HarfangLab

STATE OF CYBERSECURITY REPORT:

CYBERSECURITY IN THE BOARDROOM

Leadership, accountability and business resilience in the age of AI and geopolitical uncertainty.

2026

KEY FINDINGS

01

CYBER RISK HAS BECOME THE TOP BUSINESS CONTINUITY THREAT

European business leaders rank cyberattacks as the single biggest threat to business continuity and operations, ahead of geopolitical instability, skills shortages and AI-related risks.

02

REVENUE IMPACT HAPPENS IN HOURS, BUT RECOVERY TAKES DAYS

Almost half (48%) of businesses say a cyber incident would affect revenue within the same business day, while organisations estimate it would take an average of 4.32 days to return to normal operations.

03

CYBERSECURITY ONLY BECOMES A CEO PRIORITY WHEN REVENUE IS AT RISK

Responsibility for cybersecurity remains fragmented across CEOs, CIOs and CISOs. But where revenue would be affected within hours, businesses are twice as likely to make cybersecurity a CEO responsibility, rising from 23% overall to 46% overall.

04

LESS THAN ONE IN FIVE (18%) BUSINESSES PRIORITISE BUSINESS CONTINUITY AS THEIR PRIMARY CYBER STRATEGY

Despite cyberattacks being the top continuity threat, fewer than one in five organisations say their cybersecurity strategy is primarily focused on business continuity and rapid recovery. Most still prioritise prevention, compliance or tooling.

05

AI INVESTMENT IS GROWING, BUT GOVERNANCE IS STILL CATCHING UP

Businesses are prioritising AI investment for growth-oriented use cases such as productivity, innovation and customer experience. However, less than half require a security review before deploying AI tools, only 44% have clear rules on what data can be entered into AI systems, and just 40% have formal AI policies in place.

INTRODUCTION:
CYBER RISK HAS BECOME A BUSINESS CONTINUITY ISSUE

Business continuity is becoming increasingly difficult to manage as more factors come into play.

As developing, maintaining, or relaunching an organisation's activities is the priority, risk assessment should include all factors that can either affect or improve business health. Cybersecurity is more than ever part of it.

Organisations are no longer dealing with isolated risks. Geopolitical instability, growing regulatory obligations, rapid AI adoption and increasing dependence on a small number of technology providers are creating a more complex and interconnected operating environment. As a result, business continuity is no longer shaped solely by threats inside the organisation, but also by decisions made across supply chains, technology ecosystems and international markets.

Within that broader landscape, cybersecurity has become one of the most significant concerns facing business leaders in Europe. A cyber incident can disrupt operations, affect revenue and damage reputation within hours, making it a critical business continuity issue. These challenges and the potential impact of cyberattacks extend well beyond the remit of IT teams, which is why this research focuses on CEOs and senior decision-makers at large businesses across the region.

As cybersecurity becomes more closely linked to business continuity, leadership teams are taking greater responsibility for decisions that affect resilience, risk and organisational preparedness. Understanding how business leaders view these challenges is therefore just as important as understanding the threats themselves.

Business leaders recognise the threats facing their organisations and understand the potential impact on operations. The difference lies in how organisations are responding. Across Europe, responsibility remains fragmented, confidence often exceeds readiness, and approaches to resilience, regulation, dependency and AI vary significantly between organisations.

This report explores what those differences reveal about cyber resilience in Europe and what they mean for business continuity in the years ahead. In a world riddled with risks, cybersecurity determines competitiveness in the market. This report was conceived to help you rethink your risk management and key strategic priorities to thrive in this new reality.

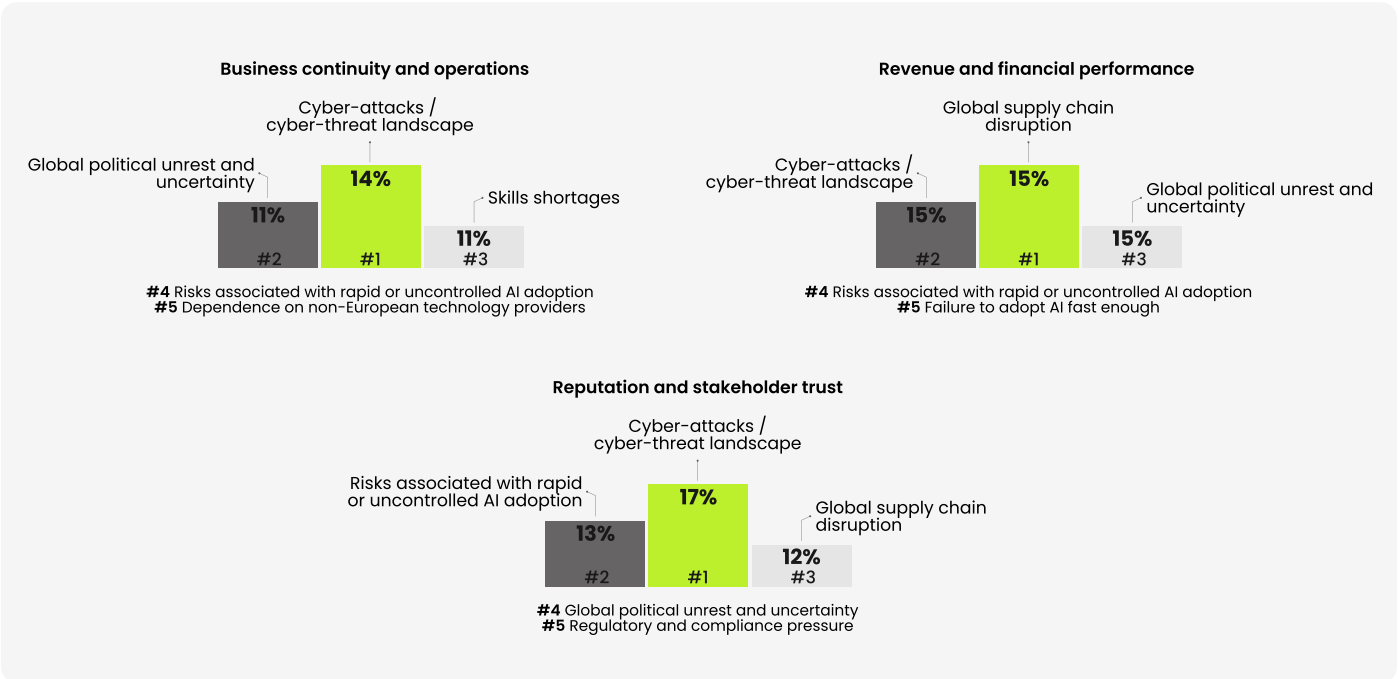
CHAPTER 1:
CYBER RISK DEFINES BUSINESS CONTINUITY

