HarfangLab

OBSERVING EUROPEAN SMB'S CYBER-RESILIENCE IN A MULTI-RISKS WORLD.

An HarfangLab report and research, analysing cyber-risks, strategies and resilience to face the actual, and future threat landscape and its consequences

2024

HARFANGLAB REPORT 2024: CYBERTHREAT RISKS, RESILIENCE AND STRATEGIES RESEARCH

EXECUTIVE SUMMARY

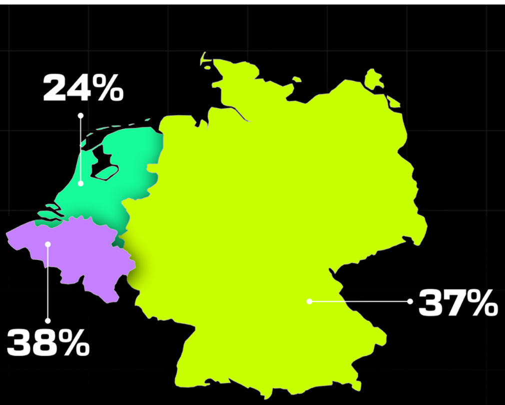
2024 is a watershed moment. Geopolitical tensions are escalating, and European organisations are more exposed to cyberthreats than ever. But how prepared are European SMEs for the challenges ahead?

SMEs represent the majority of the economic landscape of Europe and improving their cyber resilience is critical. Indeed, they are facing similar threats as big corporations, but have much fewer resources with which to defend themselves.

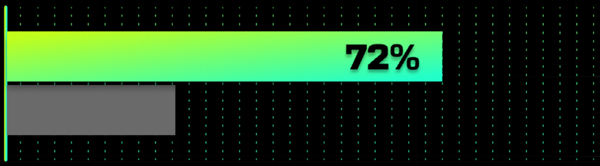
We wanted to find out how cyber resilient the continent's SMEs are. How do they perceive the threat level they are facing, what steps are they taking to defend themselves, and what is the impact of additional compliance requirements from new EU regulations? As such, we commissioned a survey of 750 IT decision makers from France, Germany, Belgium, and the Netherlands.

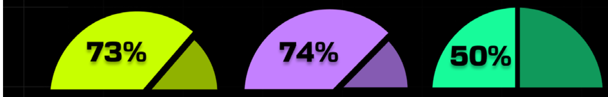
HERE ARE SOME OF OUR TOP FINDINGS:

38% of respondents in Belgium perceive the threat level is extremely or very severe compared with 37% in Germany & 24% in the Netherlands answering the same.



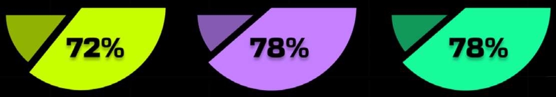
72% of respondents through Europe agree that European cybersecurity providers are in better position to develop products in line with European needs.

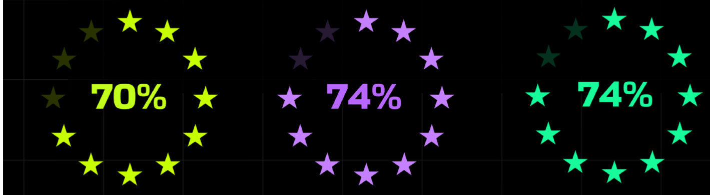




IT decision makers from Germany and Belgium are the most convinced that EU cybersecurity and data protection legislation is a competitive advantage.

All regions supported the idea of choosing European cybersecurity partners.





IT decision makers are convinced that European cybersecurity partners can better meet their needs.

INTRODUCTION:

Organisations around the world are more at risk from cyberthreats than ever. The current international situation – including geopolitical conflict, economic and political instability, and high rates of inflation – contributes to increasing crime rates and incentivises bad actors to undertake lucrative yet damaging ransomware operations. In addition, the world has never been this connected. The post-COVID era also brought higher connectivity within organisations which involves more attacking surface, and a wider IT to monitor. The adoption of new technologies within businesses, such as Gen-AI also needs to be secured. While businesses are using EDR technologies to improve the protection of their endpoints, which can be considered as the front door of their IT infrastructure, attackers are developing new tactics as they look for new ways in. This is a perpetual race against attackers' ingenuity.

European organisations are particularly exposed to cyberattacks. The continent and its companies are perceived as being wealthy and thus qualify as ripe targets. Meanwhile, the plethora of sporting events this year – such as the Olympic Games in Paris and the Euro 2024 football tournament in Germany – is expected to draw increased attention from around the world, creating opportunities for attack for threat actors including organised crime, activists, and rogue states. This may stretch European cyber defences to breaking point: according to reports , organisers of the Paris Olympics are preparing for an unprecedented level of threat, expecting the number of cybersecurity events to be multiplied by 10 compared to the Tokyo Games in 2021.

Most European companies are already aware of the threat, but they must balance the need for greater cybersecurity against the reality of increasingly tight budgets, competing priorities, and the difficulties of attracting, recruiting, and retaining cybersecurity talent. IT decisionmakers and security managers must also grapple with the challenge of raising awareness throughout the organisation: how can they make everyone in the company aware that they too can play a part in reducing cyber risk?

In this context, there is a need for regulation that can provide guidance, steering and expectations when it comes to cybersecurity. The European Union is leading the world in this regard, with legislation such as the General Data Protection Regulation (GDPR), the Digital Operational Resilience Act (DORA), and Network and Information Security 2 (NIS 2) Directive setting a mandate for a high and consistent level of cybersecurity across all member states. The framework and requirements of these regulations send a strong message to companies about the need to prioritise cyber defence and data protection. But what do European companies themselves think of the legislation?

