opinionway'

FOR CESIN

Corporate Cybersecurity Barometer

Study report – Wave 11

January 2026

Credits: Photo by Josh Sorenson on Pexels

Crédits : benjamin-davies

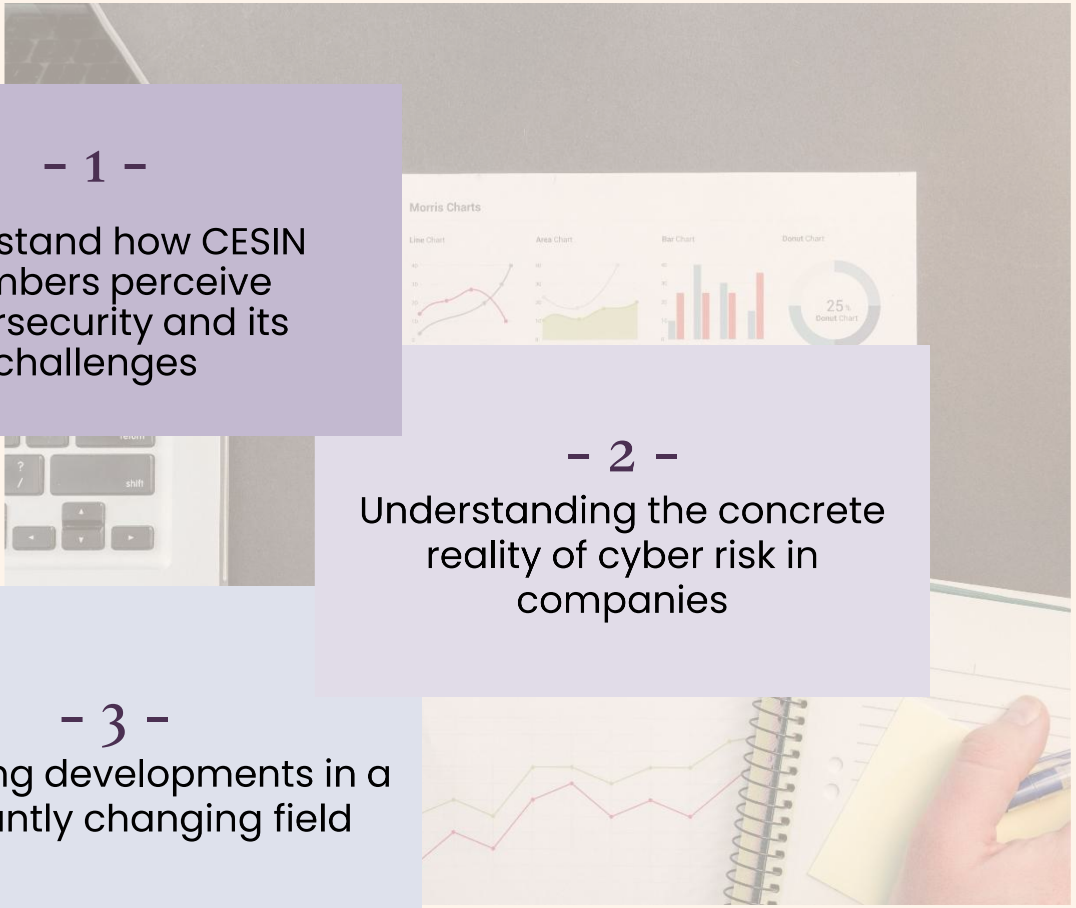
Objectives

The context

In 2015, CESIN launched its first major survey of its members in collaboration with OpinionWay.

This year, CESIN is launching the 11th wave of its cybersecurity barometer.

Objectives



- 1 -

Understand how CESIN members perceive cybersecurity and its challenges

- 2 -

Understanding the concrete reality of cyber risk in companies

- 3 -

Measuring developments in a constantly changing field

Photo by Lukas: https://www.pexels.com/fr-fr/photo/personne-tenant-un-stylo-a-bille-bleu-sur-un-ordinateur-portable-blanc-669610/

Crédits : dev-asangbam

Methodology

Methodology

Any publication, in whole or in part, must include the following complete statement:

"OpinionWay survey for CESIN"

and no part of the survey may be reproduced without this title.

Sample of **397 CESIN members**, based on the CESIN membership database.

The sample was interviewed by **online self-administered online questionnaire on a CAWI** (Computer Assisted Web Interview) system.

Questionnaire CESIN 2025

The interviews were conducted **from November 17 to December 12, 2025.**

OpinionWay conducted this survey in accordance with the procedures and rules of **ISO 20252**

afaq ISO 20252 Étude marketing et d'opinion AFNOR CERTIFICATION

The results of this survey should be read taking into account **the margins of uncertainty**: 4.9 points at most for a sample of 400 respondents.*

** Given the size of the sample, the results could vary by approximately plus or minus 4.9 points around the measured value, which represents the statistical uncertainty.*

Crédits : Adobe Stock

Sample profile

Sample profile

You are responding as:	
Group	46%
Independent company/administration	35%
Entity (management or entity) of a group	19%

Number of employees in the company	
Large companies	**40%**
50,000 employees or more	12%
Between 10,000 and 49,999 employees	16%
Between 5,000 and 9,999 employees	12%
Mid-sized companies	**43%**
Between 1,000 and 4,999 employees	26%
Between 250 and 999 employees	17%
VSE / SME (fewer than 250 employees)	**17%**

In which country is your company headquartered?	
France	93%
Germany	<1%
United Kingdom	<1%
United States	<1%
Sweden	<1%
Netherlands	<1%
Canada	<1%
Italy	<1%
Other countries	3%

What is your scope of activity?	
Only in my country	41%
European	17%
Internationally	42%

Credits: Icon from Storyset.com

Sample profile

Company's sector of activity	
Services	**40%**
Information and communication	20%
Financial and insurance activities	16%
Specialized, scientific, and technical activities	2%
Arts, entertainment, and recreation	1%
Real estate	1%
Industry/construction	**26%**
Manufacturing	13%
Construction	5%
Electricity, gas, steam, and air conditioning production and distribution	4%
Agriculture, forestry, and fishing	2%
Water supply, sewerage, waste management and remediation activities	2%
Mining and quarrying	<1%
Public services	**17%**
Public administration and defense, local government	9%
Human health and social work activities	7%
Education	1%
Trade	**13%**
Commerce	6%
Transportation and warehousing	5%
Accommodation and food services	2%
Other sectors	**4%**

Commerce sector	
B2B activities	16%
B2C activities	20%
B2B and B2C activities	64%

Credits: Icon from Storyset.com

Crédits : Adobe Stock

Results

opinionway

01

Significant cyberattacks are declining in volume, but their consequences for businesses are becoming more severe

Definition of a cyberattack

"A significant cyberattack, as defined in this survey, is when an organization is directly or indirectly targeted, through third parties, by a malicious act against all or part of its information system, impacting business processes by significantly compromising the confidentiality and/or integrity of the company's information or the availability of the information system. This cyberattack may have resulted in significant financial losses, damage to the company's image, regulatory sanctions, health or environmental impacts, and/or required significant defensive efforts to contain and deal with the attack. We do not include ***attempted*** *attacks that were stopped or mitigated by prevention, protection, and incident response systems."*

Four out of ten companies suffered at least one significant cyberattack in 2025, a figure that has fallen since last year and continues to decline year after year. Large companies are still the most targeted.

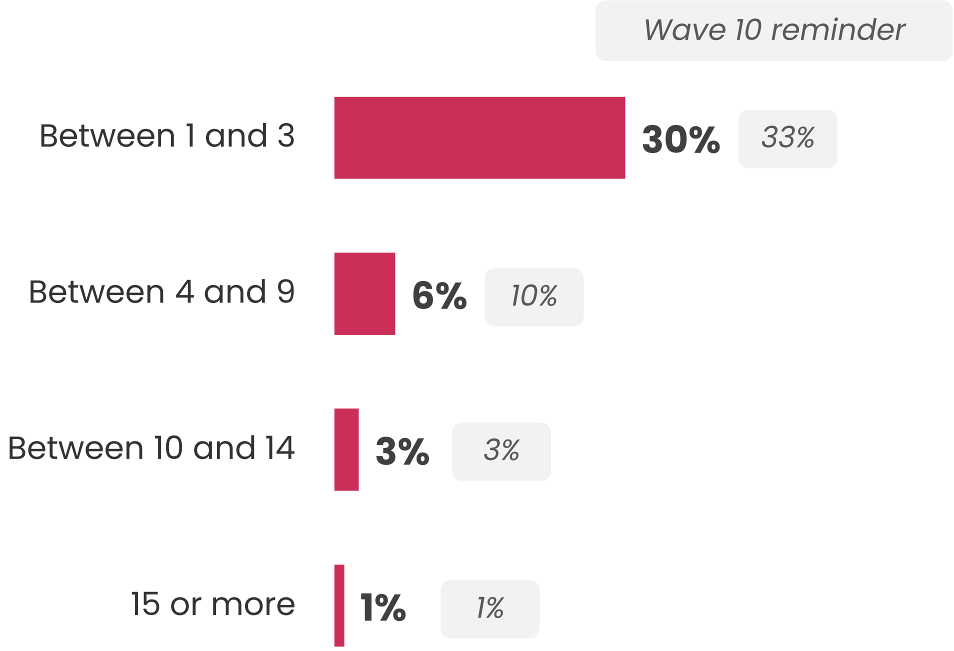
Q4. In total, how many **significant cyberattacks has your company suffered** in the last 12 months?

Base: all (397)

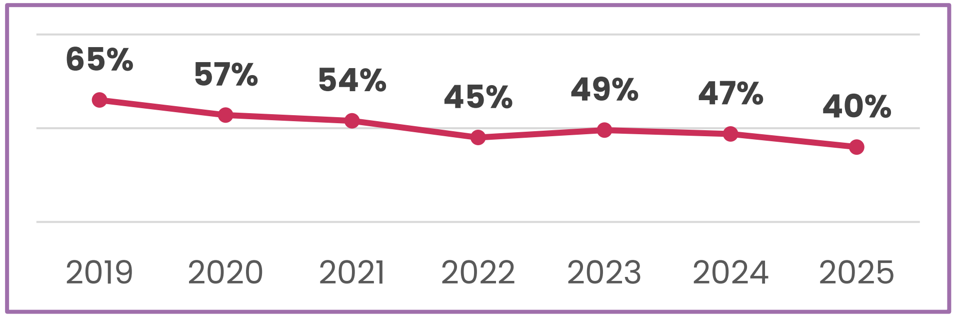
40% ↘ *(47%)*

of companies experienced at least one significant cyberattack

Large companies: **50%**
Mid-sized companies: **34%**



Previous waves reminder



↗ ↘ significantly higher/lower than the previous wave

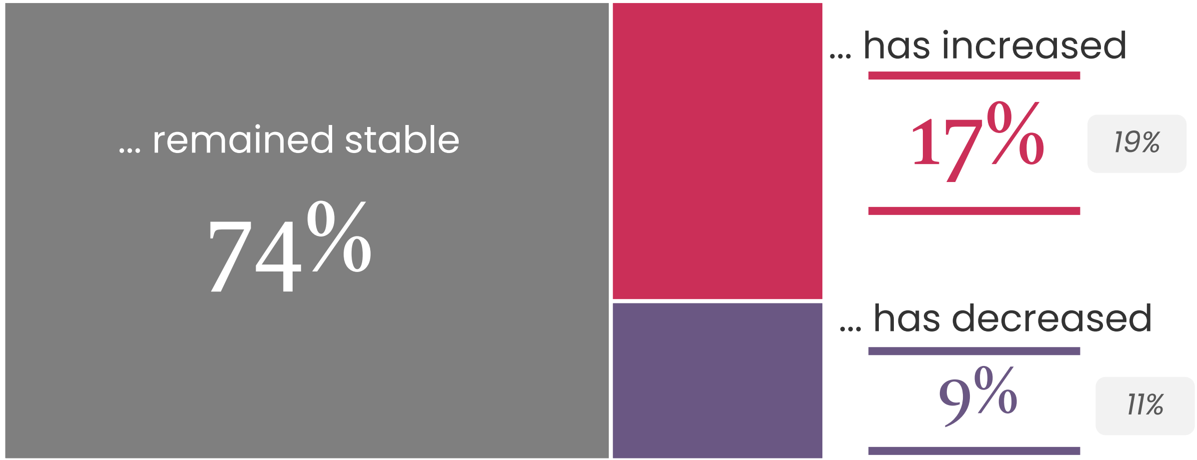
As with the previous wave, the number of attacks suffered remains stable for the majority of companies.

Q4bis. And compared to last year, **how has the number of attacks observed in your company** changed?

Base: all (397)

Among all companies

In one year, the number of attacks...

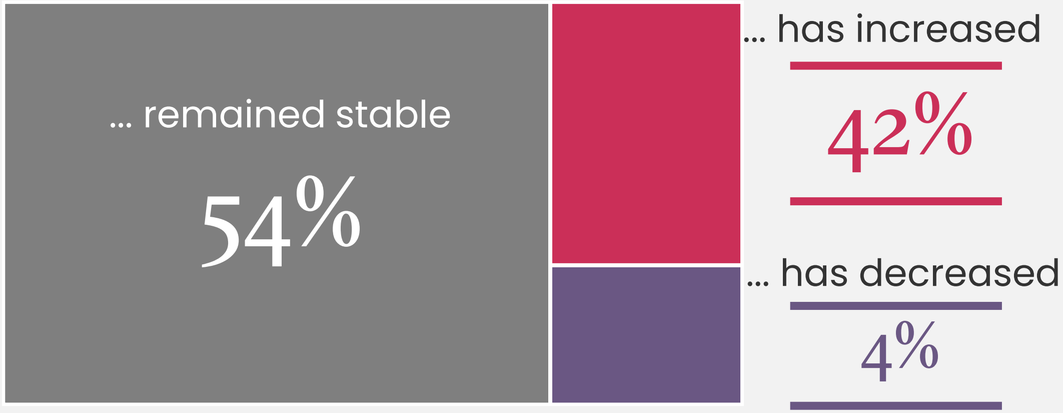


VSE/SME: **85%**

Wave 10 reminder *69%*

Among companies that have experienced at least one significant attack

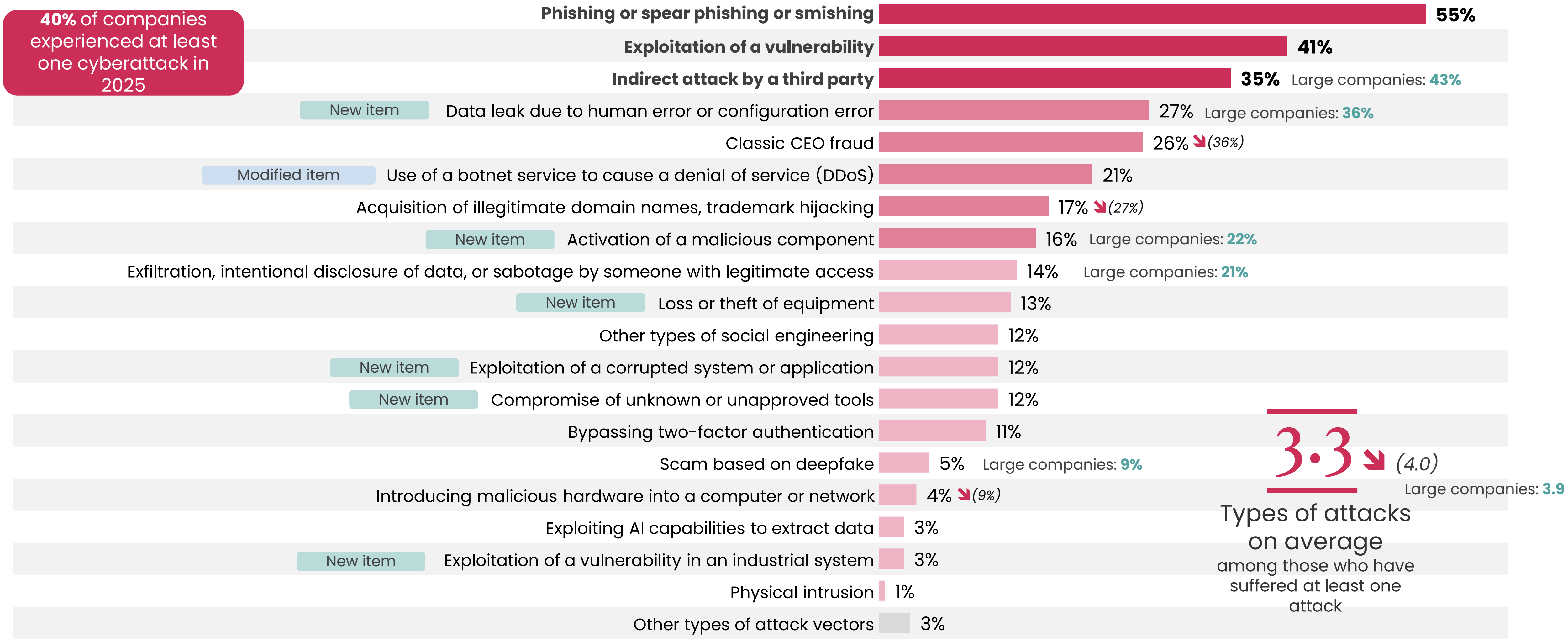
In one year, the number of attacks...



↗ ↘ significantly higher/lower than the previous wave

Despite the decline in the diversity of attack vectors, phishing, spear phishing, and smishing remain the most common, followed by vulnerability exploitation. Indirect attacks by third parties remain a priority vector, especially for large companies, while CEO fraud and domain name acquisition are on the decline.

Q5A. Of all the significant cyberattacks you have experienced in the last 12 months, indicate **the vectors that enabled these cyberattacks to start or spread**? *Base: have experienced an attack (159) - multiple answers possible*



40% of companies experienced at least one cyberattack in 2025

3.3 ↘ (4.0)
Large companies: 3.9

Types of attacks on average
among those who have suffered at least one attack

opinionway FOR CESIN

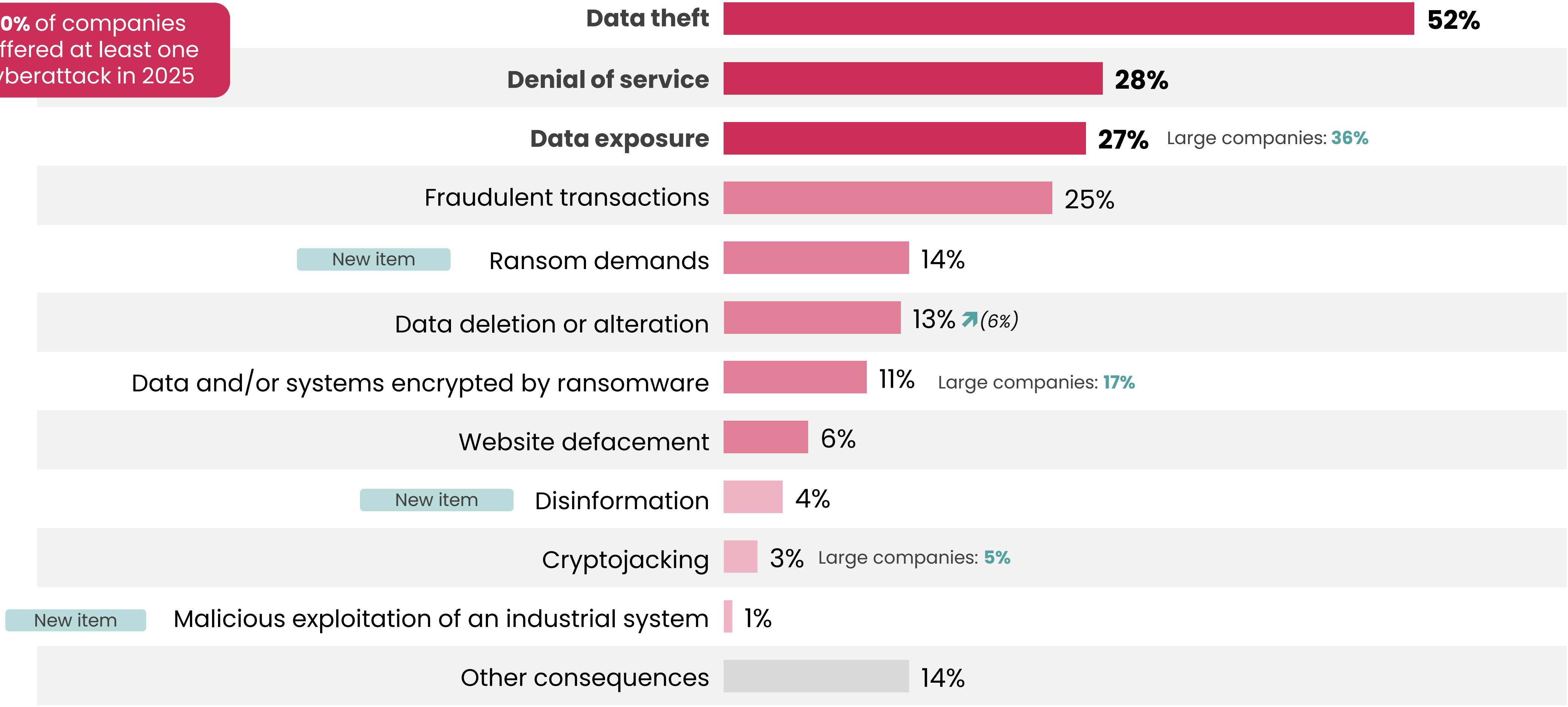
↗ ↘ significantly higher/lower than the previous wave

Data theft is by far the most common consequence of these cyberattacks. It should also be noted that data deletion or alteration is twice as common as in the previous year.

