“opinionway for CESIN

Corporate cybersecurity barometer

Wave 10 – January 2025


Photo de Pixabay sur Pexels

Press contact:
Véronique LOQUET – ***AL’X COMMUNICATION***
06 68 42 79 68 - vloquet@alx-communication.com

Context

Context and objectives

- The **Club des Experts de la Sécurité de l'Information et du Numérique** (CESIN) provides a forum for corporate **security and digital experts.**

- CESIN, with OpinionWay, launched its first major survey of its members in 2015 to find out:
  - the **perception of cybersecurity and its challenges** within CESIN member companies
  - **the** concrete **reality of** corporate IT security.

- The survey, which is renewed every year, updates the results on the perception and reality of cybersecurity, and provides new data on the impact of the digital transformation of businesses.

Methodology

The methodology

Sample of **401 CESIN members, drawn** from the CESIN membership file.

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

The interviews were conducted **between December 10, 2024 and January 7, 2025**.

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

The results of this survey should be read in the light of the margins of uncertainty: 4.9 points at most for a sample of 400 respondents.

All publications, whether in whole or in part, must use the following full wording:

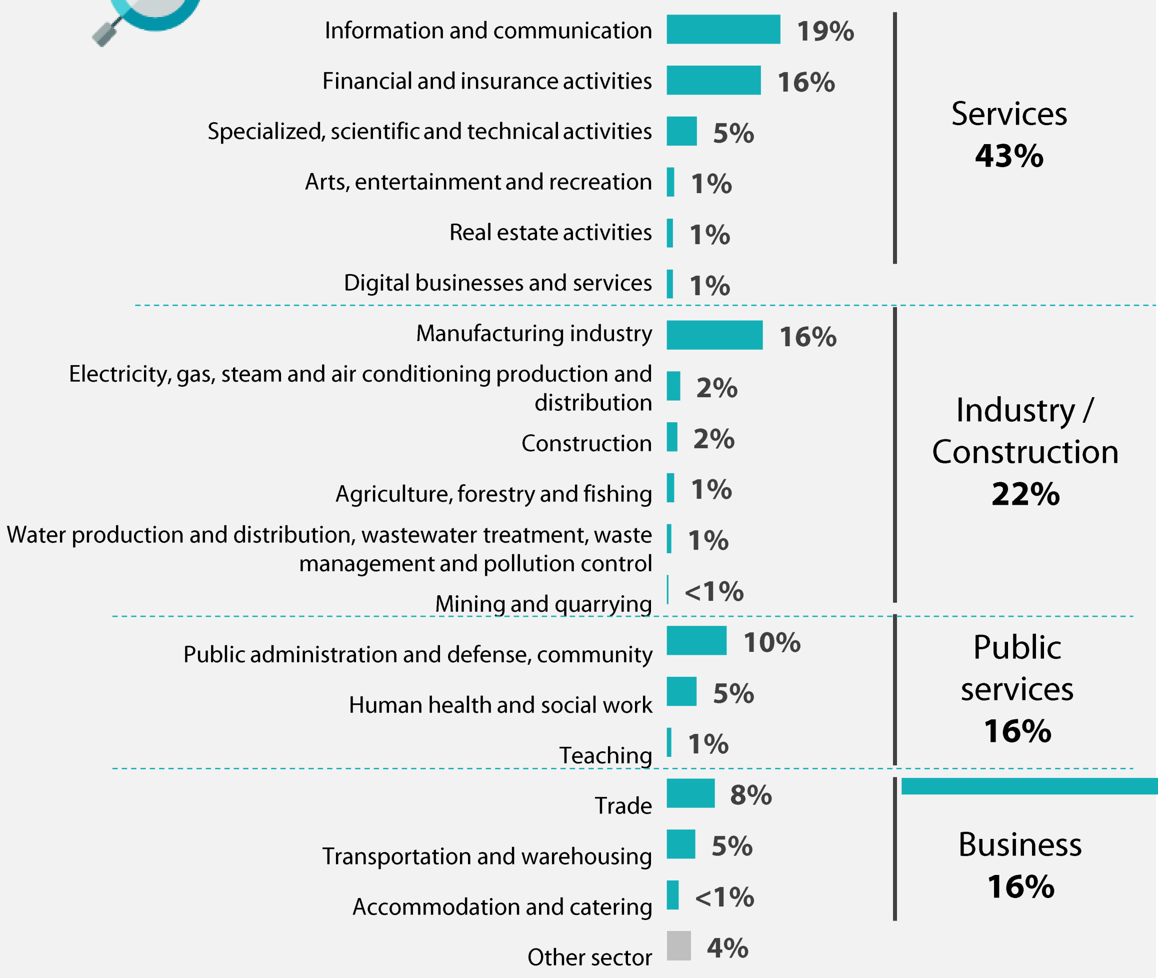
"OpinionWay survey for CESIN".