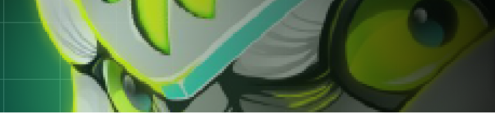
It is important to ensure that this regulatory environment does not become an additional constraint for companies, nor that it widens the already considerable gap between Chief Information Security Officers and their fellow executives, as well as the rest of the organisation. CISOs are sometimes – and unfairly – viewed as a hindrance to businesses; this should not be the case. How can CISOs ensure that their company's quest for compliance with regulation does not simply become a box-ticking exercise that undermines security?

In a digital world on the move, the question of cybersecurity is one of acculturation, in which everyone is a player. But at a time when budgets are tight and priorities must be set, what is the real level of cyber resilience across Europe?

Against this backdrop, and in an attempt to answer these questions and provide advice to European SMEs, HarfangLab commissioned Sapio Research to interview 750 IT managers across Europe to find out how they perceive their ability to deal with the reality of this ever-growing threat landscape. This way, we can better understand where the problem lies and help security players to support their businesses where they really need it.

Because in this world of protean cyber threats, where investment is slowing down, understanding where the risks really come from – and being able to address them strategically – is not only smart but essential if you wish to retain your independence, your economic advantage and, ultimately, your survival as an organisation.

In this report, we reveal what priorities and expectations SMEs have, explore some of the obstacles to better cyber security, and look to answer an essential question: how cyber resilient are European SMEs?



A NOTE ON METHODOLOGY

This report is based on a survey carried out online by Sapio Research in April 2024. 750 IT security decision makers from Belgium, France, Germany and the Netherlands were asked about their perception and awareness of cyberthreats and how prepared their organisation was to deal with cybersecurity risks.

Out of 750 respondents, 300 were from France and Germany each, 100 from Belgium and 50 from the Netherlands. The sizes of businesses spanned from 300 to 4,000 employees.

ABOUT HARFANGLAB

Headquartered in Paris, HarfangLab is a European cybersecurity specialist, helping organisations boost their overall cyber resilience with its AI-enhanced endpoint security software suite.

Founded in 2018, HarfangLab aims to protect the data assets of companies worldwide. Empowered by the expertise of its founders, Grégoire Germain (CEO) and Xavier Boreau (CFO), Mathieu Gaspard (Head of R&D), Maxime Rameau (CPO): cyber-security veterans with experiences in the military, intelligence, and telecom sectors. HarfangLab provides a unique cloud agnostic Endpoint Detection and Response (EDR) software solution which detects, analyses, and neutralizes threats made against businesses which in turn enables them to be cyber-resilient.

HarfangLab's software is one of the top worldwide EDR solutions, as proven by its best-in-class MITRE ATT&CK Evaluations and backed by its EU certification granted by the French National Cybersecurity Agency (ANSSI). It provides a trusted option for its users which includes several government agencies, businesses and international organizations operating in highly sensitive sectors.

EUROPEAN CYBER LEGISLATION PROVIDES A COMPETITIVE ADVANTAGE TO SMES

The European legislative landscape for data and cybersecurity is growing more complex. Alongside well-known regulations like GDPR, this year the European Data Act came into force. Later this year, NIS 2 will come into effect, mandating EU member states to adopt and rigorously enforce cybersecurity regulations. And from January 2025, entities in the financial industry must comply with DORA and implement suitable cybersecurity protection measures.

One might assume that European SMEs would perceive these upcoming compliance requirements regarding cybersecurity in a negative way. But the findings from our research dispel that assumption.

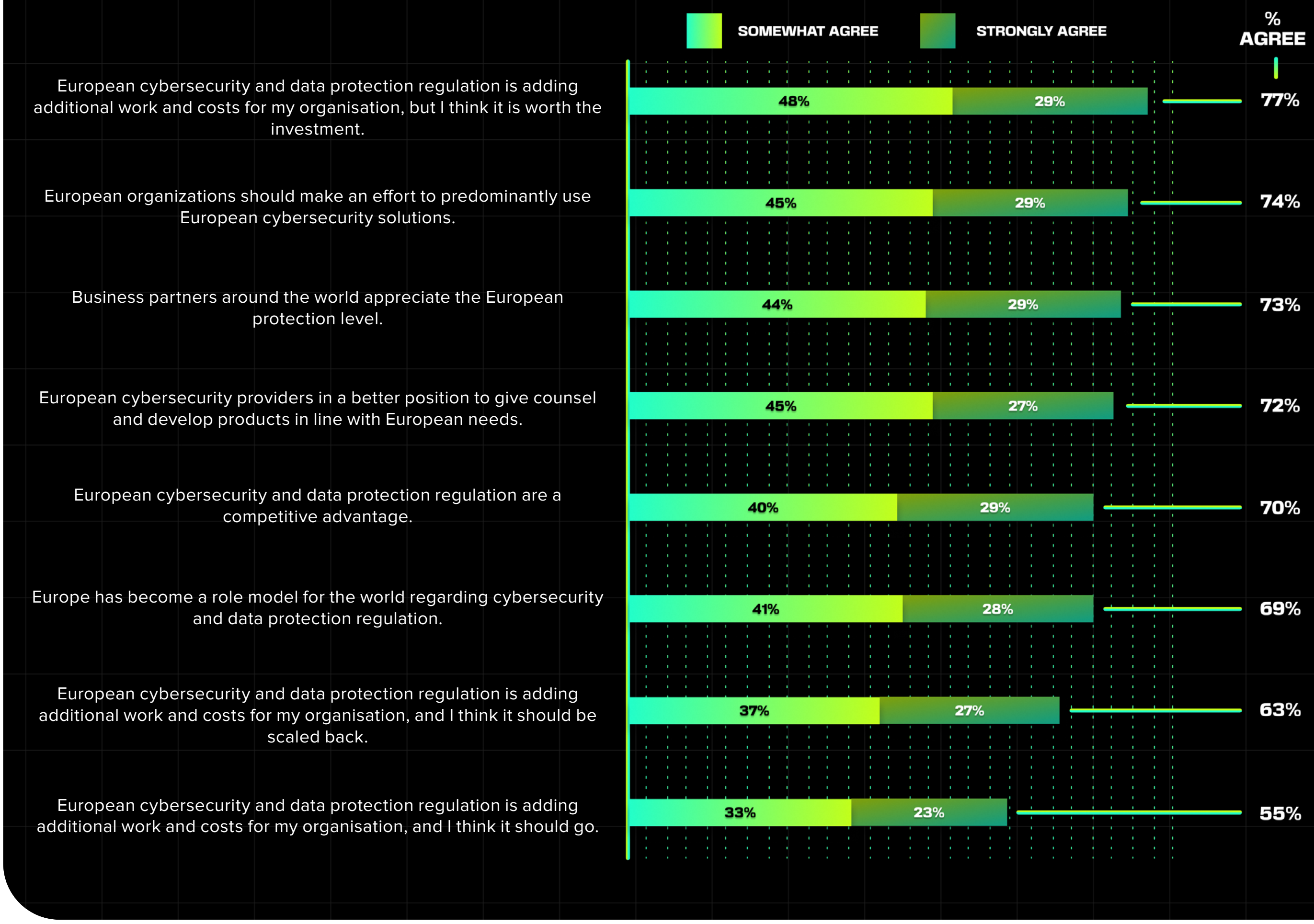
Achieving compliance with these various European cybersecurity and data protection legislation is adding additional work and costs for SMEs. However, more than three quarters (77%) of our survey respondents agreed that these efforts are ultimately worth the investment.