Q5B: What were **the technical consequences** of this/these cyberattack(s)?

Base: have experienced an attack (159) - multiple responses possible

40% of companies suffered at least one cyberattack in 2025



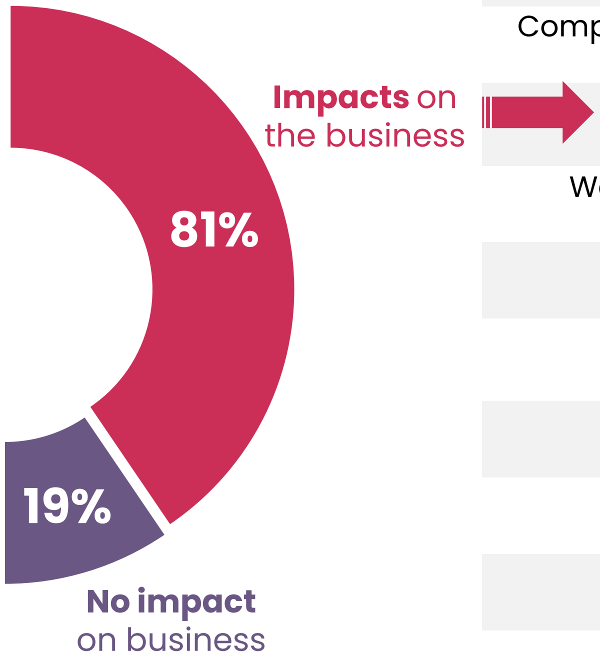
↗ ↘ significantly higher/lower than the previous wave

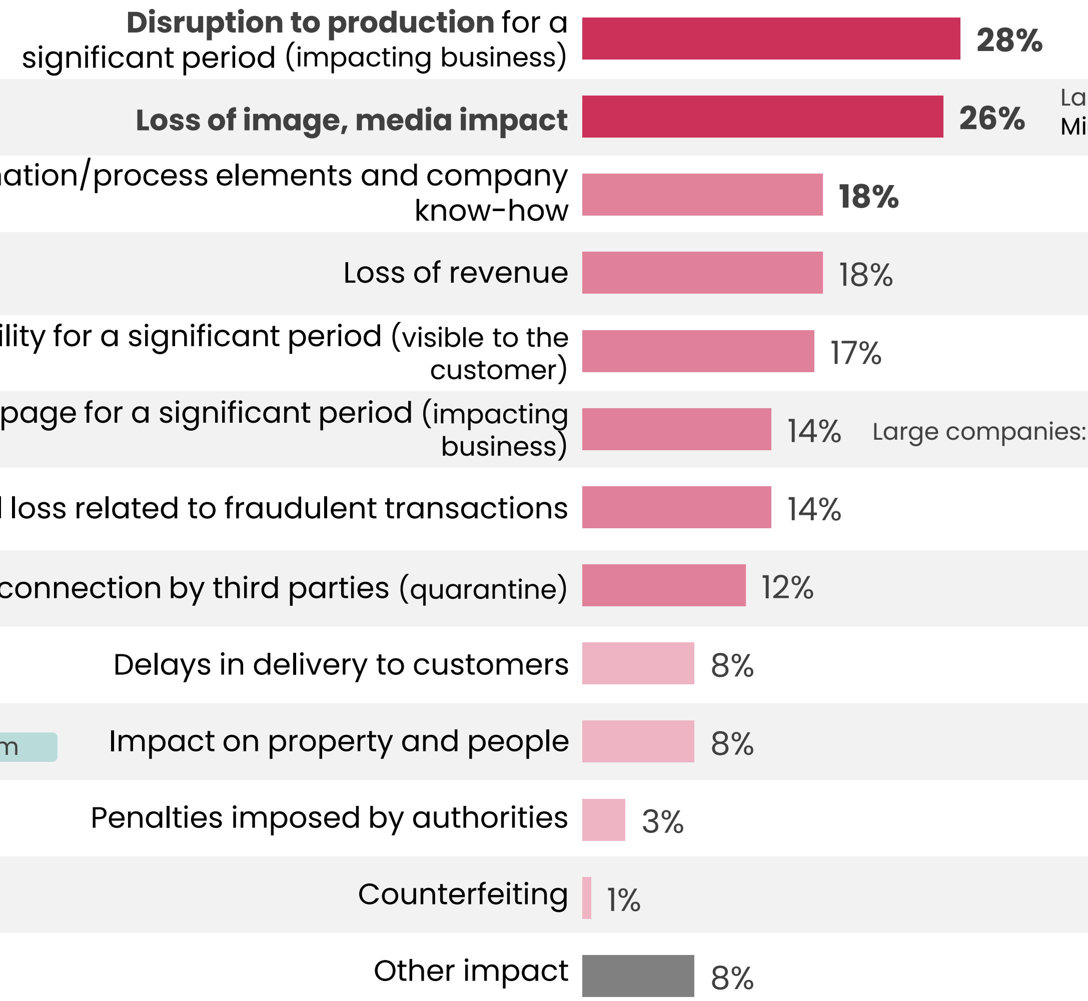
In 2025, significant cyberattacks had a major impact on businesses, affecting 4 out of 5 companies. These attacks most often resulted in production disruptions or damage to reputation.

Q7: What **impact** have **cyberattacks** had **on your business**?

Base: have experienced an attack (159)

Multiple answers possible





Large companies: : **36%**
Mid-sized companies: **14%**

Large companies: **20%**

opinionway FOR CESIN

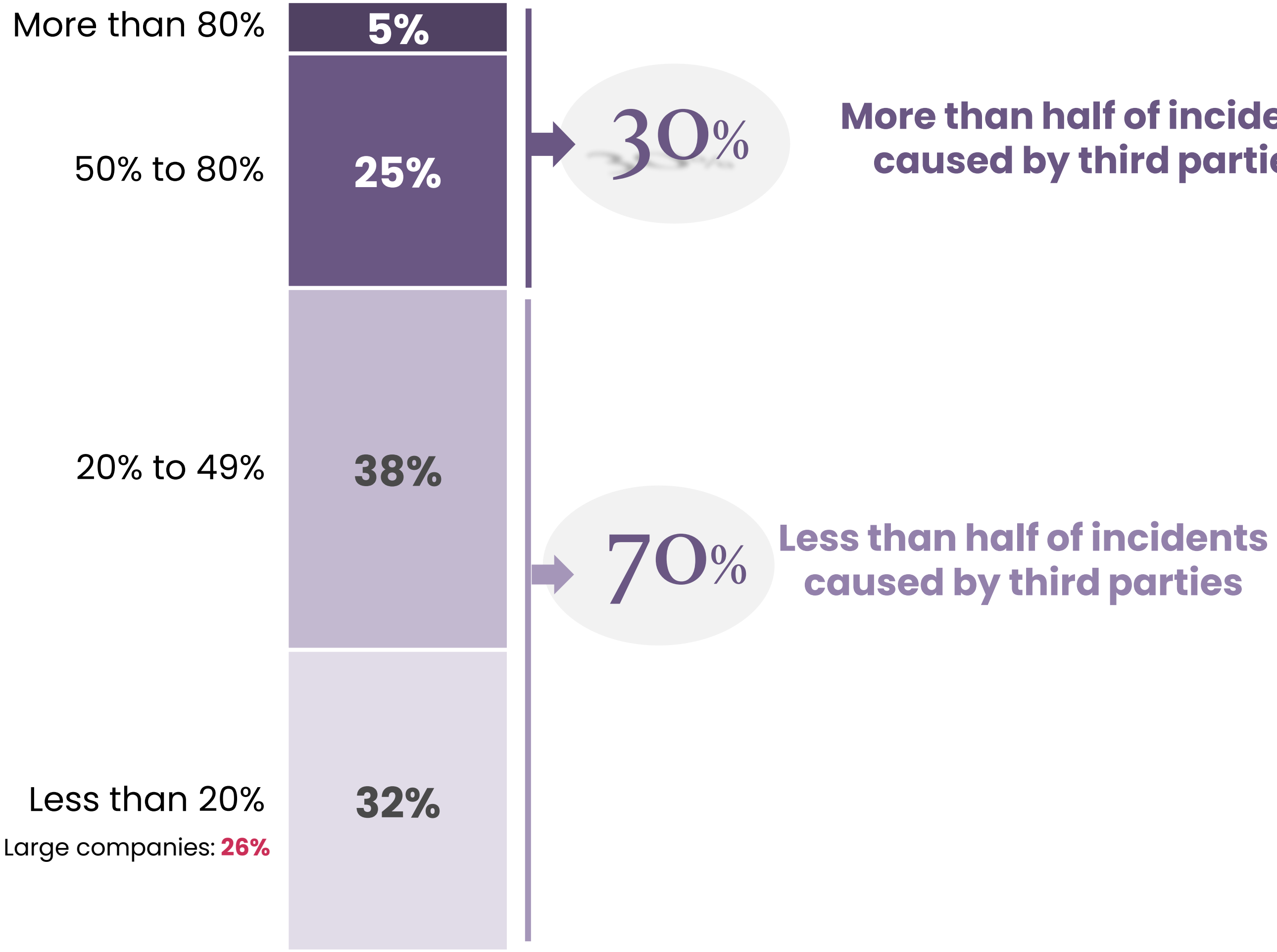
↗ ↘ significantly higher/lower than the previous wave

Nearly one-third of companies believe that more than half of cybersecurity incidents are caused by third parties.

New question in 2025

Q52: How high do you estimate **the ratio of cybersecurity incidents caused by third parties** (IT and non-IT third parties) to be?

Base: all (397)



Large companies: **26%**

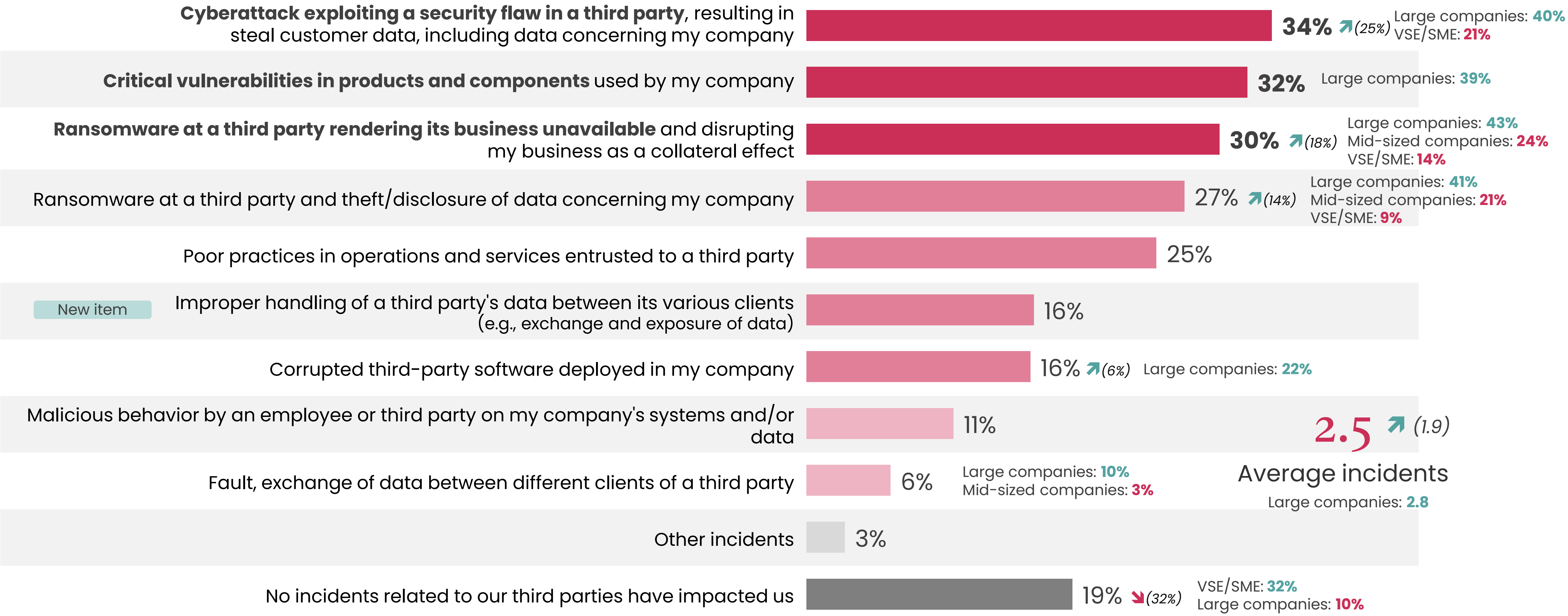
More than half of incidents caused by third parties

Less than half of incidents caused by third parties

In general, companies are identifying more incidents involving third parties than in previous years. Among these, cyberattacks exploiting a security flaw in a third party are the most common.

Q40: Which **incidents involving your third parties have impacted you**?

Base: all (397) – Multiple responses possible

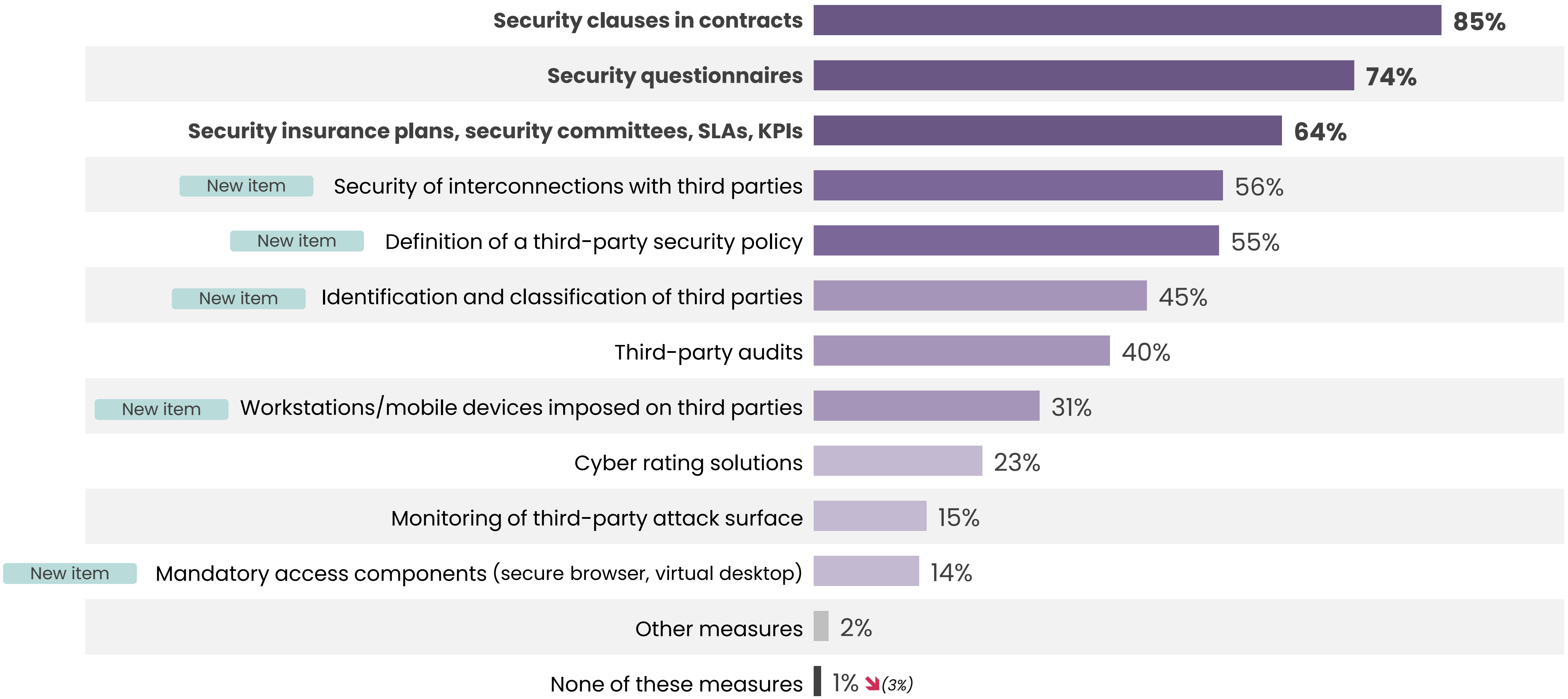


↗ ↘ significantly higher/lower than the previous wave

To limit these risks, security clauses in contracts, security questionnaires, and security insurance plans are the main measures put in place.

Q43: What **measures** have you taken **to address third-party risk**?

Base: all (397) – Multiple responses possible

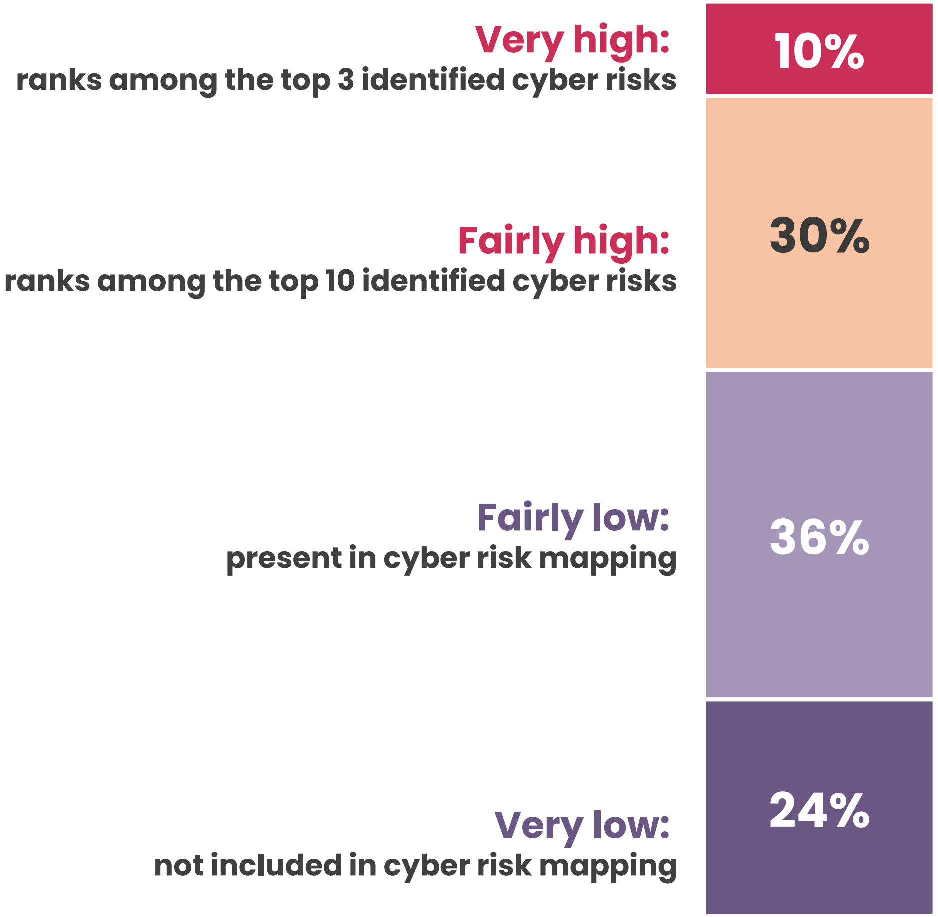


↗ ↘ significantly higher/lower than the previous wave

In 2025, 4 out of 10 companies consider the level of threats related to cyber espionage to be high, regardless of their structure.

Q9: How would you rate **the level of cyber espionage threats** to your company today, among all your cyber risks?

