersecurity is a continuous journey that demands constant agility. Standing still means falling behind. The future belongs to those who are willing to continuously develop, invest, and innovate—not only in technology, but also in organizations, processes, and above all, people.

With this first Cyber Survey Belgium 2025, we invite you to join the dialogue, share your experiences, and help strengthen Belgium's collective resilience in the face of an uncertain but digital future.

Jan De Blauwe
Chair, Cyber Security Coalition

Introduction

Trust in the crosshairs

The results of this year's Cyber Survey Belgium 2025 make one thing very clear: geopolitical conflicts have arrived in Belgium. Half of the surveyed organizations report an increase in cyberattacks over the past year, with state-backed groups and organized crime playing a decisive role. The global security environment—marked by war, political instability, and economic uncertainty— is spilling over into cyberspace and affecting Belgian companies directly.

But what does this mean for our economy? How are organizations coping with increasingly professionalized cybercrime? What role does artificial intelligence play—both as a tool for defenders and as an enabler for attackers? And how can we protect trust when disinformation campaigns are becoming part of hybrid conflict strategies?

Recognizing conflicts

Conflicts are no longer fought only on battlefields. Increasingly, they take place in cyberspace and the information domain. While these attacks are invisible to the naked eye, their consequences are tangible: business disruption, financial loss, and reputational damage.

It is not only companies that are in the crosshairs. Civil society is also being tested through disinformation and manipulation. Deepfakes and AI-generated phishing campaigns are challenging our ability to separate truth from fiction. Trust—between companies, customers, regulators, and society—is being eroded, and with it the foundations of cooperation.

Creating awareness

To preserve trust, we must strengthen our cybersecurity situational awareness. This requires open dialogue between business, government, and society. With this study, conducted together with the Cyber Security Coalition and the help of Agoria, supported by Belgian organizations across all sectors, we aim to shed light on the current situation.

By sharing insights from almost 270 respondents, we want to raise awareness, highlight areas of progress, and identify where urgent action is needed. Only through joint exchange can we ensure that Belgium is prepared for the challenges ahead.

Promoting dialogue

This year marks the first national Cyber Survey in Belgium, building on successful models abroad. We sincerely thank all participating organizations for openly sharing their experiences, and to our partners the Cyber Security Coalition and Agoria and the experts who contributed their perspectives. Their input allows us to turn data into actionable insight.

Closing thought

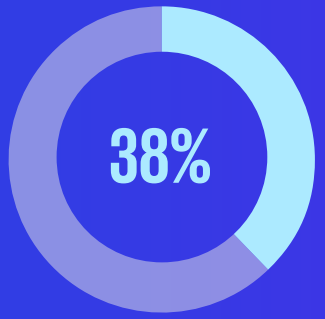
Cyber conflicts may be invisible, but their effects are real and profound. In a world where technology, politics, and society are increasingly intertwined, trust in the digital space is becoming our most valuable currency. Protecting it requires cooperation, resilience, and collective action.

We hope you find the results insightful—and we invite you to continue the dialogue with us. Only together can we strengthen Belgium's digital resilience.

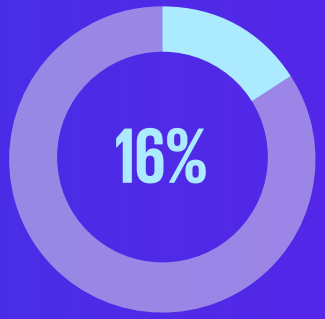
Benoit Watteyne
Partner
Cyber Security Services

Benny Bogaerts
Partner
Cyber Security Services

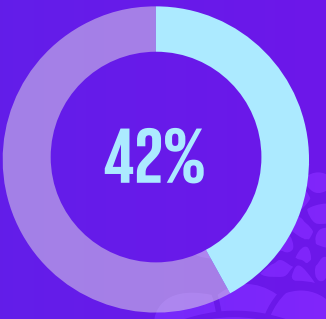
Key findings



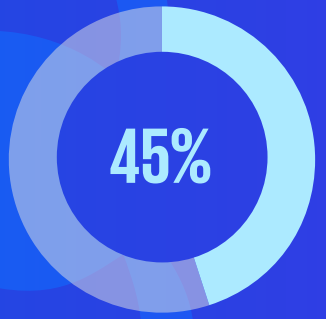
confirm specific cyberattacks against their supply chain



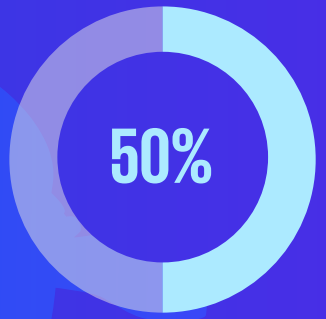
of organizations have faced one or more cyberattacks resulting in disruption or damage over the last year.



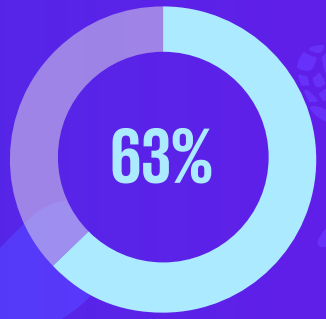
think they could become a victim of a cyber attack that could exert targeted influence on their organization via dis-/misinformation



say that Belgium is not well prepared to deal with serious cyberattacks against critical infrastructure to react



rather agree that AI will improve cybersecurity by being used to defend against attacks.



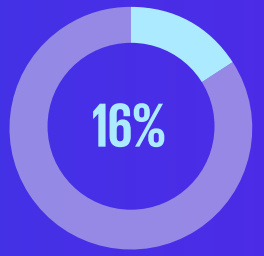
of organizations have encountered phishing attacks multiple times.

01

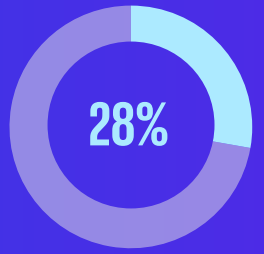
What happened

How has cybersecurity changed in the past year? Which attacks have increased, have geopolitical factors shifted, and where are organizations most at risk?

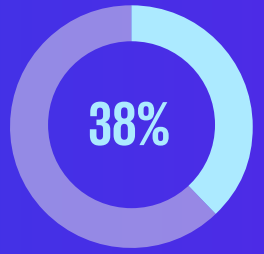
The situation remains serious, with troubling trends and no improvement in sight.



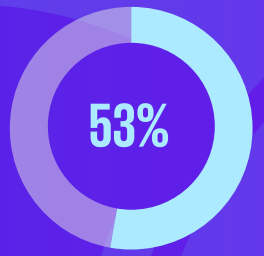
suffered at least one disruptive cyberattack in the past 12 months.



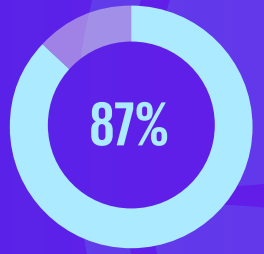
more than one in 4 attacks can be traced back to state-backed actors



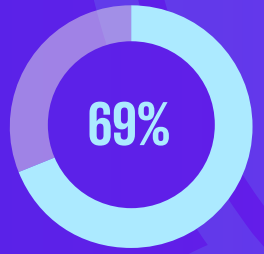
point out that inadequate email security has led to a successful phishing attack.



have observed a connection between global geopolitical conflicts and cyberattacks on their company



have observed a phishing attack over the past 12 months



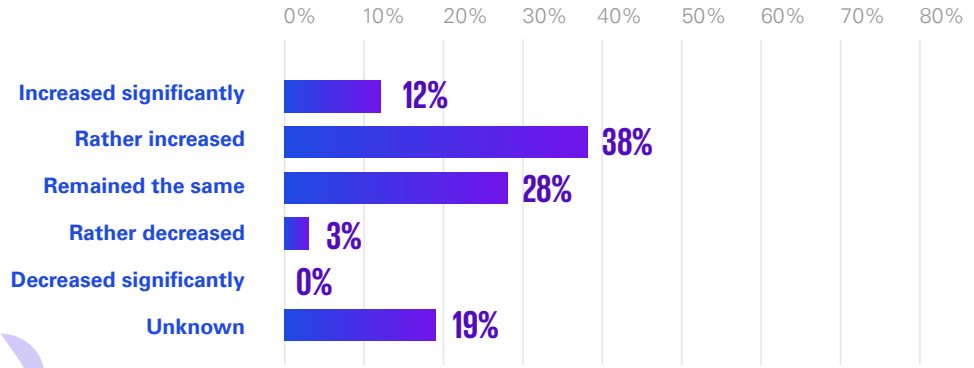
reported resolving issues within 24 hours.

What happened

Evolution of cyberattacks in the last year

The survey shows that the cyber threat landscape in Belgium remains highly dynamic and severe. Half of organizations (50 percent) report that the number of cyberattacks against them increased in the past twelve months, while 28 percent observed no change. Only a small minority noted a decline, and 20 percent admit they do not know whether attacks against them increased or not. The overall picture is clear: the level of attacks remains high, tactics are becoming more targeted, and methods more sophisticated.

Fig. 01 - How has the number of cyberattacks aimed at your organization developed over the past twelve months?



Drivers of change in cyberattacks

Respondents point to several factors behind the intensification of attacks:

- **Geopolitics** is a central driver. Russia's invasion of Ukraine and other international crises are increasingly spilling over into cyberspace, heightening the threat environment.
- **Digitalization** continues to expand the IT attack surface. The adoption of new tools, cloud platforms, and connected devices has created more entry points for attackers.
- **Artificial intelligence (AI)** has become a game-changer. Generative AI enables hyper-realistic phishing, automated attacks, and "phishing-as-a-service" offerings, lowering the entry barrier for cybercriminals.
- **Political instability and global uncertainty** are also contributing to heightened activity, particularly where state-backed groups exploit tensions for strategic or disruptive purposes.

Impact and damage

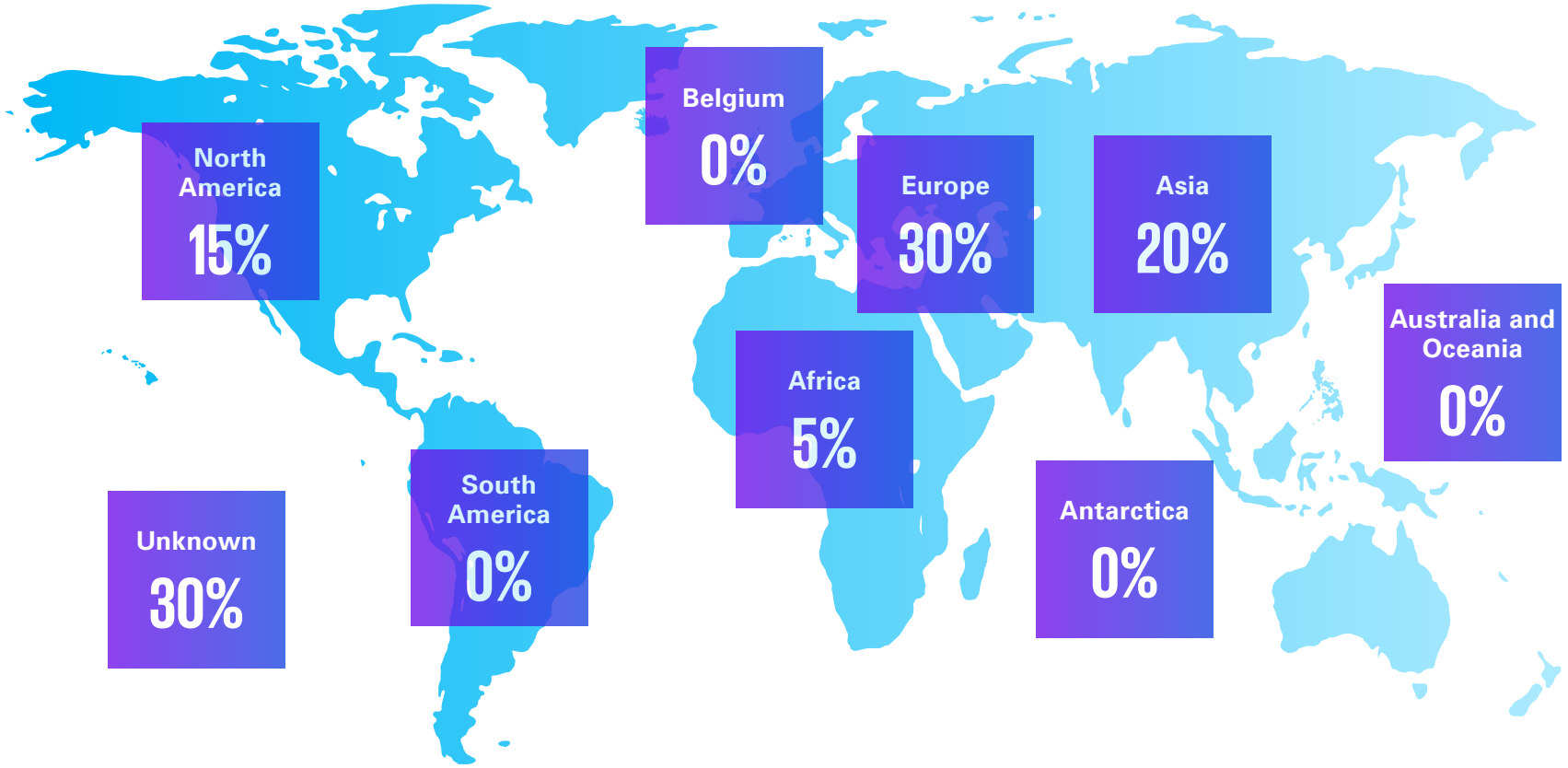
Sixteen percent of organizations experienced successful cyberattacks that caused disruption or damage in the past year—a figure notably higher than the 4 percent reported in the Vlaio CS-Barometer 2024. At the same time, 13 percent of respondents do not know whether they were victims of successful attacks, suggesting significant blind spots in monitoring and incident reporting. This lack of visibility is particularly concerning given organizations' growing dependence on digital technologies and the increasing regulatory emphasis on resilience.

Attackers and their origins

When looking at attribution, organized crime and state-sponsored actors dominate, each cited by 28 percent of respondents. This confirms that geopolitical conflicts have reached Belgium, with cybercrime becoming both more professionalized and more intertwined with state interests. However, attribution remains difficult: for 33 percent of organizations, it was not possible to identify the attacker, underscoring the growing challenge of tracking adversaries in a professionalized cybercrime ecosystem.

The perceived origin of attacks also reflects this complexity. Respondents most often pointed to Europe (30 percent) and Asia (20 percent), followed by North America (15 percent). Yet nearly one third (30 percent) could not determine the region of origin, highlighting the effectiveness of obfuscation technologies such as anonymization services, VPNs, proxies, and cloud abuse in disguising true sources.

Fig. 02 - Were you able to determine which region these attacks came from?

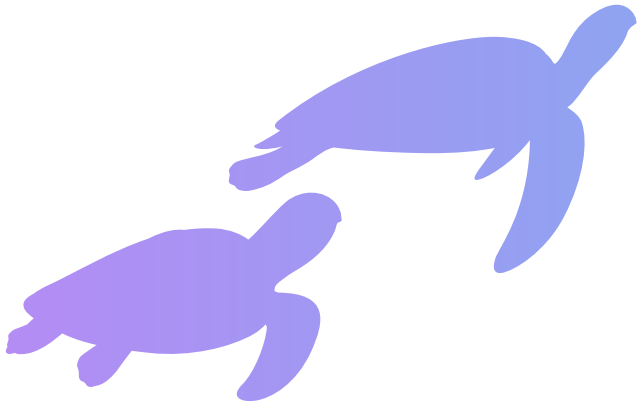


Geopolitical conflicts and cyberattacks

More than half of organizations (53 percent) reported a link between cyberattacks and global geopolitical conflicts. In most cases, these were attributed to Russia's war on Ukraine and related destabilization attempts, including denial-of-service attacks launched by pro-Russian groups.

Organizations are particularly concerned about the business consequences of such conflicts:

- Disruption of operations (71 percent)
- Financial losses (62 percent)
- Reputational damage and loss of trust (61 percent)



These results underline that digital trust has become a critical success factor: customers, employees, partners, and regulators increasingly expect organizations to demonstrate resilience, integrity, and responsible handling of digital risks.

Politically motivated attacks against the value-added industry of European countries as well as disinformation and the use of AI to influence society are also worrying for the respondents. Finally, there are fears that Distributed Denial of Service (DDoS) attacks and blackouts will lead to a complete business standstill.

We asked organizations what other cyber risks they are most concerned about in connection with geopolitical conflicts. From the responses, we noticed that Digital Sovereignty has gained importance over the past year, with President Trump being in power and the growing influence of Big Tech.

Advanced obfuscation technologies

1. AI and social engineering
Attackers use generative AI models for hyper-realistic phishing campaigns. Deep fake technologies make it possible to imitate voices in real time. The attacks take place via multi-channel strategies (e.g., by combining e-mails, SMS, messenger services, and messages on collating platforms). This increases credibility.

2. Anonymization services
Network obfuscation technologies can be used to disguise the origin of the attack and identity. The following technologies are currently in use: Tor „The Onion Router" (routing via three encrypted nodes—entry, relay, exit—for IP obfuscation), VPN (end-to-end encryption of all data traffic via remote servers), and proxies (IP masking without encryption).

3. Cloud-based obfuscation and infrastructure abuse
Cybercriminals use cloud services to disguise criminal activity as legitimate traffic. In addition, they misuse remote management tools for lateral movement. These do not leave any painting signatures.

4. Professionalization of cybercrime
The commercialization of attack tools lowers the entry barrier for perpetrators and increases the volume of attacks. The following offers are already available:

- Phishing-as-a-Service: AI-generated campaigns including target person research.
- Ransomware kits: Automated exploits scan vulnerabilities in real time and customize encryption routines.
- Darknet markets: Selling hacked VPN access or compromised proxies for attack infrastructures.

5. Defense strategies and zero trust architectures
To defend against this, experts recommend behavior-based detection (analysis of user activity for anomalies), kernel-level monitoring (tools to identify 'Living of the Land' (LotL) techniques), identity governance (access controls and MFA), and threat intelligence sharing (cross-industry exchange).

Different types of attacks

In terms of attack methods, phishing and spear-phishing remain the most common, reported by 87 percent of organizations. Business email compromise (BEC) follows closely at 75 percent. This remains a frequently observed phenomenon, particularly related to financial gain or the redirection of financial transactions (e.g., fraudulent invoices or share-seed-phrase scams). Such attacks typically aim to manipulate victims' decision-making by convincing them they are interacting with a legitimate entity. The consistently high values indicate that human vulnerabilities remain a common target for attacks.

Denial-of-service (DoS) attacks rank fourth, accounting for 57 percent. DoS activity shows little reduction despite the availability of DDoS protection solutions, which may reflect increasing botnet capabilities and vulnerabilities associated with insecure IoT devices.

Multi-Factor Authentication (MFA) bypass incidents, at 38 percent, demonstrate that attackers continue to find ways to compromise multi-factor authentication systems, including by using techniques like session hijacking or phishing tools such as Evilginx.

Ransomware remains at a high level (26 percent), reflecting the increasing professionalization of ransomware-as-a-service models and the focus on critical infrastructures.

At the same time, new vectors such as deepfake-enabled fraud and AI-driven phishing are emerging, even as traditional attack types persist.

Causes of successful attacks

A review of these figures indicates that many successful attacks on companies can be attributed to shortcomings in fundamental security practices. For instance, 38 percent of organizations reported that breaches were facilitated by insufficient email security measures. Weak login credential management was cited as the second most common cause, contributing to 31 percent of incidents involving compromised credentials. Additionally, a lack of malware protection and inadequate network security controls were frequently noted.

These findings highlight ongoing gaps in essential security requirements. Enhancing transparency, improving monitoring capabilities, and investing in advanced technical analysis to identify vulnerabilities and potential entry points are all crucial steps for strengthening organizational resilience against cyberattacks.

How to become aware of attacks

Survey results show that internal security systems are the main method for organizations to identify cyberattacks, accounting for 40 percent of detections. Employee reports are the second most common source, with 27 percent of organizations citing this method. This indicates that both employees and technology play significant roles in detecting attacks. The involvement of external service providers has decreased compared to previous years, when third parties played a larger role in attack identification. These figures suggest that organizations are increasingly investing in detection technologies and developing their own capabilities in this area.

Financial impact

Organizations report varied financial impacts from cyberattacks over the past year. Minor losses (under EUR 1,000) were reported by 17 percent of organizations, possibly due to automated attacks like phishing or malware. Mid-range losses (EUR 1,001–50,000) affected 24 percent, which may reflect improved defenses or more targeted attacks. Higher losses (EUR 100,001–1 million) accounted for eight percent, indicating some incidents threatened company survival. Notably, 34 percent could not quantify their losses, raising concerns about poor incident tracking and reporting.

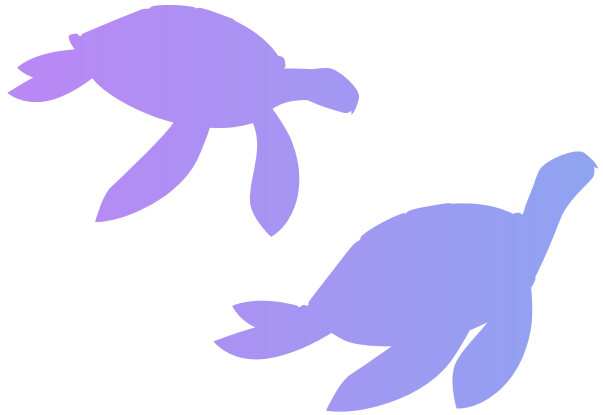
Cyberattacks bring both direct costs—such as recovery, legal fees, and lost revenue—and indirect costs like reputational harm and higher insurance premiums. Even though extreme losses are not the majority, all organizations should prepare financially through insurance or reserves. Overall, Belgian companies face ongoing cybersecurity risks, making comprehensive, proactive strategies vital to limit damage and stay competitive.

Cybersecurity incident processing time

An analysis of the time required to address cybersecurity incidents shows that 69 percent of organizations reported resolving issues within 24 hours. However, some incidents lasted longer; for instance, 16 percent of organizations indicated that resolution took between one and four weeks. The data also suggests that smaller organizations often experience longer incident durations than larger companies. These findings highlight that response times can vary significantly and demonstrate the importance of resilient crisis management to ensure organizations are prepared.

This trend may be related to the use of improved detection technologies, enhanced response processes, better-trained incident response teams, and streamlined procedures that facilitate faster containment and mitigation of attacks. Additionally, automation solutions in cyber defense might contribute to shorter response times by expediting routine tasks.

Despite these developments, there are areas of concern: 15 percent of organizations reported not knowing their processing times. This could reflect limited transparency or insufficient tracking mechanisms. Moreover, quick recovery efforts may sometimes lead to incomplete analysis of the root causes of cyberattacks, potentially resulting in underestimated impacts if remediation is not comprehensive.



What to take away from this chapter

01

State-backed actors and organized crime dominate the Belgian threat landscape, underscoring the influence of geopolitical conflict.

02

Attack levels remain high (16 percent affected) and are becoming more targeted, with no sign of easing.

03

Attribution and origin are increasingly difficult to establish, reflecting the professionalization of cybercrime.

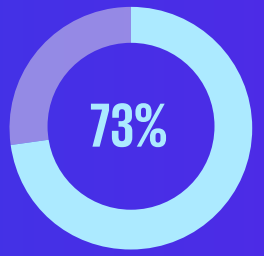
04

Human factors remain central—both as vulnerabilities exploited in phishing and BEC, and as defenders through employee reporting.