Across Europe, business leaders are facing a more connected and unpredictable risk landscape. Few threats can now be tackled in isolation. Instead, organisations must mitigate a range of interconnected issues, from cyberattacks and geopolitical unrest to supply chain disruption and concerns around digital sovereignty.

Businesses aren't alone in recognising this shift. The perceived threat in Europe has prompted the European Union to devise a new Preparedness Union Strategy to help member states anticipate, prevent and respond to potential crises. The strategy recognises that modern threats cannot be treated separately. Instead, organisations and governments must take a unified approach to resilience and crisis management.

So, what is keeping leaders awake at night? Cyber risk stands out as the most immediate concern. When asked about the biggest risks to business continuity and operations, European business leaders ranked cyberattacks as the single biggest threat, ahead of geopolitical instability and skills shortages. Geopolitical unrest remains a major concern for business leaders across Europe, with 31% saying they are significantly or very significantly worried about the impact current global events could have on their operations. Ongoing conflicts in the Middle East and Ukraine continue to create uncertainty around energy prices, supply chains and the wider economic outlook. Business leaders are also concerned about the risks linked to rapid or uncontrolled AI adoption (9%) and dependence on non-European technology providers (9%). Both are now seen as real threats to business continuity and operations, rather than theoretical issues or problems to tackle in the future.

THE TOP 5 PERCEIVED THREATS FOR EUROPEAN BUSINESSES TO....



The risk landscape has changed. Business leaders aren't dealing with isolated threats anymore, but with a connected mix of technological, geopolitical and operational pressures that can rapidly affect business operations and continuity. As a result, resilience today is less about managing individual risks in isolation and more about ensuring organisations are prepared when disruption comes from several directions at once.

CYBER-THREATS OUTRANK GEOPOLITICAL CONCERNS

While geopolitical instability continues to dominate the headlines, cyber-threats are often where businesses feel that instability most directly. Nearly three-quarters (73%) of European business leaders say a cyber incident could significantly disrupt operations and revenue. Unlike many other risks, the tangible impact of cyberattacks can be immediate. Systems can go offline, operations can be disrupted, and customers can be affected within a matter of hours. Cyber risk is also increasingly tied to wider geopolitical developments. State-backed groups, cyber criminals and hacktivists are operating in the same threat landscape, meaning organisations can be affected by international tensions even when they are not the intended target.

AI is adding further complexity. HarfangLab's 2026 Threatscape Report shows that generative AI is making sophisticated cyber capabilities more accessible and helping attackers operate at greater speed and scale. Techniques associated with state-sponsored actors are becoming available to a wider range of bad actors, increasing the volume of attacks and the number of potential victims.

With geopolitical, technological and operational pressures now closely intertwined, cyber risk is not just a security issue. It is one of the most significant threats to business continuity, with organisations often feeling the initial financial impact of disruption within just hours or days of an incident.

POTENTIAL REVENUE IMPACT WITHIN HOURS

48% of businesses would see revenue impacted within a day after a cyber incident.



For many organisations, the financial consequences of operational disruption can be felt almost immediately. Almost half (48%) of European business leaders say revenue would be affected within the same business day, while a further 31% expect the impact to be felt within two days.

The concern is not only how quickly losses are felt, but how large they can become. One quarter of organisations (25%) report that a 24-hour disruption to critical operations would result in significant or severe revenue loss, equivalent to 16% or more of daily revenue. A small number (4%) say losses could exceed 25% of daily revenue. Organisations in Belgium are most likely to fear significant disruption, with over one-third (35%) of Belgian business leaders saying that over 16% of daily revenue could be impacted.

Recovery after a cyber incident takes **4.32 DAYS** on average

Yet while the financial impact of disruption can often be felt within hours, recovery efforts typically take much longer. Business leaders estimate it can take almost a full working week, at 4.32 days on average, for operations to return to normal following a period of disruption. Four days may not sound like much, but when revenue is being lost every hour, the bottom line tells a different story. The reality that losses can build so quickly is changing how organisations in Europe think about resilience. Yet leadership teams are not always clear on who is accountable.

EXPERT INSIGHT

MORE GOVERNANCE FOR MORE RESILIENCE

Cyber risk is not purely a technical risk: **it is cross-functional and simultaneously impacts the financial, operational, reputational, and legal dimensions** of an organisation, which requires addressing it at the strategic level (Executive Committee, Board of Directors) and not solely within the IT department.

Mitigating this risk with a global approach enables **optimal resource allocation**, by focusing efforts on the most critical assets and scenarios rather than spreading investments without prioritisation.