Base: all (397)



40% **Estimate a high level of threats related to cyber espionage**

Wave 10 reminder *37%*

Credits: Icon from Storyset.com

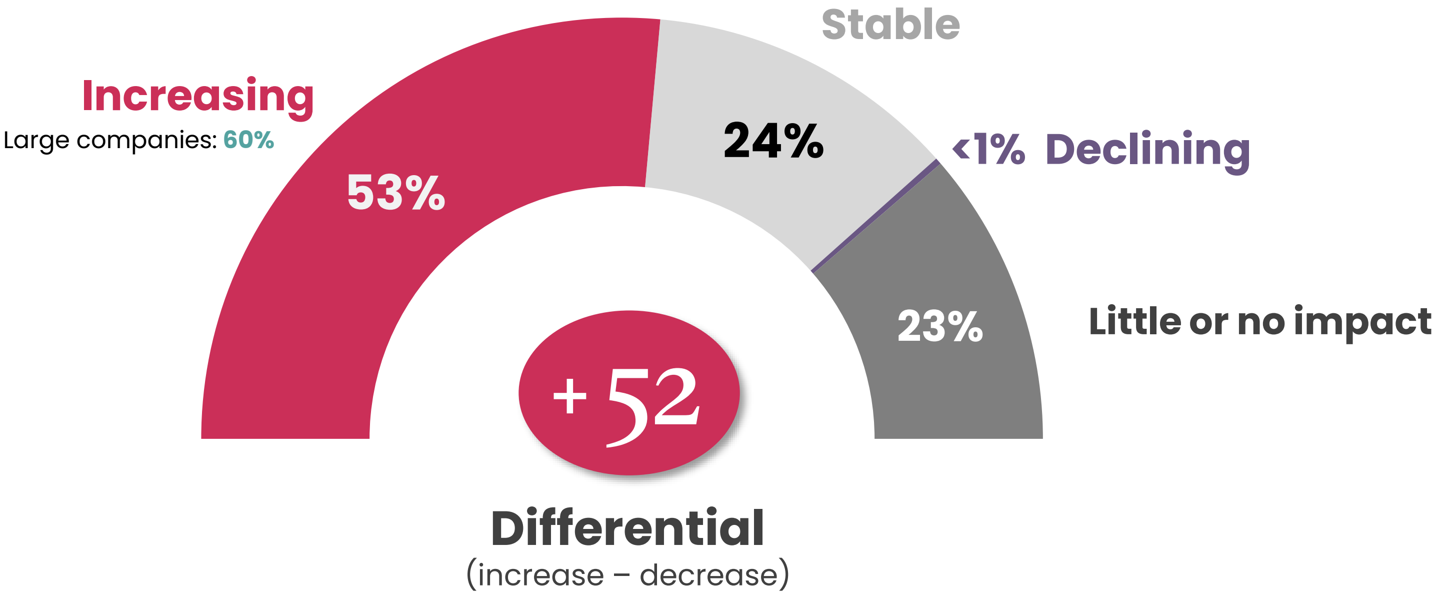
↗ ↘ significantly higher/lower than the previous wave

Half of companies believe that threats originating from states, linked to the global geopolitical context, are on the rise.

New question in 2025

Q51: In a tense geopolitical context, how do you assess **the evolution of the threat from state actors** to your company?

Base: all (397)



Credits: Icon from Storyset.com

02

Well-equipped and proactive companies facing cyber threats

The security solutions on the market are tailored to the needs of the vast majority of companies. This is especially true for large companies.

Q25: Do you think that **the security solutions and services available on the market are suited** to your company?

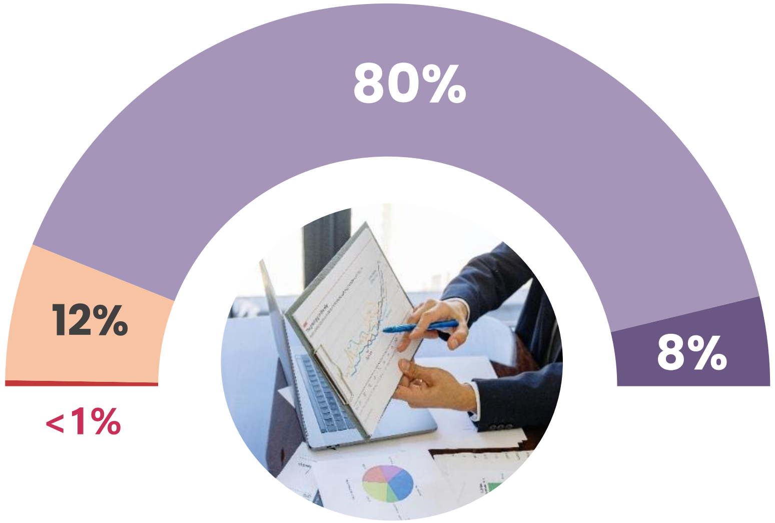
Base: all (397)

Wave 10 reminder

🟥 Not at all suited 🟧 Somewhat unsuitable 🟪 Somewhat suitable 🟪 Completely suitable

% Not suitable

16% 12%

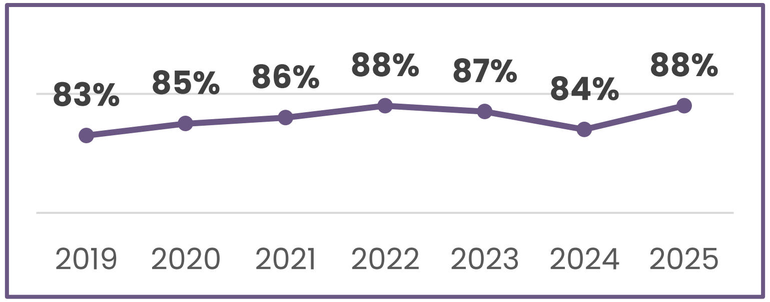


% Suitable

88%

Large companies: **92%**

Previous waves reminder

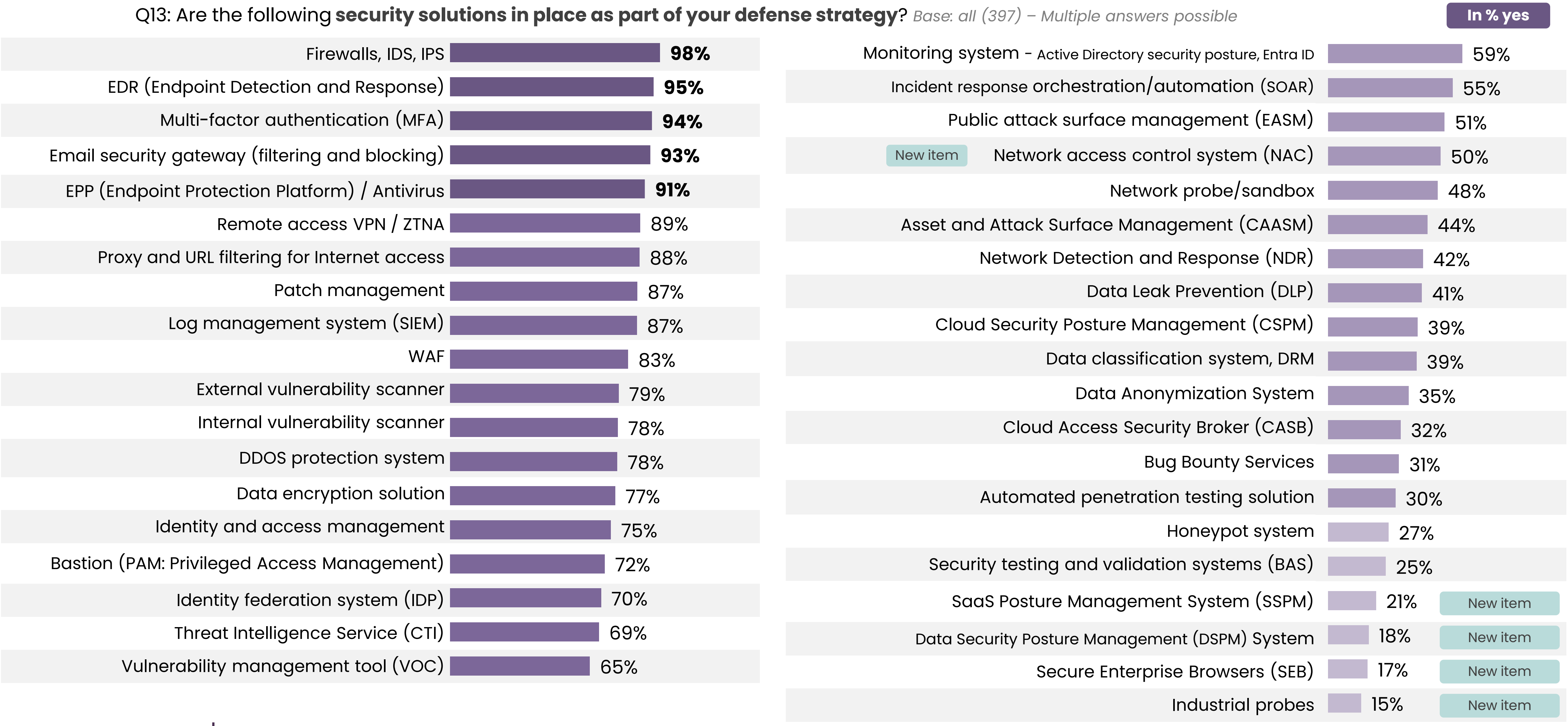


↗ ↘ significantly higher/lower than the previous wave

Credits: Photo by Anthony Shkraba on Pexels.com

The trio of firewalls, EDR, and MFA remain the most widely used solutions in businesses.

Q13: Are the following **security solutions in place as part of your defense strategy?** *Base: all (397) – Multiple answers possible*



Details of security solutions implementation

Question modified in 2025

Q13: Are the following **security solutions in place as part of your defense strategy**?

Base: all (397)

	Total Deployed in the company	Yes, and it has high value	Yes, and it has medium value	Yes, but it has low or no value	This solution is not deployed	This solution is in the planning stage
Firewalls, IDS, IPS	98%	76%	19%	3%	2%	0%
EDR (Endpoint Detection and Response)	95%	87%	7%	1%	1%	4%
Multi-factor authentication (MFA)	94%	85%	8%	1%	1%	5%
Email security gateway (filtering and blocking)	93%	72%	18%	3%	5%	2%
EPP (Endpoint Protection Platform) / Antivirus	91%	73%	15%	3%	9%	-%
Remote access VPN / ZTNA (Zero Trust Network Access)	89%	63%	23%	3%	4%	7%
Proxy and URL filtering for Internet access (SWG: Secure Web Gateway)	88%	59%	25%	4%	9%	3%
Patch management	87%	58%	26%	3%	7%	6%
Log management system (SIEM)	87%	64%	19%	4%	5%	8%
WAF (Web Application Firewall)	83%	50%	27%	6%	13%	4%
External vulnerability scanner	79%	44%	30%	5%	16%	5%
Internal vulnerability scanner	78%	43%	28%	7%	13%	9%
DDOS protection system	78%	38%	30%	10%	19%	3%
Data encryption solution	77%	37%	30%	10%	17%	6%
Identity and access management (identity governance)	75%	52%	20%	3%	9%	16%
Bastion (PAM: Privilege Access Management)	72%	48%	20%	4%	12%	16%
Identity federation system (IDP)	70%	49%	19%	2%	20%	10%
Threat Intelligence Service (CTI)	69%	32%	28%	9%	20%	11%
Vulnerability management tool (VOC)	65%	37%	23%	5%	21%	14%

Details of security solutions implementation

Question modified in 2025

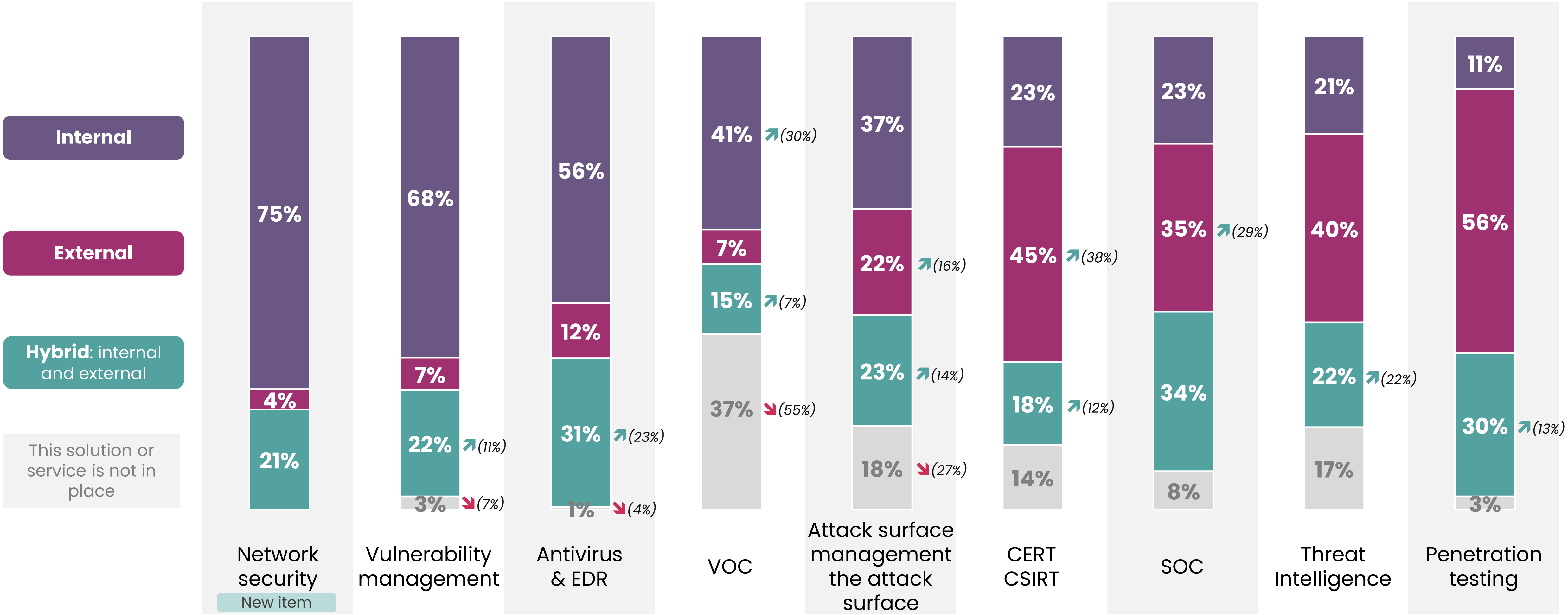
Q13: Are the following **security solutions in place as part of your defense strategy**?

Base: all (397)

	Total Deployed in the company	Yes, and it has high value	Yes, and it has medium value	Yes, but it has low or no value	This solution is not deployed	This solution is in the planning stages
Security posture monitoring system Active Directory, Entra ID (ISPM)	59%	35%	20%	4%	30%	11%
Incident response orchestration and automation (SOAR)	55%	31%	18%	6%	29%	16%
Public attack surface management (EASM)	51%	21%	23%	7%	38%	11%
Network Access Control (NAC) system	50%	27%	18%	5%	33%	17%
Network probe/sandbox	48%	17%	22%	9%	44%	8%
Asset and Attack Surface Management (CAASM)	44%	15%	20%	9%	46%	10%
Network Detection & Response (NDR) system	42%	19%	17%	6%	43%	15%
Data Leakage Prevention (DLP) System	41%	15%	17%	9%	33%	26%
Cloud Security Posture Management (CSPM)	39%	20%	13%	6%	45%	16%
Data classification system, DRM	39%	10%	16%	13%	41%	20%
Data anonymization system	35%	8%	17%	10%	53%	12%
Cloud Access Security Broker (CASB)	32%	12%	15%	5%	54%	14%
Bug Bounty Services	31%	14%	12%	5%	57%	12%
Automated intrusion testing solution	30%	11%	14%	5%	53%	17%
Honeypot system	27%	6%	11%	10%	63%	10%
Safety testing and validation systems (BAS)	25%	9%	13%	3%	64%	11%
Saas Posture Monitoring System (SSPM)	21%	7%	11%	3%	65%	14%
Data Security Posture Management (DSPM) system	18%	5%	9%	4%	68%	14%
Secure Enterprise Browsers (SEB)	17%	5%	9%	3%	71%	12%
Industrial probes	15%	6%	6%	3%	73%	12%

While management methods vary depending on the solution, intrusion testing, threat intelligence, SOC, and CERT/CSIRT are mainly managed externally.

Q30b: **How do you operate the** following **cybersecurity solutions and services?** *Base: all (397)*



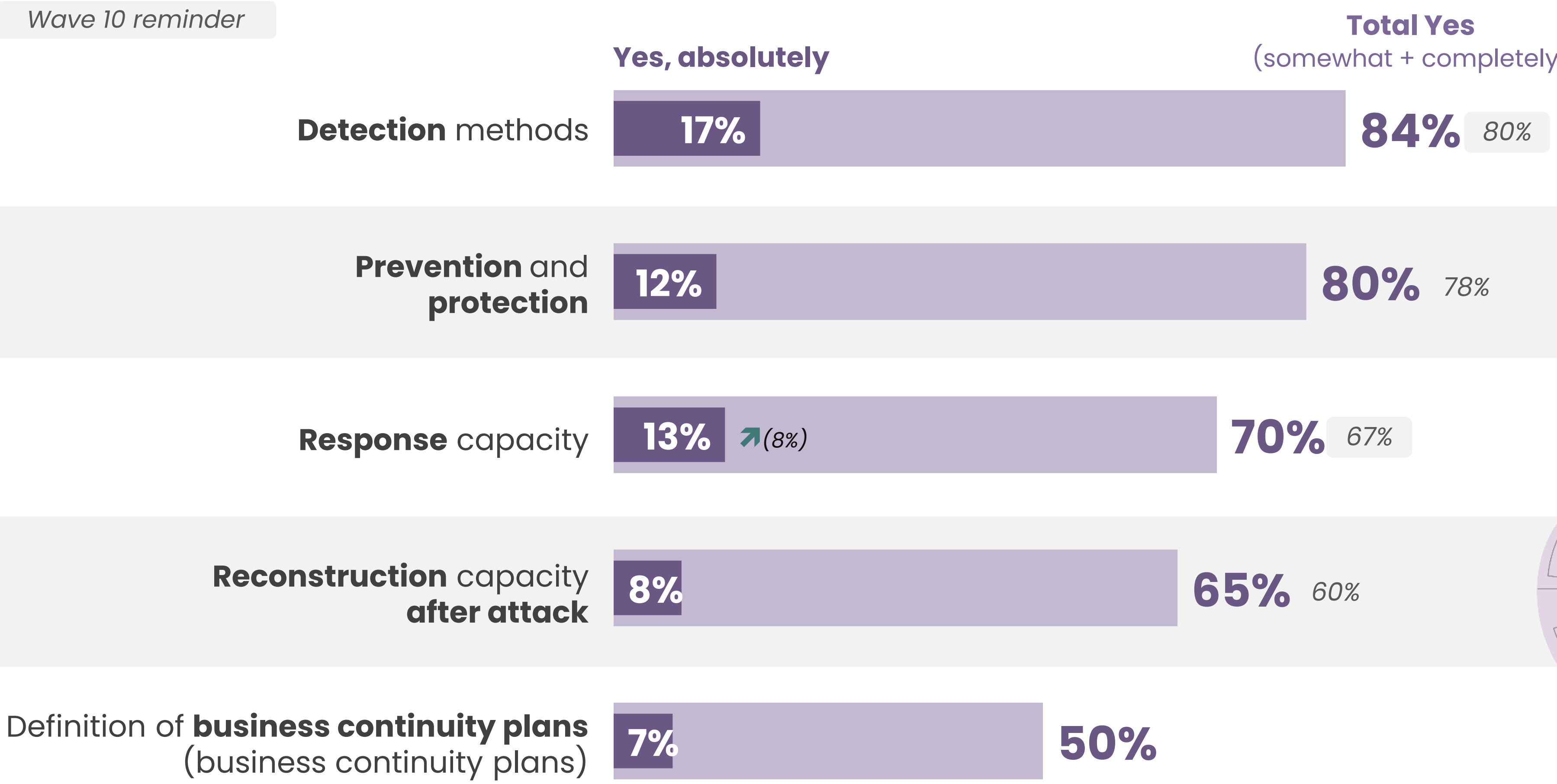
opinionway FOR CESIN

↗ ↘ significantly higher/lower than the previous wave

As in the previous survey, companies say they are better prepared to manage cyberattacks upstream than downstream. However, the definition of business continuity plans, which was newly evaluated this year, is much less developed.

Q14: In your opinion, is your company **prepared to manage a large-scale cyberattack** in terms of…?