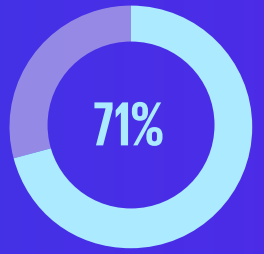
02

What was done afterwards?

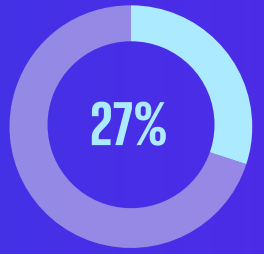
The broader consequences experienced by organizations as a result of cyberattacks over the past year are now better understood. This raises several questions: How did organizations respond to these incidents? Were relevant authorities notified? What actions were implemented following an attack, and how can the effectiveness of those actions be evaluated? Additionally, do organizations seek assistance from external service providers or opt for cyber insurance?



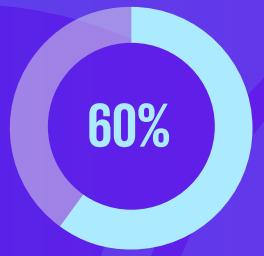
plan to conduct penetration tests to assess the effectiveness of their security and resilience measures over the next 12 months.



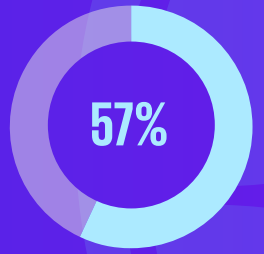
do not have difficulties finding suitable external service providers for incident handling.



believe that cyber insurance should cover the cost of ransom payments.



use external service providers for incident handling.



own cyber insurance.

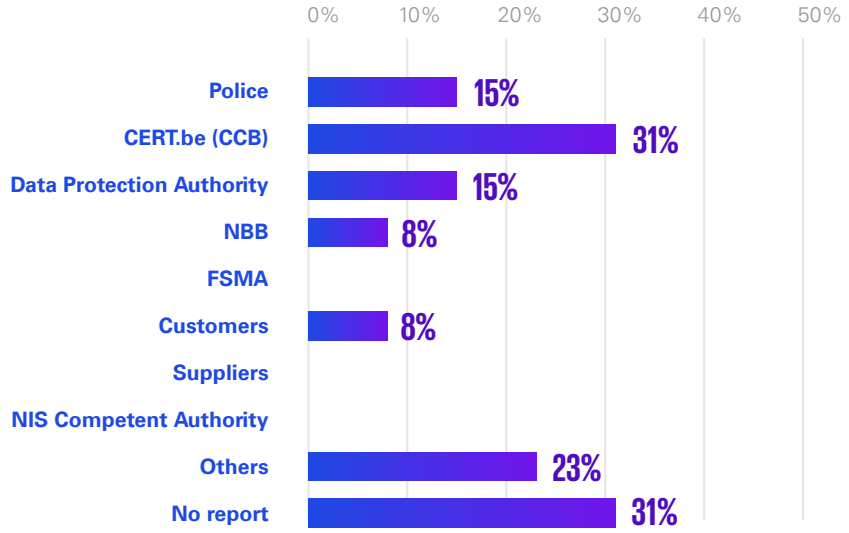
What was done afterwards?

Reporting on cyberattacks

Cyberattack incidents are primarily reported to Belgian Cyber Emergency Response Team (CERT). Reports to Data Protection Authorities (DPA) and policy departments account for 30 percent, suggesting that specialized cybersecurity institutions are regarded as reliable points of contact.

Additionally, some reports are made to financial regulators (such as the National Bank of Belgium (NBB/BNB)) and customers. The „Other" category includes reporting to suppliers or within the internal organization.

Fig. 03 - To whom did you report the incident



Reporting rates

Thirty-one percent of cybersecurity incidents went unreported. This suggests there might be a need to raise awareness about why reporting is important. People affected by cyberattacks may not know how to report them or might hesitate due to worries like harming their reputation or facing legal issues. With regulations increasing, organizations are now under greater pressure to notify authorities and maintain proper reporting procedures.

Respondents explained that many incidents weren't reported because they didn't seem serious enough, and often, reporting wasn't required if an attack failed. If damage was successfully minimized or only non-production systems were involved, organizations felt less compelled to submit a report.

Organizational incentives for cyberattack reporting

Identifying and reporting cyberattacks starts with recognizing that an incident has occurred. Security tools and internal channels help facilitate this process. According to survey responses, the most common incentive for employees to report cyber threats was targeted training and awareness programs (38 percent). While these initiatives provide necessary information, they are generally seen as fundamental rather than motivating factors.

A significant number of participants (31 percent) said their organization had no specific incentives for reporting, possibly due to cultural attitudes or the belief that staff will report incidents as part of their routine responsibilities. The lack of formal incentives may indicate organizational challenges like fear of negative consequences, distrust in the process, or the idea that reporting takes too much effort.

Other incentives mentioned include recognition and reward schemes (13 percent), anonymous reporting options (six percent), and incorporating reporting into performance reviews (six percent). These strategies can encourage openness and make reporting easier, signaling possible ways organizations can improve their reporting culture.

Overall, survey results show there's a gap between simple awareness and meaningful motivation. To overcome barriers—such as mistrust, uncertainty about the benefits of reporting, or fear—organizations may need to pair training with measures that build trust, recognize positive action, and ensure clear reporting systems.

Measures against cyberattacks

As expected, the initial response to a cyberattack remains the search for vulnerabilities in the systems (40 percent). This step is crucial to limit immediate damage and prevent further attacks. However, it is worrying that the purchase of additional security tools (40 percent) remains a high priority. This indicates that many organizations only invest in basic security measures after an incident. A more strategic approach would be desirable here.

The need for the development of security competencies (22 percent), investment in the training of employees (40 percent), updating of identity and access management (50 percent), and increased usage of cloud (20 percent) are identified as significant measures against cyberattacks. This signals a growing understanding of the need for in-house expertise and advanced technologies to effectively counter cyber threats.

Organizations seem to recognize that a sustainable security strategy must be based on in-house know-how and state-of-the-art technology. Simultaneously, the use of external help from specialized IT consultants or service providers (40 percent) is also highlighted as a measure after an attack, signifying that external expertise and continuous training play an important role in maintaining a high level of security.

The improvement in internal crisis planning for cyberattacks (30 percent) indicates that organizations are aware of the importance of response to and recovery after a cyberattack. An overestimation of the existing plans could be the reason for this. However, regular review and adjustment of crisis plans are essential to keep up with the ever-changing threat landscape.

Event-related media work (14 percent) is a positive sign of greater transparency and a sense of responsibility in dealing with cyber incidents. Open communication with customers and stakeholders is crucial to maintaining trust and protecting the company's reputation.

Finally, taking out cyber insurance (10 percent) is identified as a measure after an attack, indicating an increasing need for external assistance and protection against losses.

They are all critical towards building a comprehensive security strategy.

Overall, the data points to a positive trend towards a more proactive and competency-oriented cybersecurity strategy. However, it is important that organizations continue to invest in all aspects of security. This is the only way they can effectively counter the constantly evolving threat landscape and remain resistant to cyberattacks.

Assessing effectiveness

How do organizations plan to assess the effectiveness of their security and resilience measures over the next 12 months? Having measures in place to take after a cybersecurity incident is not enough if you can't convince yourself of their effectiveness. Organizations are therefore advised to check the effectiveness of the implemented activities, controls, and safety precautions. Luckily, we see that 41 percent of the organizations that were surveyed indicated that they have KPI reporting in place towards Management. This indicates that reporting on the effectiveness of security measures is a priority.

Penetration testing is the main priority for 73 percent of surveyed organizations. While familiar and commonly practiced, this method

provides only a snapshot, lacking regular and ongoing assessment. Although it helps improve security, its perspective is often limited.

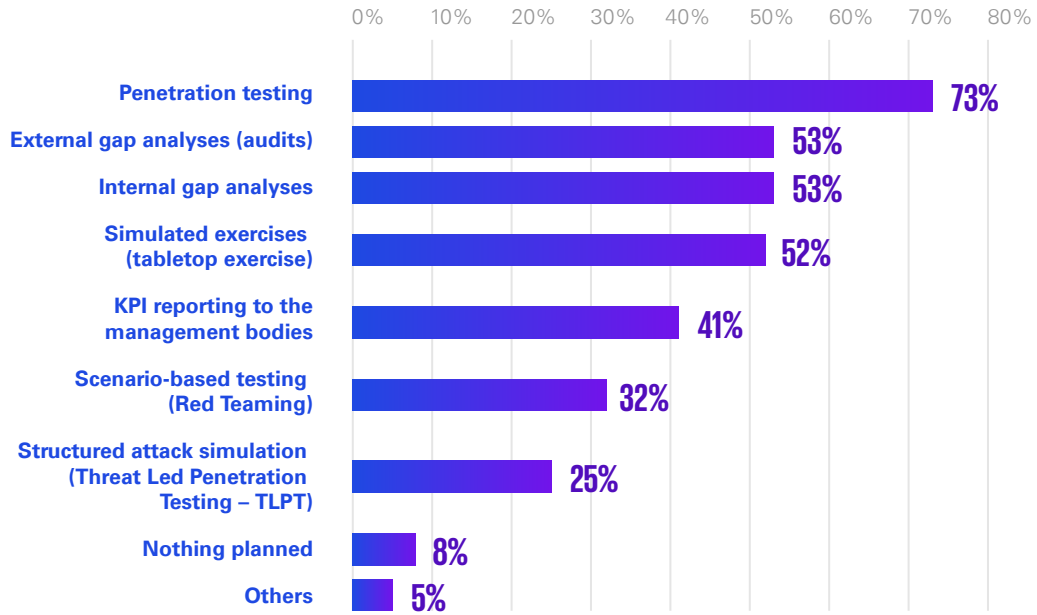
Secondly, organizations report conducting both internal and external gap analyses at a rate of 53 percent. These activities typically relate to compliance within the organizational information security domain. Gap analyses are primarily used to address compliance requirements rather than evaluating the effectiveness of measures. Additionally, five percent of organizations plan to increase audit testing and pursue ISO/IEC 27001 certification or System and Organization Controls (SOC) attestation.

The respondents try to learn more on how to deal with exceptional situations. Fifty-two percent plan to perform simulated exercises, so-called tabletop exercises, in the next 12 months. With these exercises, you can simulate the response to extraordinary situations to identify gaps, efficacy of response actions, but also successes.

Structured attack simulations, such as threat-led penetration tests (25 percent) and scenario-based tests or Red Teaming (32 percent), are advanced effectiveness assessments. Threat-led penetration tests are particularly relevant for banks and insurers due to regulatory demands, while industrial organizations, though not held to the same standards, should also include these in their testing. These end-to-end analyses help organizations evaluate the performance of their security measures and technologies.

According to the survey, eight percent of organizations do not plan to implement any measures in the next 12 months. Addressing these gaps is important, as testing the effectiveness of measures helps determine if resources have been allocated appropriately to relevant topics with suitable goals and focus.

Fig. 04 - How do you plan to test the effectiveness of your security/resilience measures over the next 12 months?



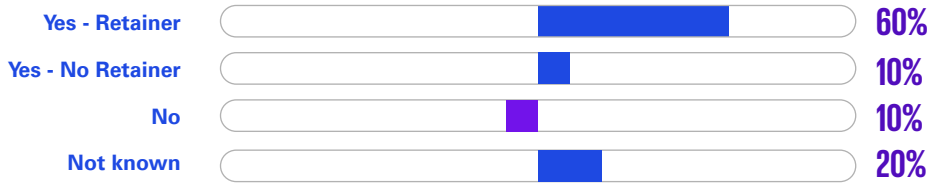
Support from an external service provider

In managing security incidents, organizations utilize appropriate resources. Some organizations also obtain external assistance during cyber security incidents; 70 percent reported working with an external service provider when addressing a security incident.

To facilitate rapid response in exceptional cases, organizations often use retainers—contractual agreements with service providers that secure on-demand support during incidents. Approximately 60 percent of surveyed organizations have retainer-based external support for security incidents, indicating the emphasis placed on response capability.

Conversely, 10 percent of respondents reported not using external support for incident processing and handling, while 20 percent were unsure if they could rely on such providers. These organizations focus on internal precautionary measures and response strategies.

Fig. 05 - Did you receive support from an external service provider in handling the security incident?



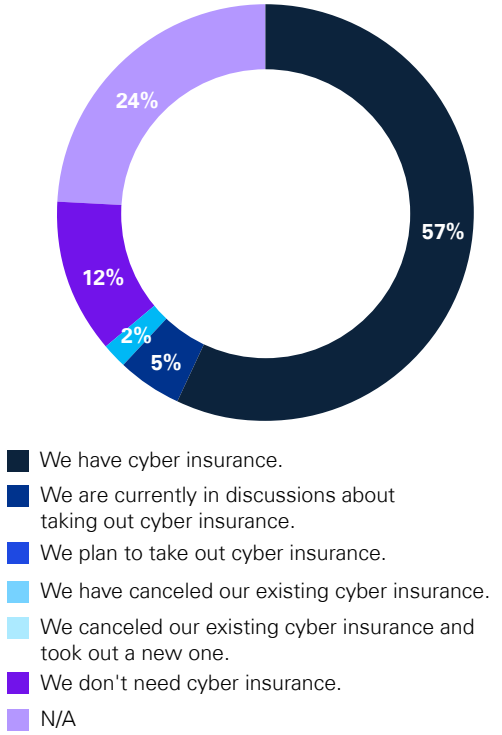
Difficulty finding the right service provider

Securing a service provider for specialized requirements often depends on trust and personal recommendations. Positive experiences tend to circulate within professional networks. However, the extent of difficulty in sourcing suitable domestic providers is still a relevant consideration. According to our study, only 14 percent of respondents reported challenges in finding an appropriate external service provider, whereas a substantial majority (71 percent) encountered no such issues. Most participants indicated that they identified their ideal service provider via established contacts or trusted referrals.

Cyber insurance

Cyber insurance is the subject of intense debate, and 57 percent of surveyed organizations own one. Almost 15 percent of the organizations surveyed currently see no need for cyber insurance or they have recently cancelled their existing cyber insurance. This indicates increased confidence in one's own security measures. However, it remains unclear to what extent these organizations actually take precautions to be able to react adequately in the event of a cyberattack.

Fig. 06 - Which of the following statements regarding cyber insurance applies to your organization?



Desired coverage by cyber insurance

Recent ransomware attacks and related insurance disputes have shown that companies' expectations of cyber insurance coverage often do not match reality. This has led to uncertainty and highlights the need for clear communication and transparency on the part of insurance providers. The adjustment of insurance companies' range of services due to the increase in ransomware cases clearly indicates the changing threat landscape.

We surveyed what organizations think should be covered by cyber insurance and identified that above all, organizations want to reduce the costs related to business interruptions and lost profits (67 percent), to reduce the costs for data loss and recovery (63 percent), and to receive expert legal advice (56 percent).

Forensic support (46 percent), repair and restoration (46 percent), third-party damages (45 percent), computer fraud (42 percent), are also important aspects for companies. This indicates that organizations acknowledge the importance of additional costs and collateral damage of a cyberattack.

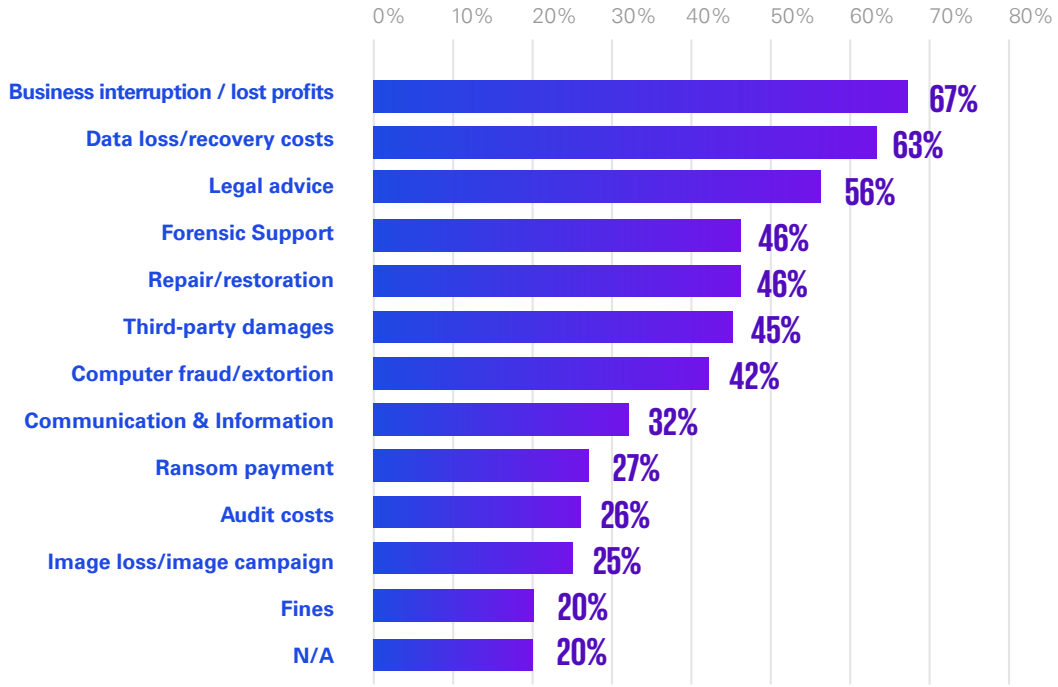
The areas communication & information (32 percent), ransom payment (27 percent), audit cost (26 percent), loss of image (25 percent), and fines (20 percent) are seen as less relevant.

The respondents who did not provide any information (20 percent) could indicate that these organizations are not fully informed about the scope of their cyber insurance.

Cyber insurance has evolved over the years and now offers a variety of packages, modules, and products. Companies' priorities for cyber insurance coverage are clearly on the cost of business interruptions, data loss, and recovery. The recovery of stolen or destroyed data is of enormous importance for companies. Cyberattacks often lead to business interruptions that can last from a few days to a few weeks. Compensating for these lost profits is therefore an important aspect of cyber insurance. Regardless of this, it is advisable to use resources for preventive measures such as vulnerability searches and the acquisition of new security tools to prevent security incidents and minimize potential damage.

Repairing and restoring business operations is also of great relevance—the cost of recovering systems after an attack can rise quickly. The increasing regulatory requirements and contractual relationships also require legal support, which explains the great importance of legal advice. Although organizations prefer not to pay ransom demands, there is still a desire for these costs to be covered by cyber insurance (27 percent), which reveals a certain contradiction.

Fig. 07 - What do you think should be covered by cyber insurance?



What to take away from this chapter

01

Organizations are reporting cyberattacks through multiple channels, both to authorities and regulators as well as to customers and third parties. One in five organizations did not report cyberattacks to any location.

02

Successful attacks act as drivers for organizations to improve their own security skills. It is only after a cyberattack that investments are often made in the development of additional security skills and the training of employees.

03

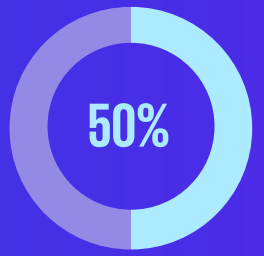
Cyber insurance is the subject of intense debate and one in two organizations own one. There is often a gap between companies' expectations of the services covered by cyber insurance and reality. This is causing uncertainty.

03

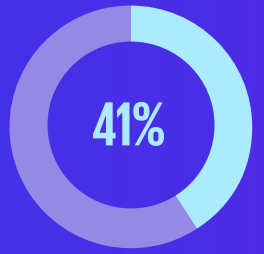
Third-party risk

The growing integration of business processes is placing greater emphasis on digital interdependence. Cybercriminals frequently target suppliers and service providers as entry points to infiltrate companies—these third parties remain the weakest link in the security chain.

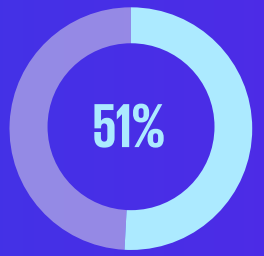
Collaboration between organizations and their suppliers or service providers is now critical to ensuring system security and resilience against cyber threats. Strengthening these partnerships is essential for implementing and expanding effective protective measures.



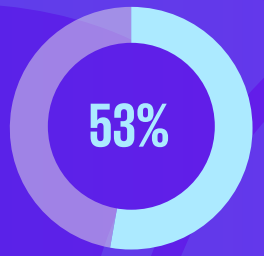
confirm specific cyberattacks on their supply chain



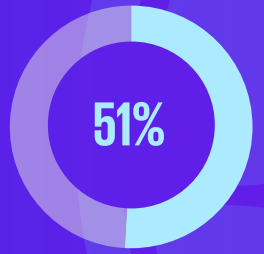
are concerned that a cyberattack against their service providers will have an impact on themselves



are concerned that suppliers do not adhere to the same security standards as they do, and thus become a gateway for attacks



don't know what impact supply chain attacks have had on them



request information security certifications from their service provider

Third-party risk

Attacks on service providers or suppliers

Organizations now know that cyberattacks on their own systems can lead to massive damage and impairment. For this reason, they have improved their protective measures, established security systems, and embarked on new investments to take their cybersecurity to a new level. Cybercriminals have also recognized this trend reversal. For example, we are seeing a shift in attacks towards customers and supplier systems that are located within the supply chain to the actual company that has been scouted out as a target.

Supply chain attacks have become increasingly important in recent years, as it is often the weakest link in the entire digital supply chain. This is also confirmed by our survey results: the results of our survey show that 38 percent of organizations confirm specific cyberattacks against their supply chain—a figure that reflects the increasing ambition of attacker tactics. Cyberattacks on managed service providers (MSPs), cloud service providers, or logistics partners, in particular, allow cybercriminals to penetrate highly secured networks via openings configured to enable third-party integrations (e.g., SolarWinds attack). Twelve percent of organizations suspect there was a cyberattack on their supply chain but were unable to confirm it, indicating insufficient forensic capacities.

The 29 percent of unknown cases reveal a structural problem: despite different regulatory requirements, many contracts lack clear SLAs (service level agreements) and obligations for reporting security incidents. Organizations with outdated vendor risk management programs often rely on annual self-disclosures from suppliers instead of real-time monitoring via APIs or security rating services. The growing use of third-party risk management tools is beginning to reduce the number of unknowns and drive more concrete responses, although their impact is not yet consistent across all organizations.

Many organizations cannot trace an incident back to the source, especially for attacks that originate through open-source software platforms or supply chain software libraries (e.g., compromises via web development frameworks).

Organizations also report disruptions and project delays—such as critical system outages caused by denial-of-service attacks on their cloud service providers. These incidents have driven up costs in cybersecurity and business continuity, forcing organizations to implement additional safeguards like severing connections and verifying system integrity. While some businesses are reconsidering their reliance on cloud services, others leverage market diversity to avoid dependency on single providers. Overall, while these attacks did not result in severe operational disruptions, they have significantly increased the burden of securing and adapting security processes.

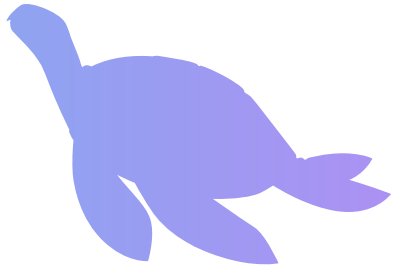
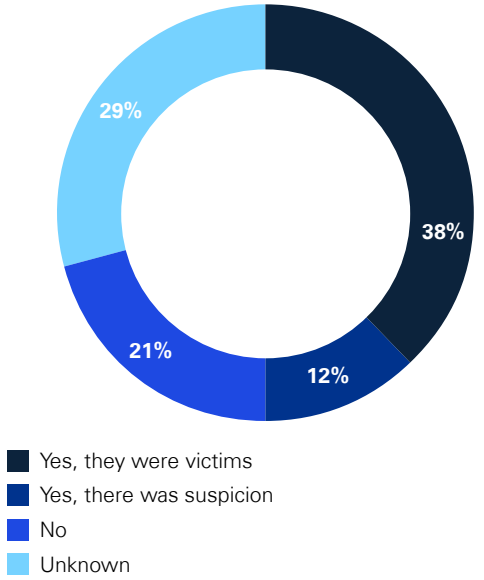
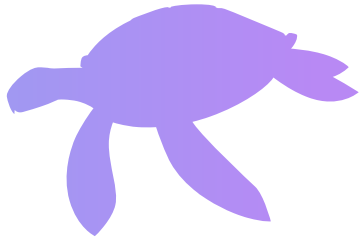


Fig. 08 - Have your organization's service providers/suppliers been affected by cyberattacks within the last 12 months?