Why is that the case? According to our results, 73% of IT security decision makers agreed that business partners around the world appreciate the levels of protection available in Europe that this legislative framework provides. As a result, 70% of respondents agreed that European cybersecurity and data protection regulation offers SMEs a competitive advantage in the global economy.

«It’s good news that most SMBs see the upcoming regulations as an opportunity, because this really is. Although not all regulations are yet in force in all countries, companies can prepare for their purpose: security. Security is not a “box-checking” process, it is a combination of people, technologies and governance. The main advice that we can give to companies in the context of NIS2, is to onboard the C-levels and business decision-makers and convince them of the importance of cybersecurity and that everyone from the company has a role to play. On this, NIS2 is a real opportunity for CISOs, to give the wake-up call to the rest of their organisation.»

Anouck Teiller, Chief Strategy Officer at Harfanglab

77% agree that the European cybersecurity and data protection regulation is adding additional work and costs for their organisation, but it is ultimately worth the investment.



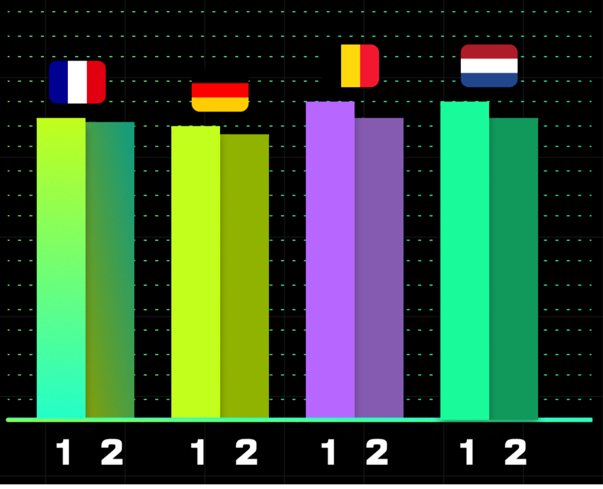
There was little disagreement between regions on this point. In fact, IT security decision makers from Germany and Belgium are even more convinced that EU cybersecurity and data protection legislation is a competitive advantage (73% and 74%) than their French (68%) counterparts. Dutch respondents were a little more sceptical: only 50% agreed with this viewpoint. However, roughly equal proportions of respondents in each country agreed that compliance efforts are worth the costs (FR 77%, GER 76%, BEL 77%, NL 82%).

A PREFERENCE FOR EUROPEAN CYBER AUTONOMY

Our research also found that European SMEs expressed a preference for working with European cybersecurity providers and solutions.

For instance, 72% agree that European cybersecurity providers are in a better position to give counsel and develop products in line with European needs, while almost three quarters (74%) are in favour of European organisations making an effort to predominantly use European cybersecurity solutions.

Again, there was little disagreement between the different countries surveyed for this report. All regions supported the idea of choosing European cybersecurity partners (1 in the following chart) and are convinced that these can better meet their needs (2 in the chart).



Why might this be the case? First, because they are subject to the same regulatory requirements as the SMEs, European solutions providers can weave compliance into their products and are better able to give advice and counsel on how to comply with new and existing legislation. Providers from outside Europe, operating in very different market conditions and legislative landscapes, may not be as able to provide this tailored support.

Another reason might be in relation to geopolitics: in fact, 28% of respondents identified escalating geopolitical conflict as the main development increasing the threat levels facing their organisation.

European organisations are more exposed to cyberthreats than ever. Our world is in tension, and international events such as the Olympics, the Euro football cup, and European elections are creating an opportunity for many threat actors – including advanced persistent threats, hacktivists or cybercriminals, and antagonistic states – to launch attacks that destabilise, disinform, spy on and disrupt organisations. These attacks may also be intended to fund illicit activity, curb economic activity, or cripple vital infrastructure.

As a result of these growing tensions, European SMEs appear to find the idea of a sovereign European cybersecurity defence architecture increasingly attractive. SMEs recognise that they need partners who understand the local threat landscape and can help them prepare for any eventuality.