Base: all (397)



↗ ↘ significantly higher/lower than the previous wave

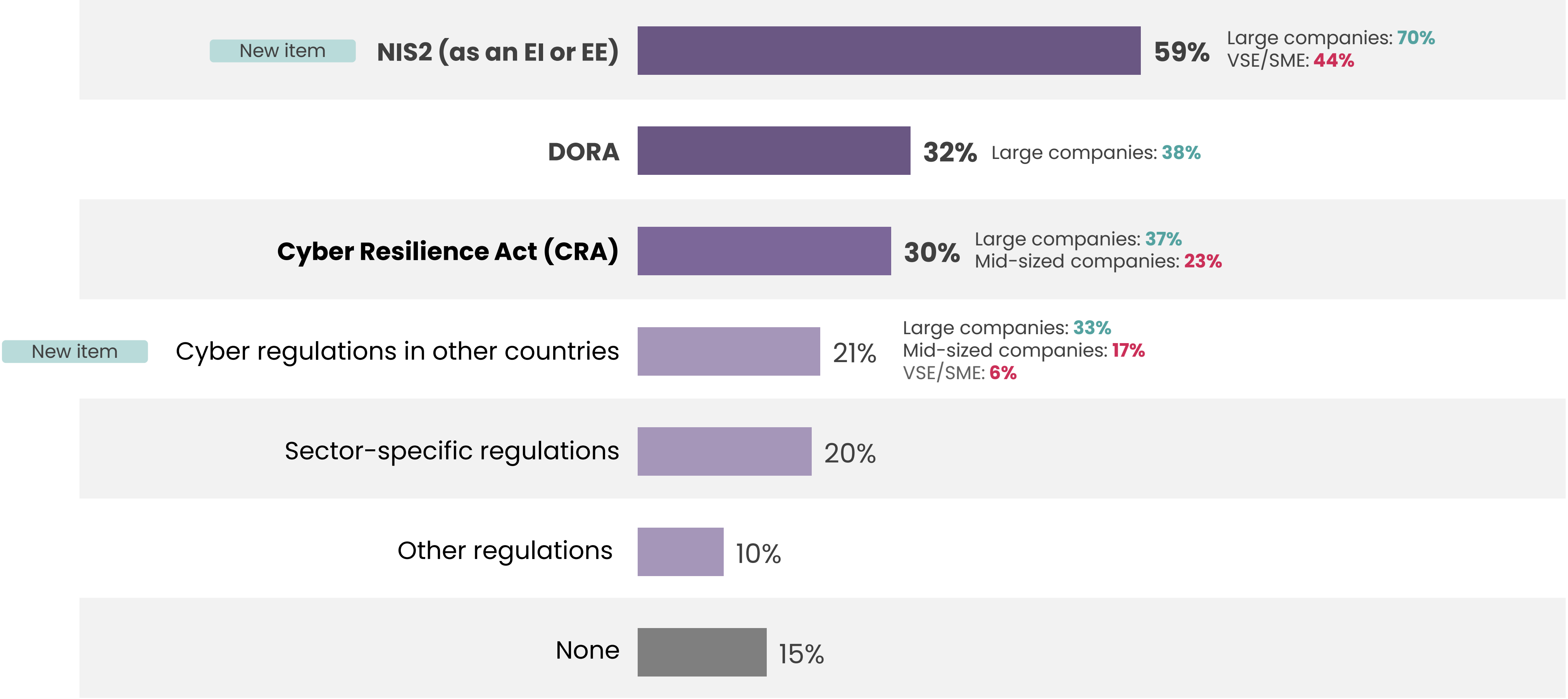
Credits: Icon from Storyset.com

Unsurprisingly, NIS2 regulations are the most widespread, ranking ahead of DORA and CRA.

Question modified in 2025

Q47: Which of these **cyber regulations** affect your company?

Base: all (397) – Multiple answers possible

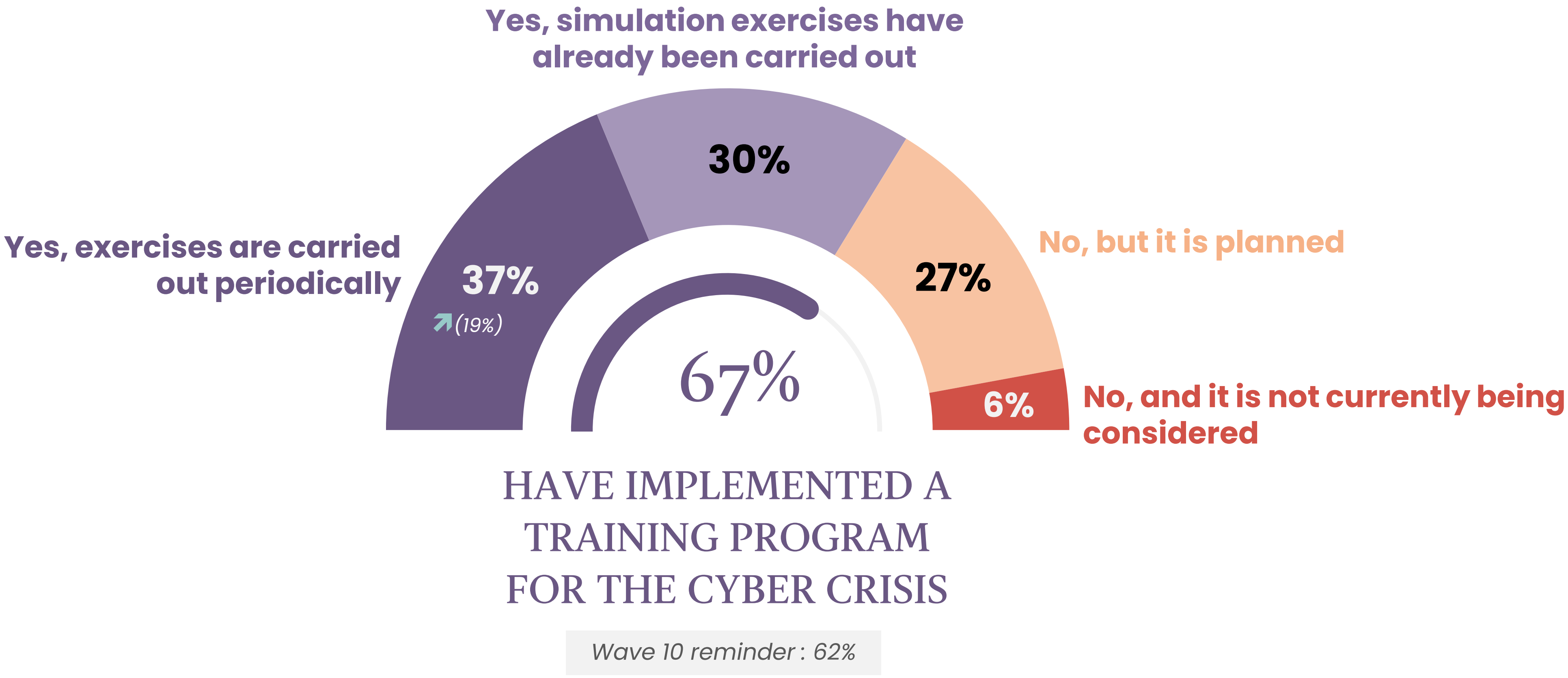


↗ ↘ significantly higher/lower than the previous wave

Two-thirds of companies have implemented a cyber crisis training program, and even more have implemented periodic exercises.

Q15: Has your company implemented **a cyber crisis management training program**?

Base: all (397)



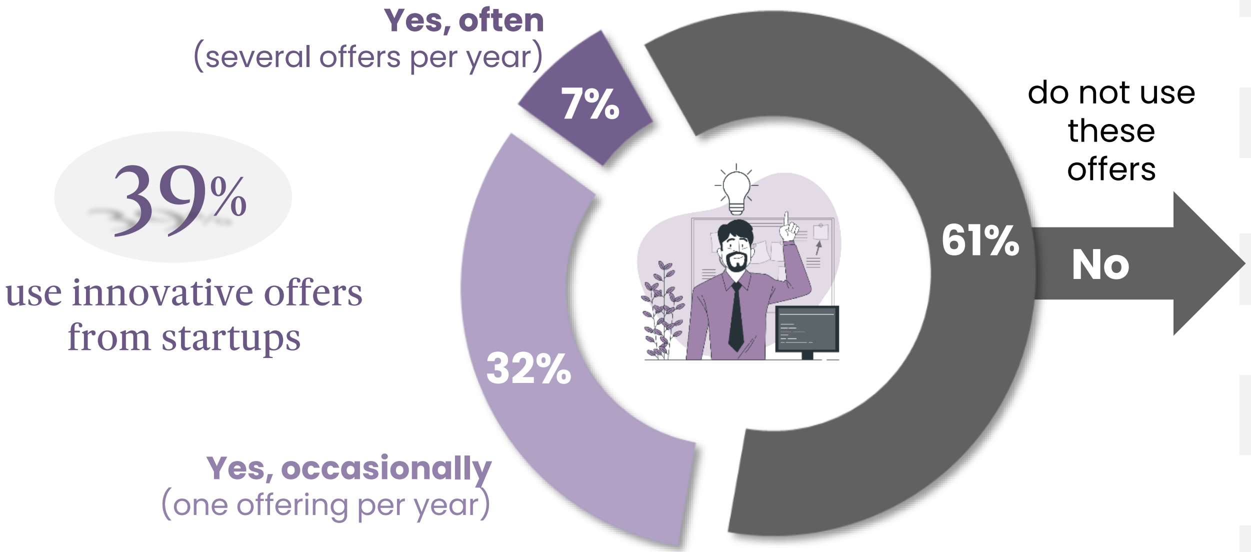
Credits: Icon from Storyset.com

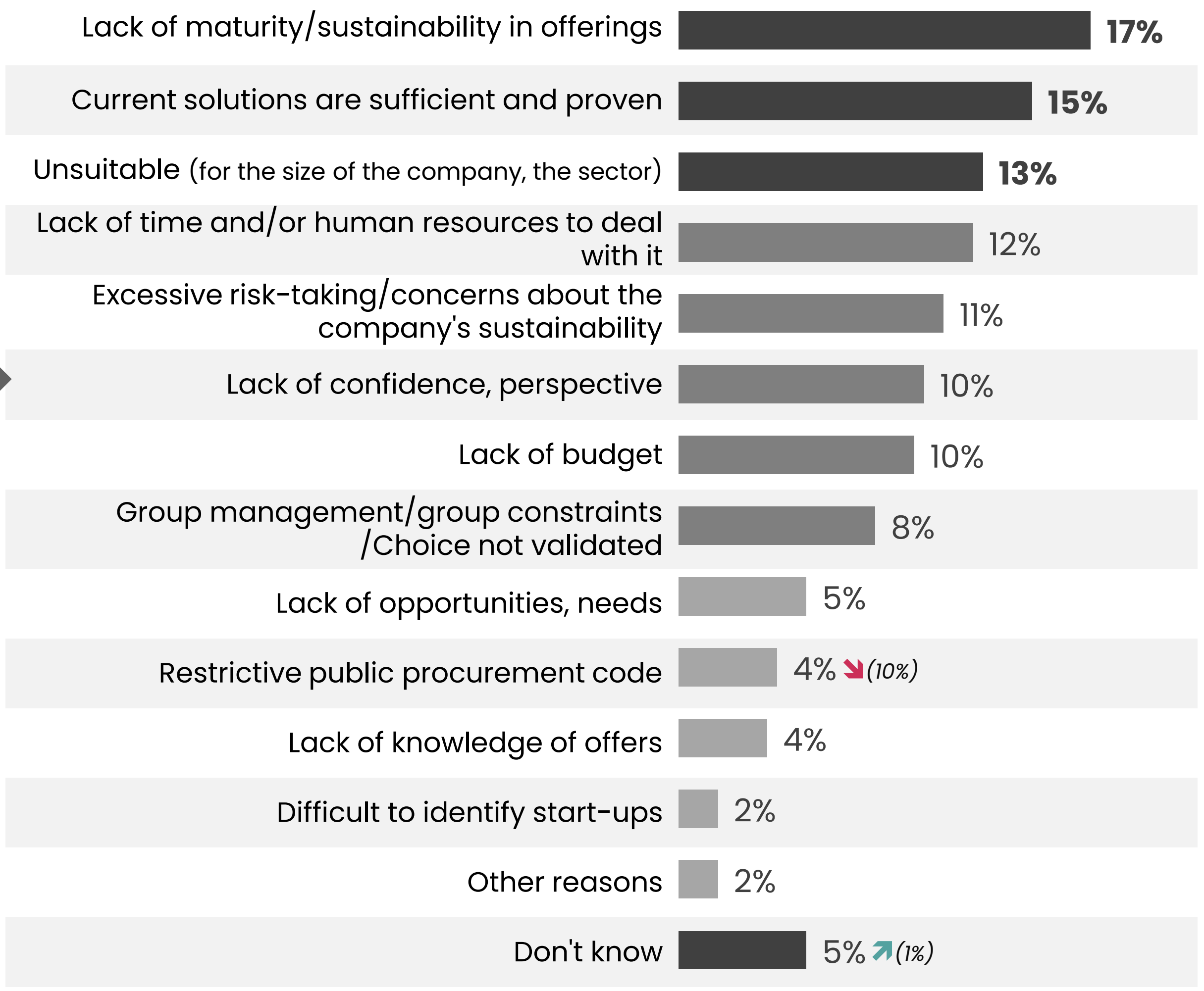
↗ ↘ significantly higher/lower than the previous wave

Four out of ten companies use innovative offerings from start-ups. For those that do not, it is most often due to a lack of maturity of the offering or satisfaction with current solutions.

Q26: When it comes to cybersecurity, do you use **innovative offerings from start-ups**? *Base: all (397)*

Q26b: Why don't you do so? *Base: do not use offerings from start-ups – excluding non-respondents (242)*





↗ ↘ significantly higher/lower than the previous wave

Most companies believe they have a complete and up-to-date view of their digital assets.

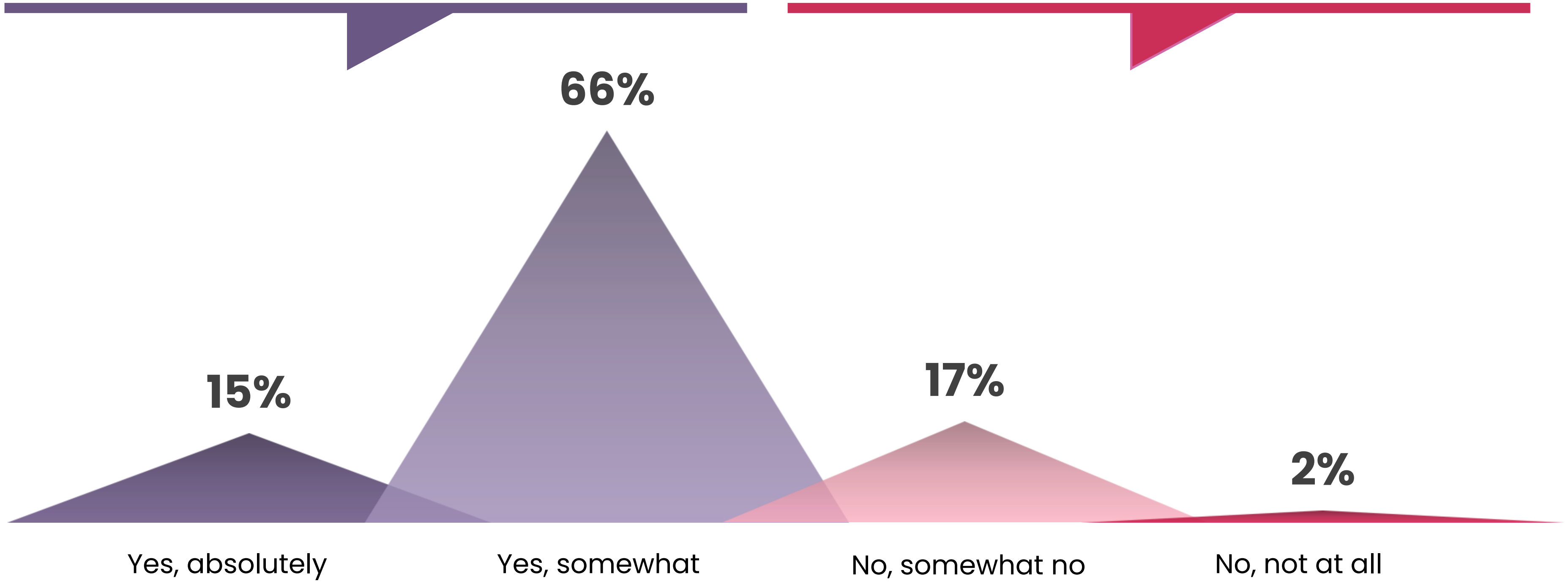
Question modified in 2025

Q41: Do you have **a complete and up-to-date view of your digital assets** (applications, infrastructure, endpoints, networks, etc.)?

Base: all (397)

81% **have a complete and up-to-date view** of their digital assets

Do not have a complete and up-to-date view of their digital assets 19%



opinionway FOR CESIN

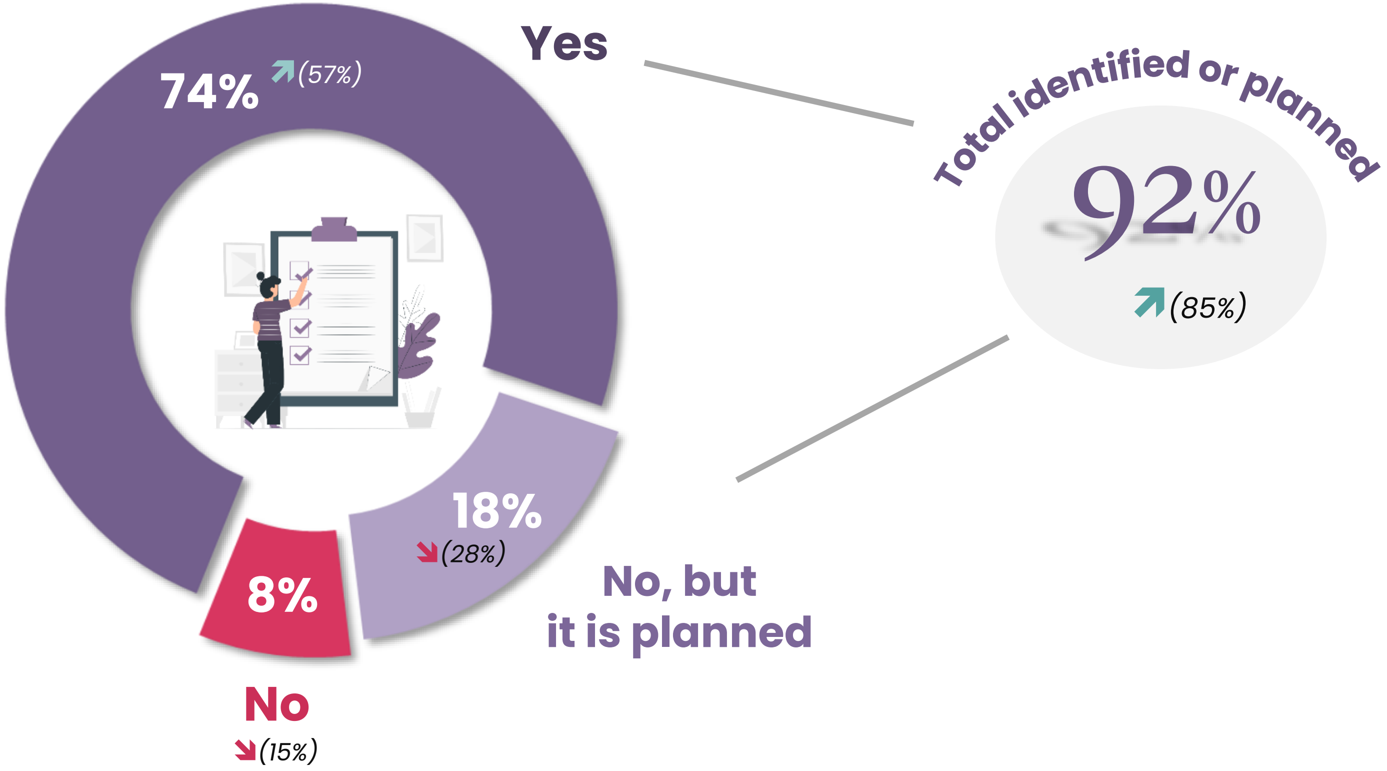
↗ ↘ significantly higher/lower than the previous wave

Since last year, the number of companies that have identified their digital assets has increased significantly.

Question modified in 2025

Q42: Have you **clearly identified your critical digital assets** ("crown jewels")?

Base: all (397)



Be careful with the interpretation, as until now we have been talking about identifying « crown jewels », so the change in wording may introduce a bias.