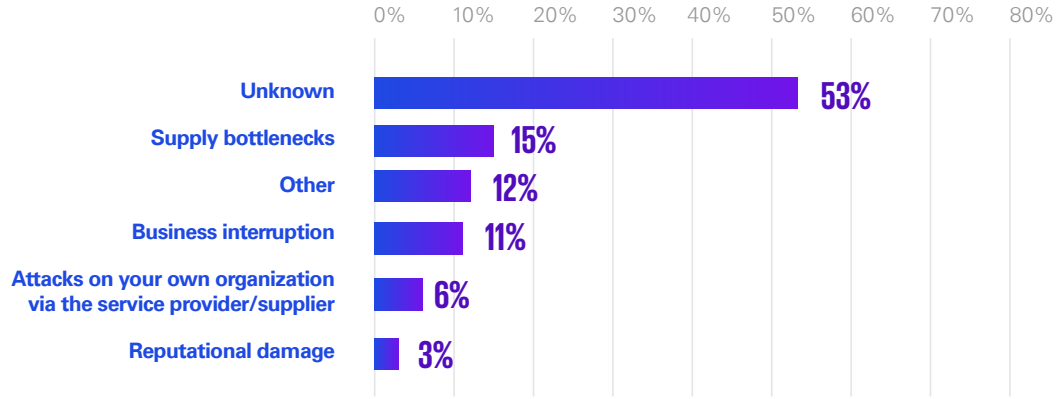


Impact of third-party attacks

Fifty-three percent of the organizations surveyed are unaware of the impact that supply chain attacks have had on them. This is completely surprising, and you can see once again that cooperation with suppliers and service providers is of particular importance.

Six percent of organizations had direct attacks on their own company due to the supply chain attack. This offers evidence for the existence of cybercriminals who infiltrate organizations via the service provider. Intensive cooperation and a transparent and open exchange to improve cybersecurity are therefore essential.

Fig. 09 - What impact did this have on your organization?



"In today's interconnected economy, supply chain risks represent a fast-growing threat to the stability of financial institutions like Crelan and the financial industry as a whole. The reliance on a complex network of technology providers, cloud solutions and third-party vendors increases both operational exposure and reputational vulnerabilities. At Crelan, we consider the possibility that every outsourced service has the potential to become a critical weakness if not adequately governed. External dependencies must be seen as a primary concern. Under the Digital Operational Resilience Act (DORA), financial institutions are required to strengthen oversight of third-party ICT providers, ensuring that risks are properly identified, assessed and mitigated. This implies movement beyond checkbox compliancy and instead establish a structured, risk-based approach to assessing external parties. This is why the security due diligence managed service has become a cornerstone within the Third Party Risk Management at Crelan. Crelan considers evaluating vendor controls, contractual safeguards and their subcontracting arrangements not only as a regulatory expectation, but mainly as a strategic necessity. By embedding supply chain oversight into the governance and risk frameworks, Crelan aims to better anticipate disruptions, safeguard customer trusts, reduce vulnerabilities and improve operational resilience overall."

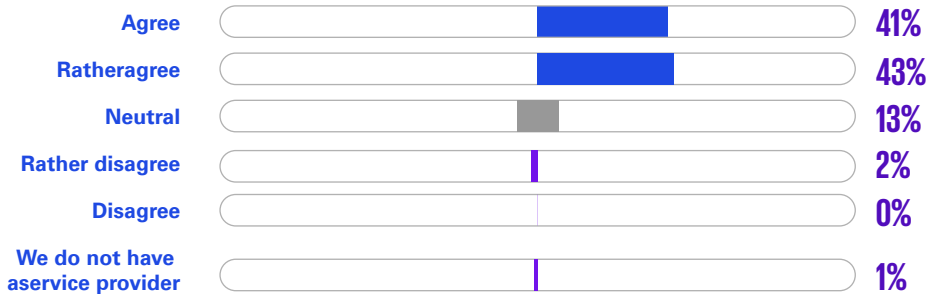
Wim Schuddinck
Director Security, Chief Security Officer Crelan

Third-party risk

Attacks on one's own company via the service provider are increasingly coming into focus. This also raises the question of whether domestic organizations are concerned that cyberattacks against their service providers will have an impact on themselves. Just over four-fifths of the organizations surveyed (84 percent) believe that it is precisely this type of attack that could lead to access or the associated effects on one's own company.

Based on these results, a clear trend can be seen that interdependence in the digital space is becoming increasingly important and that our digital resilience is being influenced by this. A paradigm shift must take place: we must move away from mutual recriminations and finger-pointing towards coordinated cooperation in the implementation of controls. Both on the part of the customer and the organization, and on the part of the service provider, there must be a closely interwoven exchange and cooperation to improve the security of the systems and the thoroughness of the controls.

Fig. 10 - We are concerned that cyberattacks against our service provider will have an impact on our organization.

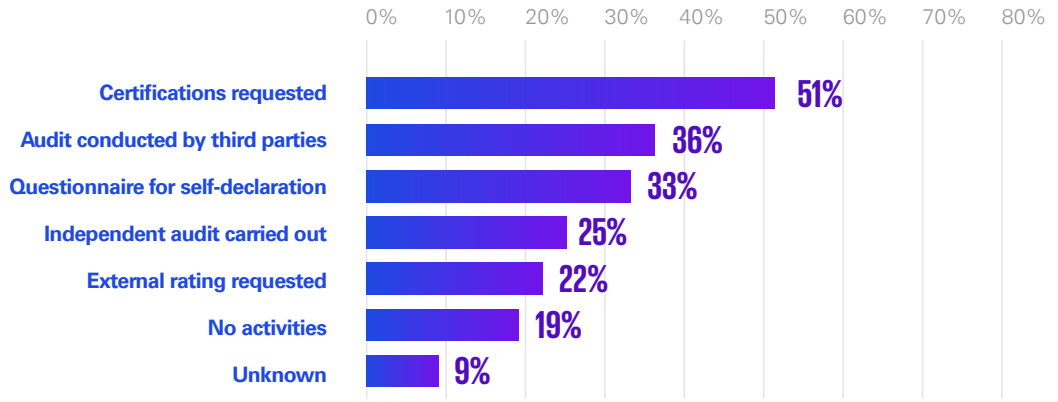


Ensuring compliance

Cooperation and transparency necessitate the open exchange of information. Open exchange entails that security assurances are routinely assessed with both suppliers and service providers. Organizations employ various strategies to maintain this level of security. Notably, 51 percent of surveyed organizations request certifications from their suppliers. The second most common measure, reported by 36 percent, involves conducting third-party audits at supplier sites. In third place, 33 percent of organizations utilize self-declaration questionnaires. Lastly, 28 percent of respondents indicate they lack awareness of the safety measures implemented by their suppliers or service providers.

Contractual agreements that prescribe specific security measures, such as NDAs (Non-Disclosure Agreements), DPAs, specific clauses and SLAs, are also used by organizations to ensure security for suppliers and service providers. However, it is more difficult for SMEs to demand security guarantees from suppliers because they have less economic influence and are thus often forced into the general terms & conditions of the vendors which tend to provide very few robust cybersecurity guarantees.

Fig. 11 - 3rd Party Risk - Effectiveness



Supply chain software

When asked whether attacks against the development pipeline in software development (software supply chain attacks) pose a major risk to organizations, 42 percent say that they do indeed see this risk. This result is not surprising, since the manipulation of code or software in particular, entails a lasting impairment of functionality. There is also a risk that backdoors or kill switches will be injected into the code, allowing unauthorized third parties to access the systems.

Above all, however, the use of online code repositories, such as those found on GitHub or other platforms, carries an inherent risk that non-quality-assured software code will circulate, and that malicious code will be built into the applications. It is precisely the convenience that these platforms offer, that software code parts can be removed quickly and easily, that makes it easier for attackers to carry out manipulations in the software development pipeline. In recent months, state or state-supported actors in particular have exploited the good faith with which this code is used. The potential risk of unauthorized access to IT systems, data, and applications, as well as cloud instances and sensitive company information by third parties, should not be underestimated.

Supply chain risk

It is worrying that 51 percent of the organizations are concerned that suppliers do not adhere to the same security standards as they do and thus could potentially become a gateway for attacks. Especially considering the threats and the figures from this study, which clearly show that there is definitely a need for action here. Only a third of organizations (31 percent) surveyed in Belgium conduct security assessments of suppliers to minimize the risk of security incidents in the supply chain. There is thus still a large margin for improvement.

This gap highlights a clear need for stronger and more consistent third-party risk management practices. Almost a third of organizations (31 percent) surveyed lacks awareness of supply chain risks. Particularly in view of the threats, many organizations are still in the transition moving away from point-in-time audits towards integrated, data-driven supply chain ecosystems. Regulatory pressure and rising cyber insurance premiums will further accelerate this transformation process.

What to take away from this chapter

01

Supply chain attacks have directly impacted 38 percent of organizations, with cybercriminals exploiting service providers as gateways to infiltrate their systems. This underscores the critical need for intensive collaboration and transparent communication to strengthen cybersecurity defense.

02

Digital interdependence is taking center stage, demanding a fundamental shift—away from blame and toward collaborative, coordinated action. Strengthening system security controls depends on open exchange and unified cooperation.

03

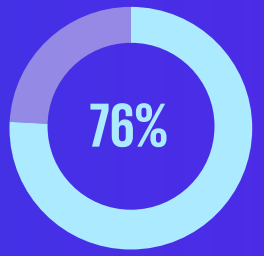
Organizations are no longer just prioritizing their own perimeter security but analyzing their advanced attack surface. However, many are still in a transition phase and need to move away from selective audits to integrated, data-driven supply chain ecosystems. Regulatory pressure and rising cyber insurance premiums will further accelerate this transformation process.

04

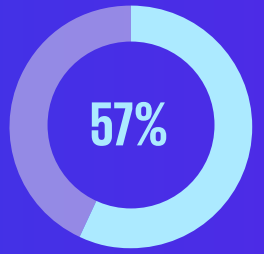
Artificial intelligence

Artificial intelligence (AI) is currently undergoing a transformative revolution, accompanied by numerous promises and widespread praise for its potential. Beyond its creative applications, such as generating artwork or composing music, AI is increasingly being utilized to help organizations improve their efficiency. In the field of cybersecurity, AI is enabling more effective defenses against cyber threats.

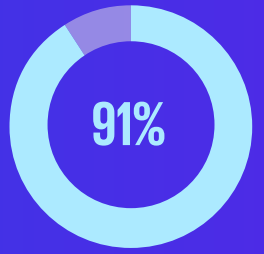
At the same time, these developments are not exclusive to defenders. Cybercriminals are also adopting AI to enhance and refine their attack tactics. As a result, we find ourselves in a race with them: using AI to enhance protection while adversaries exploit the same technology to increase the sophistication of their attacks.



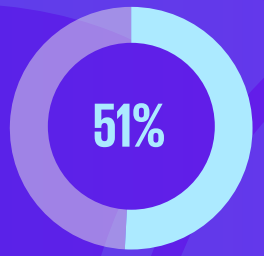
see AI as an opportunity



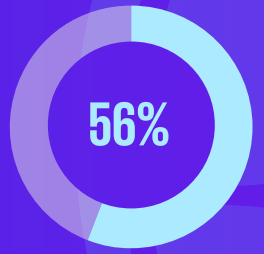
has set rules for the use of AI for employees



agrees that AI makes it easier to carry out cyber attacks



are already using AI to improve cybersecurity



the biggest obstacle for the use of AI are Data Protection requirements

Artificial intelligence

AI–opportunity or risk?

With the rapid pace of technological developments, organizations are faced with the question of whether AI is an opportunity or a risk and how they will deal with it. Our survey shows a clear tendency: 76 percent of respondents consider AI an opportunity, while 19 percent take a neutral stance. Only five percent perceive AI mainly as a risk. Thus, the trend is clearly recognizable that the opportunities outweigh the risks and that the risks, although they undoubtedly exist in the use of the new technology, tend to recede into the background.

Dealing with AI

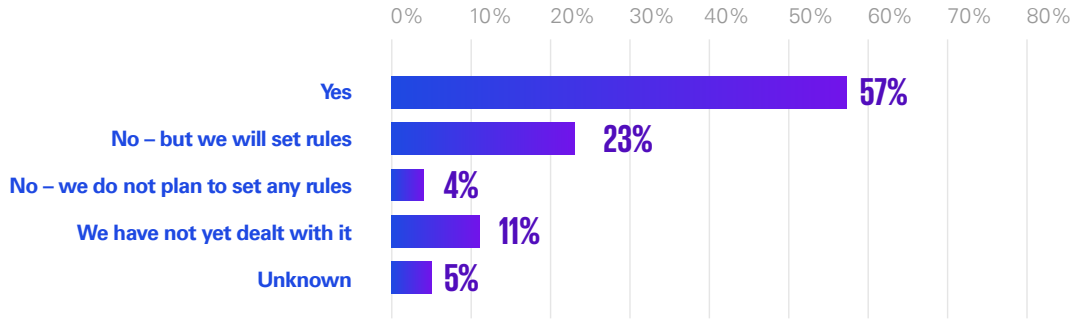
In addition to making work easier and increasing efficiency in business processes, AI solutions also offer improvements around cybersecurity. Many manufacturers offer solutions marketed as AI-powered. The extent to which these are pure algorithms that are "fattened up" with a little intelligence or actual solutions is not yet universally recognizable. Despite this ambiguity, the organizations we surveyed demonstrate a clear interest in leveraging AI to strengthen their cybersecurity measures.

According to our findings, more than half of organizations (51 percent) are already using artificial intelligence to improve their cybersecurity. Meanwhile, 29 percent are not yet utilizing AI for this purpose, but they acknowledge that the topic is important to them. Thirteen percent of respondents say that they have not yet dealt with it and that they do not consider it relevant to them.

The use of artificial intelligence in cybersecurity introduces both opportunities and potential risks. It is important to consider the possible vulnerabilities associated with new technologies, such as internet-connected systems that may be susceptible to interception or manipulation. AI solutions can also contain flaws and biases, which might result in skewed or unreliable outcomes. Therefore, conducting a balanced assessment of benefits and risks is necessary when incorporating AI into cybersecurity strategies.

Rules for the use of AI

Fig. 12 - Does your organization have rules for the use of generative AI for employees (e.g. process for assessing the safety of AI tools before use)?



AI has come at us like a tsunami. Organizations are confronted with the fact that in many cases the new developments and technologies virtually overwhelm compliance rules: new rules are needed for use in the organization. When asked whether companies have rules for the use of artificial intelligence for employees, more than a quarter (57 percent) said that rules have already been established. 23 percent currently have no rules, but plan to introduce them. 4 percent are of the opinion that no rules are needed and that no other activities are carried out for this purpose. It is interesting to note that 11 percent of respondents have already dealt with the topic and use AI while they have not yet dealt with whether rules are needed for use in the organization. This dynamic, as well as dealing with new technologies that can be used freely by employees on the Internet, poses special challenges for companies.

Barriers to the use of AI

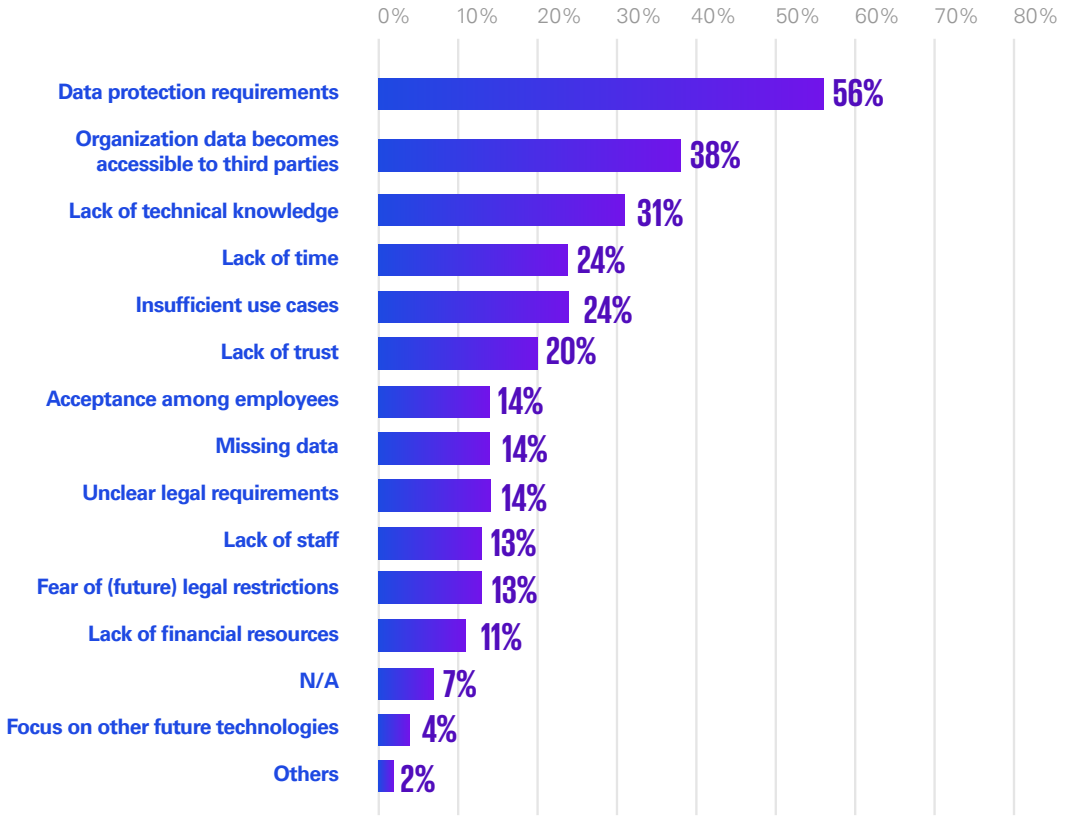
While the opportunities presented by AI currently outweigh the risks, and many organizations recognize its potential, there are still significant barriers and concerns that hinder its adoption.

The most frequently cited obstacle is compliance with data protection requirements, identified by 56 percent of respondents. This result is not surprising, because the protection of (personal) data is the top priority and it is not always clear whether third parties have access to the data. Closely related to this, 38 percent of respondents expressed concerns about data being made accessible to third parties. As AI requires data to be uploaded to external servers and thus processed and analyzed in data centers, it is, as a result, unavoidable that third parties are also involved in the processing of this data. In any case, organizations must carefully evaluate which information can leave their organization and be analyzed by AI systems.

In third place, 31 percent of respondents pointed to a lack of technical knowledge as a barrier to AI adoption. This is followed by concerns about unclear legal requirements, with 26 percent of organizations expressing uncertainty about the regulatory framework governing AI use. For example, questions often arise about where data is transferred and whether it is sent to countries with differing legal standards for data protection.

The quality of the tools and Large Language Models (LLMs) currently available is another obstacle for companies, as they are prone to errors and do not always provide satisfactory answers. The reliability of the results (risk of hallucinations) and the possibility of industrial espionage by third parties also still make the respondents skeptical. They also have ethical concerns, especially with image-generating AI that misuses third-party intellectual property for training. The potential impact on the environment of the use of AI was also mentioned.

Fig. 13 - What are the biggest obstacles to using generative AI in your organization?



Risks of using AI

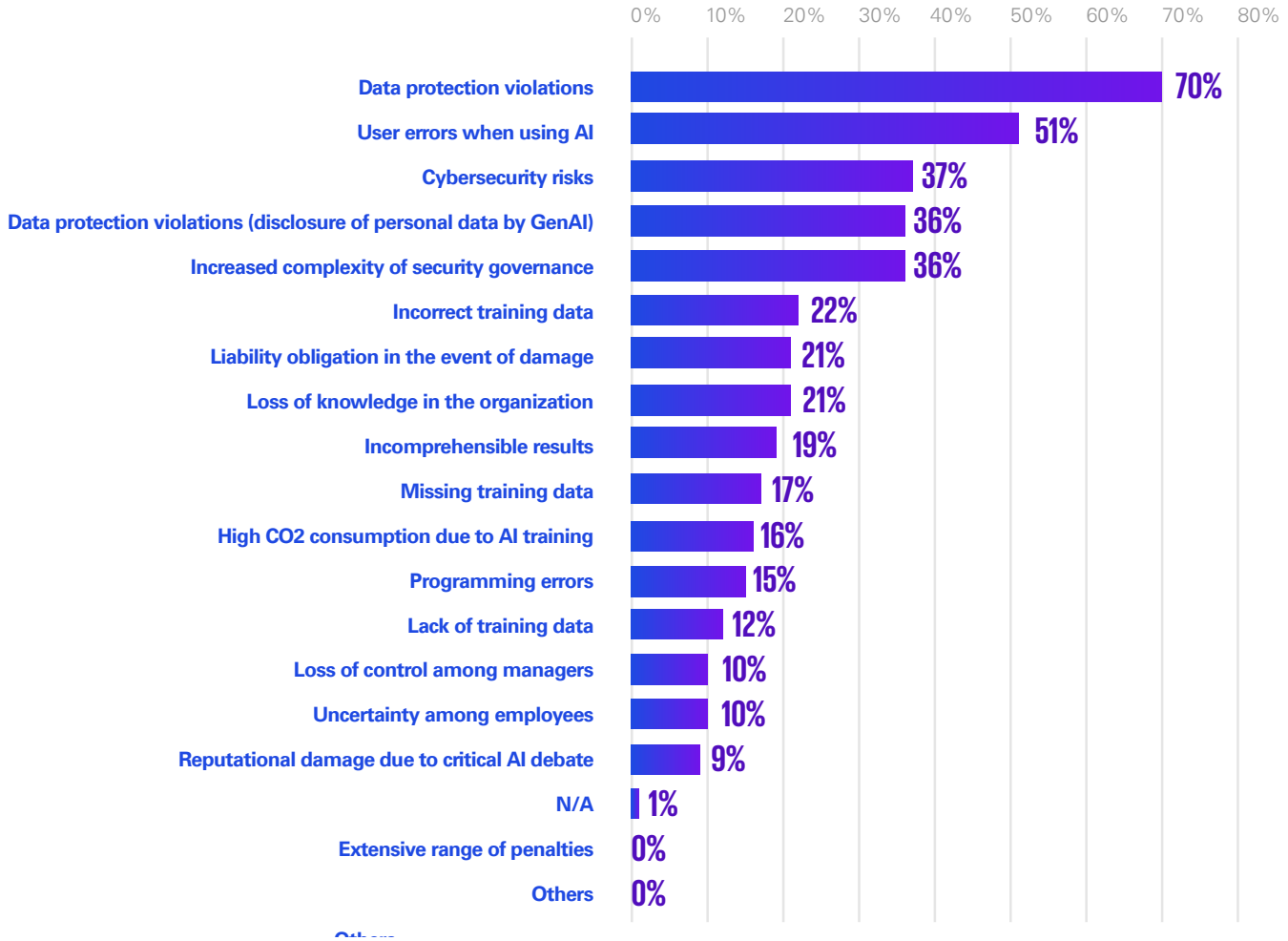
Our survey results show a multifaceted picture of the risks associated with the use of AI. The most significant concern remains data protection violations, cited by 70 percent of respondents. This underlines the continuing importance of data protection in the context of AI use and the need for robust protective measures.