This also strengthens **organizational resilience.** By accepting that a **cyberthreat will happen**, and anticipating its impacts, organizations can significantly reduce both the likelihood and severity of operational disruptions. **This comes also with identifying what data and systems are more at risk and managing their exposure (e.g. with on-premises facilities).**

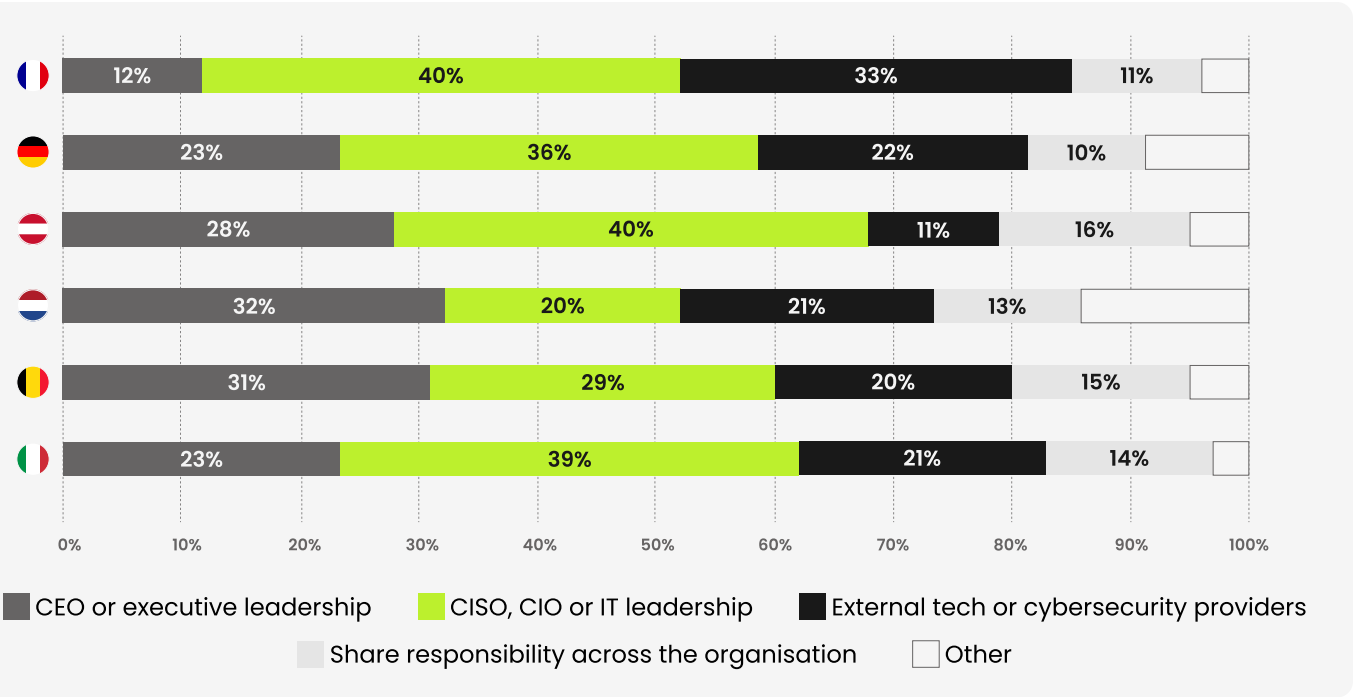
Finally, this integration creates a **continuous improvement dynamic** driven by shared metrics between business units and security teams, enabling organisations to regularly adapt their cyber posture to the evolving threat landscape and regulatory requirements.

CHAPTER 2:
LEADERSHIP WITHOUT OWNERSHIP

Business leaders are divided on who should take responsibility for cybersecurity. Around one-third (33%) point to the CIO, while 27% say the CISO and 23% the CEO. Across Europe, no single role stands out as the person ultimately in charge. Part of the issue is that cybersecurity is often seen through a technical lens. More than half (55%) of European business leaders say it is treated primarily as an IT issue, rather than a business issue owned by the C-suite. That uncertainty carries through to accountability after a breach. Just under a quarter (24%) say the CEO would be held responsible, while 36% point to CIOs, CISOs or CTOs. More than one in five (22%) say responsibility would fall on an external provider.

However, the picture is not the same across all of Europe. French organisations are the least likely to hold CEOs accountable after a breach (12%) and the most likely to blame external providers (33%).

WHO IS ACCOUNTABLE AFTER A CYBER ATTACK



These findings point to a clear contradiction. While business leaders recognise cyber risk as a significant business threat, who should take ownership is unclear. As a result, responsibility is spread across multiple roles, making accountability something of a grey area.

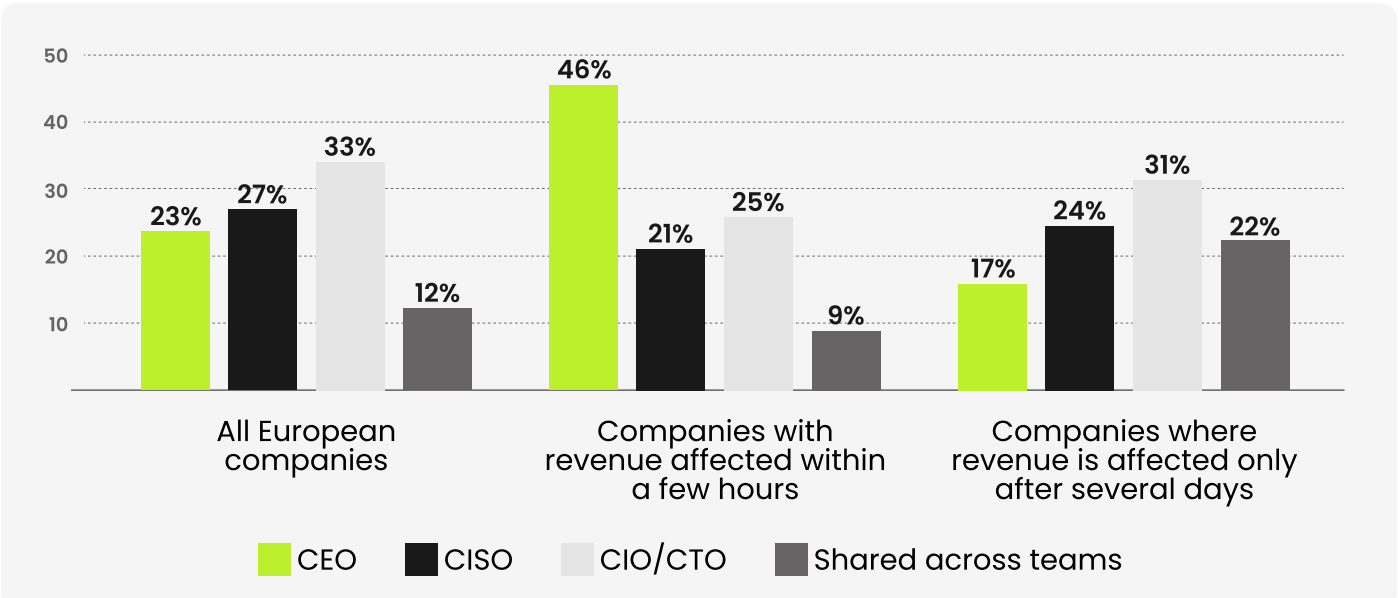
In an episode of Let's Talk About Sec, Fleur Van Leusden, CISO at a major Dutch government organisation, explains *"when there is a security breach, it is always a matter of governance, or choices that were made in the company, not the fault of an employee clicking a link or so. The legal implications of a CEO recognising that the fault is his involves that he would need to resign. I understand then, why they don't. This is why having a CISO who speaks the language of the board can help including security considerations into business and strategic decisions. And hence, influence decisions. At the end of the day the CEO signs, but the CISO gave the pen".*