> **«Today's threat landscape, combined with the geopolitical and economic stakes, reinforces the need to build a resilient Europe in terms of cybersecurity. It means improving security standards, increasing proactivity and being able to decide what your privacy and security requirements are, who can access your data and for what purpose. With the development and expansion of extraterritorial laws and regulations, this capacity is critical. This is the key to autonomy, and the key to independence. The good news is that this is not an ideology. There are solutions and technical answers to these needs.»**
>
> Anouck Teiller, Chief Strategy Officer at Harfanglab

A CALL TO ACTION FOR EUROPE

Given the links between geopolitical tension and rising rates of cybercrime, what do European SMEs need to do?

First, it is important to fully consider the value of their data, and begin to build a more effective cybersecurity strategy accordingly. SMEs represent the majority of the economic landscape in Europe, and so improving their cyber resilience is critical to the long-term wellbeing of the continent. Indeed, they are facing similar threats as big corporations, but they have far fewer resources with which to defend themselves.

No business should lower its security expectations because of its size. There are relevant approaches to provide both high-quality technologies, human expertise and a consideration for data sovereignty. Using European cybersecurity champions and providers offers greater autonomy and independence than relying on companies in states that may also be vulnerable to geopolitical conflict or cyberattacks. Selecting trusted partners who can build a bespoke offering through a ‘cybersecurity as a service’ approach is also a strategic approach to overcoming internal staffing shortages. Such a partner will be an expert in the operation of the chosen technologies, but also in the requirements of its market.

At the end of the day, what are the markers of trust? Proximity, performance, and transparency. And when we ask to SMBs decision makers what they value the most when looking for an IT security provider: value for money (44%), innovation (51%) and performance (44%) come first followed closely by “understanding my particular needs”.

Docaposte, the digital subsidiary of La Poste group, launched the first complete “ready to roll” cybersecurity offering specifically adapted to the needs and resources of VSEs, SMEs, ETIs, local authorities and healthcare establishments. It brings together the full range of prevention, protection and response solutions available in the field through a single point of contact. To provide this easy-to-access offering, Docaposte draws on its expertise in consulting, and the collaboration with a French and European ecosystem of 12 partner companies selected for their expertise. HarfangLab is included in this offering, and is also the global EDR provider.
This highlights the need for a single point of contact that understands both the ecosystem and the nuances of the market. It also addresses the difficulty of pre-selecting trusted, European and high-quality solutions to build a strong and accessible alternative for European SMEs.

Investing in digital technologies and solutions are key, as well as being able to manage those technologies, or choosing the right partner to do so. These technologies can provide a competitive advantage, enabling certain companies and industries to dominate the company. However, if harnessed or taken control of by threat actors, these same technologies can enable the subjugation of entire economies.

Therefore, Europe must be proactive not to lose this game. European SMEs understand that this requires adopting a technological approach that maintains strategic autonomy and independence, backed by strong governance.

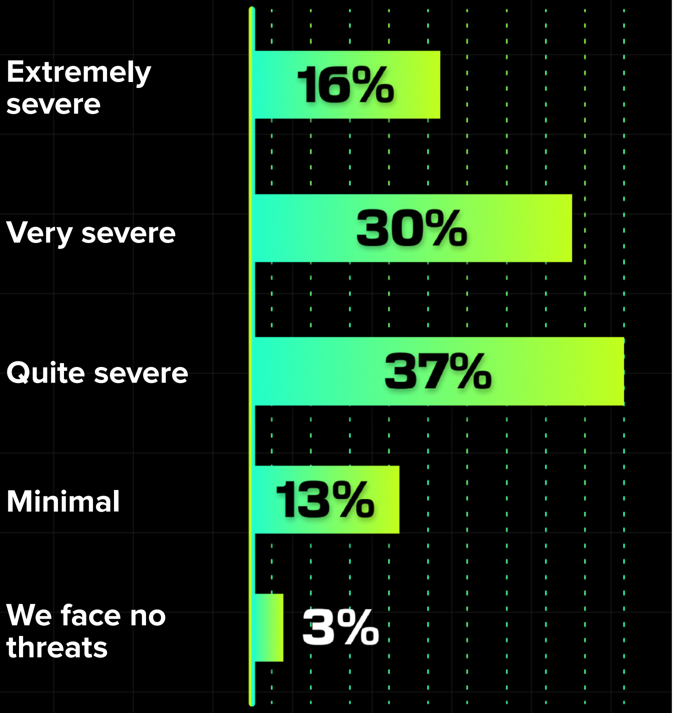
In the next section of this report, we will explore how prepared today’s SMEs are for the current threat landscape, and where they see the biggest risks.

CYBER RISKS: PERCEPTIONS, RISK FACTORS AND PREPARATIONS

With the threat landscape evolving at a rapid pace, we set out to discover what European SMEs thought of the dangers they are facing. We found that nearly half of respondents (47%) rated the current threat level as extremely or very severe, while only 3% claimed that they face no threats. This shows a healthy level of realism from the majority of IT decision makers about the current risk potential.

There is also an indication that the level of concern felt by security managers is driving action and investment. Respondents who said that they are fully prepared for a cybersecurity incident are almost three times more likely to rate current threat levels as “extreme”: 28% vs 10% of those who said they are not well-prepared rate their current threat level as “extreme”.

Nearly half (47%) rate the threat level that they are facing as extremely or very severe.



How do different regions perceive threat levels? We found that the cyberthreat level is rated highest in France: 62% of respondents in this country said the threat level was extremely or very severe, compared to 38% in Belgium, 37% in Germany and less than a quarter (24%) in the Netherlands.

Meanwhile, respondents in the healthcare sector were most concerned about cyberthreat levels: 70% of respondents rated the threat as extremely or very severe. This was followed by accounting and finance (56%), manufacturing and retail/wholesale (both at 43%) and finally education (37%).

We also discovered that the perception of cyberthreat level increases with company size. Only 40% of respondents at organisations with 300-999 employees rated the threat level as extremely or very severe, compared to more than half (52%) at organisation with more than 2,000 staff – a margin of 12 percentage points.