The second most frequently mentioned risk is user errors when operating AI systems, identified by 51 percent of respondents. This highlights the need for user training and awareness to mitigate errors that could compromise security or lead to unintended outcomes.

Cybersecurity risks were the third most cited concern, with 37 percent of respondents identifying them as a key issue. One reason for this could be that organizations are increasingly taking measures to protect their AI systems from cyberattacks. Nevertheless, AI integration into existing IT infrastructures remains a challenge that requires careful security considerations.

Closely tied to the broader concern of data protection violations, 36 percent of respondents specifically cited the disclosure of personal data by generative AI systems as

Fig. 14 - What risks do you see when using AI in your organization?



a key risk. Another 36 percent of respondents pointed to the increased complexity of security governance. The integration of AI into organizations requires a comprehensive review and adaptation of existing security policies and processes.

Other risks such as incorrect or missing training data, loss of knowledge in the company, and programming errors are also classified as relevant by the organizations surveyed. Additionally, respondents highlighted ecological and legal risks, such as the high CO^2 emissions associated with AI training and the extensive criminal liability framework. These findings emphasize that, beyond immediate safety risks, organizations must also consider the broader environmental and legal implications of AI adoption.

Organizations must pursue a holistic approach that considers not only technological but also organizational and legal aspects. This is the only way to fully exploit the advantages of AI and at the same time keep the risks low. CISOs need to set realistic expectations and communicate the true potential of AI to senior management and the Board.

This involves highlighting the current limitations and having a strategic approach to adoption. By encouraging a culture of experimentation, CISOs can help with the discovery of appropriate use cases that align with the organization's unique needs and priorities. As AI continues to mature and evolve, CISOs must remain vigilant in assessing its capabilities and limitations.

Advances in cybersecurity through AI

For many, AI is seen as a lifeline for addressing previously unsolved threats and challenges, offering the potential to drive significant improvements within organizations. When asked about the role of generative AI in enhancing cybersecurity and defending against attacks, 67 percent of the organizations surveyed identified AI as a key to success. In contrast, eight percent expressed skepticism, stating that they (rather) do not believe AI can effectively improve cybersecurity or defend against attacks.

Although the vast majority have high hopes for AI, its use remains a big question mark. In the end, we are dealing with a cat-and-mouse game: due to its technological capabilities, AI can correlate attacks, bring together results, and put information into context. Data becomes information, information becomes intelligence, intelligence becomes contextualized information that can contribute to better decision-making . Large amounts of information in particular can only be analyzed effectively with technical solutions, making AI an essential tool for the future.

"The real battle is not attacker versus defender, but adopters versus laggards."

AI is no longer just a buzzword in cybersecurity — it's a race. On the one hand, it lowers the barriers for attackers: phishing in flawless language, automated scanning, and scalable campaigns are now cheaper and more effective than ever. That's why 91% of Belgian companies rightly believe AI makes cyberattacks easier to carry out. On the other hand, AI also gives defenders an unprecedented advantage: detecting anomalies earlier, cutting through alert noise, and responding faster than before. More than half of Belgian companies are already using AI to strengthen their cybersecurity, and those who embed it in a deliberate way are seeing measurable impact. The key insight is this: AI will not automatically balance itself between good and bad actors. Offense benefits the moment criminals apply it; defense only closes the gap when organizations put AI at the core of their resilience — and protect the AI they deploy themselves. The real divide ahead will not be between attackers and defenders, but between companies that harness AI responsibly and those that fall behind.

Peter Van Den Spiegel
Partner, KPMG Advisory, Head of Lighthouse & AI

Cybersecurity impact from AI

Fig. 15 - The proliferation of generative AI will improve cybersecurity by being used to defend against attacks.

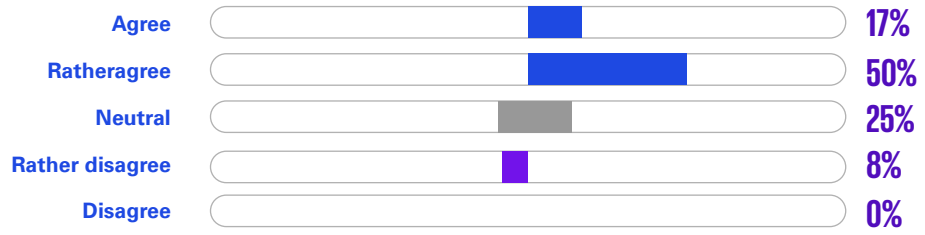
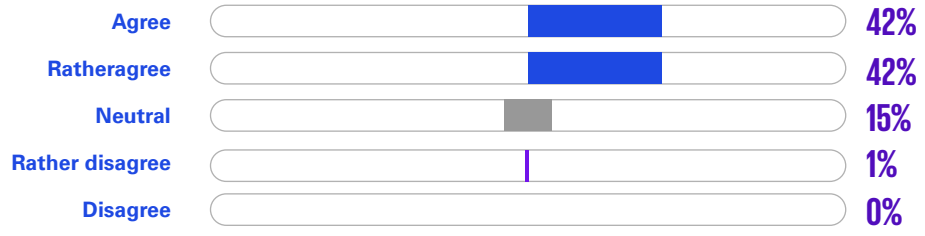


Fig. 16 - The proliferation of generative AI will impact cybersecurity because it can be exploited by attackers



When it comes to AI, we see a significant number of contradictions. For instance, when asked whether AI can be used by attackers, 84 percent of respondents answer that they (rather) agree. If you compare these answers with the answers about whether AI is seen as a key solution to improving cybersecurity, it is clearly seen that there is hope on the one hand but also concerns about the use of AI on the other.

The fact is that the human-created models and algorithms behind AI are error-prone and can be manipulated and thus used to the advantage of the attackers.. We attempt to address threats to technical systems with technical solutions. It becomes a case of technology versus technology—but the question remains: where is the human controlling these systems?

Exacerbating the threat landscape from AI

With the introduction of new technologies such as artificial intelligence, the threat situation naturally intensifies. Eighty-one percent of the organizations surveyed agree that AI contributes to an increasingly complex and challenging cybersecurity environment. In contrast, only two percent of respondents are of the opinion that no change in the threat situation is to be expected from the use of artificial intelligence.

Facilitating cyberattacks through AI

On the downside, artificial intelligence significantly lowers the barriers for attackers to carry out cyberattacks against companies. It has never been easier to prepare highly targeted attacks tailored to specific individuals or groups. Let's think, for example, of phishing messages that can be tailored precisely to the context of the respective person. Accordingly, 91 percent of respondents believe that AI will in any case contribute to facilitating cyberattacks.

Improving cybersecurity over the past 12 months

Has artificial intelligence significantly improved the cybersecurity of the organizations surveyed over the past 12 months? According to the data, only 30 percent of respondents believe that AI has contributed to (rather) improving cybersecurity, while 13 percent remain skeptical, stating that AI has not made a meaningful impact.

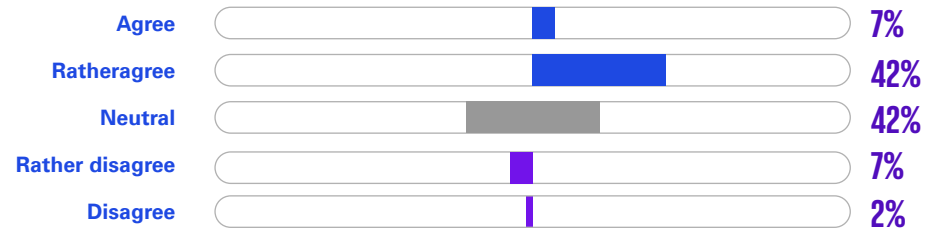
Despite high expectations, AI has not delivered the transformative improvements many had hoped for. The reality is that AI is not a magic wand capable of compensating for fundamental security flaws. Algorithms cannot address security gaps that organizations are unaware of, nor can AI-powered detection systems resolve issues without proper foundational security measures in place.

The survey reveals a tension between optimism about technological progress and the actual experiences of companies. While 30 percent of respondents are (rather)

positive about AI's impact so far, this figure rises to 49 percent when looking at future expectations. This jump of 19 percentage-point, stands in stark contrast to reality: 56 percent of respondents are neutral about the subject as to whether artificial intelligence has improved cybersecurity in the last 12 months, and remain passive.

This sentiment can be summed up as follows: "AI in cybersecurity is a guaranteed success—but only if there is a clear will to shape its use and strengthen underlying security practices." At the same time, the numbers also point to an unspoken dilemma: the more artificial intelligence is hyped in cybersecurity, the clearer it becomes that it is not a cure-all, but a tool that only works as well as the infrastructure and processes in which it is embedded. Many organizations view AI as a lifebuoy for their security boats with holes, while ignoring the basic leaks—unpatched systems, poor access controls, and untrained employees.

Fig. 17 - AI will bring about a significant improvement in cybersecurity in the following 12 months.



Between belief in progress and denial of reality

While AI can be beneficial in detecting anomalies and fighting deepfake attacks more effectively, no algorithm in the world will ever compensate for a weak password or an unpatched Exchange server. Our survey results suggest that the cybersecurity sector is hoping for AI as a kind of deus ex machina, rather than addressing the essential fundamentals.

Perhaps the most important metric in our next survey should be: "How many of your AI security tools are running on systems that are no longer supported?" This could be a wake-up call for those who prefer to invest in the AI hype rather than in basic patch management.

Opportunities for improvement through AI in various areas

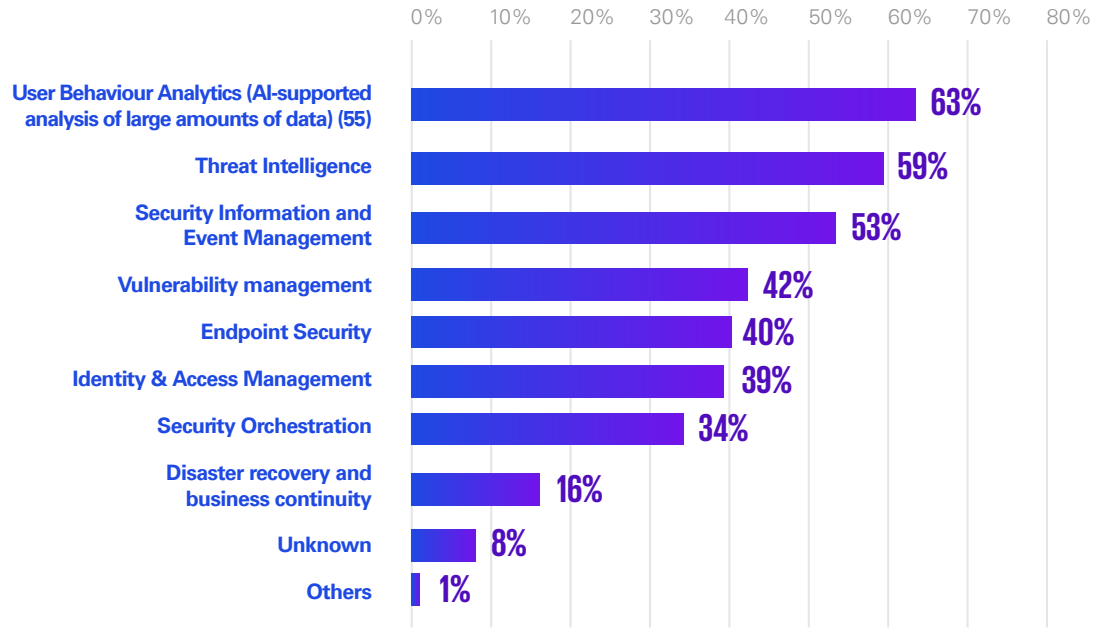
Survey participants identified several key areas where AI could improve cybersecurity. The top opportunity lies in user behavior analytics, with 63 percent highlighting AI-supported analysis of large amounts of data as a critical area for improvement. This is followed by threat intelligence (59 percent) and security information and event management (53 percent). Vulnerability management (42 percent) and endpoint security (40 percent) also ranked highly, reflecting the growing importance of proactive measures in cybersecurity.

Identity and access management (39 percent) was another area where respondents saw potential for AI-driven advancements. Security orchestration (31 percent) and disaster recovery and business continuity (16 percent) were mentioned less frequently. This suggests that most organizations have not fully addressed the risks of autonomous decision-making systems.

Interestingly, eight percent of respondents admitted they currently do not know in which areas AI could improve cybersecurity. This suggests that there may still be gaps in the respondents' knowledge of the use of AI.

This data highlights a paradigm shift in cybersecurity strategies, with traditional perimeter-based approaches losing relevance in favor of behavior-based protection mechanisms. This shift aligns with the increasing migration of services to the cloud and the need to protect distributed workloads through AI-driven contextual analysis. Organizations are therefore increasingly relying on proactive analysis and prevention instead of just reacting to attacks.

Fig. 18 - Areas where AI can most improve cybersecurity.



What to take away from this chapter

01

For many, AI is seen as the key to solving previously unsolved threats and problems and driving improvements in organizations. AI enables the analysis of large amounts of information that would otherwise be impossible. On the flip side, AI also lowers the barriers for cybercriminals, making it easier than ever to carry out highly targeted attacks.

02

In the last 12 months, AI has not yet delivered the transformative improvements many had hoped for in cybersecurity. While great expectations were placed on AI to enhance safety, these promises have not (yet) been fully realized. However, looking ahead, almost half of respondents believe that AI will drive significant improvements in cybersecurity over the next 12 months, reflecting optimism about its future potential.

03

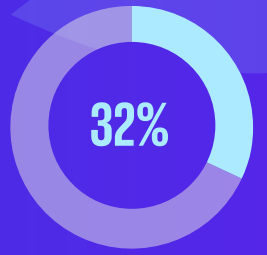
AI can interpret complex scenarios and make connections that were not possible before. However, it is also flawed and the algorithms used have a certain bias. A balanced analysis and weighing of the benefits and risks is essential for organizations.

05

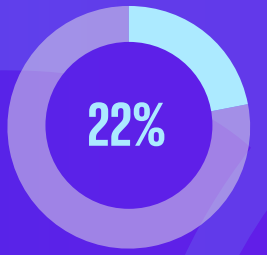
Dis- and misinformation

Disinformation and misinformation as well as all other forms of (hybrid) influence have a direct and unfiltered effect on our society – especially in times of geopolitical tensions. Our world order is beginning to falter.

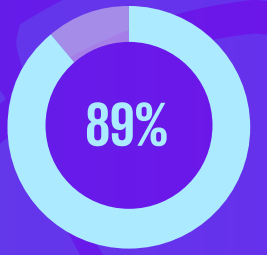
Security is no longer something that can be planned, nor is it a given, because all areas (whether economy, technology, environment, or our society) are simultaneously coming under pressure. The options available to perpetrators are diverse, while the impacts and consequences are hardly predictable.



rather believe that their company can fall victim to a cyber-attack that could exert targeted influence on the organization



do rather not believe that their company can fall victim to a cyberattack that could exert a targeted influence on the organization



believe that political activists are the largest actor to emanate disinformation and misinformation

see state institutions as actors in disinformation campaigns

say that disinformation campaigns influence our societal resilience.

Dis- and misinformation

Disinformation and misinformation as a threat to companies

Intellectual property, construction plans and corporate values in particular, but also patents, marketing concepts and similar ideas are often at the center of attacks. The targeted influence on organizations through the spread of misinformation and disinformation is becoming increasingly important.

Our survey results indicate an evolving perspective within organizations regarding the risks associated with cyber-attacks and disinformation campaigns. There seems to be a notable shift in how organizations perceive cyber risk. In earlier years, many organizations primarily associated cyberattacks with opportunistic threats such as ransomware campaigns or indiscriminate malware infections. Today, however, 42 percent of survey participants believe their company could be the victim of a targeted attack aimed at influencing business operations or decision-making.

This development tells us two important things:

- Organizations are beginning to recognize that cyber risk is not only about data theft or financial fraud, but also about strategic influence and disruption. Disinformation campaigns, supply chain manipulation, and attacks aligned with geopolitical or competitive motives are entering the corporate risk radar.
- The fact that nearly half of the respondents now see themselves as potential victims of targeted influence attacks shows that awareness is catching up with reality. This suggests that boards and executives are increasingly factoring cyber threats into strategic risk management, though the other 58 percent may still underestimate their exposure.

In practice, this shift means organizations will need to go beyond traditional perimeter defense and incident response. They must strengthen threat intelligence, crisis communication strategies, and resilience planning, particularly in scenarios where cyberattacks and disinformation are used together to destabilize trust in the company.

Fig. 19 - Do you believe that your organization could become a victim of a cyber attack that could exert targeted influence on the organization?

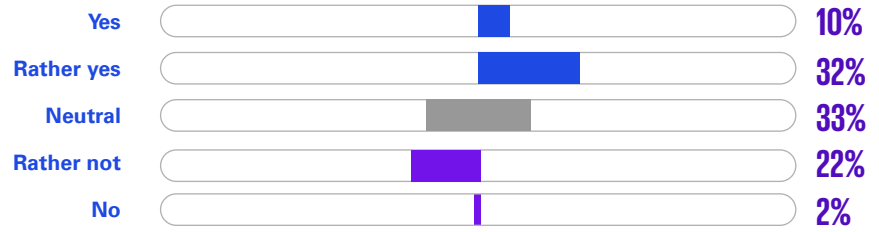
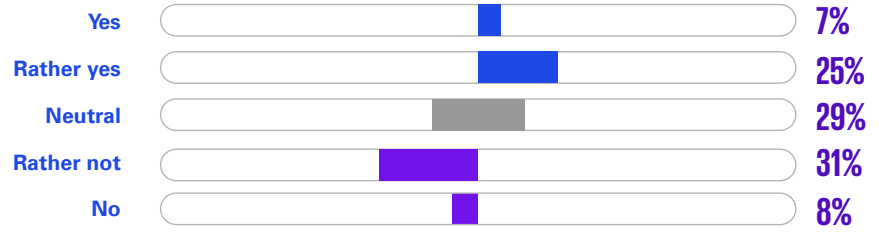


Fig. 20 - Do you think your business activities can be influenced by online disinformation campaigns?



International observation indicates an increasing use of disinformation to influence organizations abroad, within Europe, and in Belgium. Although Belgium is a smaller country, we do have headquarter large important international and governmental organizations (NATO and European Institutions). This makes us a more likely target of misinformation and disinformation. Such activities are intended to exert influence and alter the behavior of targeted organizations.

24 percent believe that no influence is possible. So, while a significant proportion of organizations take the threat of disinformation seriously, there is also a group that is less concerned. This could be due to different experiences, industries, and the existence of internal safeguards against disinformation.

The underestimated danger of narrative warfare

The fundamental concern that disinformation influences corporate activities remains very high: 32 percent of those surveyed consider it possible to exert an influence on the company through online disinformation campaigns. The discrepancy between perceived and actual threat can partly be explained by the "iceberg phenomenon of disinformation" - there is a visible risk (direct attacks such as fake news campaigns are becoming increasingly detected and repelled). Underneath, however, there is a concealed mass. Indirect methods such as undermining employee trust, manipulating investors, or disrupting supply chains through false information often go undetected.

The underestimation of indirect disinformation creates a false sense of security. While direct fake news campaigns are detected more frequently and their short-term effects countered, more subsistent and sustained misinformation campaigns (investors, suppliers, employees) often go undetected. In its annual report on global risks, the World Economic Forum identifies "Misinformation and Disinformation" alongside five supply chain attacks as a growing risk - for example, the targeted dissemination of false information about working conditions, which leads to reputational losses and regulatory sanctions .

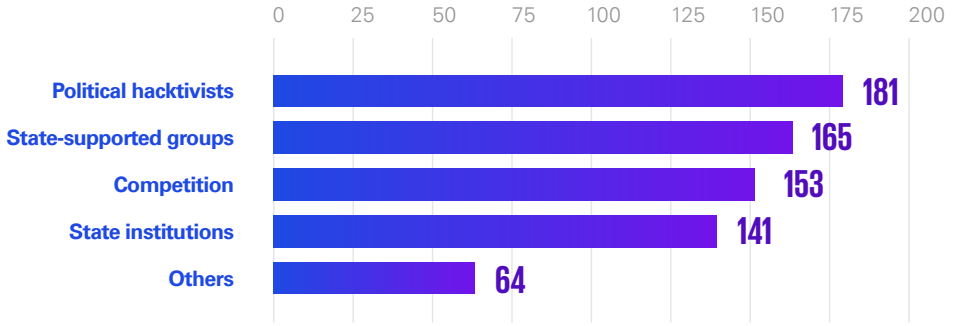
Actors from whom disinformation originates

Especially in the field of disinformation campaigns, there is a diverse spectrum of actors who operate in this environment.

- Political hacktivists: These are usually motivated by political or social concerns and spread disinformation to draw attention to certain issues or to bring about a change in business practices at the attacked companies. The effects of disinformation campaigns range from short-term damage to the image to long-term changes in corporate policy.
- State or state-supported actors: They often act within the framework of geopolitical strategies. The aim of disinformation campaigns is to trigger economic instability, create a competitive advantage for their own national organizations, or exacerbate political tensions.

Domestic organizations view political hacktivists as the primary source of disinformation and misinformation, followed by state-backed actors. Competitors are also seen as significant threats. Some survey participants highlighted competition as a particular concern. State institutions were ranked fourth, with some being involved in disinformation efforts. Respondents noted that former employees may use internal knowledge to harm companies, while dissatisfied customers and negative anonymous reviews can also damage corporate reputations.

Fig. 21 - Which actors do you think pose the greatest threats to disinformation/misinformation against your organization?



Geopolitical instrumentalization

State institutions use disinformation in the context of hybrid warfare. Examples such as the "deepfake diplomacy" campaigns in the context of the Russian invasion of Ukraine have shown how state actors deliberately destabilize organizations to exert economic pressure on them.

Blurring boundaries: A fusion of state and private actors (e.g., by outsourcing cyberattacks to "patriotic" hacker groups) makes attribution more difficult. This creates a new form of hybrid threat actors.

Disinformation influences our societal resilience

65 percent of the organizations surveyed believe that disinformation and misinformation campaigns undermine societal resilience. International democratic structures, shaped by diplomatic negotiations and cooperation, often move slowly and feel distant from everyday concerns. This places significant challenges on societies. As a result, people increasingly look to their own nations to take responsibility for building resilience.

The greatest risk to societal resilience arises when cohesion breaks down. Security is a shared responsibility, and it is precisely the active involvement of civil society that enables cohesion in turbulent times. Scandinavian countries provide a strong example: through the inclusion of civil society, the development of emergency concepts, and the use of overarching platforms, they demonstrate how comprehensive strategies can strengthen resilience.

Technological tools to counter disinformation are important, but they are not sufficient on their own. What is needed is a clear narrative, a coherent strategy, and collective action. The question is not whether misinformation will trigger events, but whether we are prepared for them. If we fail to act today, we risk being caught off guard tomorrow.

Strategies to defend against disinformation campaigns

Organizations can take various measures to protect themselves against disinformation:

- Implement systems for monitoring online content and analyses of potential disinformation campaigns.
- Develop clear and transparent communication strategies to refute misinformation and maintain stakeholder trust.

"Foreign Information Manipulation and Interference (FIMI), the intentional weaponization of information, is an existential threat to our democratic values and trust in our institutions, which also directly undermines and affects our business environment. This forces us to rethink our understanding of security, as deliberate disinformation is a powerful and elusive Trojan horse, especially in combination with other hybrid attacks. Lacking an attractive societal alternative, our adversaries spend incredible amounts of money to alter who we are as a society by polarizing and radicalizing, until we doubt everything and stop believing in anything: "your truth is as good as mine" is the effective death of democracy, because democracy relies on free and well- informed citizens. Therefore, we need to wake up quickly and understand that for our adversaries, disinformation is a central and crucial tool."