Credits: Icon from Storyset.com

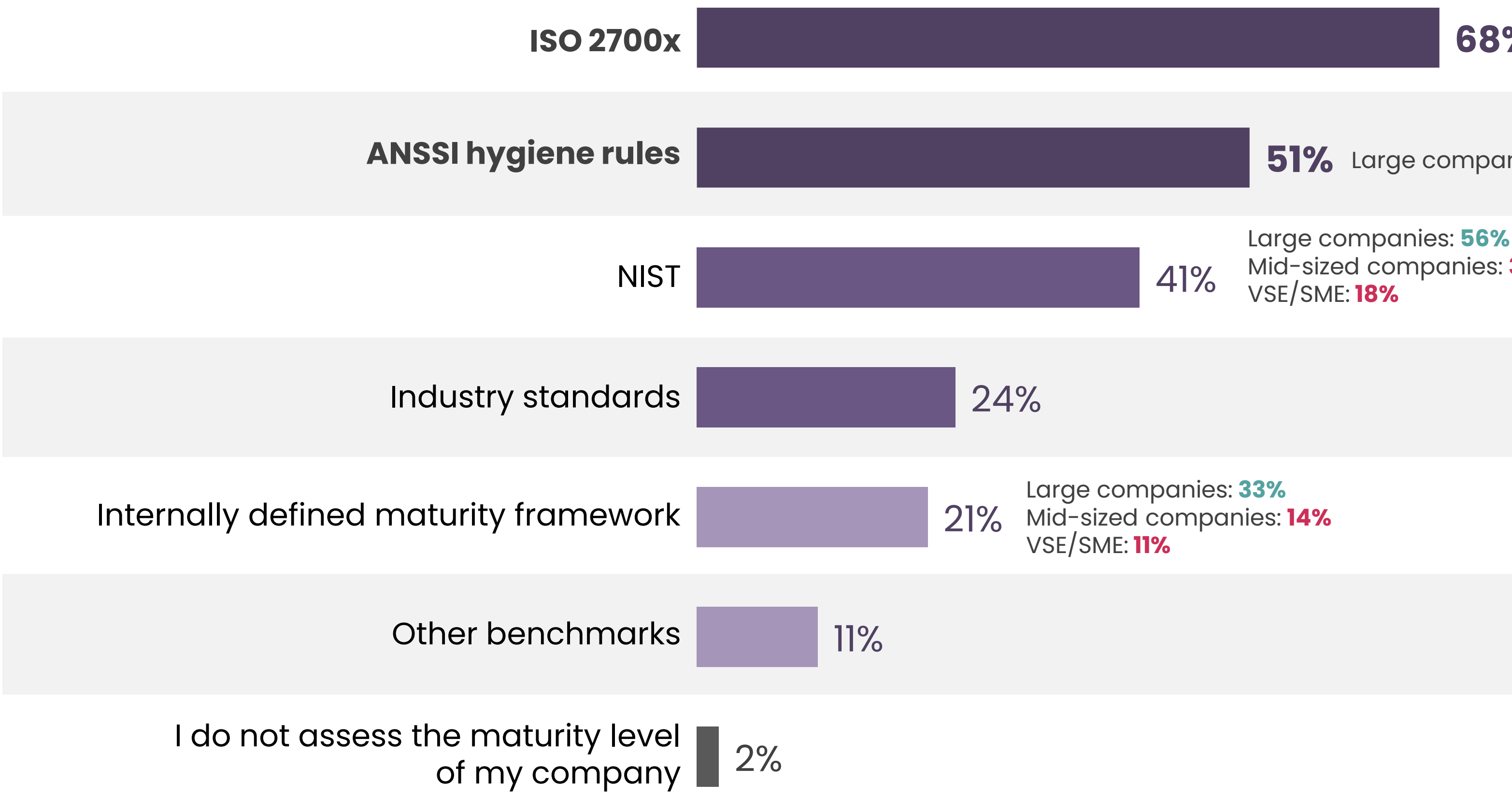
↗ ↘ significantly higher/lower than the previous wave

Almost all companies assess their maturity level, most often using the ISO 2700x standard. Large companies, which consult more standards, rely in particular on NIST or internally defined standards.

New question in 2025

Q54: Which standard(s) do you use to assess your company's **maturity level**?

Base: all (397) – Multiple answers possible

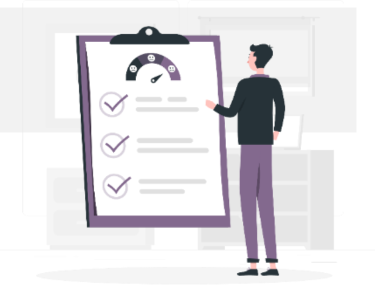


ISO 2700x: VSE/SME: **85%**
Large companies: **62%**

ANSSI hygiene rules: Large companies: **43%**

NIST: Large companies: **56%**
Mid-sized companies: **34%**
VSE/SME: **18%**

Internally defined maturity framework: Large companies: **33%**
Mid-sized companies: **14%**
VSE/SME: **11%**



Average number of responses cited: **2.2**

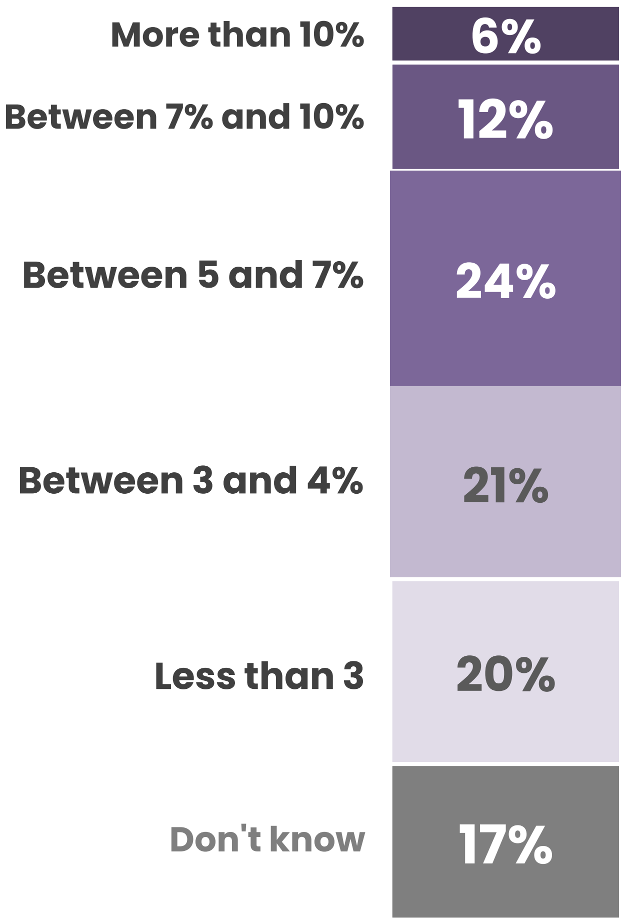
Large companies: **2.3**

Credits: Icon from Storyset.com

For the first time in three years, there has been a downward trend in the number of companies spending 5% or more of their IT/digital budget on cybersecurity.

Q18: In your company, **what proportion of the IT/digital budget is devoted to security**?

Base: all (397)



VSE/SME: **13%**

5% or more of the IT/digital budget is devoted to security:

42%

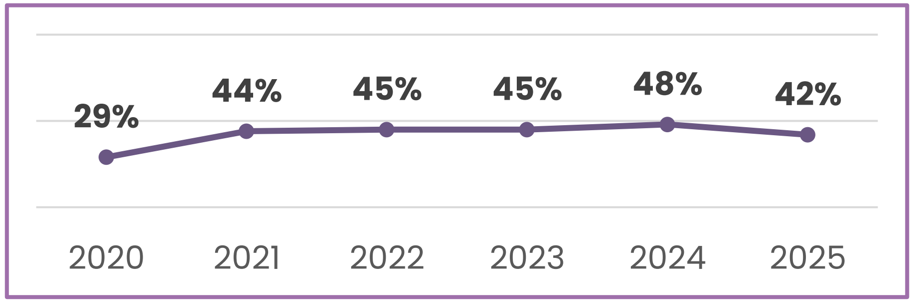
Large companies: **31%**

Mid-sized companies: **25%**

↗ *(11%)*

Wave 10 reminder : 48%

Previous waves reminder



↗ ↘ significantly higher/lower than the previous wave

03

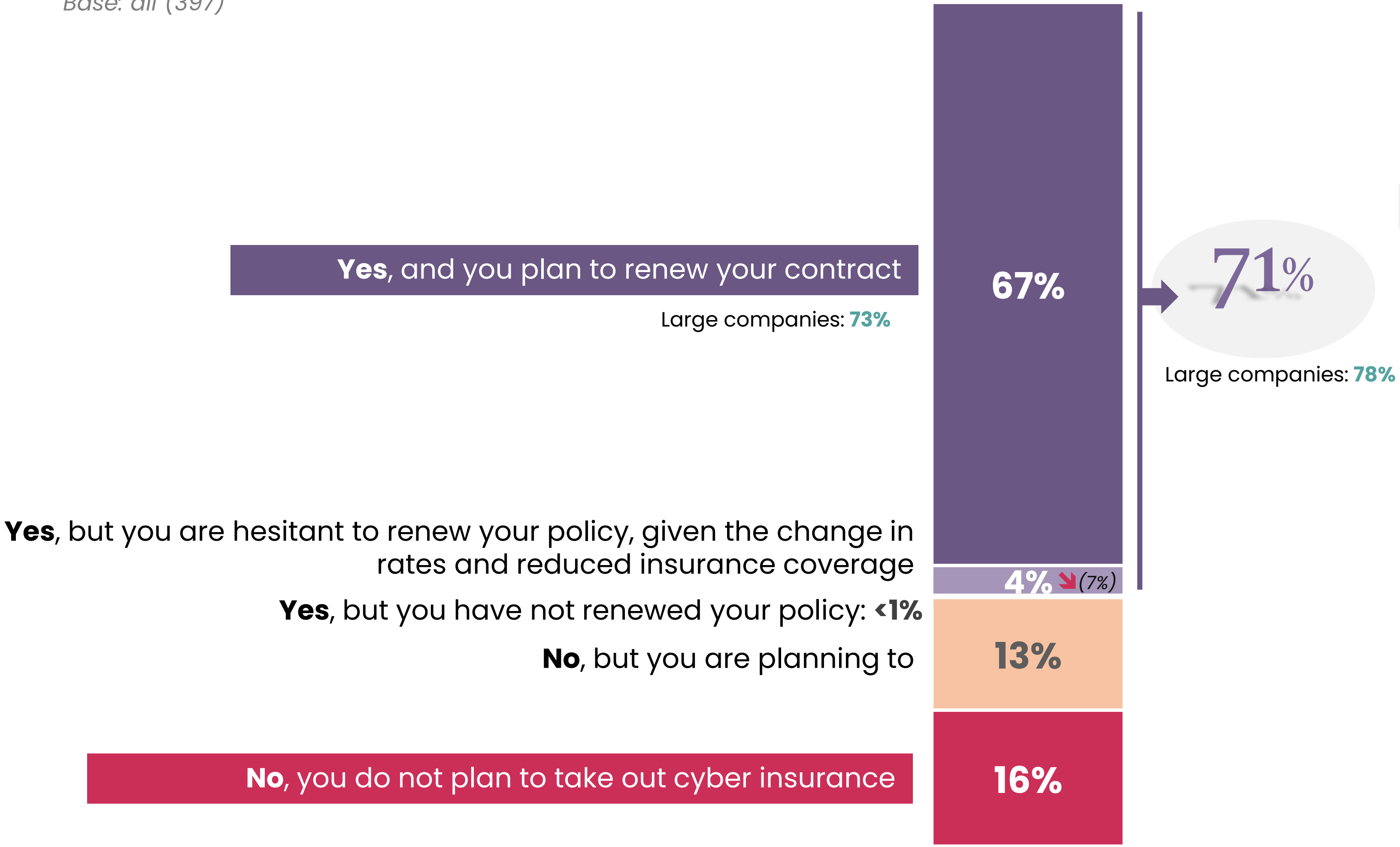
Focus on ...

Cyber insurance

Seven out of ten companies have taken out cyber insurance, and almost all of them plan to renew their policies.

Q31: Have you **taken out cyber insurance**?

Base: all (397)



Wave 10 reminder : 72%

Have taken out cyber insurance

Credits: Icon from Storyset.com

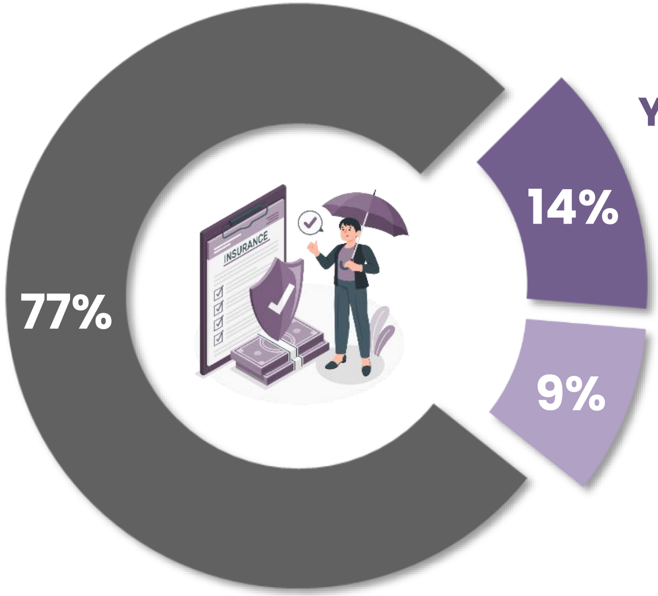
↗ ↘ significantly higher/lower than the previous wave

And as in 2025, nearly 1 in 4 companies with cyber insurance made a claim.

Q32: Has your company **ever used its cyber insurance** in the event of a cyberattack?

Base: have cyber insurance (280)

Use of cyber insurance



Yes, and it went well

Large companies: 19%

Yes, but it was complicated

Total yes

23%

Wave 10 reminder : 23%

Large companies: 32%

Credits: Icon from Storyset.com

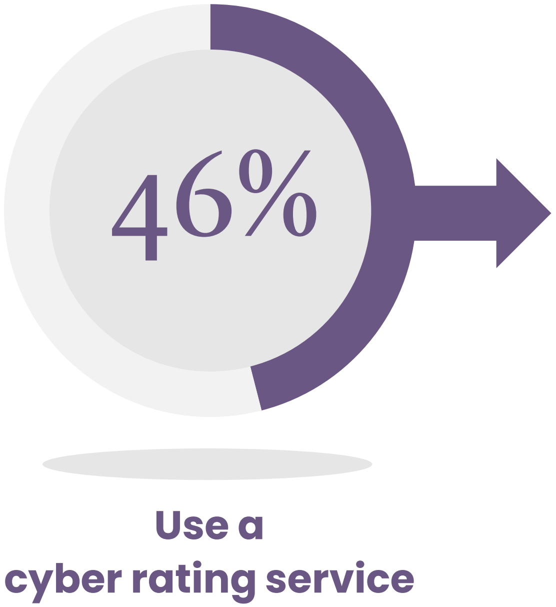
↗ ↘ significantly higher/lower than the previous wave

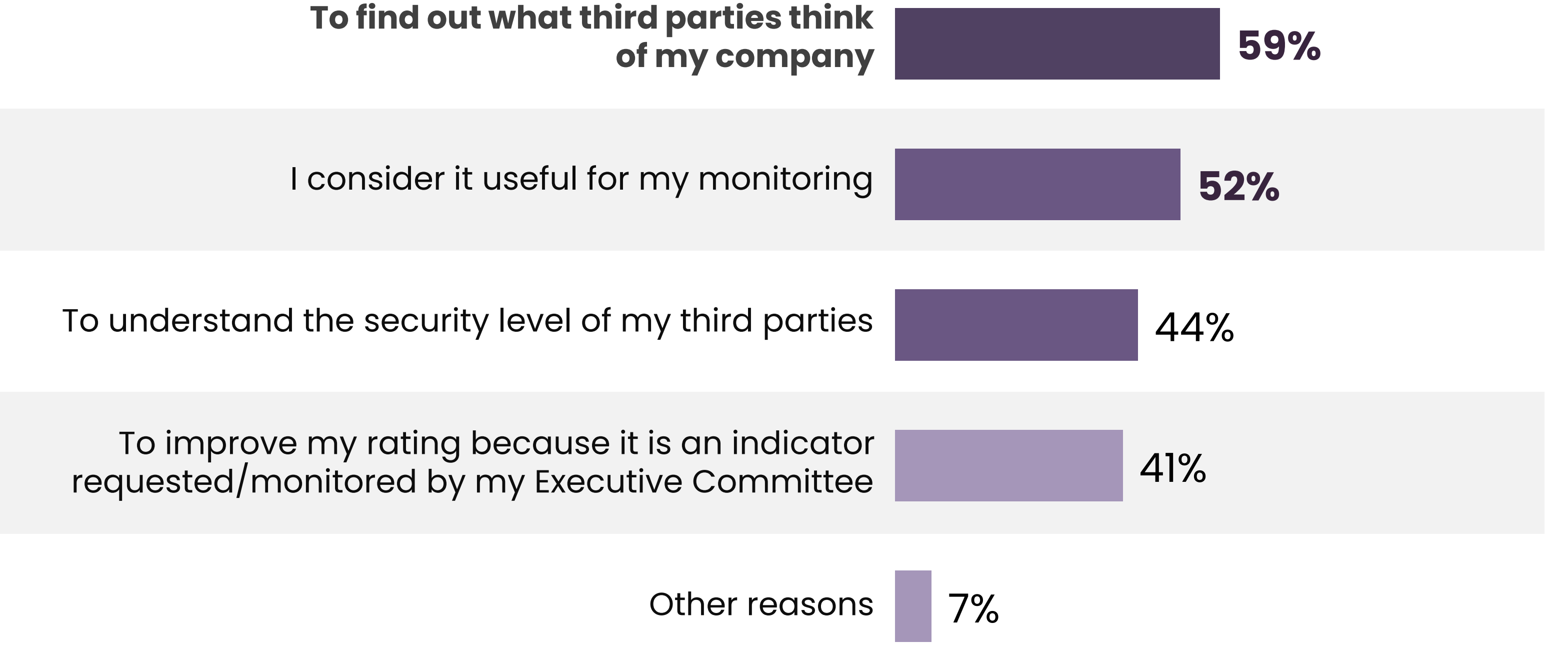
opinionway FOR CESIN

Cyber rating is becoming an essential tool, with nearly half of companies using this service. Most often, the goal is to find out what third parties think about them in terms of cybersecurity, but it is also useful for monitoring purposes.

Q33b: If you use **a cyber rating service**, what is your reason for doing so?

Base: use a cyber rating service (181) – Multiple answers possible





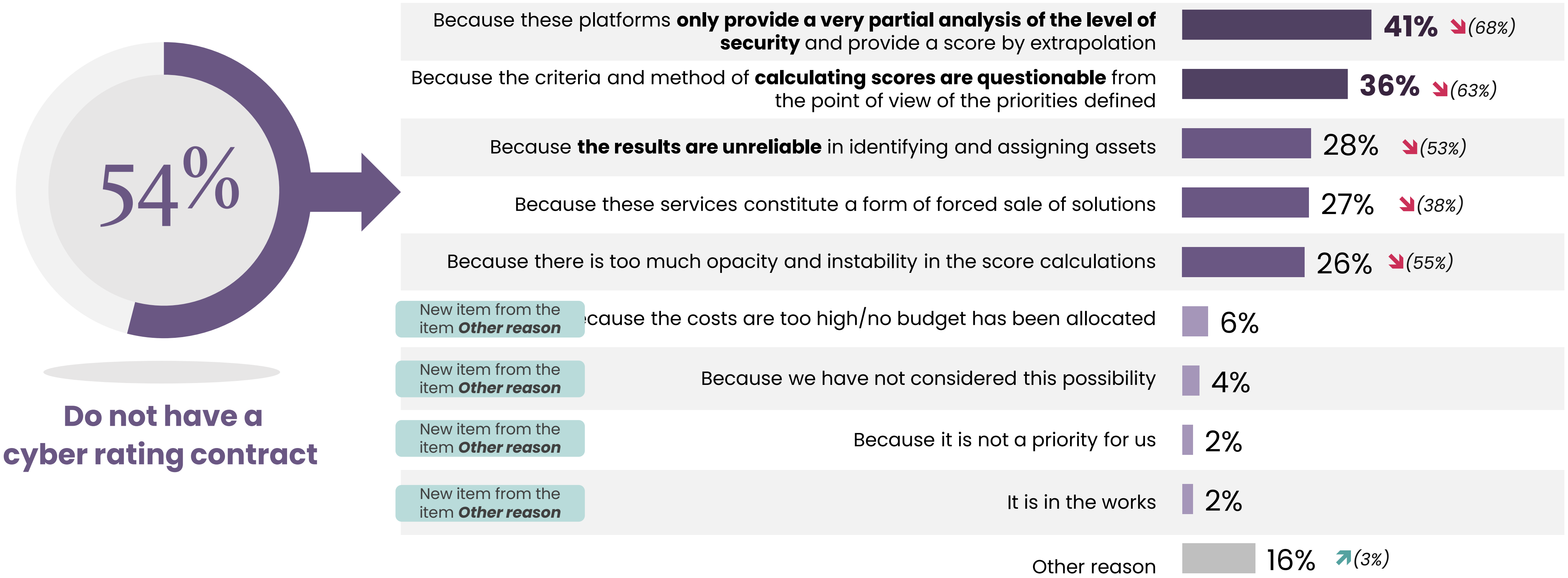
54% do not have a cyber rating contract

↗ ↘ significantly higher/lower than the previous wave

The reasons for mistrust among companies without cyber rating services are diminishing this year, demonstrating growing confidence.