At first glance, this may align with certain assumptions about cyberthreats: larger organisations are more visible and likely to be perceived as having more data and financial resources – and thus make for more valuable targets – than smaller organisations. But the reality is that cyberattacks affect all types of companies, regardless of size or market. SMEs are particularly exposed: in 2022 alone, they suffered over 330,000 attacks, and the consequences can go as far as receivership or bankruptcy. The lesson, therefore, is that smaller companies cannot afford to be complacent with their cybersecurity and must treat the threat seriously.

EXPERT'S EYE: THE DIFFERENT TYPES OF CYBER-RISKS FOR AN ORGANISATION

by Léna Jakubowicz, Pre-Sales Engineer at HarfangLab

A cyber crisis is a particular type of crisis that a company can face as the risks it involves are very diverse, and for each risk, comes a consequence. Having that in mind, also enables a proper crisis management plan, to focus on what could bring the most damages for a company.

FINANCIAL RISK: Colonial Pipeline attack in 2021. A ransomware attack led by the DarkSide group forced Colonial Pipeline to temporarily close its pipeline network, also affecting the fuel supply in the East of the United States for a couple of days. It cost Coloniel Pipeline more than $4.4 million in ransom paid to regain access to its systems, plus the financial losses caused by the ongoing supply disruptions.

REPUTATION RISKS: Databreach at Facebook (2021). Personal data of more than 530 million Facebook users was exposed online, including phone numbers and profile identification information. This breach raised serious questions over Facebook's data protection procedures, affecting its users' and the wider public's trust in the platform.

OPERATIONAL RISKS: Ransomware attack against JBS (2021). The world's largest meat supplier was hit by a ransomware attack, forcing JBS to close several production centres and halt production in North America and Australia. This caused major disruption to the meat supply chain, affecting distribution.

LEGAL RISKS: In 2018, a data breach occurred at British Airways, exposing personal data from 429,612 clients. In 2020, the UK's ICO fined the company millions of pounds after it was found to have «poor security practices». The upcoming European regulations also expose businesses to fines - if they don't comply with security procedures and practices.

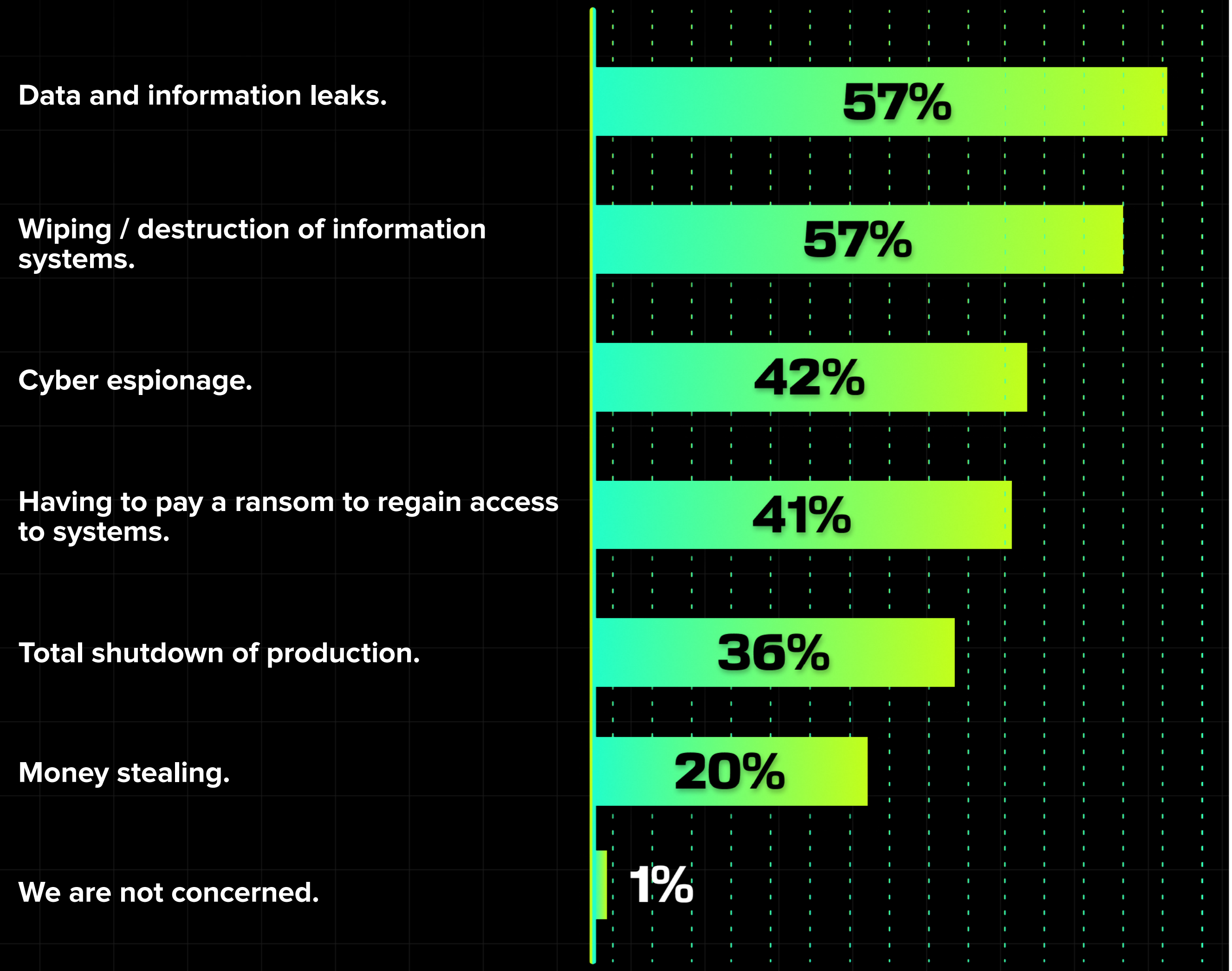
THE IMPACT OF A CYBER INCIDENT

Unsurprisingly, practically all the survey's respondents (99%) said they are concerned about the consequences of a cyberattack. But cyberattacks come in many shapes and forms; which are causing IT decision makers the most consternation?