Peter Booms
Counselor (Hybrid threats, FIMI, Disinformation, Crisis Management, CSDP), Permanent Representation of Belgium to the European Union

- Work with cybersecurity experts and Public Relations specialists to identify threats and respond appropriately.
- Train employees to be aware of the risks of disinformation and to have tools to detect and respond. These strategies help organizations increase their resilience and protect their operations.

Escalation of strategic disinformation campaigns: causes and effects on companies

The increase in disinformation campaigns against organizations by competitors and state institutions is due to technological, geopolitical, and economic factors:

Technological empowerment of attackers

Advances in generative AI (e.g., ChatGPT, deepfake synthesizers) and automation tools are helping cybercriminals produce hyper-realistic misinformation on an industrial scale. AI-controlled bot networks generate thousands of social media postings within a few minutes, which deliberately cause reputational damage. For example, forged documents on alleged compliance violations or manipulated video statements by executives are generated.

Competitive dynamics in the digital space

Against the backdrop of global recession fears and increased market competition, competitors are using disinformation campaigns to gain competitive advantages at low cost. For example, manipulated reviews are published on platforms such as Trustpilot or Google Reviews. Another tactic is to spread false supply shortage reports. This is intended to persuade partner organizations to end cooperations.

Geopolitical instrumentalization by states

State actors use disinformation campaigns to achieve their trade or security policy goals, for example by deliberately circulating false reports. At the same time, authoritarian regimes use disinformation to destabilize critical infrastructures. An example of this would be spreading rumors about alleged cyberattacks on energy suppliers to undermine confidence in their operational security.

Systemic vulnerabilities of the information ecosystem

A fragmented media landscape and algorithm-driven distribution of content on platforms such as X or Telegram promote the spread of false narratives. In addition, advertising tools enable cybercriminals to place paid disinformation campaigns with investors, employees, or the general public.

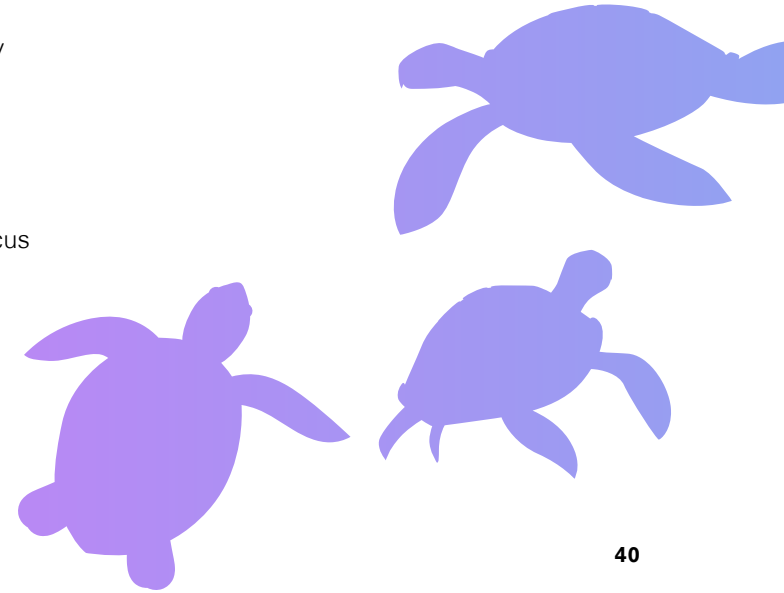
A new risk paradigm

Systematic hybrid attacks are a reality in geopolitical negotiations, with disinformation becoming a reality. To be socially resilient, organizations must expand their crisis collaborations and invest in deepfake-detection technologies. In addition, international standards are needed to combat the strategic misuse of disinformation as a competitive tool.

Strategic implications

Our survey results make it clear that early targeted disinformation strategies are reaching their limits. In addition to technological detection and prevention, respondents pointed out the following:

- Analysis teams in organizations that focus on hybrid threats in the media space.
- Training programs for the detection of cognitive distortions (“prebunking”) to immunize employees against narrative manipulation.
- Cross-sectoral initiatives to strengthen collective resilience against hybrid threats.
- Increased cooperation with supervisory authorities to develop uniform standards for countering disinformation.
- Ethical guidelines for the use of generic AI to detect disinformation to prevent loss of trust due to surveillance fears.



What to take away from this chapter

01

Online disinformation campaigns help to change the opinions of society and entrepreneurs in a targeted manner. The aim is to exert pressure and elicit the behavior desired by the attackers.

02

Organizations and our economy are in the crosshairs of disinformation campaigns. The options available to groups of perpetrators are manifold, and the effects and consequences are hardly foreseeable.

03

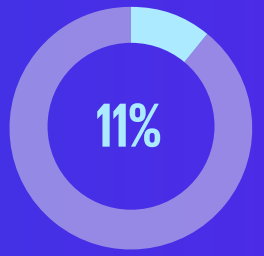
Reality has shown that there is an increasing influence on organizations in Belgium as well. As a rather small country, Belgium does play a relatively large geopolitical role compared to other nations due to the presence of NATO and the European Institutions. This means that the risk of misinformation and disinformation is very present here in Belgium.

06

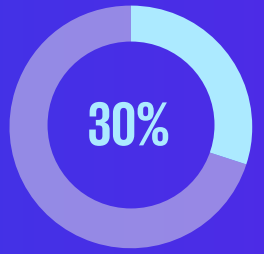
Regulatory

The regulatory landscape is currently very diverse and developments in the European Union on this topic are bringing to light many new requirements regarding cybersecurity.

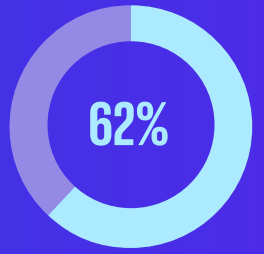
The regulations that are currently emerging are a consequence of the fact that organizations and economies are under increasing pressure from cyberattacks and there is a growing concern that best practices alone won't suffice to address these emerging challenges. The new regulations are also intended to improve cybersecurity maturity level across the European market.



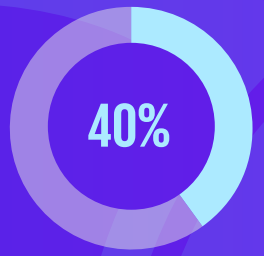
are not directly impacted by regulations.



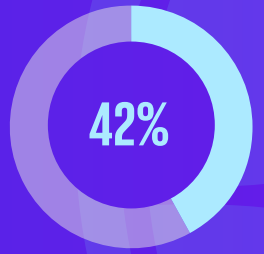
say they are affected by DORA



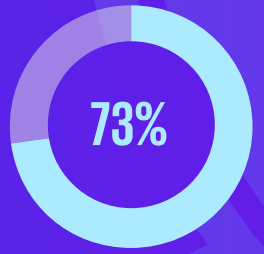
are impacted by the NIS2 Directive



say that they are affected by the Cyber Resilience Act



are affected by the AI Act.



are on track to meet NIS2 deadlines in Belgium

Regulatory

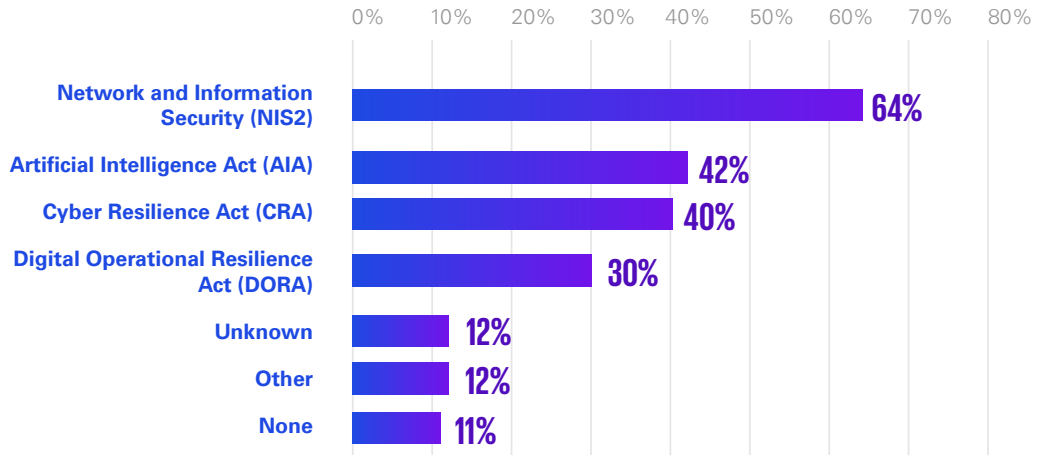
The regulatory landscape in Belgium

European cybersecurity regulation will increasingly affect how Belgian organizations need to approach security. However, the implementation is not as straightforward as there are multiple regulations that need to be considered, and most organizations face a challenge with integrating them into existing processes via a uniform compliance framework. When asked which regulations are likely to affect your organization, we observed that most respondents view NIS2 as the main driver (around 64 percent, followed by the AI Act (42 percent) and the Cyber Resilience Act (40 percent)). This confirms that organizations anticipate a broad EU regulatory wave beyond cybersecurity, extending into AI and product security. Only 30 percent have to comply with DORA, which reflects its sector-specific nature (mostly financial institutions).

Respondents who selected "Other" were asked to specify which additional regulations they deem as relevant. The list includes GDPR, Radio Equipment Directive, eIDAS, Basel, and SOx. These answers reflect the breadth of obligations organizations would need to address, often sector-specific (for instance, Basel for finance, SOx for listed entities). GDPR's repeated reference demonstrates that privacy remains a top priority for security professionals, even though it is already in force since 2016. The diversity underscores that concerned teams need an integrated approach rather than treating each regulatory instrument (i.e., NIS2, the Cyber Resilience Act, the AI Act, etc.) separately. Robust regulatory requirements to security controls mapping and alignment across different organizational functions (i.e., legal, IT, compliance) would avoid siloed responses and duplication of efforts.

The 12 percent "unknown" and 11 percent "none" highlight a potential knowledge gap: some organizations either lack regulatory knowledge or tools (e.g., scanning capacity) or underestimate their exposure and applicability of such regulations to their organization. This misalignment could result into late compliance efforts and potential fines and sanctions. A proactive approach includes monitoring regulatory landscapes for applicable requirements and gap assessments. Moreover, a unified control framework can help streamline efforts to address multiple overlapping regulatory requirements.

Fig. 22 - Which regulations are (likely) to affect your organization?



EU NIS2 Directive and Belgian NIS2 Transposition Law

EU NIS 2 Directive is an essential measure to improve cybersecurity across the EU. This sets requirements for the security of network and information systems and obliges organizations to implement appropriate cybersecurity risk management measures and incident reporting mechanism. The national implementation of the law further specifies these requirements for Belgian organizations. It is expected that most organizations will be affected by these measures.

Of the 67 percent of organizations that believe that Network and Information Security Directive (NIS2) is applicable to them, nearly half (44 percent) fall under "Essential", and another 42 percent under "Important",

confirming that most respondents are significant entities subject to significant requirements. Only 9 percent are "Basic", and 5 percent are unsure. This distribution aligns with NIS2's broad coverage of essential services. However, the small "don't know" share indicates potentially that not all organizations have mapped themselves properly. Early engagement with the Belgian Centre for Cybersecurity (CCB) - which is the competent authority in Belgium responsible for enforcing NIS2 - and a solid information security management system, including a robust information security risk management framework, would optimize resources allocation and control implementation prioritization (risk-based approach).

Fig. 23 - Is your organization in scope of NIS2?

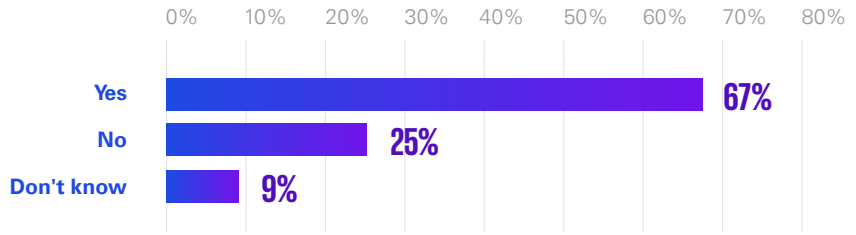
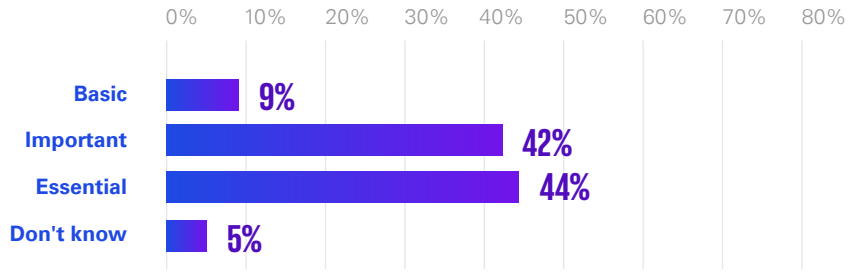


Fig. 24 - Which CyberFundamentals™ level is applicable to your organization?



CRA, NIS2 and CSA as the three musketeers in cybersecurity legislation'

Although the regulatory landscape is very divers, the cyber related aspects are a transversal aspect along a lot of different legislations.

Therefore, it is necessary to reveal the logic that currently is a bit hidden throughout all these legislative pieces. Revealing this structure might also help to streamline the simplification package and review of legislation.

When we look at the core transversal legislative aspects, we recognize three legislations. First, the NIS2 is the legislation that requires entities that are important to our economic and societal tissue to be resilient. This legislation therefore focusses on the protection of entities as a whole. Second, we have the Cyber Resilience Act that targets the manufacturing and provisioning of cybersecure products and services. Thirdly, we have the Cyber Security Act that provides the structure to use certification under accreditation as a tool for market supervision and enforcement.

These three cornerstone legislations complement each other and are building blocks for common transversal cybersecurity requirements in different types of legislation, such as the artificial intelligence act, eIDAS2.

Every new legislation that incorporates cybersecurity must maximize the use of these elements to underline that resilience is a share mission that requires smart implementation of legislation: One for all, All for one shared mission.

Johan Klykens
Director Cybersecurity Certification Authority, CCB

Digital Operational Resilience Act (DORA)

Since its binding application on January 17, 2025, our survey shows that 30 percent of respondents already prioritize DORA. This finding aligns with the strong representation of financial sector organizations in our sample.

Given DORA's role as a lex specialis, prevailing over NIS2 for the financial sector, this level of prioritization can be interpreted as a positive signal of regulatory awareness and preparedness. Organizations appear to recognize the strategic importance of DORA, not only for compliance but also for strengthening their resilience and risk management practices.

The financial sector is moving early to integrate DORA requirements, which may set a benchmark for other industries. In addition, awareness of regulatory hierarchy (DORA vs. NIS2) indicates a maturing understanding of compliance obligations. This proactive stance could facilitate smoother adoption of related frameworks, enhance cross-sector resilience, and reduce regulatory misalignment.

Artificial Intelligence Act (AI Act)

The AI Act governs the use and development of artificial intelligence, aiming to minimize risks and ensure safe, ethical deployment. In our survey, 42 percent of organizations expect to be affected, underlining the growing strategic relevance of AI in today's corporate landscape. Organizations increasingly recognize that AI is not only a driver of innovation but also a regulatory priority that will shape business models, governance, and compliance in the years ahead.

Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) seeks to enhance IT system resilience against cyber threats by requiring products to be designed with security in mind. In our survey, 40 percent of organizations report being affected, highlighting the increasing importance of robust, product-specific, cybersecurity requirements - especially for manufacturers of connected devices. CRA underscores a shift from reactive defense to security-by-design, making cybersecurity an essential part of product development and market readiness.

NIS2 – Implementation

When it comes to NIS2 implementation, most organizations adopt either the CCB's Cyber Fundamentals™ framework or ISO27001. In our survey, 49 percent rely directly on Cyber Fundamentals, reflecting strong alignment with the national baseline, while 43 percent apply ISO27001 (certified or aligned), underscoring trust in international standards. This split shows organizations balancing national regulatory expectations with global credibility.

However, this duality also raises risks. Fragmentation could complicate audits, especially if regulators enforce strict adherence to Cyber Fundamentals. A dual alignment strategy using ISO27001 for international recognition and Cyber Fundamentals for Belgian compliance appears most pragmatic, provided both are integrated into a centralized framework.

The 8 percent using "other" approaches cited internal frameworks, ongoing evaluation, reliance on DORA as lex specialis, and supplier compliance. While innovative, these approaches carry blind spots: depending solely on suppliers neglects internal responsibilities, and assuming DORA fully covers NIS2 could prove risky without regulatory confirmation.

Organizations must avoid "compliance by assumption" and instead pursue coordinated, multi-framework strategies that satisfy both national and international expectations.

Fig. 25 - How are you complying with NIS2 Law in Belgium?

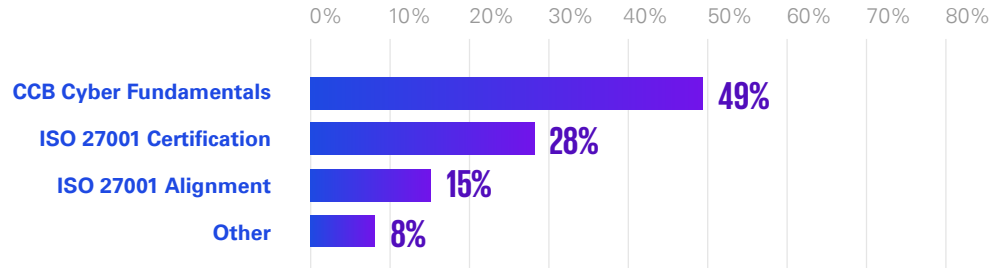
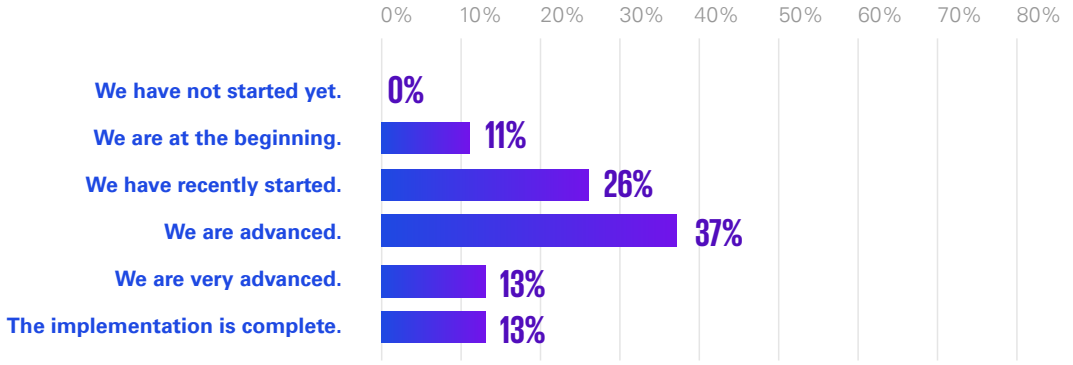


Fig. 26 - How far along are you with the implementation of NIS2?



On NIS2 implementation progress, our survey reveals a mixed picture. 37 percent of organizations report being advanced, while 26 percent have only recently started. Encouragingly, 13 percent claim completion, though in some cases this may reflect reliance on existing ISO27001 maturity rather than full NIS2 readiness - a position that could be challenged in audits.

Still, 37 percent remain at the early stages, highlighting a divide between proactive movers and reactive laggards. Delays often stem from awaiting final Belgian guidance, limited resources, or competing priorities such as DORA.

Early movers will benefit from stronger resilience and smoother compliance, while late starters risk bottlenecks and regulatory pressure as deadlines approach.

When asked whether respondents will be able to meet the NIS2 deadline, a strong majority (73 percent) believe they are on track, 9 percent admit they are not, and 18 percent don't know. The optimism is encouraging but could be misleading if it rests on assumptions about ISO27001 equivalence or incomplete Cyber Fundamentals mapping. The "Don't know" group highlights a lack of structured monitoring and executive visibility. Organizations should implement readiness assessments and governance checkpoints to ensure confidence is based on evidence rather than perception.

It remains unclear how the first NIS2 audits and inspections will be conducted, and whether current implementation levels will meet the expectations of supervisory authorities. What is certain, however, is that NIS2 serves as a critical building block for strengthening risk management measures and sustainably improving organizational resilience. organizations should prepare beyond minimal compliance, as early audits may set the tone for supervisory expectations and define what "good practice" looks like in NIS2 implementation.

Challenges in NIS2 implementation

Our survey results show that organizations are aware of the importance of cybersecurity and have begun to prepare for the new requirements that regulation brings. Nevertheless, their self-assessment does not always go hand-in-hand with the actual progress of implementation and there is still a lot to do for companies. The official audits will be decisive for assessing the status. Domestic organizations may have to revise their security strategies again and increase their resources to comply with the changed requirements and new regulations as well as to better protect their systems from cyberattacks in the long term.

Resilience as a shared mission

The successful implementation of cyber regulation depends on the active participation of companies. Those organizations that see regulatory compliance as an opportunity and accept or actively demand the necessary support offers establish themselves as trustworthy partners and at the same time strengthen Belgium's digital sovereignty in the EU internal market.

What to take away from this chapter

01

Regulation as a response to systemic risk: The surge of new EU regulations such as DORA, the AI Act, the Cyber Resilience Act, and NIS2 is a direct response to escalating cyber threats and digital dependencies. Together, they aim to protect the European internal market, ensure digital trust, and drive long-term resilience across sectors.

02

NIS2 as the universal baseline: NIS2 is set to impact most Belgian organizations across various sectors, establishing mandatory risk management measures for network and information systems. While many organizations report progress, self-assessment often outpaces reality, and the first supervisory audits will be defining moments for interpreting compliance expectations.

03

Financial sector leading under DORA: With DORA being fully binding since January 17, 2025, the financial sector has been among the most proactive, with 30 percent of surveyed organizations already prioritizing it. DORA, as lex specialis, demonstrates how sector-specific regulation can drive early maturity and set benchmarks for other industries.

04

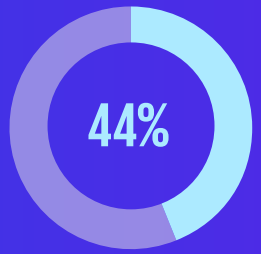
AI as a strategic and regulatory priority: The AI Act is emerging as a dual challenge and opportunity. With 42 percent of organizations expecting to be affected, organizations are beginning to acknowledge that AI is not only an innovation driver but also a regulated domain, requiring governance, risk management, and ethical safeguards.

07

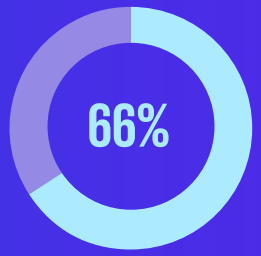
Organization and resources

How well are organizations organized in terms of cybersecurity and what resources they have at their disposal plays a significant role. Do Belgian organizations know which assets are worth protecting, which of their data are held by third parties, or how they will react in the event of a cyberattack? Can they measure their current cyber risk and plan for their financial losses?

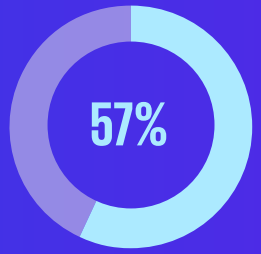
Their dedicated cybersecurity budget and how it is evolving are also essential. In addition to all these topics, the human factor is also decisive, as is the number of people who deal with cybersecurity in organizations.