HIGH CONFIDENCE WITHOUT CLEAR OWNERSHIP

Despite concern around cyber risk, most European business leaders are confident they could cope with a serious incident. Nearly three-quarters (74%) say they are confident in their organisation's ability to respond to a cyber-attack, while over two-thirds (67%) believe they could maintain operations during a period of disruption. Business leaders recognise the damage cyber incidents can cause yet remain confident they could manage the impact. Whether that confidence is fully justified is less clear. This may help to explain why cybersecurity is often left to IT and security teams rather than the CEO. If leaders believe their organisation is prepared, there is less reason for them to take ownership themselves. It also becomes easier to delegate ownership elsewhere. But by the time those assumptions are tested by a cyber incident, it may already be too late.

UNDERSTANDING IMPACT SHIFTS LEADERSHIP PRIORITIES

Not every organisation views cybersecurity the same way. The clearest difference comes when leaders expect a cyber incident to hit revenue quickly. Among organisations that believe a cyber incident would affect revenue within hours, 46% say cybersecurity is a CEO priority. Across all businesses, that figure falls to 23%.



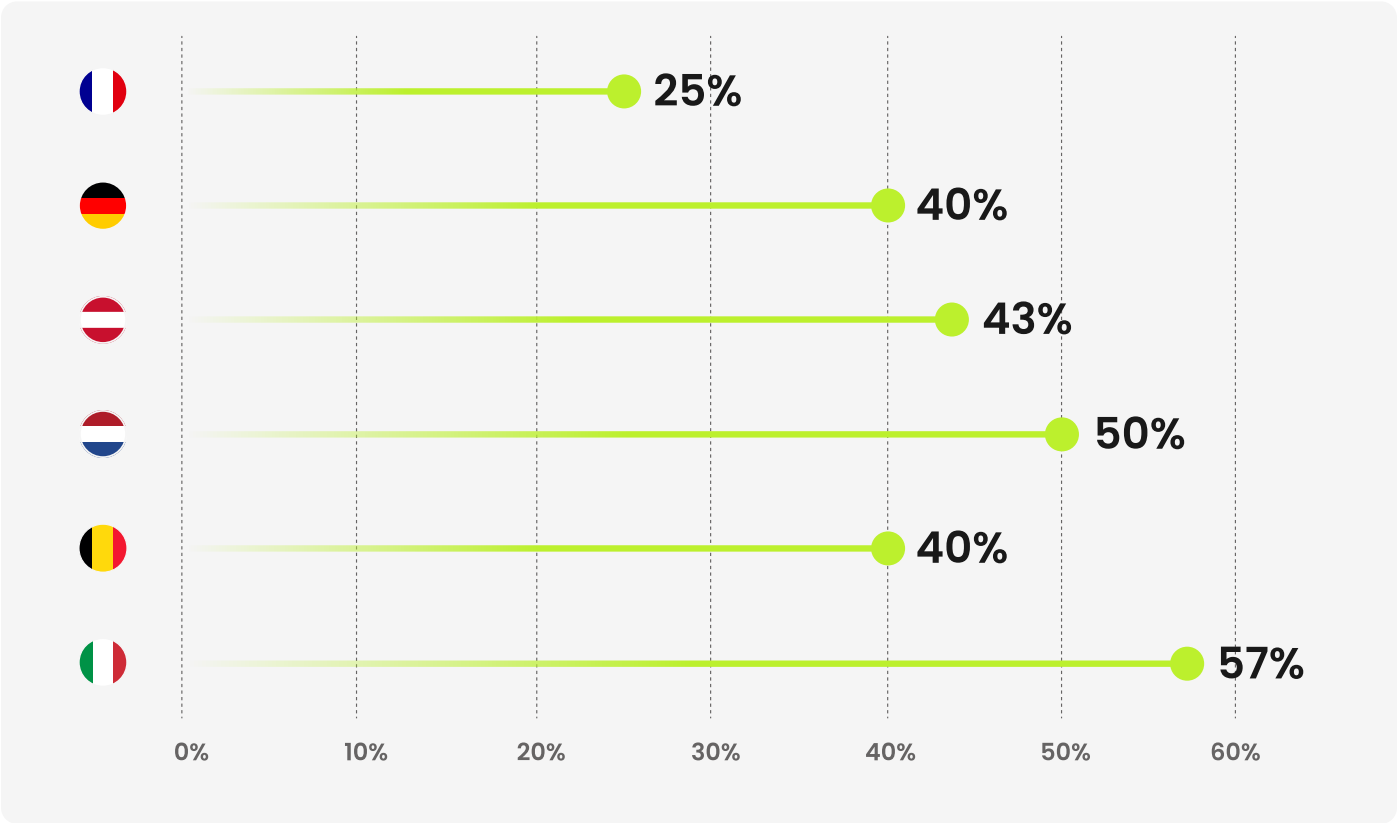
Organisations facing the prospect of immediate financial damage are twice as likely to make cybersecurity a CEO responsibility. When the consequences are real and immediate, cybersecurity becomes much harder for leadership teams to treat as someone else's responsibility.