Q33bis: For what reason(s) do you not have cyber rating services?

Base: do not have a cyber rating contract (216) – Multiple answers possible



54%

Do not have a cyber rating contract

Because these platforms **only provide a very partial analysis of the level of security** and provide a score by extrapolation	**41%**	↘(68%)
Because the criteria and method of **calculating scores are questionable** from the point of view of the priorities defined	**36%**	↘(63%)
Because **the results are unreliable** in identifying and assigning assets	28%	↘(53%)
Because these services constitute a form of forced sale of solutions	27%	↘(38%)
Because there is too much opacity and instability in the score calculations	26%	↘(55%)
New item from the item ***Other reason*** ecause the costs are too high/no budget has been allocated	6%	
New item from the item ***Other reason*** Because we have not considered this possibility	4%	
New item from the item ***Other reason*** Because it is not a priority for us	2%	
New item from the item ***Other reason*** It is in the works	2%	
Other reason	16%	↗(3%)

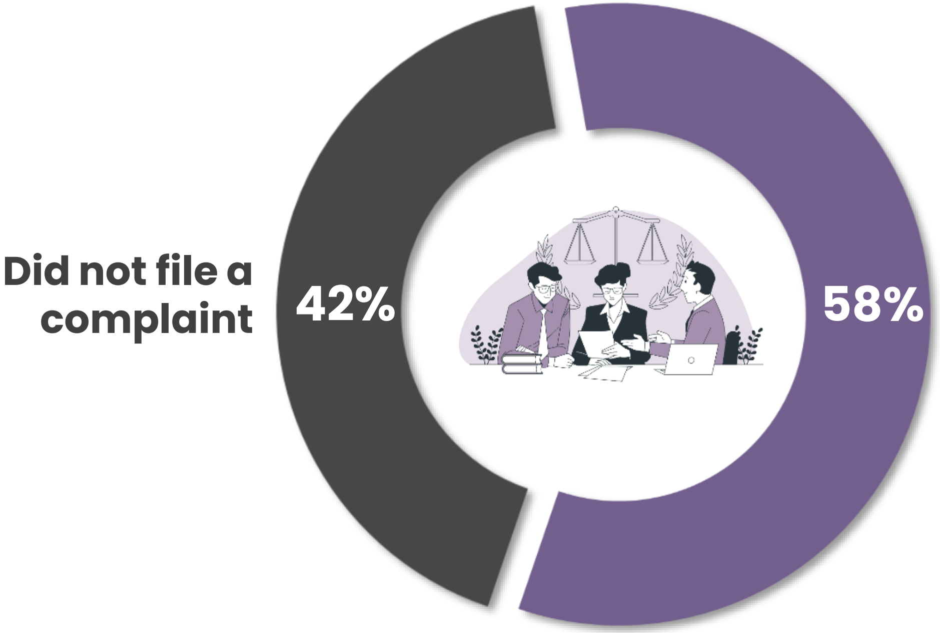
↗ ↘ significantly higher/lower than the previous wave

As was the case last year, more than half of companies that were victims of cyberattacks filed a complaint. However, only one-third did so for all attacks.

Q8: **Did you file a complaint** following the cyberattack(s) your company suffered?

Base: experienced an attack (159)

Reminder: **40%** of companies suffered at least one cyberattack in 2024



Filed a complaint

Wave 10 reminder : 62%

Large companies: **68%**

For **all attacks**: **35%**

for **some attacks**: **23%**

Credits: Icon from Storyset.com

↗ ↘ significantly higher/lower than the previous wave

04

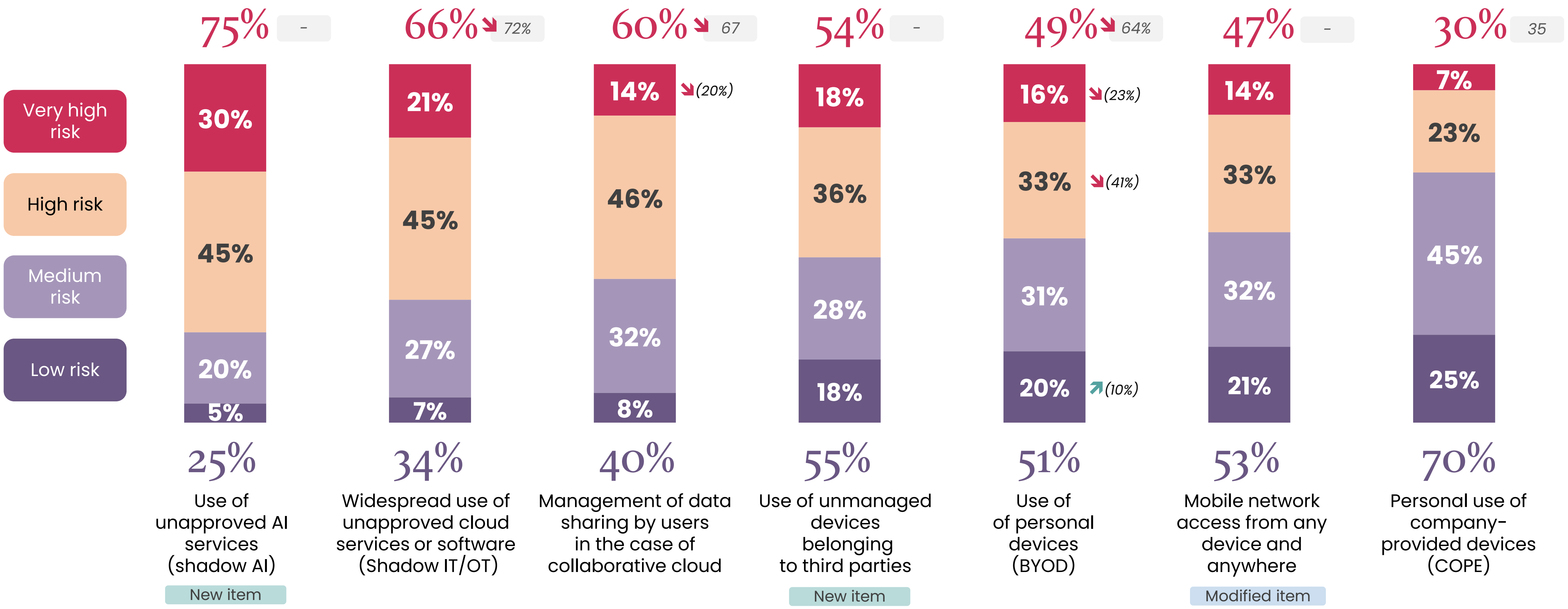
New risks are emerging in connection with changes in employees' working habits

This year, the use of AI that has not been approved by employees has become the behavior considered most risky.

Q23: How do you assess **the level of risk posed by the following uses** of digital technology by employees?

Base: all (397)

Vague 10 recall

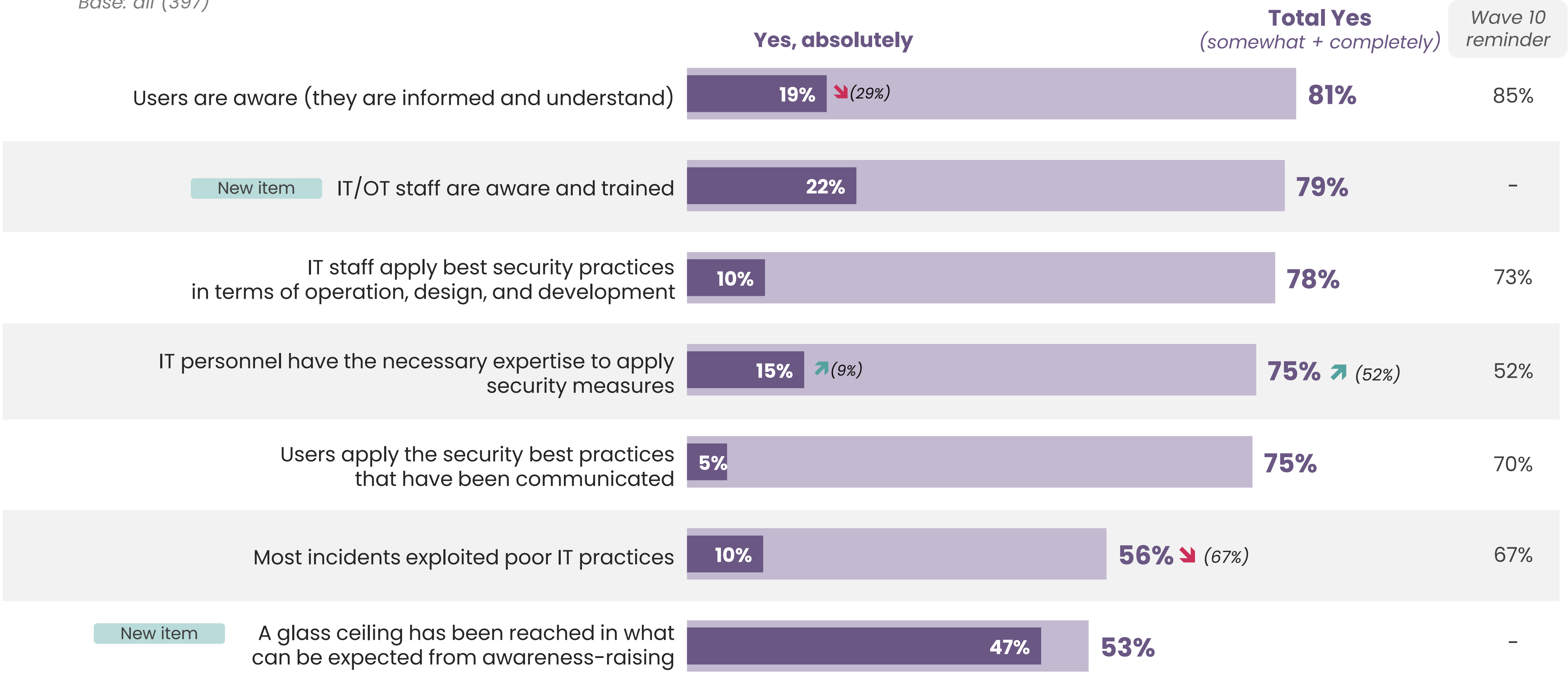


↗ ↘ significantly higher/lower than the previous wave

When it comes to awareness and training, half of companies believe that a glass ceiling has been reached, and most of them are completely convinced of this. Overall, 4 out of 5 companies believe that users and IT/OT staff are well aware of cybersecurity issues.

Q19: With regard to **cybersecurity awareness and training**, do you think that ...?

Base: all (397)



↗ ↘ significantly higher/lower than the previous wave

05

Focus on ...

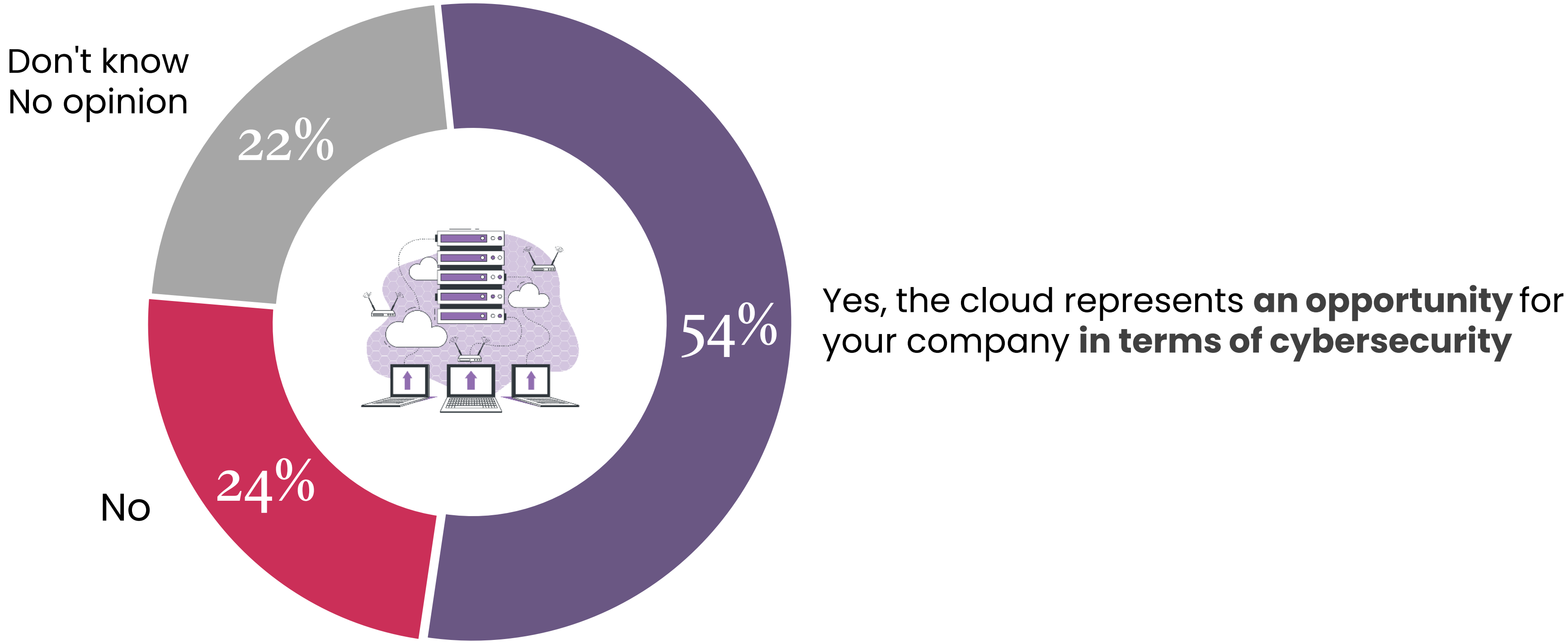
The Cloud

Although a quarter of companies are undecided or unsure, more than half still see the cloud as an opportunity in terms of cybersecurity.

New question in 2025

Q57: In your opinion, does the cloud represent **an opportunity** for your company **in terms of cybersecurity**?

Base: all (397)



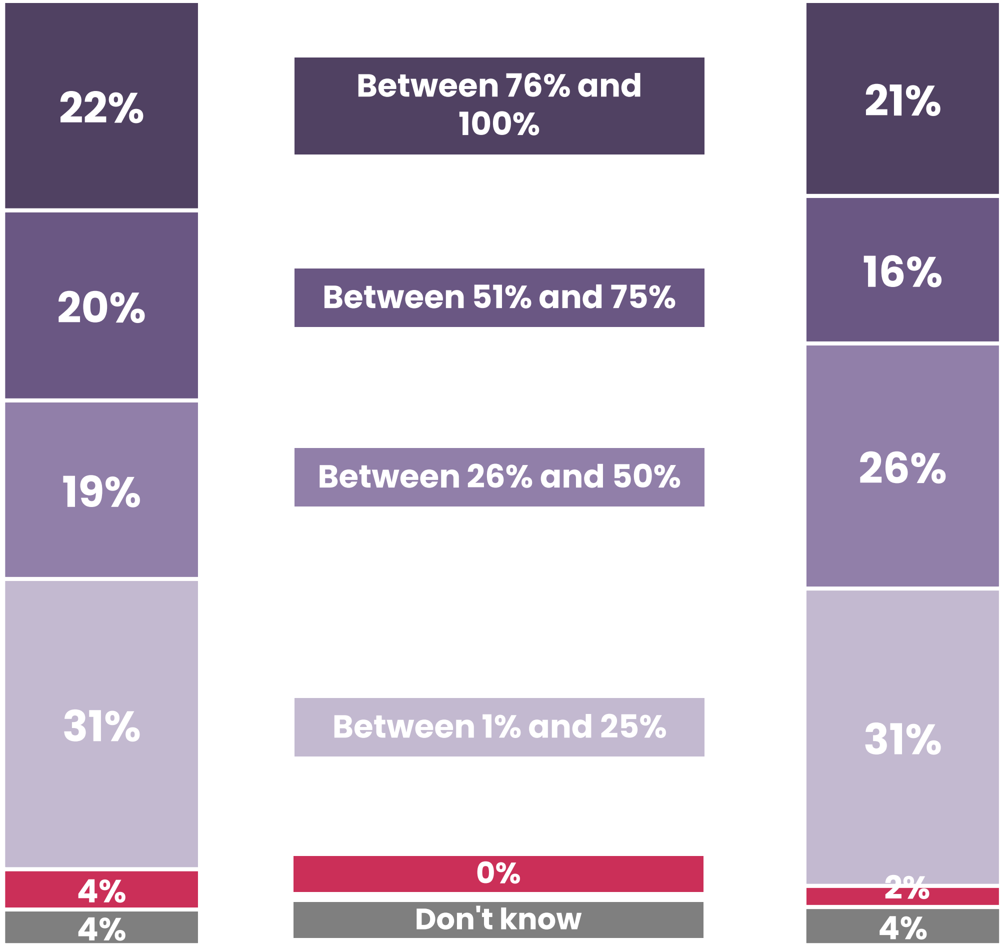
Credits: Icon from Storyset.com

As in the last survey, the adoption rates for IaaS, PaaS, and SaaS are fairly similar, although small businesses and SMEs seem to be adopting SaaS more widely.

Q20b: What is **the adoption rate of the cloud in your IT system**, whether IaaS, PaaS, or SaaS?

Base: all (397)

In IaaS, PaaS mode



In SaaS mode

VSE/SME: 38%

↗ ↘ significantly higher/lower than the previous wave

Credits: Icon from Storyset.com

With regard to cloud usage, the high risk of data hosting being subject to extraterritorial laws is increasing this year and is mentioned by 1 in 2 companies, as is the rigidity of contract clause negotiations.

Q21: In your opinion, do the following factors represent **a low, moderate, or high risk with regard to cloud usage**?