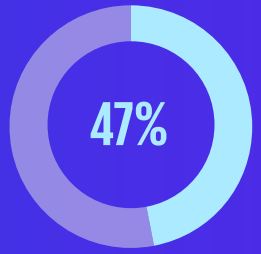
respondents need 4 to 6 months to recruit IT professionals for their company.



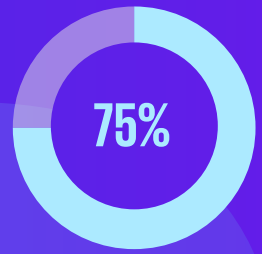
rather agree that they can measure their cybersecurity risk.



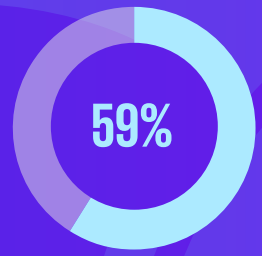
organizations' cybersecurity budgets have increased over the last twelve months.



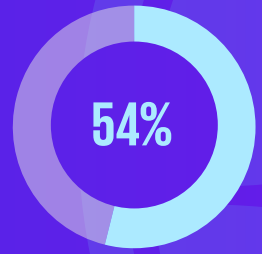
cannot estimate potential financial damage from cyberattacks over the next year.



have a complete overview of their assets worth protecting.



know how they will react in the event of a major cyberattack.

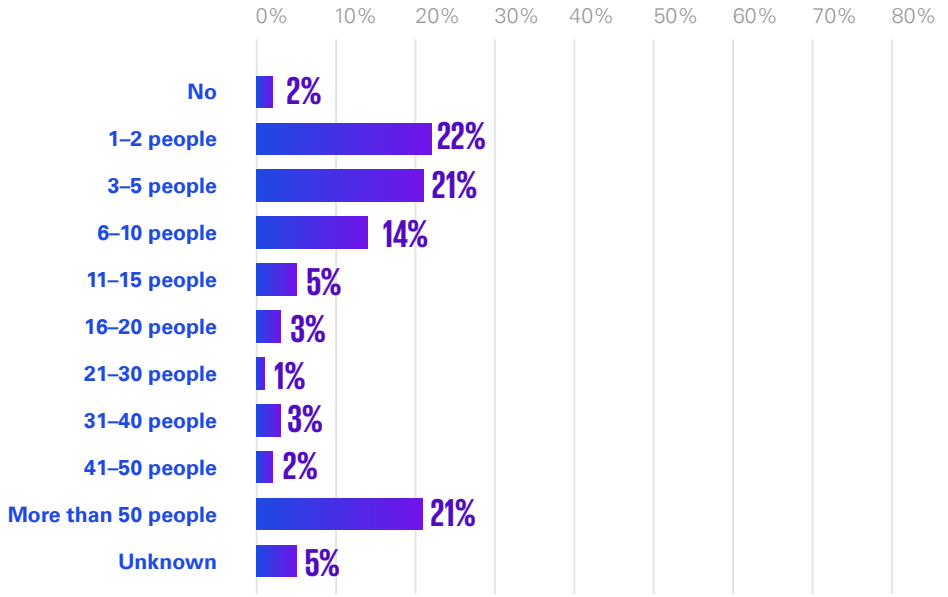


say that regulatory requirements are a driver for budget change.

Organization and resources

Employees in cybersecurity departments

Fig. 27 - How many people at your organization are involved in cybersecurity?



The survey highlights a clear two-speed reality in the organization of cybersecurity teams across Belgian enterprises. While 21 percent of respondents report more than 50 dedicated cybersecurity professionals, another half operate with only 1–5 specialists. A very small minority even indicated having no dedicated security staff at all. Team size correlates strongly with company size: smaller organizations - particularly those with fewer than 100 employees - almost exclusively rely on a handful of cybersecurity specialists, often combining security responsibilities with broader IT functions. Mid-sized organizations cluster around 3–15 cybersecurity staff, while very large enterprises with more than 20,000 employees typically sustain teams of 50 or more. This pattern underscores how scale and regulatory obligations drive investment, with financial services and telecoms often leading the way, while SMEs and less regulated sectors remain constrained by limited internal capacity.

Industry further amplifies these differences. Financial services, technology, media, and telecommunications stand out with the largest and most mature teams, often exceeding 50 employees. These sectors are strongly influenced by regulatory frameworks such as NIS2 and DORA, which impose strict governance and resourcing requirements. The public sector presents a more fragmented picture: some central and regional authorities maintain sizeable security departments, while smaller agencies operate with only a handful of staff. In contrast, sectors such as construction, healthcare, and professional services typically report very small teams, usually below 10 employees. These industries are undergoing rapid digitalization, yet cybersecurity investment has not kept pace with their expanding risk exposure.

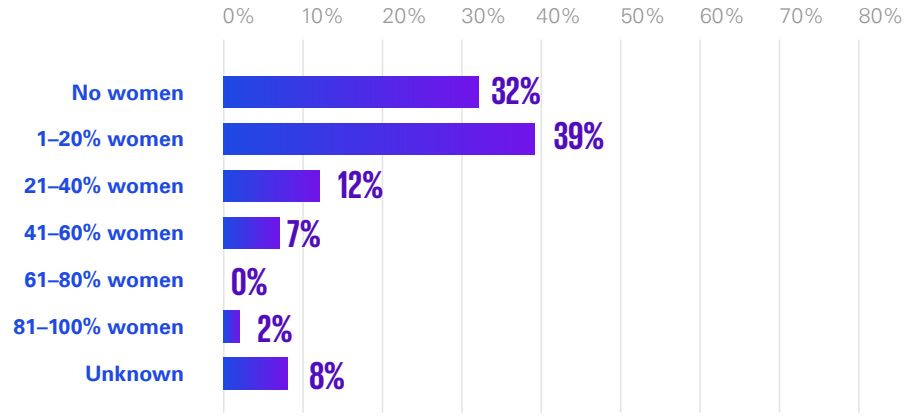
Room for improvement in the proportion of women

Gender diversity remains a challenge in cybersecurity, with 39% of organizations reporting women make up only 1–20% of their workforce, and a third having no women in these roles. More balanced teams are uncommon and found mainly in larger organizations. Progress toward inclusivity is slow due to ongoing structural barriers like limited role models and recruitment biases.

Taken together, the findings point to a coherent pattern: larger organizations in regulated industries are building substantial cybersecurity teams with somewhat greater diversity and more structured recruitment processes, while smaller and mid-sized organizations remain constrained by limited resources, long hiring cycles, and greater dependence on external providers. Across all

sectors, however, Belgium faces the same fundamental issues of a scarce talent pool, slow progress on inclusivity, and the need for coordinated investment in skills and training. Addressing these challenges requires a dual approach: individual organizations must strengthen internal pipelines through upskilling, graduate programs, and inclusive recruitment practices, while sectoral and national initiatives should foster collaboration, shared services, and education partnerships to expand the available pool of expertise and ensure resilience across the entire economy.

Fig. 28 - Of the people who deal with cybersecurity within your organization, what percentage are women?



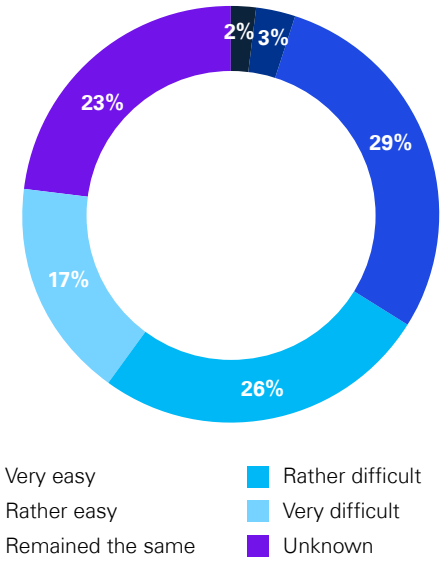
"These numbers reveal a harsh reality: with 4,000 open vacancies and 44% of organizations needing 4 to 6 months to recruit cybersecurity talent, we're losing precious time. But the real problem runs deeper. Only 32% of organizations have women in their cyber teams, while it's precisely human skills - the ability to connect technical and strategic people, bring teams together in synergy - that make the difference between organizations that can measure their cyber risks and the 35% that cannot. The sector needs to reposition cybersecurity: not as ‚hackers in hoodies', but as professionals working on safer critical societal challenges like climate, healthcare, and mobility. Every woman in cyber is an ambassador who can shift this perception. The challenge? Women are hired less than men with identical qualifications, forcing them to prove their worth through more certifications. We cannot afford to waste this talent.

The question is not whether we need diversity in cyber - the question is how much risk we're still willing to accept by ignoring it."

Saskia Van Uffelen
Manager Agoria Future Workforce

Recruitment of IT experts

Fig. 29 - Compared to the previous year: How difficult or easy was it to recruit IT experts in the last twelve months?



Cybersecurity requires expert knowledge to be able to react in a targeted manner. In this study, 43 percent of the organizations surveyed stated that it is still rather difficult to very difficult to recruit cybersecurity experts compared to the previous year. Less than a third (29 percent) of the organizations surveyed believe that the situation has not changed compared to last year, which was already difficult in principle, and that it remains a challenge to hire suitable specialists.

Time to hire suitable IT experts

When asked about the time required to hire a suitable IT expert, respondents indicated that they needed an average of 4 to 6 months to recruit IT experts for their company (44 percent). One in five organizations needed between 7 and 12 months (19 percent) to hire the appropriate experts. These results demonstrate the difficulties that organizations face when trying to hire the appropriate experts that are required to design and implement a cybersecurity strategy.

Recruitment and retention challenges affect organizations across all sizes and sectors, but in different ways. Smaller organizations often face the greatest difficulties, with many reporting that recruitment takes up to 12 months or remains unpredictable. Their limited visibility and lower salary competitiveness make it hard to attract qualified candidates. Mid-sized organizations show somewhat more stability, generally reporting hiring cycles of three to six months, while large organizations typically fall in the four-to-six-month range. Yet even the largest enterprises, despite stronger employer branding and higher budgets, struggle with long internal processes and high turnover. This convergence around a four-to-six month hiring cycle illustrates the depth of the talent shortage: attracting, hiring, and retaining cybersecurity professionals is a structural challenge for the entire Belgian market.

Training initiatives

When asked where the respondents would like to see initiatives when they think of cybersecurity training, the responses converge on three big priorities: embed cybersecurity in education early, provide practical and affordable training for SMEs and employees, and strengthen collective/governmental initiatives (awareness campaigns, free training, regulation). A balanced training ecosystem should combine mass awareness, role-specific professional skills, and advanced topics like AI and NIS2.

The following main insights emerged from our survey:

01

Cybersecurity training demand is universal: people want initiatives at all levels - from schools and citizens to SMEs, large enterprises, and regulators.

02

Balance awareness with depth: there's a tension between "general awareness for everyone" and "advanced skills for professionals." Both are necessary, but audiences need differentiation.

03

SMEs are a weak spot: repeated mentions show they lack resources and need tailored, practical, affordable support.

04

Use modern delivery methods: suggestions like media, social networks, and incident-based simulations show a desire for more engaging, realistic formats.

05

Government is expected to step up: both as a regulator and as a facilitator (free training, collective campaigns).

Detailed analysis of the results

Early education

Many answers stressed teaching cybersecurity in schools (mid-school, high school, university) and making curricula more practical and up-to-date.

Workplace training and awareness

Strong emphasis on company initiatives: awareness programs, simulations, on-the-job training, board-to-employee coverage.

SME-focused training

Several responses highlighted the struggles of small and micro-enterprises: need for simple, practical, affordable training that is adapted to limited budgets.

Embedding cybersecurity in every generation

To embed cybersecurity in every generation, comprehensive education and training are desired for the organizations surveyed. Ensuring cybersecurity reaches every generation requires a layered approach:

- **Schools & youth:** integrate practical education early.
- **Adults & workforce:** continuous, role-specific training and engaging simulations.
- **Seniors & vulnerable groups:** targeted protection and campaigns via trusted channels (banks, TV, government).
- **Government & society:** large-scale campaigns (like traffic safety), supported by modern media and influencers.

Ultimately, the challenge is not just about generations but about tailoring methods to different levels of digital literacy, life stages, and user fatigue.

The following insights were derived from the survey answers

Awareness is the core answer:

almost every respondent mentioned awareness, campaigns, or communication in some form. This shows consensus but also indicates fatigue with generic approaches - people want awareness to be fresh, engaging, and realistic.

Tailoring is critical:

different age groups, roles, and profiles require different formats (e.g., TikTok for youth, banks for seniors, hands-on cases for employees).

Education must start early and continue for life:

schools, universities, and re-skilling programs are essential to reach “every generation.”

Government has a legitimizing role:

national campaigns, Safeonweb materials, and collective approaches are trusted channels to reach the whole population.

Address the human factor barriers:

digital illiteracy, user fatigue, and abstract messaging reduce impact. Training must be simple, relevant, and emotionally engaging.

Practicality and realism matter:

simulations, real incidents, and relatable case studies can close the gap between “awareness” and actual secure behavior.

Cyberattack Response

To be able to address risks, it is necessary to establish proper response measures in the event of a cybersecurity incident. This means having a cyberattack plan ready, practicing them and training employees regularly.

59 percent of the organizations surveyed stated that they already know how they will react in the event of a cyberattack, especially through concrete guidelines is laudable; especially in the case of major security incidents, it is the first 70 minutes after the attack that are processed in such a way that there are no negative consequences for the company.18 percent of the organizations surveyed said that they do not yet know how they will react. There is definitely a need to catch up here. It is precisely these respondents, who have honestly disclosed their incompleteness in dealing with the topics, who should be made aware that the first reaction is often decisive.

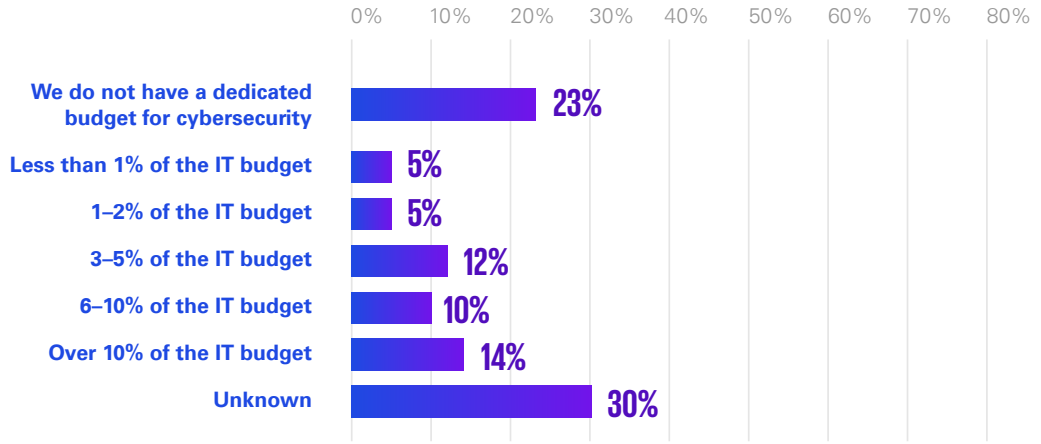
Necessary costs

Almost one in two organizations (45 percent) agree with the statement that the effort for cybersecurity is a necessary cost that can be better spent elsewhere. It is consistently surprising that cybersecurity is seen as a necessary cost factor, because it is precisely this that determines whether organizations continue to survive after digital attacks or not.

21 percent say that they do not see the effort for cybersecurity as a necessary cost that can be better spent elsewhere. In our digitally networked world, which is influenced by geopolitical changes and the shift of threats to the digital and information space, there is no alternative to dealing with cybersecurity.

Budget for cybersecurity

Fig. 30 - What is your organization's annual budget for implementing and maintaining your cybersecurity?



The survey highlights significant variation in how Belgian organizations allocate budgets to cybersecurity. While some organizations report dedicating over 10 percent of their IT budget to security, a large share of them still allocate only 1–5 percent, and a concerning number indicate that they have no dedicated cybersecurity budget at all. This unevenness reflects not only differences in company size but also sectoral maturity and regulatory pressure.

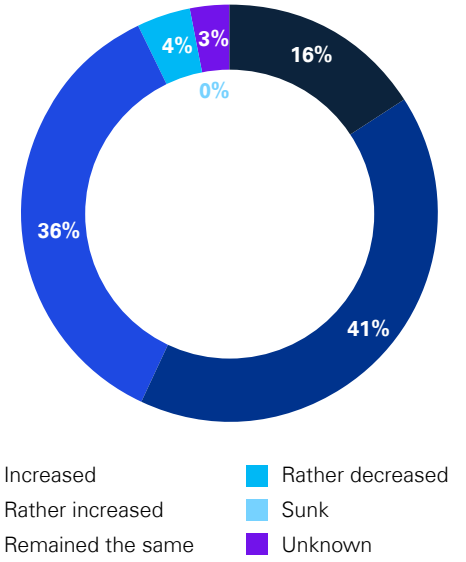
Smaller organizations are the most likely to report very low allocations or no formal budget, with security spending often absorbed into broader IT functions. Mid-sized organizations tend to cluster around 3–10 percent of IT budgets, showing growing awareness but still limited capacity. In contrast, large enterprises - particularly those in regulated industries - are far more likely to allocate more than 10 percent of IT budgets to cybersecurity, reflecting both their scale and heightened exposure.

Industry patterns follow a similar logic. Financial services, technology, media, and telecommunications stand out with the highest allocations, often exceeding 10 percent, driven by the dual pressure of heavy regulation and frequent targeting by cybercriminals. The public sector shows a mixed picture: some central and regional entities maintain substantial budgets, while others report minimal or no dedicated funding, reflecting fragmentation across government layers. Sectors such as construction, healthcare, and professional services, meanwhile, generally dedicate only small portions of their IT budgets to cybersecurity, despite their increasing reliance on digital technologies.

Change in budget compared to the previous year

When looking at how budgets evolve, most organizations report that spending has either increased or remained stable over the past year. The drivers behind these changes provide important context. The most frequently cited reason is new or changing threats (58 percent), confirming that many organizations adjust budgets in response to the evolving risk landscape rather than through long-term strategic planning. Regulatory requirements (56 percent) come a close second, reflecting the influence of NIS2, DORA, and sector-specific obligations in shaping investment. Encouragingly, corporate strategy (51 percent) is also a major driver, indicating that cybersecurity is increasingly seen as integral to digital transformation, resilience, and competitiveness. Secondary factors include economic necessity (20 percent), geopolitical conflicts (13 percent), and new market expansion (8 percent), each shaping investment decisions in specific organizational contexts.

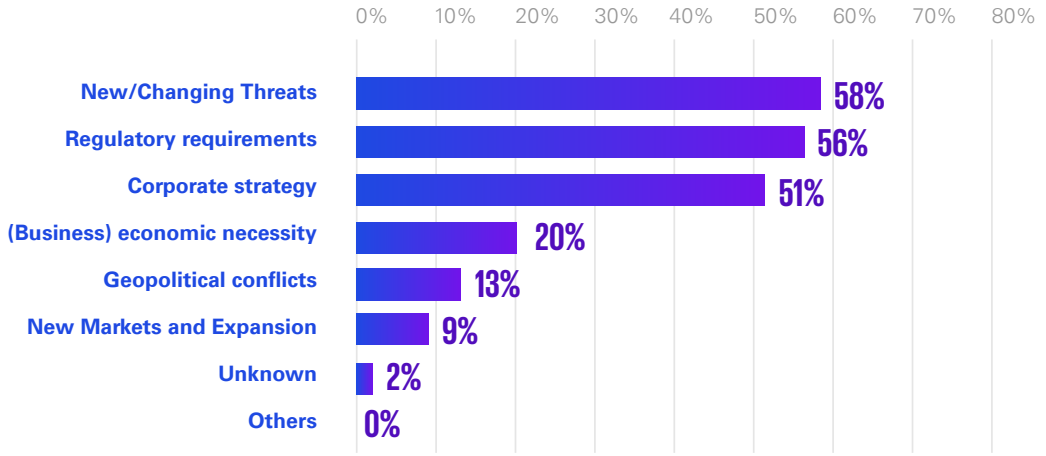
Fig. 31 - How has your organization's cybersecurity budget changed over the last twelve months?



Taken together, the findings paint a picture of progress, but also of imbalance. Large and regulated organizations are making significant, often strategic, investments in cybersecurity, while smaller players and less regulated industries lag behind, in some cases without a clear budget at all. The fact that most budget increases are driven by threats and compliance suggests a reactive posture across much of the economy. Moving forward, a shift towards proactive and risk-based budgeting will be critical to ensuring that investment is not only sufficient but also aligned with long-term business priorities and the evolving threat environment.

Trends in budget changes offer a more positive outlook. Across all sectors and company sizes, most organizations report that cybersecurity budgets have increased or remained stable over the past year, with relatively few indicating a decline. This suggests that cybersecurity is steadily consolidating its position as a fixed line item in IT and enterprise planning, though the absolute level of investment remains uneven.

Fig. 32 - What were the reasons for the change in the budget?



Measuring current cyber risk

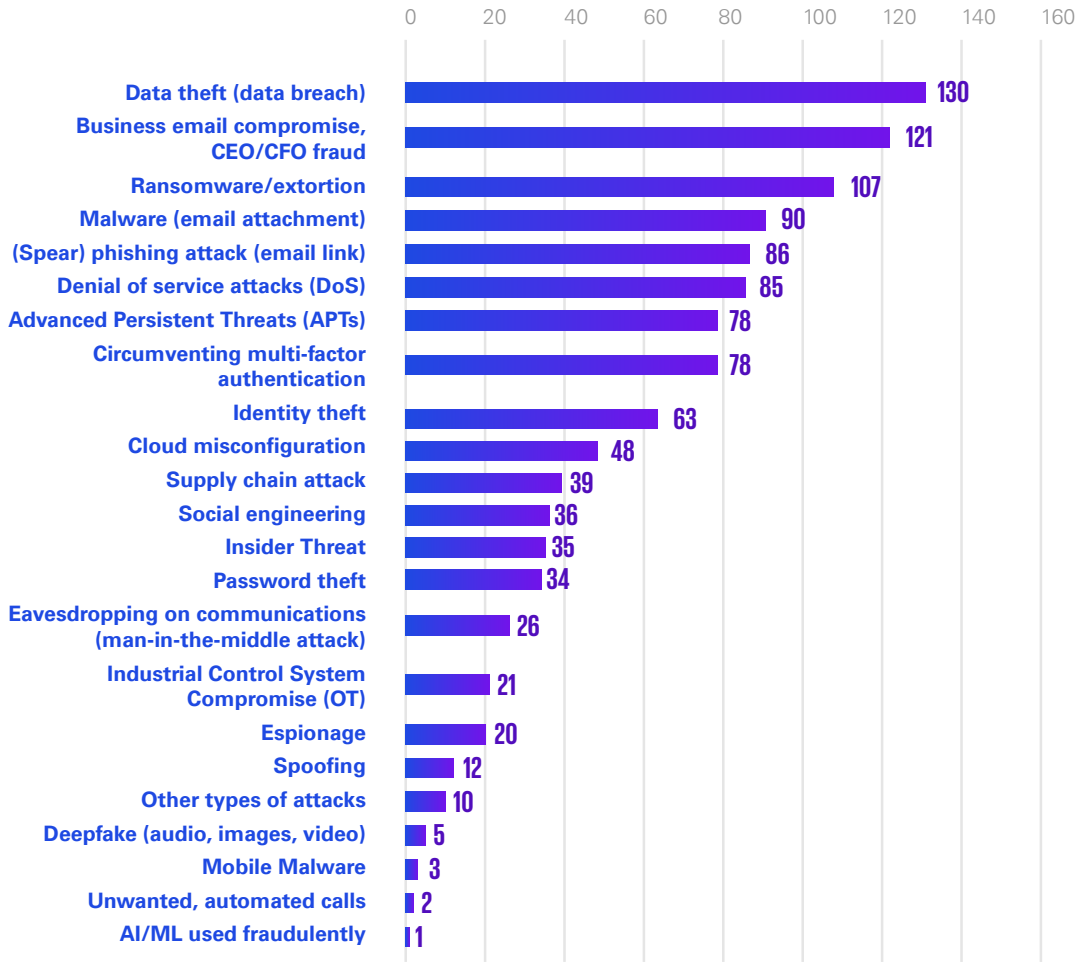
The survey results reveal that Belgian organizations are still in the early stages of cyber risk quantification. While half of respondents (50 percent) “rather agree” that they can measure cyber risk, only 16 percent feel confident enough to fully agree. Another 16 percent remain neutral, while 13 percent “rather disagree” and 3 percent outright “disagree” with the statement. A small fraction (3 percent) reported not knowing.