EXPERTISE GAPS LEAVE LEADERS EXPOSED

As cybersecurity becomes a bigger continuity concern, many organisations face a clear problem. The leaders expected to own cyber risk are not always equipped to manage it. One in five (20%) business leaders say their board or executive leadership team has limited or no meaningful cybersecurity expertise. At the same time, almost three-fifths (59%) of executives are concerned about being held personally accountable if a cyber incident occurs. This leaves many organisations in a difficult position. Leaders are expected to make decisions that affect resilience and continuity, but do not always have the knowledge or experience to do so with real confidence. It's important to remember that resilience is not just about preventing attacks. It is also about making the right decisions when disruption occurs. Yet the research suggests organisations may lack the experience needed to support decision-making when it matters most.

Across Europe, Italian businesses claim to have the highest levels of cybersecurity expertise within the C-suite (57%), while France reports the lowest (25%). This may be part of the reason why French organisations are the most likely to place accountability on external providers.

% OF COMPANIES WITH STRONG CYBERSECURITY EXPERTISE WITHIN THE BOARD OR EXECUTIVE LEADERSHIP TEAM



CHAPTER 3:
STRATEGIC AWARENESS, LIMITED ACTION

Rising geopolitical tensions, growing concerns around digital sovereignty and increasing dependence on a small number of global technology providers have brought supply chain risk into sharper focus. Over two-fifths (41%) of European business leaders acknowledge the risks associated with relying on global cybersecurity providers. Yet that awareness does not appear to be translating into widespread action. Less than one in ten (9%) leaders are actively prioritising European providers to reduce risk. Almost a quarter (23%) are significantly reducing dependence on non-European providers. While many organisations recognise the risks of dependency, replacing or reducing reliance on established providers can be hard to do. Critical systems, data and day-to-day operations are often tied to a small number of trusted suppliers, making change complex and disruptive. This gap between awareness and action is also visible in how leaders view geopolitical risk more broadly.



Anouck Teiller
Deputy CEO, HarfangLab

Anouck Teiller, Deputy CEO of HarfangLab, explains: *"The topic of dependency is not only a topic of 'where does your security provider come from'. It's a matter of mindset and of visibility. What is your critical activity about? What is your most critical infrastructure or data? Do you want to hand over the control of your data to external providers without knowing where it goes, who governs it, and if loss of access results in a service disruption? That's why strategic autonomy is crucial. Organisations who put their trust in external providers should be able to fully understand what happens to their data. That is why we provide transparent guidelines, on-premises capabilities and an open platform at HarfangLab."*

MIND THE RISK-RESPONSE GAP

Despite the attention given to geopolitical instability, just 31% of business leaders expressed significant concerns that these developments may affect business operations. Many organisations appear to view geopolitical risk as a future concern rather than an immediate issue. Conflicts, trade disputes and political tensions continue to shape the operating environment, but they are not yet prompting widespread changes in strategy. However, attitudes differ across Europe. Nearly half (46%) of Dutch business leaders are significantly concerned about geopolitical developments affecting business operations, compared with just 24% of their counterparts in Italy. The contrast shows how differently geopolitical risk is viewed across the region.

EXPERT INSIGHT

GEOPOLITICAL-LINKED CYBER-THREAT PREDICTIONS FROM HARFANGLAB'S CYBERSECURITY RESEARCHERS.

The 2026 Threatscape Report opens with a striking example: during the US military operation in Venezuela (January 2026), Cyber Command reportedly "turned off the lights of Caracas" by attacking critical infrastructure. This confirms HarfangLab's core thesis: the frontier between the physical and digital worlds is shrinking.

FOUR KEY GEOPOLITICAL DYNAMICS ARE SHAPING THE THREAT LANDSCAPE:

Erosion of state power in cyberspace. Governments are losing control over digital spaces to "digital giants", cybercriminal organisations, and offensive cyber-mercenaries. The growing demand for intrusion tools from intelligence and military agencies fuels a deregulated "grey zone" market that states themselves are reluctant to dismantle.

Internet fragmentation. Geopolitical rivalries are breaking up the global internet. Russia has built the legal framework to sever "Runet" at will; China is exporting its Great Firewall technology to authoritarian governments (Myanmar, Pakistan, Kazakhstan, Ethiopia). To improve EU resilience, the EU introduced a Data Sovereignty Framework, that follows the same trend of fragmenting the cloud market. In 2025, nearly **50% of major internet outages** were government-directed shutdowns.

States using cyber proxies. Russia, China, and Iran increasingly rely on hacktivist groups, private companies, and criminal actors as proxies for offensive operations. China formalized this in late 2025 with a legal framework mandating private sector cooperation in national cyber objectives. Threat actor RomCom is a prime example, pivoting from cybercrime to pre-positioning backdoors in European infrastructure in preparation for hybrid warfare.

AI-powered information warfare. The Moscow-based "Pravda" disinformation network successfully poisoned major AI chatbots with pro-Kremlin narratives, which were repeated approximately 33 percent of the time. Manipulated content also targeted European elections via AI scrapers.

CYBERSECURITY ON-PREMISES – A PATH TO MORE CONTROL?

As control is crucial when it comes to building a cybersecurity strategy, on-premises cybersecurity solutions are gaining renewed attention. Far from being an outdated model, it represents a deliberate choice made by organisations that cannot afford to leave the control of their most sensitive data in the hands of a third party.

For regulated industries such as defense, government, finance, energy, or critical national infrastructure, on-premises deployment is sometimes not even a choice; it is a legal or regulatory obligation. But beyond compliance, it is also a response to a deeper concern: the need to know exactly where your data lives and who can access it under what conditions.

However, on-premises is not a universal answer. It requires in-house IT resources, a mature infrastructure, and the willingness to take on the operational responsibility of deploying and maintaining a solution. Organisations without those capabilities, or without specific data sovereignty constraints, will often find that a cloud-based solution better fits their needs.