and no survey can be dissociated from this title.

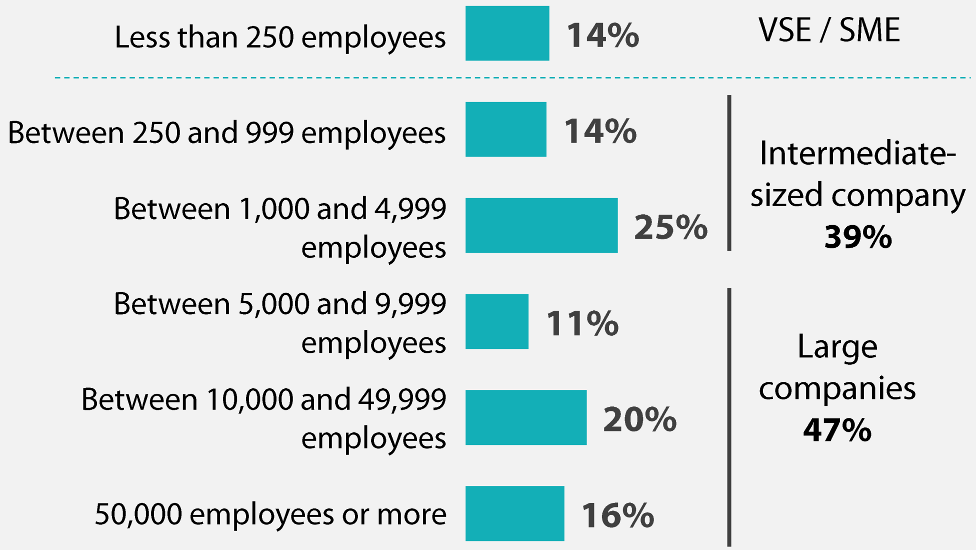
Sample

A sample that perfectly reflects the diversity of the population surveyed

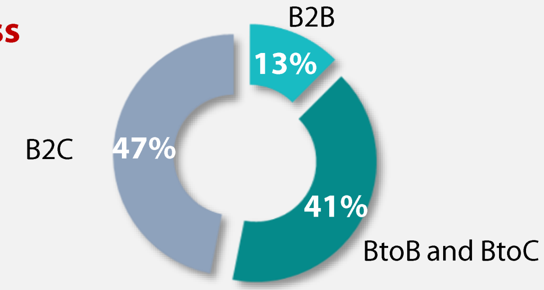
Company sector



Number of company employees



Business



Analysis

01

A stable volume of cyberattacks in 2024, with the contours and consequences remaining broadly identical to the previous year

Definition of a cyberattack

"A cyberattack, for the purposes of this survey, is the occurrence of a malicious act against an IT device that significantly impairs the confidentiality and/or integrity of the company's information or the availability of the information system, resulting in significant financial loss and/or damage to the company's image and/or significant defense efforts to contain and deal with the attack. This does not include attempted attacks that have been stopped by your prevention systems."

Half the companies suffered at least one cyberattack in 2024, a proportion that remains stable compared to the previous year.