This distribution highlights that the majority of organizations acknowledge having some form of cyber risk measurement in place, but with limited maturity. The dominance of “rather agree” suggests that many rely on qualitative methods - such as risk registers, compliance audits, or maturity models - rather than quantitative, business-aligned approaches that link cyber risks directly to financial and operational outcomes.

The relatively high share of neutral and negative responses underscores a persistent gap: cyber risk is still difficult to measure in a consistent and comparable way, especially for organizations with smaller teams and fewer resources. This aligns with broader findings that many Belgian organizations are still reactive in their cyber investments, adjusting budgets and priorities in response to threats or regulatory demands rather than using structured risk quantification to guide strategy.

Overall, the findings suggest that while organizations are increasingly aware of the need to measure cyber risk, most are still working with immature frameworks. Progress will depend on adopting more advanced practices such as scenario analysis, financial quantification of risk, and integration into enterprise risk management, which can transform cyber risk measurement from a compliance exercise into a strategic business tool.

Fig. 33 - Cyber risks ranking for organizations



Top five types of attacks

The survey highlights a clear hierarchy of cyber risks as perceived by Belgian organizations. Data theft and data breaches stand out as the number one concern, far ahead of other categories. This reflects the high regulatory pressure under GDPR, the reputational damage associated with breaches, and the tangible financial consequences of lost or stolen data.

Business email compromise and CEO/CFO fraud is a growing threat where attackers impersonate executives or suppliers to trick staff into transferring funds or data. Increasingly supported by AI tools, these schemes highlight the need for stronger verification processes and technical safeguards beyond awareness training.

Close behind is ransomware and extortion, which continues to dominate the threat landscape. Its strong position underscores the persistence of this attack type, which combines technical disruption with direct financial and operational impact.

Malware and Phishing and spear-phishing (email-based) follows as the third most cited risk, demonstrating that human-targeted attacks remain one of the most common entry points for cyber incidents.

Denial-of-Service (DoS) attacks remains a high risk to disrupt business operations, often used for extortion or as a diversion for other intrusions. Their increasing scale and availability as a service underline the need for resilient network architectures and rapid response capabilities.

Interestingly, Advanced Persistent Threats (APTs) appear high on the list, indicating that organizations are increasingly aware of long-term, stealthy intrusions, often linked to state-sponsored actors or highly organized criminal groups. This shows a maturing awareness that goes beyond “visible” attacks.

Identity theft, supply chain attacks, and insider threats also appear in the top tier. These highlight growing concerns around ecosystem vulnerabilities and the human factor within organizations. The prominence of supply chain attacks is notable, reflecting the increasing interconnectivity of organizations and reliance on third-party vendors.

Further down the ranking, risks such as eavesdropping on communications, password theft, and social engineering still feature but with less intensity. Emerging risks - including deepfakes and fraudulent use of AI/ML - are mentioned, though currently at a much lower level, suggesting they are recognized but not yet seen as immediate top priorities.

Overall, the results show that Belgian organizations remain primarily focused on risks with direct, immediate, and monetizable consequences (data breaches, ransomware, phishing). At the same time, there is growing awareness of systemic and advanced risks such as APTs and supply chain compromise. However, emerging threats linked to AI manipulation or deepfakes are not yet high on the agenda, even though they are rapidly gaining relevance internationally.

Assessment of the probability of occurrence of cyber risks

When asked to assess the probability of cyber risks materializing, most Belgian organizations placed themselves in the middle of the spectrum. A majority (55 percent) rate the probability of cyber risks as average, while another 27 percent consider it rather high. Smaller shares rate the probability as low (8 percent) or high (8 percent), and only 1 percent indicated "unknown."

This distribution indicates that organizations see cyber risk as a persistent and significant challenge, but not necessarily as an existential threat. The dominance of the "average" response suggests a tendency to normalize risk, treating cyber threats as a constant background condition rather than an exceptional danger. The relatively strong share of "rather high" responses shows that a substantial portion of organizations - often those in regulated or highly digitalized sectors - perceive cyber risk as elevated, likely reflecting their higher exposure to attacks such as ransomware, phishing, and data breaches.

The very limited number of "high" responses suggests that few organizations perceive themselves to be at the highest levels of exposure. This may reflect either confidence in controls or, more critically, a lack of mature risk quantification: without robust financial or statistical modeling, many organizations default to "average" classifications rather than differentiating precisely across risk levels.

Taken together with the earlier findings on risk measurement maturity, the results confirm that Belgian organizations are largely relying on qualitative, perception-based assessments when rating cyber risk probabilities. This reinforces the need to evolve toward quantitative methods that express probability and impact in financial terms, enabling boards and executives to make more informed decisions on risk appetite and investment.

Looking to the future: estimating and planning financial losses

The survey reveals a significant gap between how Belgian organizations estimate the potential financial damage of future cyber incidents and how they plan for it.

When asked to estimate future financial damage, responses vary across a wide spectrum, with organizations spread from very small amounts to very large exposures. A small portion expect losses below EUR 10,000, while a meaningful minority foresee possible damages in the range of EUR 100,000 to EUR 1 million or more. Notably, 47 percent selected “unknown”, reflecting that nearly half of organizations are unable to put a concrete figure on potential losses.

In contrast, when asked about financial planning for future cyber damage, organizations appear even less prepared. More than half (54 percent) answered “unknown,” indicating that they do not actively plan financially (e.g., through reserves, cyber insurance, or contingency funds) for potential incidents. The remainder spread across categories, with most clustering in relatively modest ranges up to EUR 100,000. Very few organizations reported planning for damages above EUR 500,000, even though actual incidents - especially ransomware or large-scale breaches - can easily exceed these levels.

This discrepancy suggests that while many organizations have some intuitive sense of possible damage, few have embedded these figures into structured financial planning or risk management frameworks. In practice, most are relying on reactive measures rather than systematically preparing for high-impact scenarios.

The findings reinforce earlier observations on risk measurement maturity: Belgian organizations still largely operate with qualitative or perception-based approaches and struggle to translate cyber risk into financial terms. The high percentage of “unknown” responses - both in estimation and in planning - underlines a lack of quantitative tools and methodologies (e.g., FAIR, Monte Carlo simulations, loss exceedance curves) that could help decision-makers align cybersecurity budgets, insurance, and resilience investments with potential financial exposure.

In short, while awareness of cyber risk is high, the ability to translate this into concrete financial impact and preparedness remains limited. This leaves many organizations vulnerable to underestimating potential losses and underfunding their resilience measures.

Business as usual vs. Special challenge

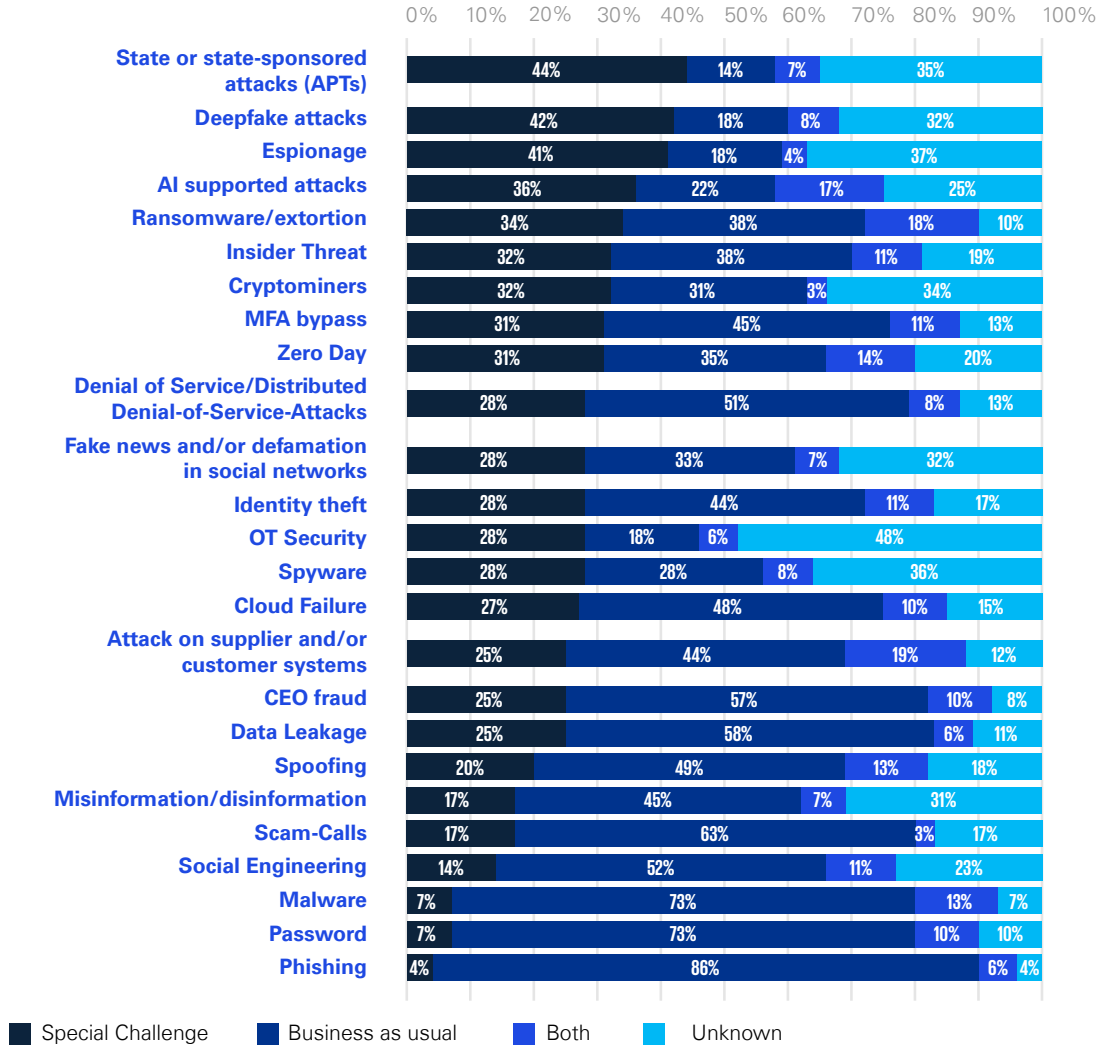
We also asked respondents to classify cyber risks as normal business as usual or as a particular challenge. New technologies, especially artificial intelligence, are becoming a particular challenge for companies. In first and second place, we find state or state-sponsored attacks (44 percent) and deep-fake attacks (42 percent). Related to the attack types, in fourth place we find related AI supported attacks (36 percent). This can be attributed to geopolitical changes and the rapid pace of technological development. Deepfakes use AI technologies to simulate security and trust. Access to these tools is becoming increasingly easy, and as a result, they represent an ever-growing problem.

Espionage ranks third among the top special challenges, cited by 41 percent of organizations. Its targeted, covert nature and focus on stealing sensitive information make it one of the most difficult threats to detect and counter.

Ransomware ranks fifth at 34 percent, yet it remains a major challenge for many organizations due to its diverse and often treacherous nature. Notably, at the same time, 38 percent of respondents state they are already able to handle ransomware as part of their day-to-day operations. In the area of special geopolitical trends, we clearly see the change in the above-mentioned types of attacks because it is precisely these types of attacks that come into focus in times of increasing interstate conflicts.

Let's now look at normal day-to-day business, i.e., attacks and threats that we are already very familiar and have already learned to deal with: Phishing is in first place (86 percent). Phishing attacks are often the gateway for perpetrators into companies. In second place are malware attacks, which is increasingly becoming a normal day-to-day business for companies. 73 percent state that they already have suitable means to be able to take a targeted response here. Third place is occupied by scam calls, which are (attempted) fraudulent extortion via telephony (63 percent).

Fig. 34 - Comparing business as usual cyber risks vs risks which require special attention.



What to take away from this chapter

01

Cybersecurity budgets are generally stable or increasing, but spending is still driven mainly by threats and compliance rather than long-term, risk-based strategy—leaving smaller and less regulated organizations at risk of falling behind.

02

Legislation requires that organizations must be able to qualify their risks. Larger organizations and major institutions also have to quantify their risks. Currently, however, risk assessment procedures are handled very superficially and do not yet have the depth needed to manage risks. Above all, the reference to the assets worthy of protection is often still missing here.

03

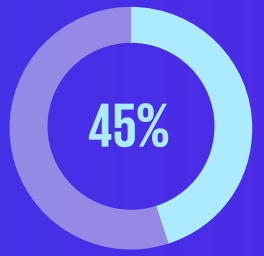
Those attacks that pose a particular challenge for organizations show us the changed geopolitical conditions. For it is precisely these types of attacks that are increasingly becoming the focus of attention in times of increasing interstate conflicts.

08

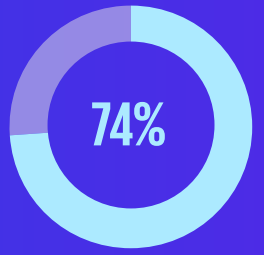
Outlook

In which direction will domestic organizations move in the future and what technological challenges do they face?

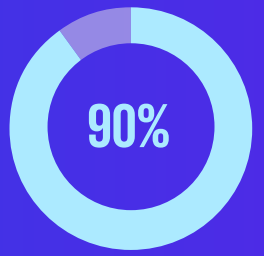
What are the top topics they plan to use to address cybersecurity in the next 12 months? The top five in 2025 show a clear picture.



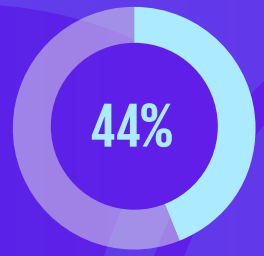
say that Belgium is not well prepared to respond to serious cyberattacks against critical infrastructure.



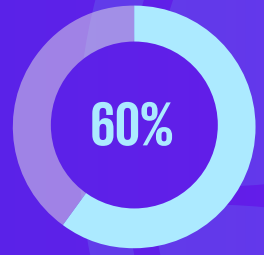
agree that there is little chance of identifying the perpetrators of attacks from abroad



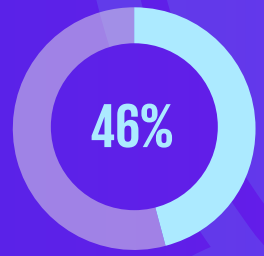
agree that there is a need for increased EU-wide cooperation on cybersecurity



agree that cyberattacks threaten their business existence.



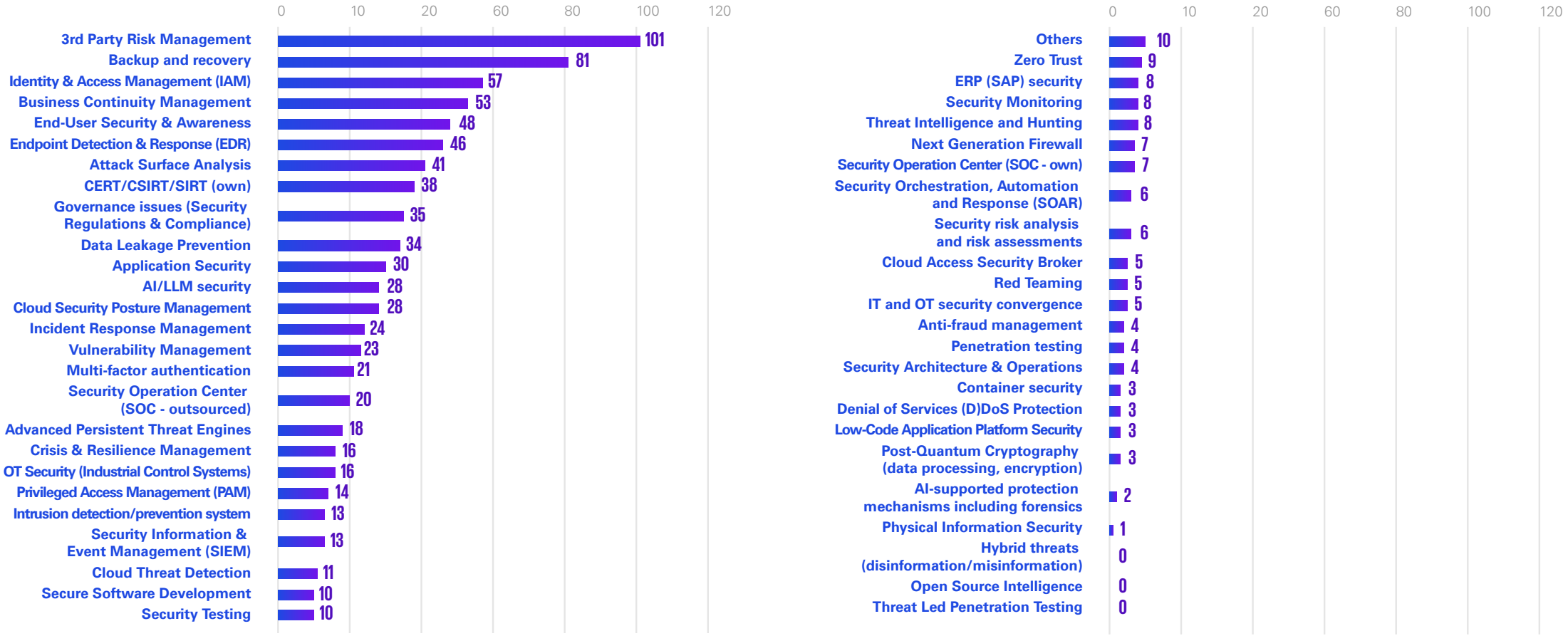
say that power authorities need to be expanded to solve cyberattacks.



would prefer to use security solutions from Belgian organizations.

Outlook

Fig. 36 - Technologies & Topics - Top 5



Technologies and topics – Top five

Analysis of the top five cybersecurity technologies and topics for 2025 shows a focus on pragmatic items that directly affect security posture and exposure. The survey results highlight Third-party Risk Management, Backup and Recovery, Identity & Access Management (IAM), Business Continuity Management (BCM), and End-User Security as the most critical focus areas. These domains are not only foundational to strengthening organizational resilience but also directly support compliance with cyber regulation (such as NIS2 and DORA). These trends reflect the changing threat landscape and highlight the strategic adjustments needed to meet the increasingly complex challenges in cybersecurity. The emphasis on these five areas reflects a balanced view of resilience: covering suppliers, technology, people, and governance. However, the simultaneous presence of Backup and Recovery and BCM points to a possible fragmentation between technical continuity solutions and organizational continuity planning and could undermine compliance with DORA and NIS2, which both require end-to-end operational resilience - not just technical recovery.

By far, the most mentioned topic is Third-party Risk Management and can really be seen as a key focus from a regulatory point of view and as source of resilience risk – one that increases with the dependency on technology providers to support key business operations. Maturing Third-party Risk Management frameworks ensure visibility of dependencies, early detection of supplier failures, and clear accountability in incident response.

DORA explicitly requires organizations to demonstrate that they can recover ICT services within tolerance levels, while NIS2 demands the ability to ensure availability, authenticity, integrity, and confidentiality of critical data and systems. This coincides with the second most mentioned topic: backup and recovery. Reliable data backup and tested recovery procedures are central to operational continuity and enhancing resilience. Furthermore, strong backup governance reduces downtime after cyber incidents such as ransomware and other operational crises.

Identity & Access Management is also highlighted as a focus area. Rightfully so, as is one of the most decisive enablers of cyber resilience. By ensuring that only the right individuals and systems gain access to critical resources, IAM directly reduces the risk of unauthorized access, privilege misuse, and lateral movement - attack techniques frequently seen in high-impact incidents such as ransomware or data exfiltration. The prioritization of IAM in the survey suggests recognition of its critical role, yet it also indicates a need for maturity improvements:

- Moving beyond baseline controls (password policies, MFA) toward integrated IAM governance and Privileged Access Management (PAM).
- Ensuring IAM is not siloed in IT but embedded into business continuity and crisis management planning.
- Linking IAM with third-party access controls, ensuring suppliers and external partners are subject to the same resilience standards.

Seeing Business Continuity Management in the top five takes the importance of this resilience one step further. On the one hand, regulations such as DORA and NIS2 require organizations to safeguard their business processes to ensure the resilience of critical institutions. On the other hand, there is simply no alternative: the reliable functioning of digital systems, infrastructure, and services is a fundamental prerequisite for organizational success. Business Continuity Management is therefore a crucial supporting pillar, ensuring that business processes can continue - even if only partially - in the face of security incidents.

The importance of End-User Security indicates that companies recognize that people are often the weakest link in the security chain. Phishing attacks and social engineering remain one of the most common methods for attackers to gain access to networks. Training to raise awareness among employees is therefore crucial to minimize these threats. The focus on end-user awareness could also be driven by the proliferation of hybrid workspaces, which are potentially more vulnerable to security risks.

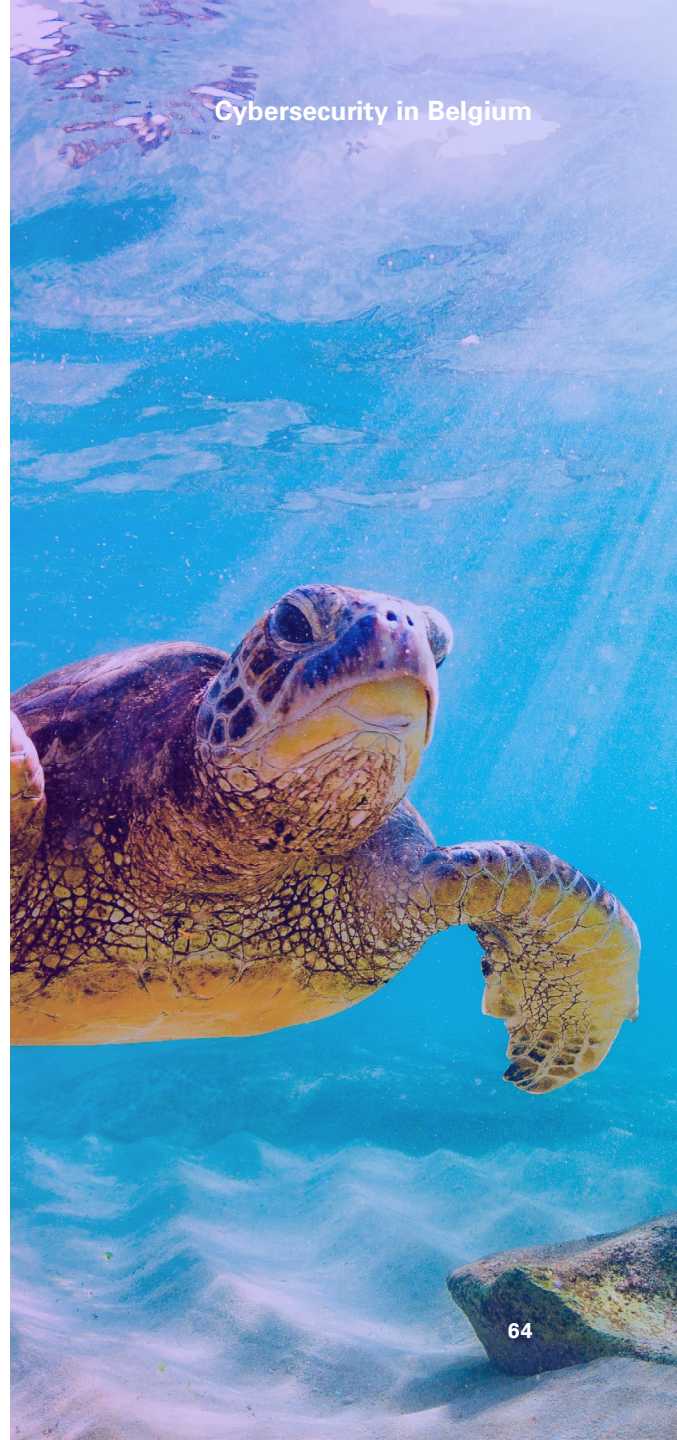
Organizations should view these top five not as isolated priorities, but as interdependent pillars of resilience. The strong attention on Business Continuity Management, next to more technical measures, signals a recognition that Business Continuity Management must be elevated and integrated with supplier oversight, IAM, and recovery practices to meet regulatory obligations and ensure true operational resilience.