Perhaps surprisingly, money being stolen seemed to cause the least concern: only 20% of respondents expressed this fear, perhaps because of the difficulties involved, any insurance policy they have that may cover the loss, or the financial controls they have in place to prevent theft.

On the other hand, 57% of respondents stated they were concerned about data and information leaks. A data breach can cause significant reputational damage and potentially lead to significant fines from regulations like GDPR. Similarly, more than half of respondents (51%) were concerned about a cyber incident wiping or destroying their information systems.

99% of IT security decision makers are concerned about the consequences of a cybersecurity attack, most concerning for 57% are data and information leaks, followed by the destruction of information systems (51%)



THE CONNECTED ECONOMY IS EXACERBATING CYBER RISKS

We now understand what consequences of a cybersecurity incidents today's SMEs are concerned about, but where do IT decision makers see the biggest risks that could lead to a successful cyberattack?
Around half of respondents said technical vulnerabilities (56%) posed the most substantial risk. This concern was higher in the education sector (61%) and the manufacturing and energy/utilities industries (64%).

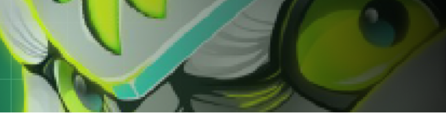
Anther risk highlighted was employees clicking on malicious links or files (52%), indicating the importance of educating colleagues and raising awareness of cyberthreats throughout an organisation. Just under half (49%) stated weaknesses in their supply chain posed a substantial risk. This ties into another question in our survey, where we asked which developments are increasing threat levels the most.

When asked this question, 48% of respondents said the connected economy was their number one perceived reason for the high risks facing their organisation. In today's market, many European SMEs recognise the potential value of exchanging data with their supply and customer chains – the upcoming EU Data Act is also designed to facilitate and encourage data sharing between private companies, citizens, and the public sector. However, every opportunity comes with risks, and this increasingly connected economy expands the number of potential holes, vulnerabilities and attack vectors for criminals to target. A consequence of this connected economy is that IT security managers will need to start looking beyond their own IT architecture and include their partners in their cybersecurity strategies. Securing their value chains should definitely be among every organisation's top priorities.

Other risks factors included a new flood of endpoints and skilled worker shortages (both cited by 47% of respondents). The lack of talent was of greater concern among respondents from Belgium (52%) and the Netherlands (56%), and was the highest rated concern in the retail/wholesale industry (58%).

The rise of generative AI was also called out by 46% of respondents. This was the top factor increasing threat level for the healthcare sector (59%). According to European SME leaders, AI is expected to lead to more sophisticated attacks (81% agree), yet they also believe AI will enable a better understanding of the threat landscape and help to build better security strategies (85%), as well as help beat AI-enhanced attacks in general (82%).

> **«The digital world is connecting people and economies like never before, but it is also creating opportunities for cyber attackers to thrive at the expense of businesses. The pace of technological development in this field is much faster than human training and expertise can keep up with. We are facing a talent shortage on an international scale. This is also one of the reasons why defence tools and technologies must be able to support experts in their work, to multiply their efficiency instead of creating a skills gap. Every technology comes with opportunities and risks, and it's our call, in the defence industry to make sure to build our offering based on the latest innovations, to raise awareness, and contribute to the global improvement of security skills and levels.»**
>
> Anouck Teiller, Chief Strategy Officer at Harfanglab



HOW PREPARED ARE TODAY'S SMES AT HANDLING CYBER RISKS?

IT decision makers show a considerable understanding of the threat landscape, the consequences of a successful cyberattack, and the ability to identify factors exacerbating the risks to their organisation. But how prepared are European SMEs to face incoming cyberattacks?

Currently, only 17% consider themselves to be "fully prepared" when it comes to their cybersecurity defence. Around half (50%) consider themselves to be "very prepared", 30% claim to be "somewhat prepared", and 2% admit that they are not very prepared.

A higher proportion of IT decision makers say they are 'fully prepared' in the IT (32%), healthcare (28%), and finance (26%), sectors. This makes intuitive sense: IT companies are likely to be more technically proficient and able to understand the threats they face and what steps to take to defend their organization; respondents in the healthcare sector previously expressed that they were most concerned about cyberthreat levels, which seems to have spurred them to take action and prepare their defences; and the financial industry has had to take steps to comply with the EU's DORA regulation which came into force in January 2023 and will apply from January 2025.

Similarly, those operating internationally are also more likely to say they are "fully prepared" than those operating nationally (19% vs 15%).

But what do these preparations look like? And what steps can the 83% of respondents who are not "fully prepared" do to increase their cyber resilience? We will explore these questions in the final section of this report.

- **ANTICIPATION**: Controlling risk requires flawless knowledge of information systems, critical assets, data, and of threats and context. A cybersecurity incident also requires the ability to quickly deploy a crisis unit to manage both technical and communications issues.
- **DETECTION**: Efficient detection requires the right tools and resources. More precisely, the Information System needs to be protected by relevant and high-performance solutions set up and managed by expert staff – either in-house or with the help of partners.
- **ANALYSIS**: Once a tool has detected a security event, experts must assess its severity and document it, in order to define what actions to take.
 This stage also aims to understand the threat and the attacker's goals to limit its spread in the moment and in the future.
- **RESPONSE**: After analysing the situation, depending on the context, the experts can block the threat, kill processes, isolate endpoints, quarantine files - with a view to recovering the system or data. In addition to the technical aspects, the response phase may also include internal and external communications actions.
- **REPORT**: Post-incident analysis enables lessons to be learned from the incident, so that the protection of the Information System can be strengthened, and user awareness improved in anticipation of future attacks.