Base: all (397)

Reminder of 2024 ranking	% High risk		
	52%	**Contractual clauses that are very difficult to negotiate**	New item
↗ *(34%)*	48%	**Data hosting subject to extraterritorial laws, including in France and Europe**	
1	44%	**Lack of control over the hosting provider's subcontracting chain**	
↗ *(15%)*	37%	Compromise of a SaaS platform	
	35%	Unavailability of data/application due to an attack on the hosting provider	
2	34%	Difficulty conducting audits (penetration testing, configuration checks, on-site visits)	
	34%	Data confidentiality vis-à-vis the host provider	
	34%	Insufficient skills in my company regarding cloud security	New item
3	33%	Difficulty controlling access to data by the hosting provider's administrators	
	32%	Lack of control over the hosting provider's security level	
	29%	Systemic risk	
	28%	Failure of the host to delete data during or at the end of the contract (normal or early termination)	New item
	27%	Lack of partitioning between the hosting provider's different customers	
	24%	Difficulty or impossibility of feeding the SIEM with logs from a SaaS service	
	23%	High frequency of new versions being released online with potential uncontrolled changes to security principles or settings	
	21%	Failure of the host to return data at the end of the contract (normal or early termination)	
	21%	Processing and use of data by the host, data ownership issues	

Credits: Icon from Storyset.com

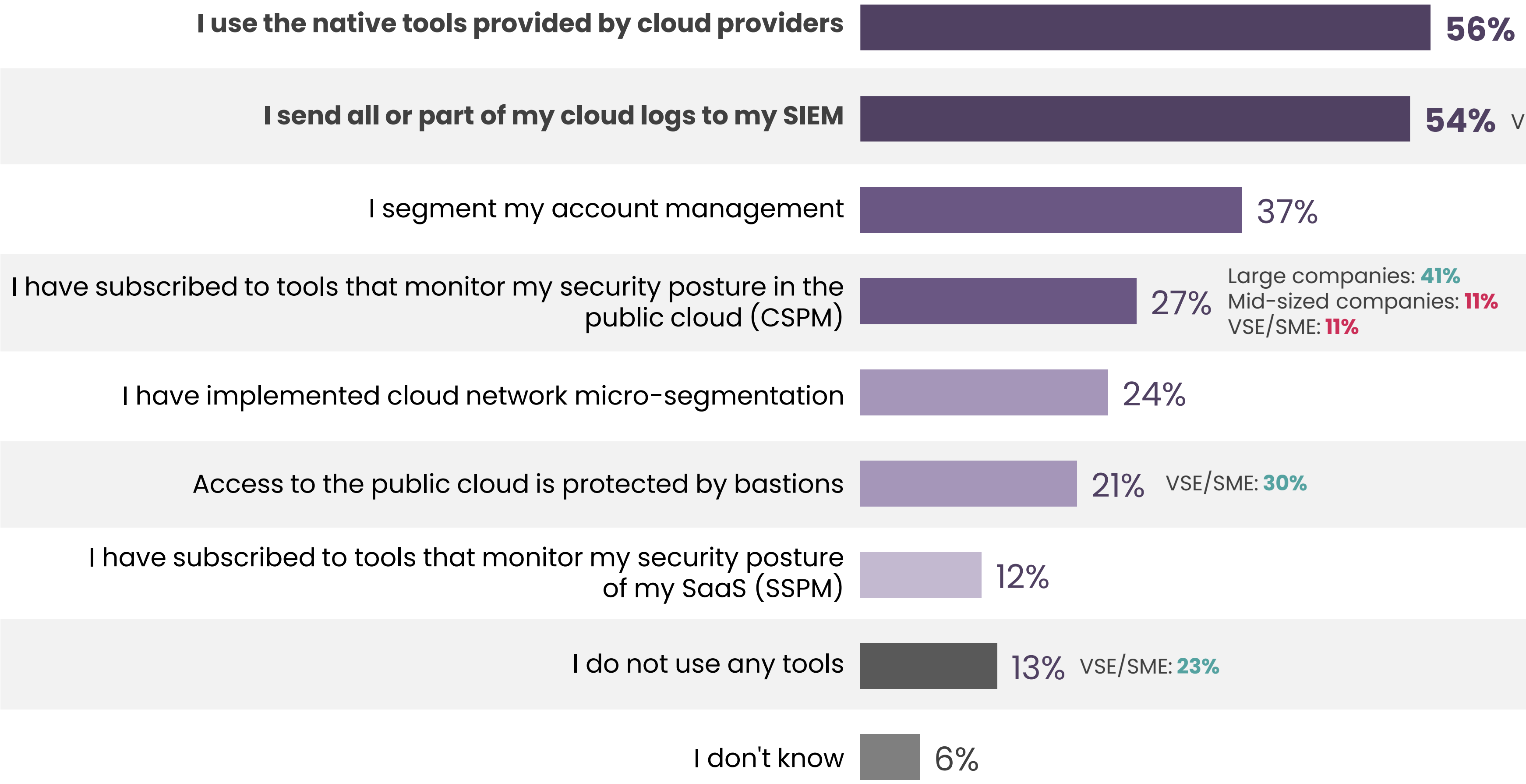
↗ ↘ significantly higher/lower than the previous wave

To secure their cloud, companies favor two solutions: using cloud providers' native tools and sending logs to the SIEM.

New question in 2025

Q58: What tools do you use **to secure your cloud**?

Base: all (397) – Multiple answers possible



Average number of tools cited: **2.9**

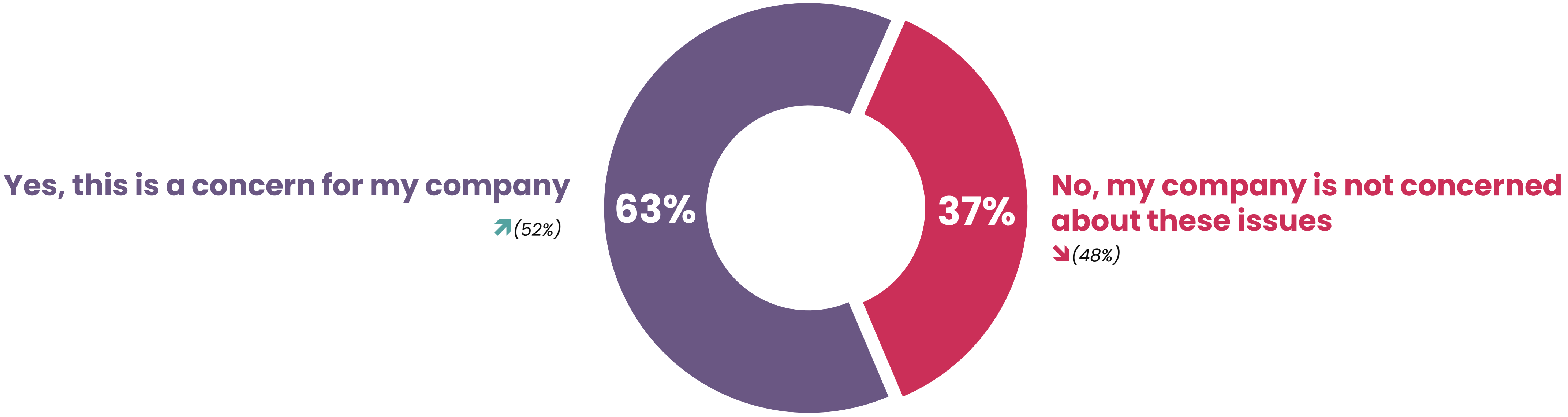
Credits: Icon from Storyset.com

Nearly two out of three companies feel concerned about issues of sovereignty and trusted cloud computing, an increase of 11 points since last year.

Q35: Numerous initiatives have recently been launched in the areas of sovereignty and trusted cloud computing. **Are you concerned about these issues**?

Base: all (397)

Sovereignty & Trusted Cloud



↗ ↘ significantly higher/lower than the previous wave

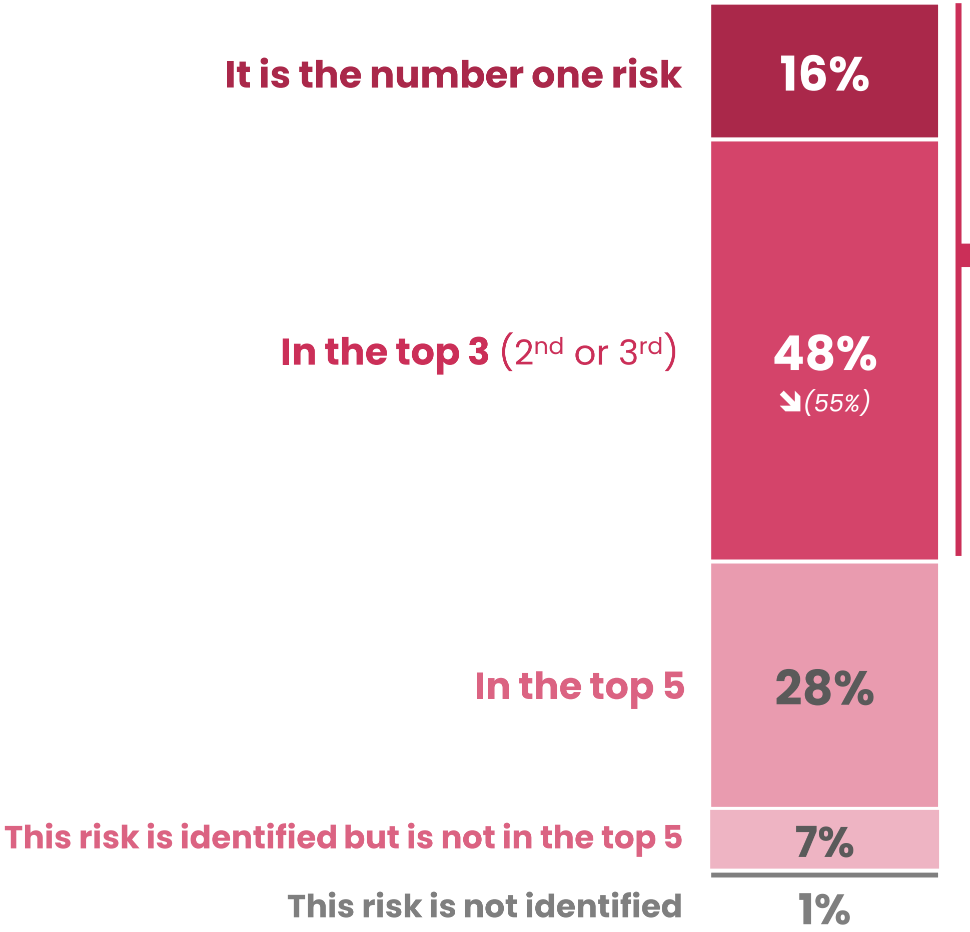
06

Cybersecurity in business: A strategic function in constant adaptation

Cyber risk is identified in the TOP5 by companies, and for nearly two-thirds, it is even identified in the TOP3.

Q48: **How is cyber risk positioned in** your company's **risk mapping**?

Base: all (397)

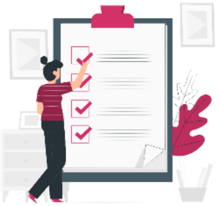


64%

Consider cyber risk to be in the top 3

92%

Estimate that cyber risk is identified in the top 5



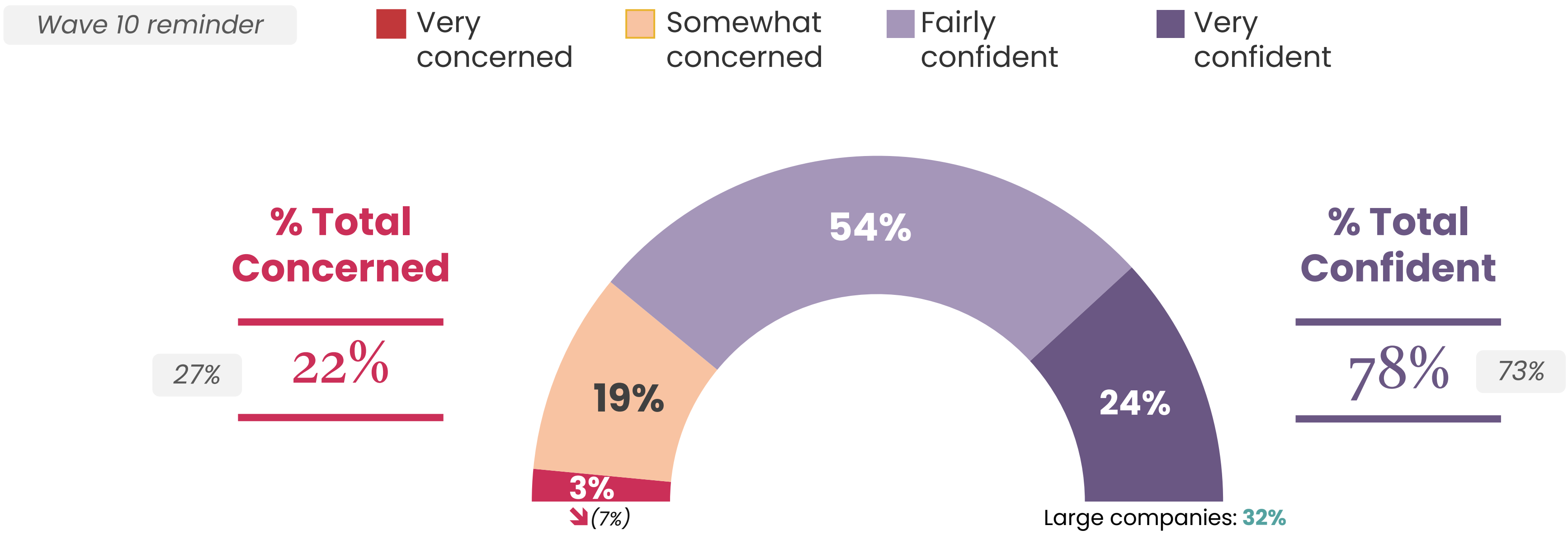
Credits: Icon from Storyset.com

In line with the previous wave, the consideration of cybersecurity within the Executive Committee is not a concern.

Q24: Looking ahead, would you say you are very confident, fairly confident, fairly concerned, or very concerned about...?

Base: all (397)

Consideration of cybersecurity issues within your company's executive committee



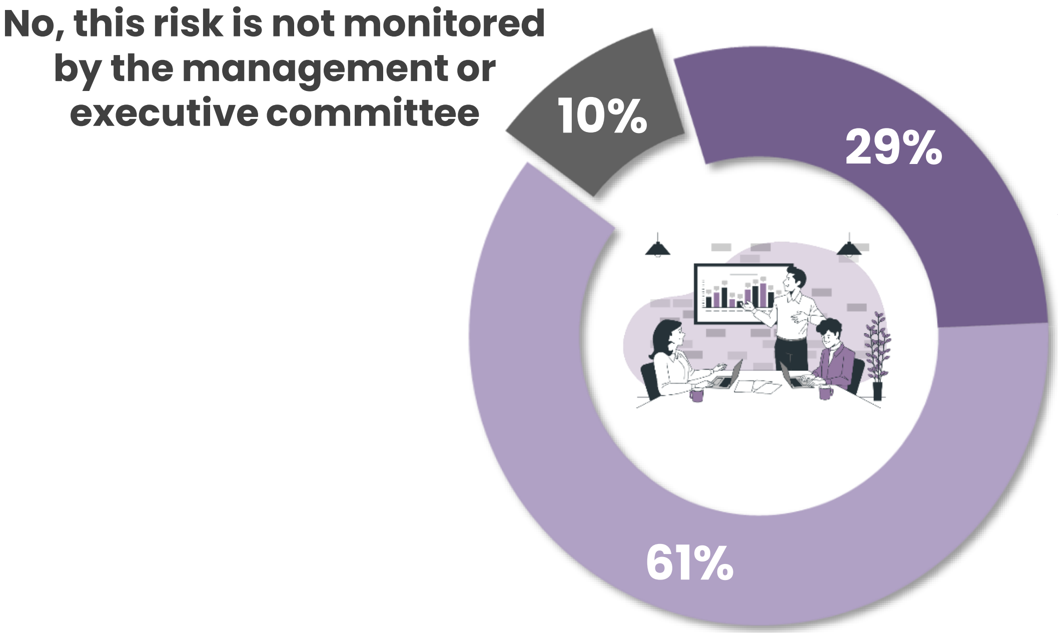
↗ ↘ significantly higher/lower than the previous wave

This is because cyber risk monitoring by senior management is a regular and institutionalized practice.

New question in 2025

Q50: Is this risk **monitored regularly** by the management committee or executive committee?

Base: all (397)



Yes, **this risk is monitored once a year** by the Executive Committee or Management Committee

Yes, **this risk is monitored several times a year** by the Executive Committee or Management Committee

Total yes

90%

Large companies: **94%**
Mid-sized companies: **86%**

Credits: Icon from Storyset.com

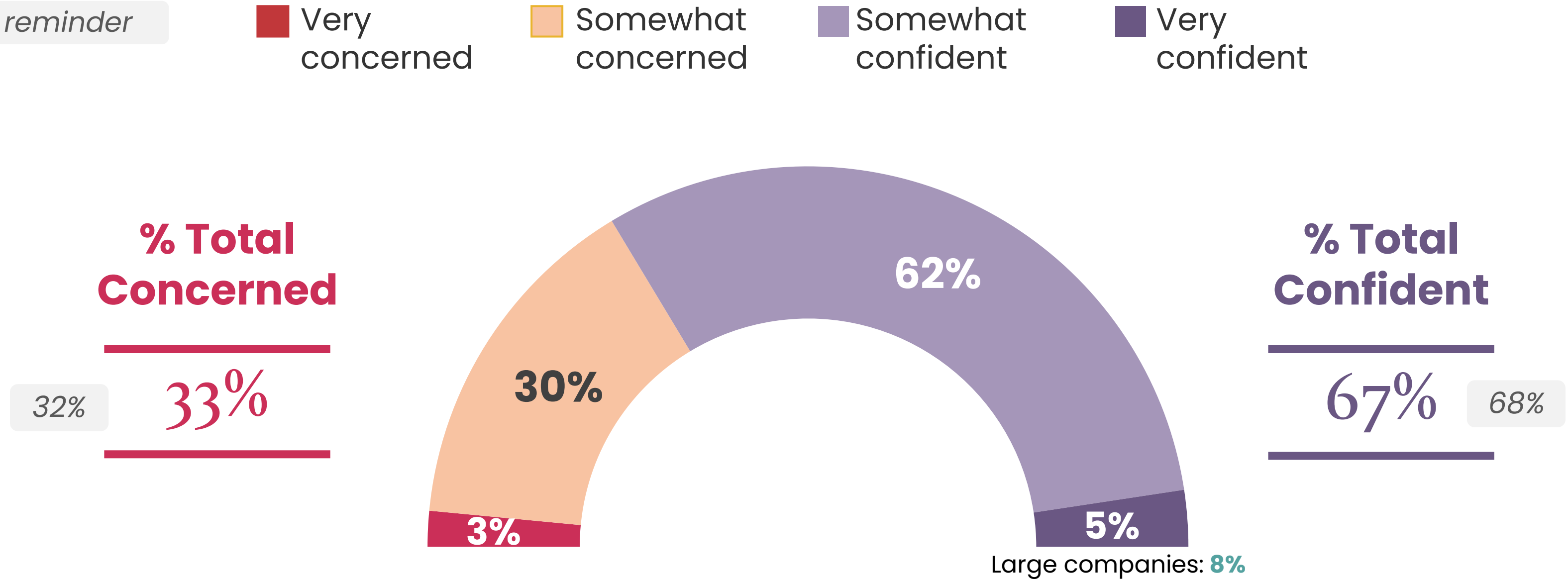
Although companies feel capable of dealing with cyber risks, this confidence is more often moderate than total.

Q24: Looking ahead, would you say you are very confident, fairly confident, fairly concerned, or very concerned about... ?

Base: all (397)

Your company's ability to deal with cyber risks

Wave 10 reminder



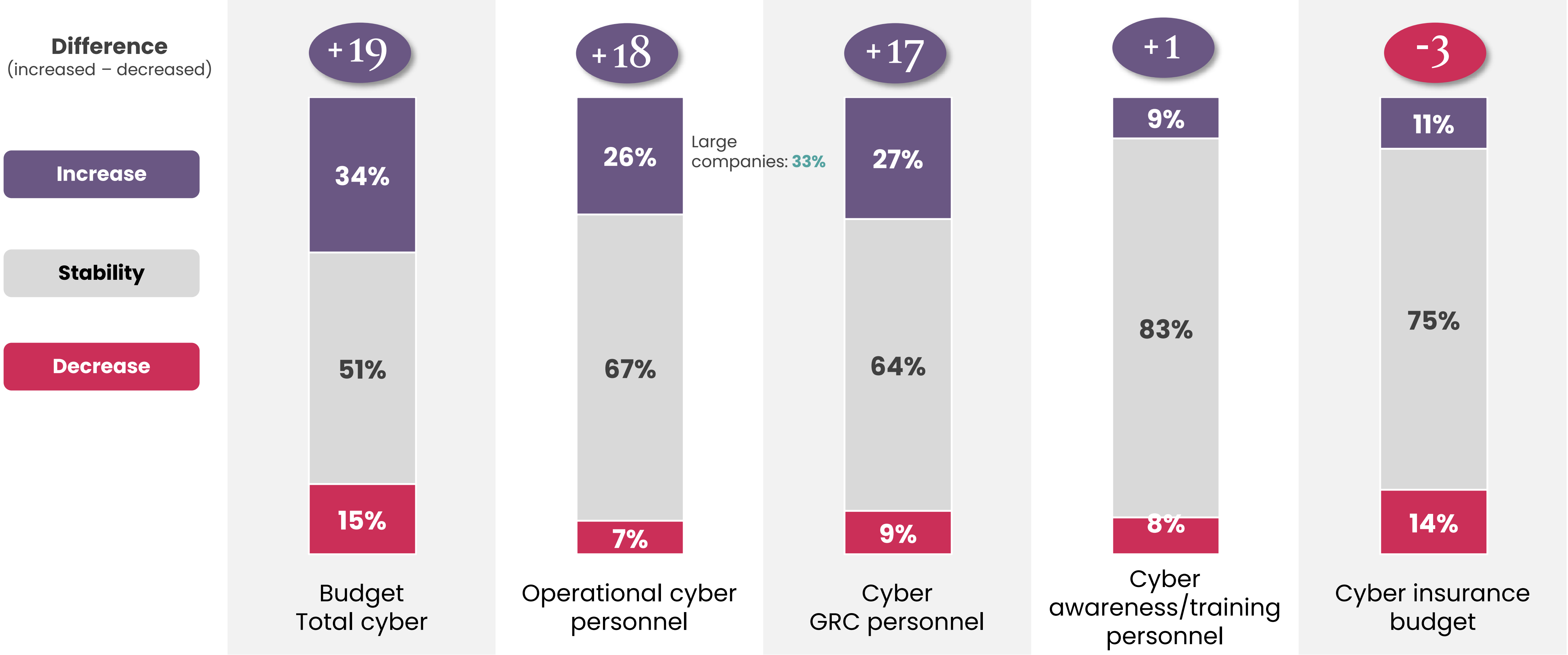
↗ ↘ significantly higher/lower than the previous wave

Cyber resource forecasts for 2026 show a prioritization of budget and operational and GRC staffing, potentially at the expense of cyber insurance.