Lack of resources

The survey results highlight several security measures that organizations consider necessary but are unable to implement due to resource constraints, including personnel, financial limitations, and time. These measures span various aspects of cybersecurity, reflecting the diverse challenges organizations face in addressing evolving threats.

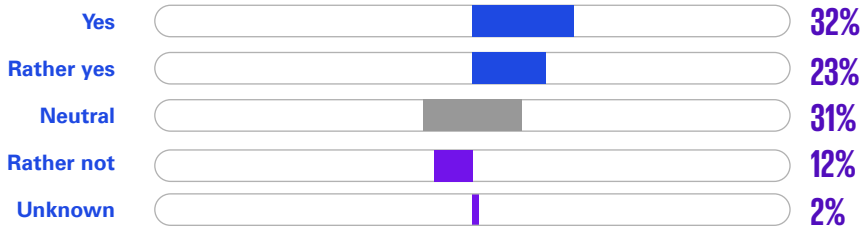
- Security testing and vulnerability management: Many organizations recognize the importance of regular security testing, such as penetration testing, vulnerability management, and structured attack simulations (e.g., threat-led penetration testing and red teaming). However, the lack of skilled personnel and financial resources often prevents these measures from being conducted effectively or at all. Additionally, maintaining up-to-date vulnerability management systems is seen as critical but resource intensive.
- Advanced security tools and technologies: The adoption of advanced tools, such as Zero Trust frameworks, Advanced Persistent Threat (APT) engines, and post-quantum cryptography solutions, is considered essential for staying ahead of sophisticated cyber threats. However, the high costs associated with acquiring and implementing these technologies, coupled with the need for specialized expertise, pose significant barriers.
- Internal crisis planning and training: Improving internal crisis planning for cyberattacks and investing in employee training are widely regarded as necessary measures. Organizations acknowledge the need to build a robust cybersecurity culture and enhance awareness among employees. However, the time and effort required to develop and maintain these initiatives are often cited as obstacles.
- Supply chain and third-party risk management: Organizations express concerns about the security risks posed by their supply chains and third-party vendors. While regular security assessments and emergency response plans for supply chain incidents are deemed critical, limited resources hinder their implementation. This gap leaves organizations vulnerable to attacks originating from less secure suppliers.
- Operational technology (OT) security: For organizations with OT environments, the integration of IT and OT security measures is a pressing need. Traditional IT security technologies are often incompatible with OT systems, leading to disruptions. Additionally, the lack of personnel with expertise in OT operational requirements exacerbates the challenge of securing these environments.
- External support and specialized expertise: Many organizations recognize the value of external support, such as hiring specialized IT consultants or outsourcing security operations (e.g., security operations centers). However, budgetary constraints and the difficulty of justifying these expenditures internally often prevent organizations from leveraging such resources.
- Modernization of security infrastructure: The replacement or modernization of outdated security tools - such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems - is seen as a priority. However, the financial and time investments required for these upgrades are often prohibitive.

In summary, while organizations are aware of the critical security measures needed to protect against cyber threats, resource limitations - whether in terms of personnel, budget, or time - remain a significant barrier to their implementation. Addressing these gaps will require strategic prioritization, increased investment, and potentially external support to ensure comprehensive cybersecurity readiness.



Emotional significance of cybersecurity due to geopolitical conflicts

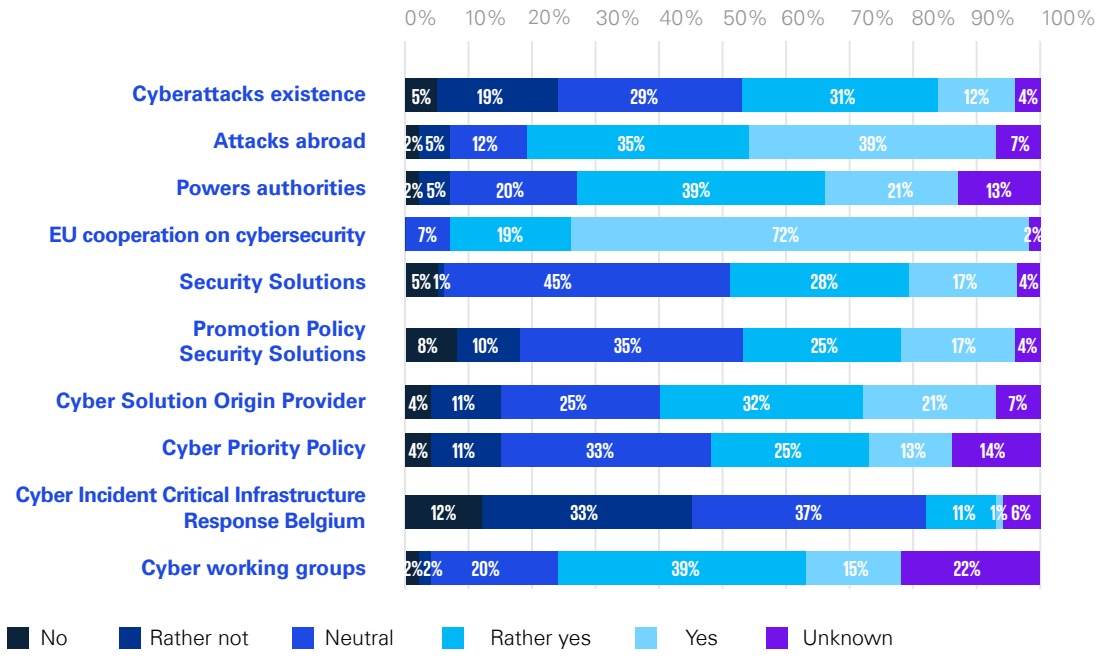
Fig. 38 - The emotional meaning of cybersecurity has changed in our organization due to the current geopolitical conflicts.



In a geopolitically tense environment, international conflicts also affect organizations and cause a change in the perception of cybersecurity. For half of the organizations surveyed (53 percent), the importance of cybersecurity has changed particularly significantly due to current geopolitical conflicts. Especially in international competition, threats in the cyber environment triggered by geopolitical conflicts know no borders.

Similarly, 55 percent agreed that the emotional meaning of cybersecurity has changed in their organization due to the current geopolitical conflicts. While the emotional significance is not directly quantified, the survey underscores the indirect emotional toll that geopolitical conflicts and their associated cyber risks can impose on organizations and their personnel. Geopolitical conflicts are linked to increased risks such as cyber espionage, disinformation campaigns, and financial losses due to cyberattacks, which can create a sense of urgency and stress within organizations. Additionally, the disruption of business operations and the potential loss of sensitive information or intellectual property due to cyberattacks tied to geopolitical tensions can lead to reputational damage and a loss of customer trust. These outcomes may evoke emotional responses such as anxiety, frustration, and a sense of vulnerability among employees and stakeholders.

Fig. 39 - Sentiment on the cybersecurity situation



Cyber policy: The emotional meaning of cybersecurity has changed in our organization due to the current geopolitical conflicts.

Cyberattacks existence: Cyberattacks threaten our business existence.

Attacks abroad: It is frustrating that when attacks come from abroad, there is little chance of identifying the perpetrators.

Powers authorities: In order to solve cyberattacks, the (technical) possibilities and powers (e.g., state Trojans) need to be expanded.

EU cooperation on cybersecurity: There is a need for increased EU-wide cooperation on cybersecurity.

Security solutions: I would prefer to use security solutions from Belgian organizations.

Promotion policy security solutions: Domestic cybersecurity companies should be specifically supported by politicians.

Cyber solution origin provider: We pay particular attention to the country of origin of the provider when procuring cybersecurity solutions.

Cyber priority policy: In international comparison, domestic politics neglects the issue of cybersecurity.

Cyber Incident Critical Infrastructure Response Belgium: I am confident that Belgium is well prepared to respond to serious cyberattacks against critical infrastructure.

Cyber working groups: Working groups, such as the Cyber Security Coalition, promote active dialogue between public administration and companies.

Cyberattacks as a threat to business existence

A significant concern among respondents is the existential threat posed by cyberattacks. We see that 44 percent of those surveyed recognize the existential dimension of cyberattacks - they believe that cyberattacks threaten their business existence. This once again illustrates the increasing professionalization of the attackers. Foresight, innovation, and determination are shaping the cybersecurity of the future. Meanwhile, 24 percent see no impact on their entrepreneurial existence. Smaller organizations in particular underestimate their vulnerability here. Only 4 percent of those surveyed are unsure whether cyberattacks threaten their business existence. This means that the topic is now anchored in almost all companies' awareness and risk management competence. The figures underline that awareness of the importance of cyberattacks is becoming increasingly important for organizations in their risk assessment.

Lack of identifiability of foreign attackers

The high level of agreement (74 percent) of those surveyed who find it frustrating that there is little chance of identifying the perpetrators of attacks from abroad underscores a core problem of modern cybersecurity: despite advances in AI-supported threat hunting, the attribution of cyberattacks is rarely successful. There is a substantial frustration among domestic companies. Reasons for this are in particular the limited access to global TOR networks, the concealment of origin by proxy servers in third countries or the use of known attack tools.

Expansion of the investigative powers of the authorities

Around 60 percent of the organizations surveyed believe that more government surveillance is necessary. Measures in this regard could include a concrete expansion of government surveillance or the investigative powers of national bodies. It is interesting to note that those who approve feel that there is no need for an expansion of powers.

EU-wide cooperation on cybersecurity

Beyond technical measures, effective information sharing among EU member states is crucial for cybersecurity. With 90 percent of respondents supporting more EU-wide cooperation, it's clear that unilateral national efforts are less effective against transnational threats like ransomware-as-a-service or state-sponsored APT groups. This perspective is also reflected in support for the EU Cyber Resilience Act. The low rejection rate of 7 percent is a clear signal: even more EU-skeptical organizations are in favor of common cybersecurity standards.

Corresponding steps have already been taken, especially in the area of regulation to improve cybersecurity. However, there is a need for improved exchange and faster flow of information, especially for organizations and for affected authorities that are responsible for critical infrastructure, for example. This can only happen if the data is exchanged quickly between the data themselves in this area of tension. NIS2 provides for appropriate committees for Europe-wide crisis management, although crisis management in itself can only be the last stage of escalation.

Preference for Belgian security solutions

In addition to state monitoring of communications involving cybercrime, it is also important for organizations to monitor their own networks and protect their infrastructure. There is currently a significant reliance on manufacturers outside the European Union. Reducing this dependence is considered necessary to increase technological sovereignty in cybersecurity measures and solutions. 46 percent of organizations would prefer to use security solutions from Belgian companies.

A call has been made to develop a market for Belgian security solutions, supported by targeted initiatives. Enhancing self-sufficiency is seen as essential for ensuring technological sovereignty and protecting critical facilities, independent of international providers. While it is not realistic to exclusively use Belgian solutions due to global interdependencies, ongoing changes in the geopolitical landscape present an opportunity to address this issue and introduce new measures and strategies.

Funding from politics

The role model function is best fulfilled when organizations receive targeted support from decision-makers, policymakers, and relevant stakeholders. Such support can take various forms. Notably, 44 percent agree that domestic cybersecurity organizations should receive specific promotion from policymakers, indicating a clear preference for government backing of local providers. Cybersecurity is widely regarded as a vital strategic sector, with organizations expressing expectations for funding in areas such as post-quantum cryptography, AI-driven attack detection, and talent development initiatives to address the ongoing shortage of skilled professionals.

Country of origin as a procurement criterion

The procurement of cybersecurity solutions requires a certain connection with the respective economic area and state. On the other hand, there are technological dependencies that go hand-in-hand with the purchase of various security solutions. This also creates risks if, for example, third-country vendors provide security solutions with additional features that no one is aware of (think surveillance, for example). 53 percent of the organizations surveyed already pay particular attention to the country of origin of their providers when they procure cybersecurity solutions. This once again underlines the growing importance of geopolitical risk assessment in supply chain security. Preference is given to domestic or EU-based providers to minimize dependencies on countries with controversial surveillance laws.

Confidence in Belgium's crisis resilience

This perception is a logical consequence of the fact that the problem of cybersecurity for organizations does not always seem to fit in between public administration and companies.

We are facing a crisis of confidence in Belgium's cyber defense: 45 percent of all organizations surveyed are not confident that the government is prepared to respond to serious cyber-attacks against critical infrastructure. Only 12 percent have (very) confident that sufficient protection is anchored here.

It is therefore important to establish trust among the population. The figures are a clear call to improve the cybersecurity of our critical infrastructure.

Cybersecurity Working Groups

Important aspects can be brought to light when protection is reported as part of working group events that raises awareness for cybersecurity information, politics, or organizations. For example, 54 percent of respondents see the measures of such groups, such as events organized by the CCB and the Cyber Security Coalition, promote active dialogue between public administration and companies.

What to take away from this chapter

01

The technology priorities of organizations are focused on pragmatic solutions to real world threats targeting cloud solutions or ransomware disruption. Resilience, alongside limiting the probability and impact of these cyber incidents is a clear priority, alongside other drivers like regulation and assurance.

02

Especially in international competition, threats in the cyber environment triggered by geopolitical conflicts know no borders. Half of the organizations surveyed perceive cyber threats more emotionally in 2025 than in previous years.

03

There is currently a very high level of dependence on manufacturers outside the European Union. It is precisely this dependence that needs to be curbed in order to regain technological sovereignty in the field of cybersecurity measures and solutions. In times of geopolitical changes and a shift in values, there is now an opportunity to pick up on this momentum and set an example with our own measures and initiatives.

09

Survey methodology

The issue of the annual KPMG & Cyber Security Coalition study "Cybersecurity in Belgium" examines how organizations in Belgium are responding to the growing threats posed by cybercrime and what security measures they are taking.

Survey methodology

Overview

In the period April-June 2025, KPMG conducted a survey of 266 Belgian respondents. The respondents came from small, medium-sized, and large companies in various sectors, including automotive, banking, construction, education, chemicals, services, energy, healthcare, real estate, industry, consumer goods, media, public sector, technology, telecommunications, tourism, and insurance.

Analysis

Each participant received an online questionnaire including a maximum of 177 questions, tailored to their role in the company. In addition to the quantitative questions, which were based on a Likert scale, qualitative aspects were also accounted for, to give respondents the opportunity to share additional impressions and comments. The evaluation distinguished between the internal view (experts, division heads, CSOs, etc.) and the external view (board members, owners, supervisory boards). A team of KPMG experts from the field of cybersecurity consulting analyzed the results.

Fig. 40 - What is your role in the organization?

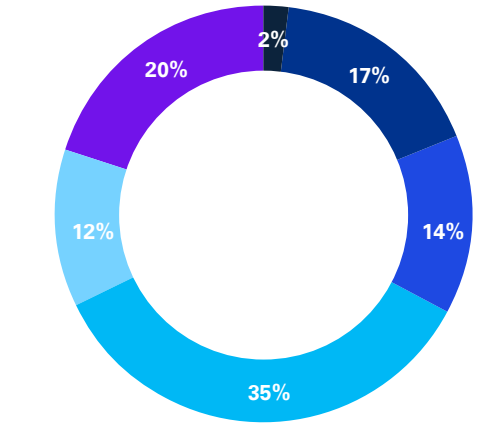


Fig. 41 - Gender

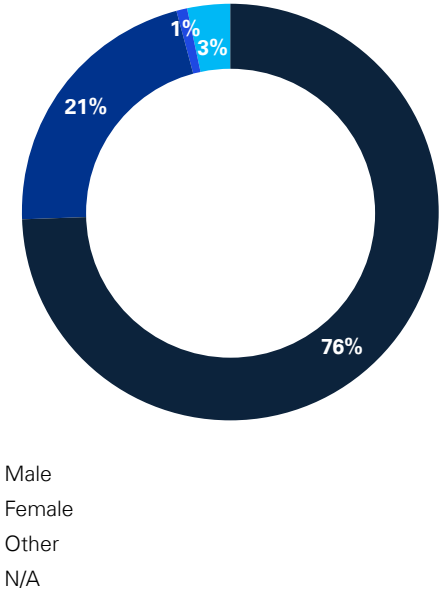


Fig. 42 - In which industry does your organization primarily operate?

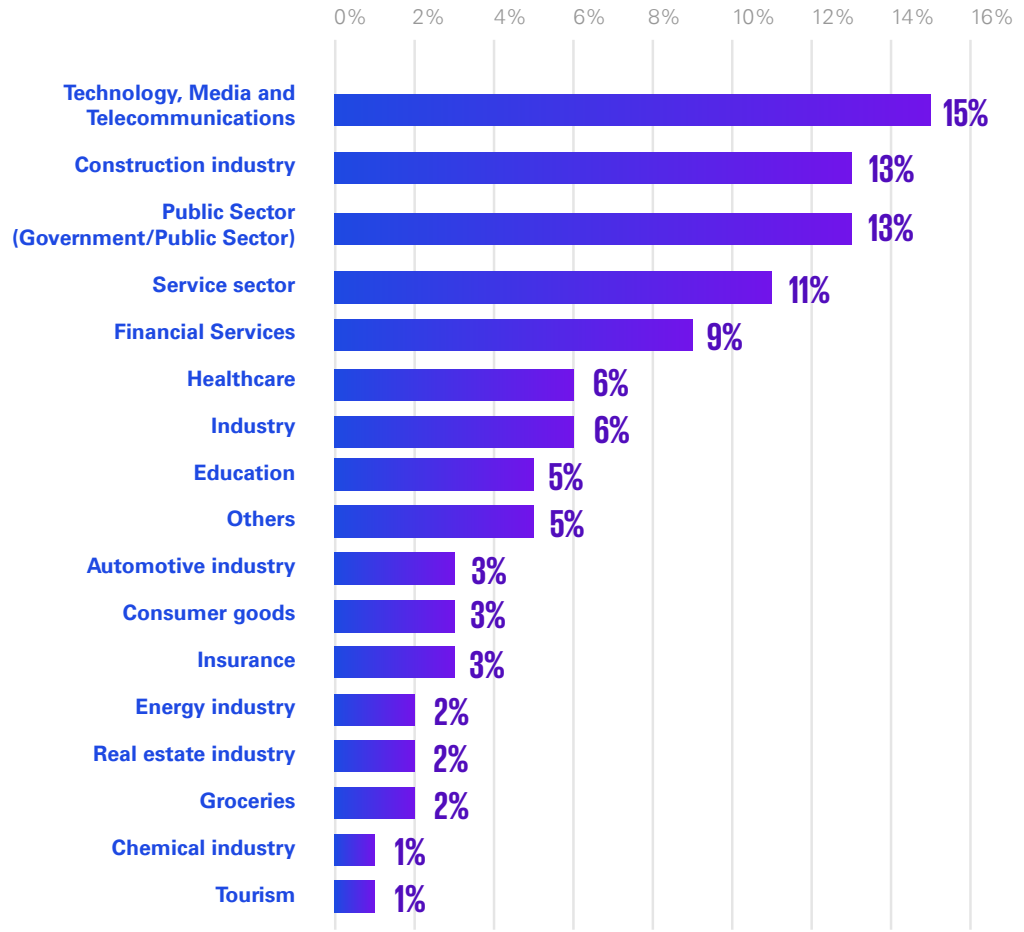


Fig. 43 - In which region does your organization have its Belgian headquarters?

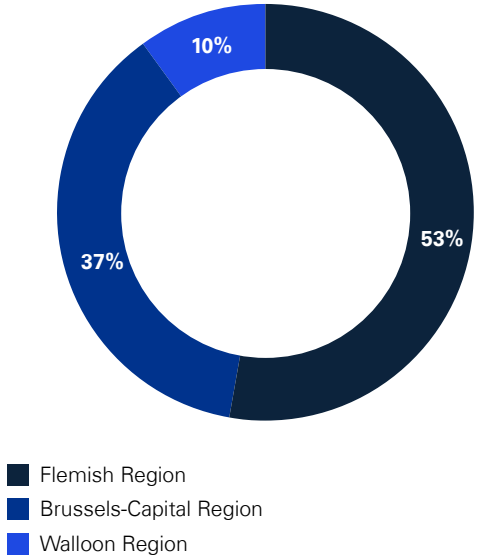


Fig. 44 - How many employees are employed in your organization?

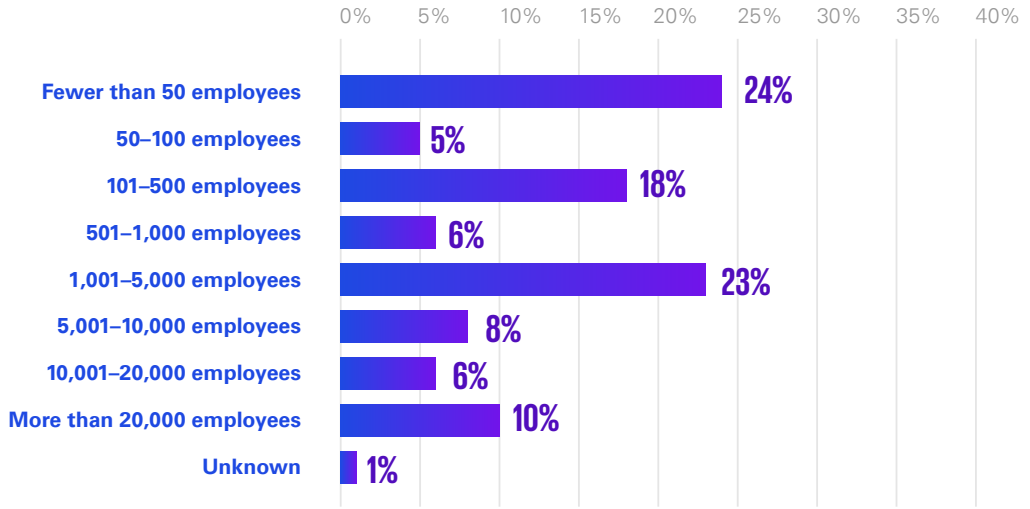
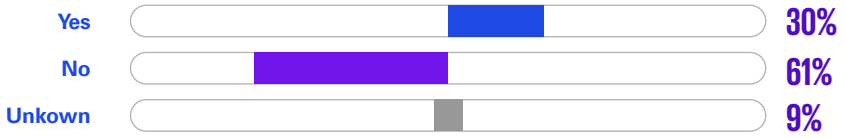


Fig. 45 - The emotional meaning of cybersecurity has changed in our organization due to the current geopolitical conflicts.



CYBER SECURITY COALITION.be

.AGORIA

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