What matters most is that choosing on-premises should never mean accepting a lower standard of protection. This is precisely where HarfangLab stands out: its on-premises solution delivers the exact same detection capabilities, features, and performance as its cloud version, including full air-gapped compatibility. Control, in other words, does not have to come at the cost of security. With the right solution, organisations can have both.

CHAPTER 4:
REGULATION IS BECOMING A STRATEGIC ADVANTAGE

Europe is at the forefront of cybersecurity regulation, with frameworks such as NIS2 raising expectations around resilience, risk management and incident reporting. Most business leaders understand that regulation is becoming a bigger part of cybersecurity. Almost three-quarters (73%) say they are familiar with major European cybersecurity regulations and the implications for executives.

Organisations also appear to know what is expected of them. A similar number (74%) say they are clear on what would be required legally in the first 72 hours following a serious cyber incident. But regulation is not only being viewed as a compliance issue. 72% of business leaders believe stronger regulation offers them a competitive advantage. Meeting higher standards is now seen as a way to build trust, strengthen resilience and stand out in a global market where security expectations continue to rise.

IMPLEMENTATION IS EASIER SAID THAN DONE

65%

say organisations struggle to understand how to implement regulatory requirements in practice.

Understanding regulation is one thing. Putting it into practice is another. Nearly two-thirds (65%) of business leaders say organisations struggle to understand how regulatory requirements should be implemented in practice. Meanwhile, 60% say the pace of regulatory change is difficult to keep up with, while 71% say regulation increases operational cost and workload. Organisations may understand what regulators expect, but translating those expectations into day-to-day operations is often more difficult to achieve. The challenge is not only understanding the rules, but finding the time, resources and expertise to keep up with them.

EXPERT INSIGHT

MORE COMPLIANCE TOWARD MORE RESILIENCE

Having a cyber-resilient approach will make you both safe and compliant. Changing your cyber strategy shouldn't be done to tick a box but to actually improve your security procedures. Mindset, governance, and risk analysis need to be adapted. But once done, they can keep pace with regulations as a cybersecurity baseline.

ACCOUNTABILITY INCREASING FASTER THAN CAPABILITY

The demands of regulation are not just increasing the workload for cybersecurity teams; they are also increasing accountability at the top of the organisation. Almost three-quarters (74%) of European business leaders say regulation increases accountability at board level, while 59% are concerned about being held personally accountable for cybersecurity incidents affecting the business.

74%

acknowledge that regulation increases board-level accountability.

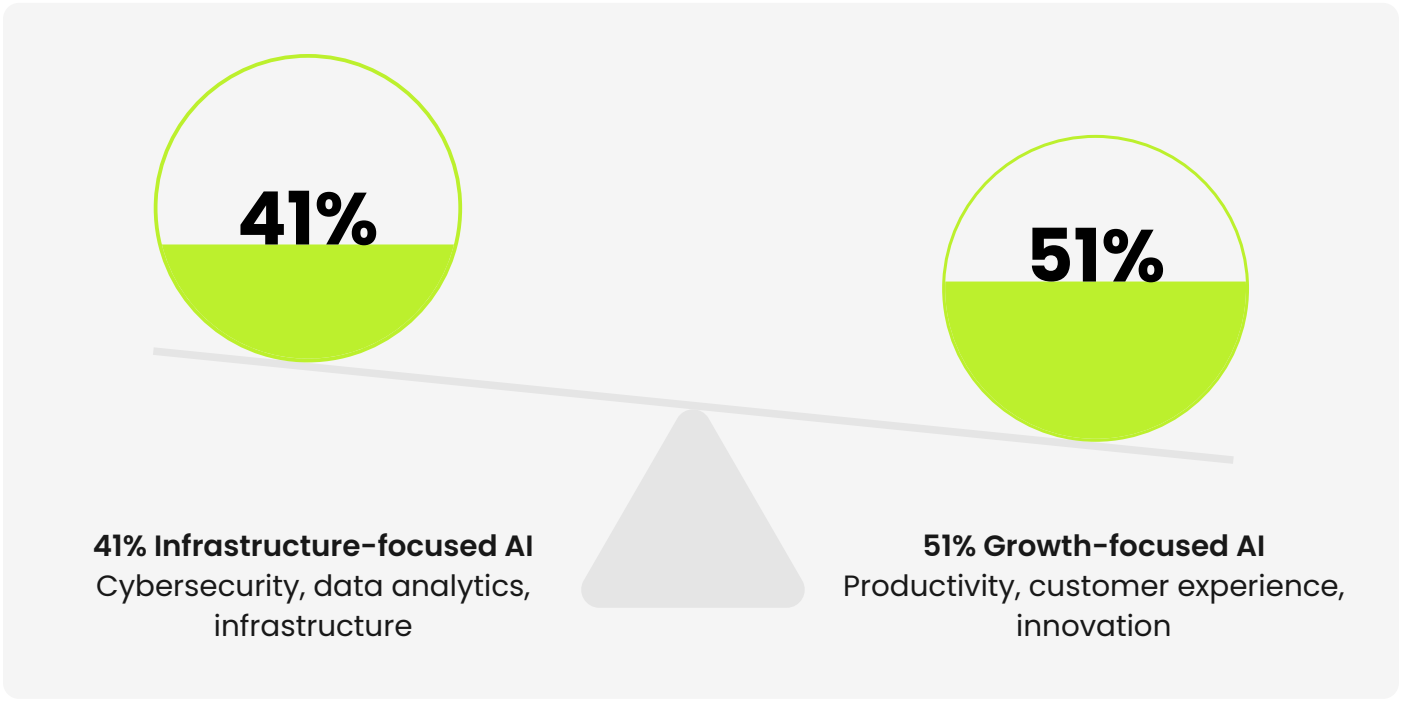
Greater accountability does not always come with greater ownership. As previous chapters showed, responsibility for cybersecurity often remains fragmented, while leadership expertise varies significantly between organisations.