THE IMPACT OF A CYBER INCIDENT

Cyber resilience is the capacity of an organisation to maintain its core purpose and integrity in the face of cyberattacks and other disruptive events. It goes beyond traditional cybersecurity measures such as prevention and defence to encompass preparedness, detection, response, and recovery. Cyber resilience involves not only protecting against threats, but also being the ability to detect and mitigate them quickly, as well as adapt to changing circumstances and continue operations without disruption. Technical solutions, robust processes, employee training, and a proactive mindset are all essential to ensure an organisation can withstand and recover from cyber incidents effectively.

With that in mind, how resilient are European SMEs if threatened by a cyberattack? Most SMEs (81%) have a cyber crisis management plan in place, and 80% are entirely or very confident in their plan. However, less than one third would rate themselves “excellent” in preventing or detecting (27% each), responding (28%) or recovering from (26%) cybersecurity incidents.

Confidence in these capabilities varies by country, but overall, those in France rate their capabilities around cyber incidents higher than neighbouring countries: for instance, three quarters of French respondents (75%) estimate their ability to prevent and detect cyber threats as excellent or fairly good.

In terms of budgeting for cyber defence, more than half (57%) of European SMEs confirm that they will spend more in 2024, compared with 17% who will spend less.

Similarly, countries where the cyberthreat level is deemed greater are spending more on cybersecurity: in France, 58% are planning to spend more in 2024, compared to 44% of respondents in the Netherlands. What do they plan to spend these budgets on? More than half (52%) intend to invest in regular employee awareness trainings, 50% will invest in securing their cloud-based systems and applications, and 49% will commit to and regular audits.

From the 17% of SME leaders who fully trust their defenses, significantly higher numbers indicate that they plan to invest more in establishing a cybersecurity culture, structure, and processes (53% versus 39% among the less confident) and securing their supply chain, which includes educating their partners (49% versus 40%). Almost all (93%) of the confident group also have a cybersecurity defense plan in place; only 65% of the less confident do.

But despite these increasing budgets, over a third (35%) of respondents do not feel their cybersecurity budget adequately reflects the level of threat they face. This increases to 46% of respondents in the healthcare sector and 58% in the automotive and aviation sector.

Confidence in capabilities varies by country, although on the whole, those in France rate their capabilities around cyber security incidents higher than neighbouring countries

	🇧🇪	🇫🇷	🇩🇪	🇳🇱
Preventing	69%	75%	69%	72%
Detecting	65%	75%	73%	66%
Responding	68%	74%	72%	70%
Recovering from	74%	72%	71%	68%

Lowest rating - Highest rating

«There is a common belief that a cybersecurity strategy needs to be expensive to be effective, and that the more layers we build, the more protected we are. We believe this doesn’t have to be true. In fact, focusing on the most critical threats to your business and building a strong foundation (endpoint protection, awareness, IT monitoring, etc.) can be enough to prevent most cyber threats. We are seeing more and more complete cybersecurity baseline offerings on the market through a single trusted partner, such as Docaposte in France.»

Anouck Teiller, Chief Strategy Officer at Harfanglab

ADVICE ON HANDLING A CYBER CRISIS

SMEs can benefit greatly from working with a European cybersecurity champion, who can support them in planning how they will deal with a cyber crisis. Organisations might opt for adopting a risk-based management approach, as this can help to build resilience, enhance overall security, and effectively navigate the complex cybersecurity landscape.
The benefits of a risk-based management approach include:

1 **PROACTIVE APPROACH**: Risk-based management allows organisations to proactively identify and address cyber risks before they escalate into crises.

2 **RESOURCE OPTIMISATION**: By prioritising risks based on their potential impact, organisations can allocate resources more effectively, focusing on the most critical areas first.

3 **RESILIENCE**: Risk-based management builds resilience by enabling organisations to anticipate and mitigate cyber threats, reducing the likelihood and impact of disruptions to their operations.

4 **CONTINUOUS IMPROVEMENT**: By promoting a culture of continuous improvement, organisations can regularly assess and adapt their cybersecurity measures in response to evolving threats and changing business requirements.

> **«There are different ways to build cyber-resilience and one of them is through risked-based management. This means accepting that a cyberthreat will likely affect your organisation and mitigating risk by taking actions to recover quickly. This approach also includes understanding your organisation, your IT infrastructure, your threat landscape and focusing most of your efforts to minimize or even prevent the risks that might be the most harmful to your organisation. This approach can save resource and help analysts to focus on what matters the most. The TDIR (Threat Detection Investigation Response) approach is an efficient strategy to address risked-based cybersecurity management.»**
>
> Anouck Teiller, Chief Strategy Officer at Harfanglab

Organisations can no longer afford to take a reactive approach towards protecting their valuable assets. By working with cybersecurity partners who actively research and study new and emerging threats, they can be more prepared to fully defend themselves.

CONCLUSION

From the research, we can see that organisations can benefit most when they work with actors who understand what is at stake, as well as the cultural and regulatory environment that exists in Europe.

Rather than relying on external providers, European SMEs state a preference for cyber autonomy. They want to be able to deploy tools and solutions within their own infrastructure, as well as through the cloud. These technologies should be a help, not a hindrance. Similarly, IT decision makers should be able to build their own trust environment and to decide who and what can access their organisation's strategic data.

Finally, we know that strong cybersecurity requires cutting-edge technology paired with human skills and expertise, but our research also points to a third pillar of cyber defence: legislation. Europe's cybersecurity and data protection regulations are providing firms with a competitive advantage, by reassuring customers and partners that their data will be safe.

Power comes from information. European SMEs need to understand what types of threats are more likely to target them and where they are most likely to be vulnerable. There is perhaps a need to work with European security champions who can provide threat intelligence tailored to what is most likely to concern Europe, which is something that partners outside of the continent may not be able to provide.