New question in 2025

Q55: Over the next 12 months, **how will your cyber resources evolve**?

Base: all (397)



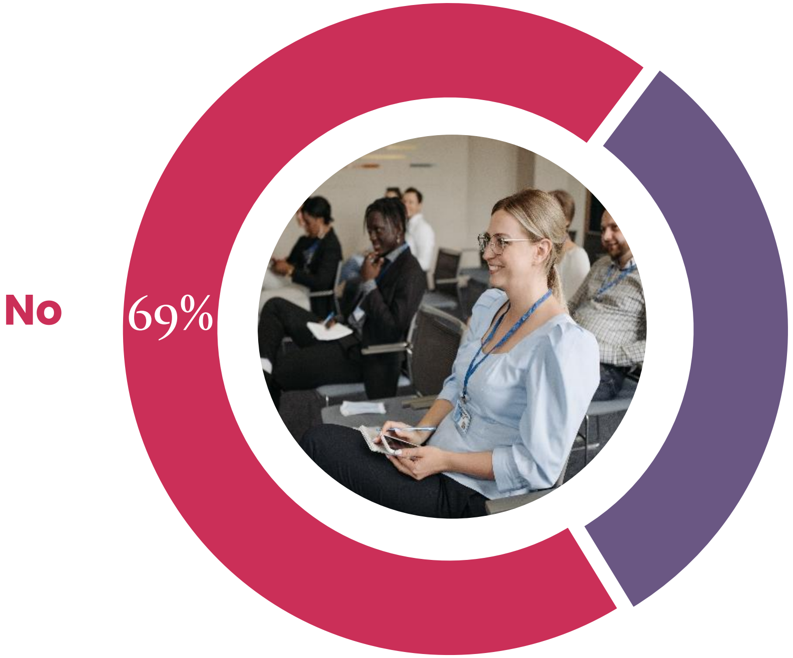
opinionway FOR CESIN

This is a positive trend, as two-thirds of companies believe they currently lack the human and financial resources needed to address the various challenges they face.

New question in 2025

Q56: In your opinion, do you **have sufficient human and financial resources** to respond to current challenges?

Base: all (397)



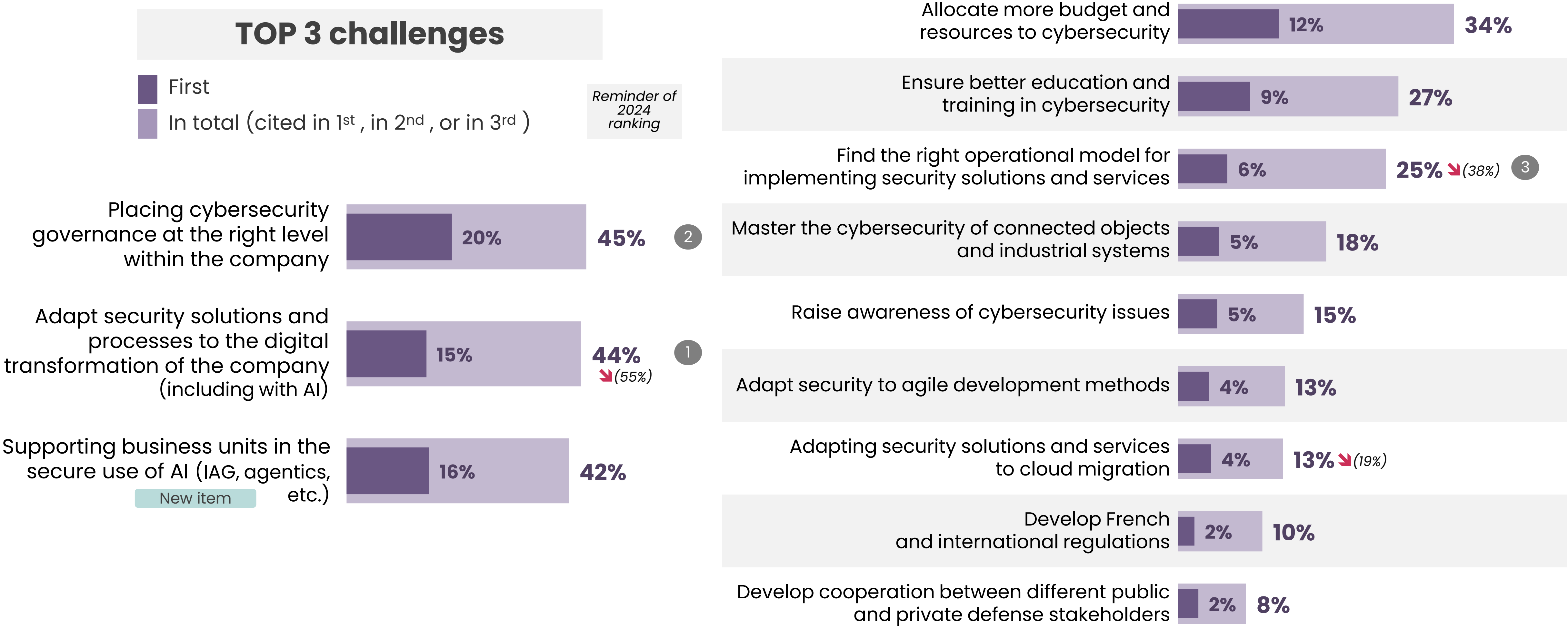
31% believe they have sufficient human and financial resources to meet current challenges

Credits: Photo by Pavel Danilyuk on Pexels.com

The role of cybersecurity in governance, adapting solutions to digital transformations, and supporting businesses in the use of AI are the main cybersecurity challenges of tomorrow identified by companies.

Q27. Among the following challenges, which **three** do you think will be **the most important for the future of** corporate **cybersecurity**?

Base: all (397) – Three possible answers



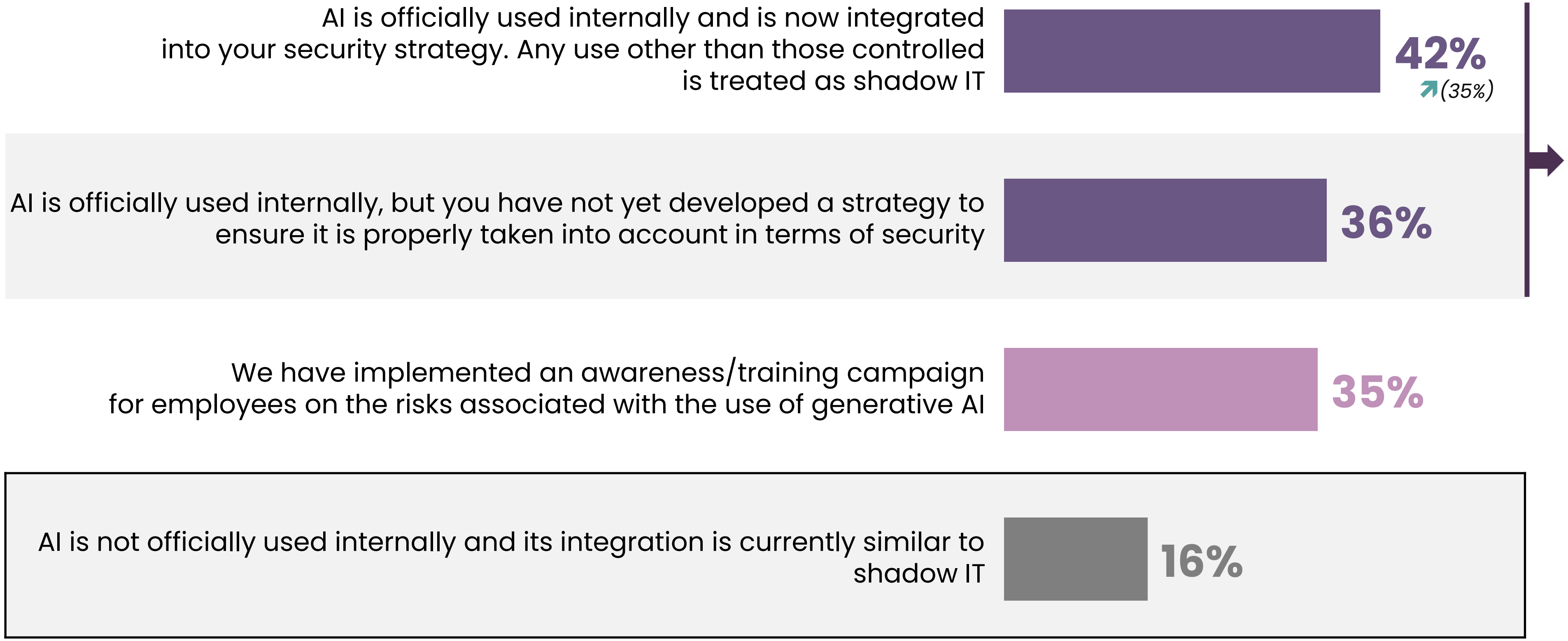
opinionway FOR CESIN

↗ ↘ significantly higher/lower than the previous wave

Artificial intelligence is now widely used internally.

Q39: AI, which is already used to varying degrees in certain cyber solutions, has become established in our information systems, particularly with a large number of initiatives around generative AI. **What role does AI play in your organization today**?

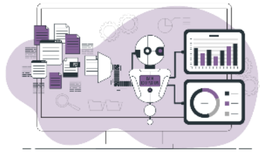
Base: all (397) – Multiple answers possible



AI used

79% ↗(69%)

Large companies: **84%**
VSE/SME: **65%**



Credits: Icon from Storyset.com

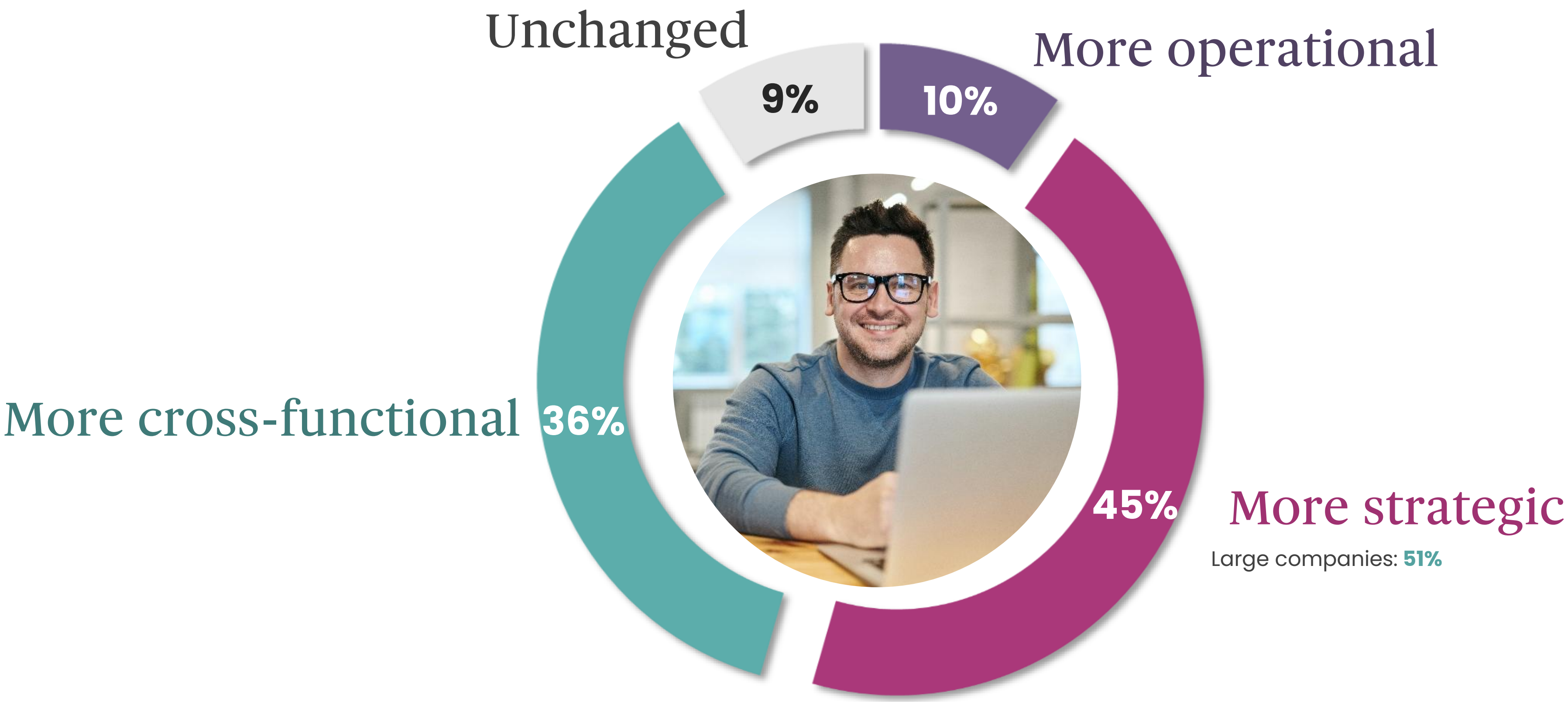
↗ ↘ significantly higher/lower than the previous wave

The role of CISOs is evolving significantly toward more cross-functional and strategic roles within organizations.

New question in 2025

Q59: How have you seen **your role** evolve in recent years?

Base: all (397)



Large companies: **51%**

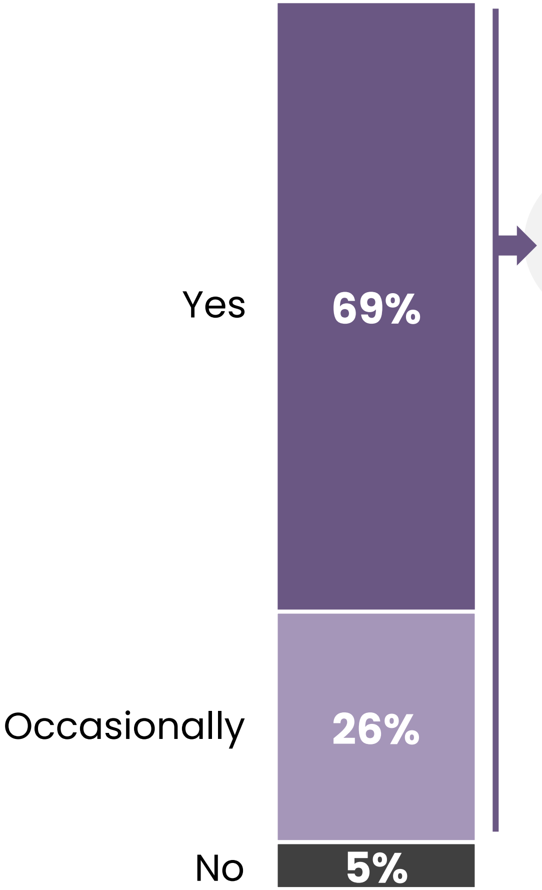
Credits: Photo by Fauxels on Pexels.com

Collaboration between CISOs is very common.

New question in 2025

Q60: **Do you regularly work with other CISOs** (clubs, industry networks, etc.)?

Base: all (397)



95%

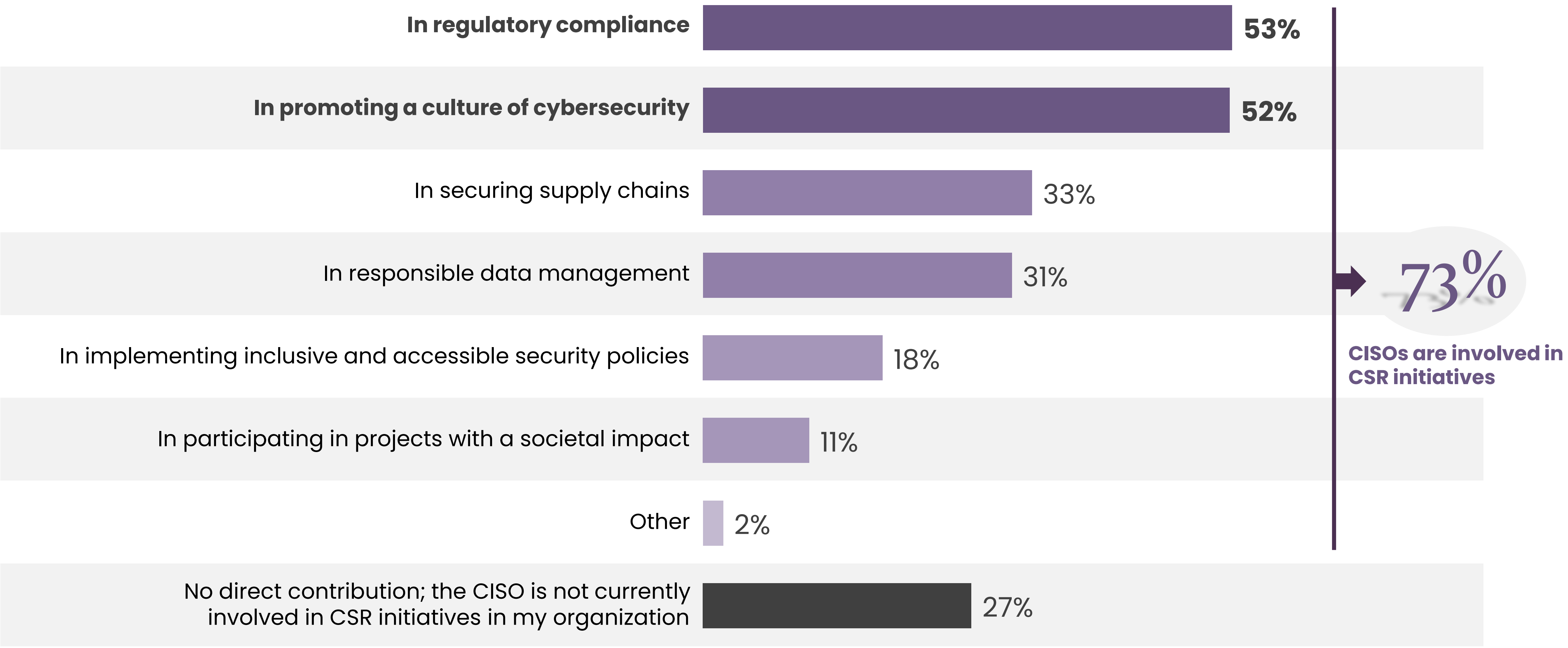
Work with other CISOs
(clubs, industry networks, etc.)

Large companies: **97%**

Credits: Icon from Storyset.com

Three out of four CISOs feel integrated into social and environmental responsibility objectives, which most often manifest themselves in regulatory compliance and the promotion of a cybersecurity culture.

Q49: To what extent does your role contribute, or could contribute, to your organization's **social and environmental responsibility (CSR)** objectives? *Base: all (397) – Multiple responses possible*



↗ ↘ significantly higher/lower than the previous wave

opinionway

PARIS • BORDEAUX • BRUSSELS • WARSAW • CASABLANCA • ABIDJAN

Founded in 2000 on what was then a radically innovative idea, OpinionWay was a pioneer in transforming the practices of the marketing and opinion research profession.

Building on continuous growth since its inception, the company has consistently expanded its horizons to better address all marketing and societal challenges. It has incorporated into its methodologies Social Media Intelligence, the use of smart data, creative co-creation dynamics, community-driven approaches, and storytelling. Today, OpinionWay continues its growth momentum by geographically expanding into high-potential regions such as Eastern Europe and Africa.

Enable *today*, shape tomorrow

This mission drives the employees of OpinionWay and underpins the relationships they build with their clients.

The pleasure they take in providing answers to the questions their clients ask, reducing uncertainty in decision-making, tracking relevant insights, and co-creating future solutions fuels every project they undertake. This enthusiasm, combined with a genuine passion for innovation and knowledge-sharing, explains why clients report high levels of satisfaction after each collaboration – 8.9/10 – and a strong recommendation rate – 3.88/4.Enjoyment, commitment, and intellectual stimulation are the three guiding principles of our work.

ESOMAR 25 Corporate

afaq ISO 20252 Étude marketing et d'opinion AFNOR CERTIFICATION

Let's stay *connected*!

Receive our latest research results in your inbox every week by subscribing to our newsletter!

Subscribe

Your OpinionWay contact

Stéphane Lefebvre-Mazurel
Deputy Managing Director
Tel. +33 1 81 81 83 48
slefebvre@opinion-way.com

Valentin Heritier
Research Director
Tel. +33 1 81 81 83 63
vheritier@opinion-way.com