The difference can be seen across Europe. In France, 79% of business leaders say they are familiar with major cybersecurity regulations and their implications for executives, yet only 9% say the CEO or executive leadership team has primary responsibility for cybersecurity strategy. By contrast, Austria is far more likely to place responsibility at the top of the organisation, with 32% saying cybersecurity strategy sits with the CEO or executive leadership team. Accountability is rising, but the ownership, expertise and operational support needed to meet those expectations are not always keeping pace.

CHAPTER 5:
AI PRESENTS OPPORTUNITY AND RISK

AI is becoming another major challenge for leaders to navigate. Across Europe, organisations are investing heavily in the technology, and their priorities reveal where they see the greatest value. Overall, AI investment is weighted slightly more towards growth-focused initiatives than infrastructure-focused ones. Around 51% of investment is directed towards areas such as productivity, customer experience and innovation, compared with 41% focused on cybersecurity, data analytics and infrastructure.

AI INVESTMENT PRIORITIES

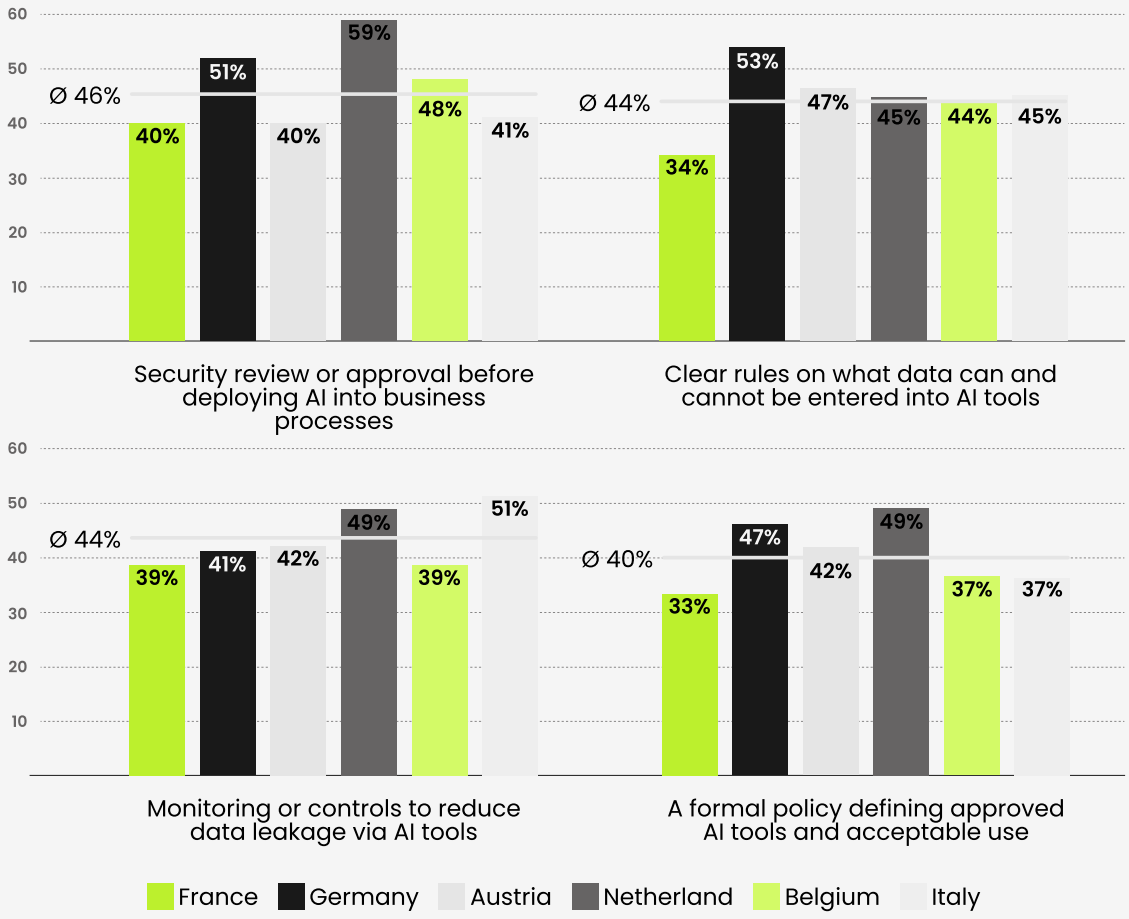


The largest share of investment is going towards productivity.
On average, 23% of AI budgets are being spent on improving efficiency and helping people work more effectively. At the same time, organisations are also investing heavily in the foundations needed to support and protect those gains. Cyber defence is the second-largest area of investment, accounting for 16% of spend. This reflects the growing role AI is playing in cybersecurity. Organisations are using the technology to improve visibility, automate routine tasks, speed up detection and response, and help security teams keep pace with today's complex threat landscape. The findings show that European businesses view AI as more than just a productivity tool, but as an important part of how they strengthen resilience and support day-to-day operations.

AI ADOPTION LACKS CONSISTENT GUARDRAILS

Organisations are moving quickly to take advantage of AI, but the safeguards needed to use it securely are not always being introduced at the same pace. Less than half (46%) of European businesses require a security review before deploying AI tools. Only 44% have clear rules on what data can and cannot be entered into AI systems, while 40% have formal policies governing AI use. Across Europe, Germany and the Netherlands have the strongest governance practices. Organisations in France are the least likely to have measures in place to support the secure use of AI tools, despite the country's ambition to position itself as a global leader in AI.

AI INVESTMENT PRIORITIES



What's clear from these findings and the differences throughout the region is that AI adoption is moving faster than the governance, policies and controls needed to support it.

CYBER STRATEGIES REMAIN DEEPLY FRAGMENTED

While organisations are embracing new technologies at a blistering pace, there is still no clear consensus on what cyber resilience should prioritise. Just under a quarter (23%) of European business leaders say their strategy is focused on preventing cyberattacks through strong technical controls. A further 21% balance prevention, compliance and resilience equally, while another 21% prioritise using multiple technologies and tools to address potential security risks.