APPENDIX

CYBER RESILIENCE IN 7 KEY POINTS

Preventing all cyber threats and incidents is simply impossible, as disappointing as it may seem.
As every organisation has to deal with the fact that the threat is constant and a fact of life in the digital world, cyber-resilience is key. It is critical to focus on building an organization's capacity to withstand, respond to, and recover from disruptions while maintaining essential functions and services.

In an ever-changing and challenging cyber landscape, this will help organizations and their security teams to better navigate and adapt to the dynamic nature of cyber threats. We believe there are seven key points to consider.

1. PREVENTION AND PROTECTION

Enforcing the protection of your infrastructure is essential to reduce the risks of intrusion, spying, data theft or ransom demand. Implement tools to prevent and protect against cyber threats, such as EDR, next-gen antivirus, IT monitoring tools, and firewalls, but also measures such as multi-factor authentication (MFA) and a zero-trust approach.
You also need to keep all your solutions, such as software, applications, operations systems, up to date to avoid vulnerabilities.

All these prevention and protection actions must be applied by suppliers and third-party vendors as well: check that they comply with best practices and security rules, so that they do not represent an entry point to your Information System.

Also, to be able to recover as fast as possible, you need a perfect knowledge of the Information System and segment your IT fleet properly depending on the importance of your assets. Segmentation will help limit the impact of an attack as bad actors won't be able to move laterally; and mapping the Information System will help identify more easily where the incident started and spread, and isolate parts of it if necessary.

2. DETECTION AND RESPONSE

As mentioned above, investing in resources and up to date technologies is part of the prerequisites for optimum protection of your IT assets against ever evolving threats.
You'll then be able to quickly detect and respond to cybersecurity incidents. This involves monitoring and analyzing tools and incident response teams (in-house or outsourced) to investigate and mitigate threats promptly.

Note that detection and response tools are essential, and they are even more efficient when deployed as part of an holistic approach to cybersecurity. It means it's in your interest to rely on open, API-enabled solutions that allow you to collect, access and correlate data about security events. It is also essential to rely on solutions that enable you to detect both known and unknown threats, –which is made possible with the help of AI - and to block them automatically.

3. RECOVERY AND CONTINUITY

Plan and implement strategies for recovering from cyber incidents and maintaining business continuity. This includes having robust backup and recovery processes and plans for restoring critical systems and data, which must be stored in an isolated and secure environment.
Of course, making plans is all well and good, but you also need to test them regularly, with a view to identifying the key services and tools that need to be restarted first in the event of an incident, and those that may need to be cut off. It is also important to anticipate the operations that may be interrupted and how that may affect your ability to communicate to manage a crisis effectively.

This approach is essential to getting your Information System and business back up and running as quickly as possible in the event of an attack. This is facilitated by IT monitoring features and the ability of tools such as EDRs to collect and aggregate data related to an IT fleet's activity.

4. ADAPTABILITY AND LEARNING

Organizations must prepare for and learn from incidents, update policies and procedures, and enhance security posture over time. In other words: continuously assess and adapt cybersecurity measures based on the evolving threat landscape – which involves a constant monitoring of context and new threats.
To do this, you must be ready to deploy an incident response plan in an attack. And to be ready, regular mock exercises will ensure that your processes are right and that everyone involved in crisis management is aware of their roles and responsibilities. This agility is key to dealing with an attack by making the right decisions at the right time for the fastest possible recovery, while learning from the incident to harden protection.

5. COLLABORATION AND COMMUNICATION

Establishing effective communication channels and collaboration mechanisms both internally and externally is essential for cyber resilience. This involves coordination among different departments within the organization, as well as sharing threat intelligence and best practices with external partners and industry peers.

Also, breaking down internal silos to ease communication between security teams and other departments ensures a better and faster response in the event of a security incident.
In terms of external communication, collaboration and communication are also key to ensure a fast, coherent and transparent response for customers, press, investors, and other stakeholders in the event of an attack or security incident. Any in-house stakeholder must be able to identify which resource or people to call on, which validation circuits information must follow, and on which channels it must be shared.

6. EMPLOYEE TRAINING AND AWARENESS

Your people are crucial in preventing social engineering attacks and maintaining overall cyber resilience. This is why educating employees on cybersecurity best practices and creating a security-aware culture within the organization is essential. Indeed, human error remains the leading cause of data breaches, with 31% of enterprises pinpointing this as the root cause according to a study by Thales in 2023.

To maintain a high level of awareness and vigilance, plan regular cybersecurity training sessions about the threat landscape and run phishing simulations. Cybersecurity is a rich and fascinating subject that can be applied to a wide range of fields, from high tech to geopolitics - you're sure to find angles that speak to your teams, whatever their expertise and sensibilities.

7. GOVERNANCE AND LEADERSHIP

Establishing strong governance structures, policies, and leadership commitment to cybersecurity must be based on clear roles and responsibilities, risk management processes, and support from top management.

It's important to remember that cyber culture has to come from the top. Decision-makers must show a willingness to take the subject seriously. Whether they take it upon themselves or entrust it to others, it needs to be prioritized. In fact, it's not at the time of a crisis that security needs to be addressed, but rather on an ongoing basis, involving all teams.

In this sense, compliance with legal and regulatory obligations also has a role to play in guaranteeing an optimum level of upstream and downstream safety (NIS2, RGPD compliance...).

To this end, it's important to perform regular security audits to assess risks and identify vulnerabilities that attackers could try to exploit, with a view to prioritizing the work to be carried out by our technical and security teams.

Similarly, understanding the threats the organisation faces is critical to knowing what risks it needs to protect against and to being able to respond with the appropriate resources when needed.

harfanglab.io   Inside the Lab   @harfanglab   HarfangLab

PRESS CONTACT

Noémie Minster
PR & Communications Manager
noemie.minster@harfanglab.fr