By comparison, only 18% of leaders say business continuity and rapid recovery from incidents is the primary focus of their cybersecurity strategy, while 15% place compliance at the centre of their approach. Leaders are aware of the disruption cyber incidents can cause, yet relatively few are putting recovery and continuity at the heart of their strategy. As AI becomes more embedded across organisations in Europe, that balance becomes even more important. New technologies can strengthen cyber defences, but they can also create new dependencies and potential points of failure.

Despite these different approaches, more than two-thirds (71%) of business leaders believe their current investment in cybersecurity is sufficient. The most revealing finding may be that organisations are taking very different approaches to cybersecurity, yet most believe they are investing in the right places.



Anouck Teiller
Deputy CEO, HarfangLab

Anouck Teiller says: *"What is tricky with AI, is that the main threats are not always where we tend to believe they are. If cyber-attackers are accelerating some attack procedures through AI, it's still not a real problem for detection and response tools that can actually absorb and detect those threats. We actually see more risks with the massive and rapid development of multi-purpose agentic AI which eventually reinvents how security solutions are built and where to focus."*

EXPERT INSIGHT

AI FOR ENHANCED CYBER CAPACITIES

At HarfangLab, the goal has always been to develop concrete use cases that directly address the real challenges faced by cyber analysts, rather than following the hype.

At the core of HarfangLab's AI strategy sits Ashley, the detection engine embedded in our EDR. Ashley combines Machine Learning and Deep Learning to detect unknown threats through behavioural analysis, examining executable files and Windows scripts, even obfuscated ones. Its models are regularly retrained to keep pace with the ever-evolving threat landscape.

Alongside Ashley, HarfangLab developed Kio, a generative AI assistant integrated directly into the console. Kio allows analysts to navigate the platform in natural language, filter investigation data, generate playbooks, help with alert triage and prioritisation, and automate a number of incident response tasks. Its model runs entirely on HarfangLab's own servers, ensuring full data confidentiality.

From a defence perspective, AI brings several fundamental benefits. It enables the detection of unknown threats before they are even referenced in any database. It dramatically reduces alert fatigue by filtering and prioritising what matters most, so analysts can focus on high-value decisions rather than sifting through thousands of events. And it enhances threat intelligence by summarising attack campaigns and vulnerabilities, and correlating sources to accelerate investigations.

A SECURED AI APPROACH RELIES ON THREE NON-NEGOTIABLE PILLARS:

technology that is robust and well-governed,
transparency into how models work
and **what data they use,** and **human expertise**
that remains central to every critical decision.

TYING IT ALL TOGETHER: WHAT THIS MEANS FOR BUSINESS LEADERS

Across Europe, organisations are more aware of cyber risk, but not all of them are responding in the same way. Responsibility remains fragmented, confidence often exceeds readiness, and approaches to resilience, regulation, and AI vary significantly.

SUMMARY

THE RESEARCH IDENTIFIES FIVE RECURRING CHALLENGES FOR ORGANISATIONS:

01 Cyber risk is recognised, but ownership remains unclear: Cybersecurity is widely seen as a business risk, yet responsibility is often split across multiple roles or delegated to an external provider. In many organisations, it remains unclear who ultimately owns cyber resilience when disruption occurs.

02 Confidence exceeds preparedness: Most business leaders are confident in their ability to respond to cyber incidents and maintain operations. However, that confidence is not always supported by clear ownership, expertise or operational readiness.

03 Dependency remains a source of vulnerability: Many organisations recognise the risks associated with relying on a small number of non-European technology providers. Yet relatively few are actively reducing that dependence, despite growing concerns around resilience, sovereignty and supply chain security.

04 Regulation is raising accountability: Business leaders increasingly see regulation as a competitive advantage, but many continue to struggle with implementation. Accountability is increasing faster than the operational capacity needed to meet those expectations.

05 AI adoption is outpacing governance: Organisations are investing heavily in AI for both productivity and cyber defence. However, the controls, policies and governance needed to support its secure use are not yet consistently in place.

Most organisations understand the risks they face. The challenge is turning that understanding into resilience. Business leaders who continue to treat cybersecurity primarily as an IT or compliance issue may struggle to respond when disruption occurs. Those who align leadership, ownership, operational resilience and strategic decision-making will be better placed to maintain continuity under pressure.

Resilience depends on more than technology. It depends on whether leadership teams know who is responsible, understand the risks they face and can make the right decisions when disruption occurs. The organisations most likely to succeed will not be those that avoid disruption altogether, but those best prepared when it arrives.

METHODOLOGY:

This report is based on research conducted by Sapio Research, commissioned by HarfangLab. The interviews took place in April 2026 and surveyed 750 business leaders across France, Germany, Belgium, the Netherlands, Austria and Italy. The businesses surveyed employ 250 or more employees, covering sectors including healthcare, manufacturing, technology, and government services.

ABOUT HARFANGLAB:

HarfangLab is a global cybersecurity provider specializing in endpoint protection against known and unknown threats. Founded in 2018, HarfangLab detects 100% of attacks and neutralizes them on workstations and servers.

Its EDR was the first to be certified by the French National Cybersecurity Agency (ANSSI) and by the German Federal Office for Information Security (BSI). Recognized in the European Gartner Magic Quadrant and named a Forrester Notable Vendor, HarfangLab protects hundreds of customers worldwide, including public administrations and organizations of all sizes, through its EDR, EPP, and ASM solutions that secure modern workspaces.

Your security, your choice: deploy complete detection and response via the Cloud, Hybrid, or On-Prem. The HarfangLab platform integrates natively with industry-leading security tools, leverages in-house AI, is fully operable via API, and ensures full transparency into data and detection rules – delivering strategic autonomy for SOC teams and the workspaces they defend.

HarfangLab

For more information, visit us

harfanglab.io HarfangLab

Press contact:
Noémie Minster
noemie.minster@harfanglab.fr

Marketing contact:
marketing@harfanglab.fr