401 people

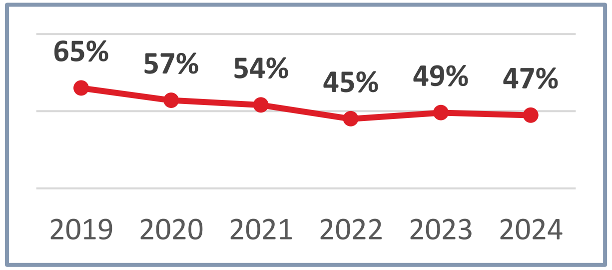
Q4. In total, how many significant cyberattacks has your company suffered in the last 12 months?
Base: all

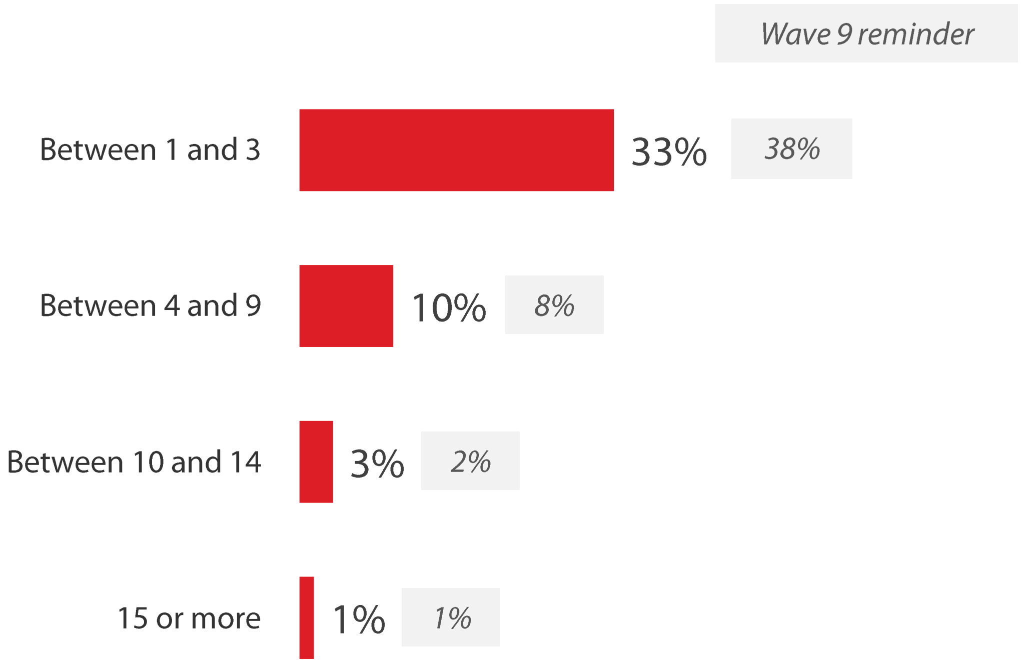
47%

of companies have experienced at least a cyberattack

Large companies: 53%

Previous waves reminder





The number of attacks is stabilizing for most companies, although 1/5 are seeing an increase.

401 people

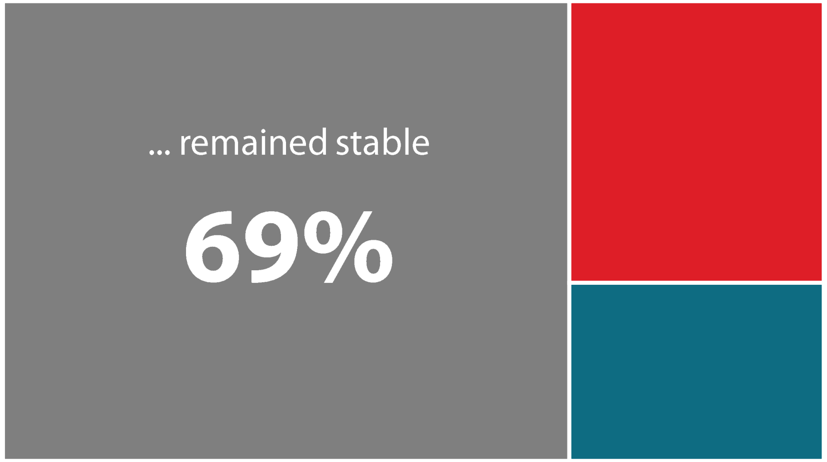
Q4bis. And compared to last year, has the number of attacks in your company … ?

Base: all

*Among the companies that reported having suffered at least one attack in 2024, **37%** indicated that they had noticed an increase in such attacks.*

In one year, the number of attacks...

Wave 9 reminder: 66%



... increased

19%

Wave 9 reminder: 23%

Intermediate-sized company : 25%

... decreased

12%

Wave 9 reminder: 11%

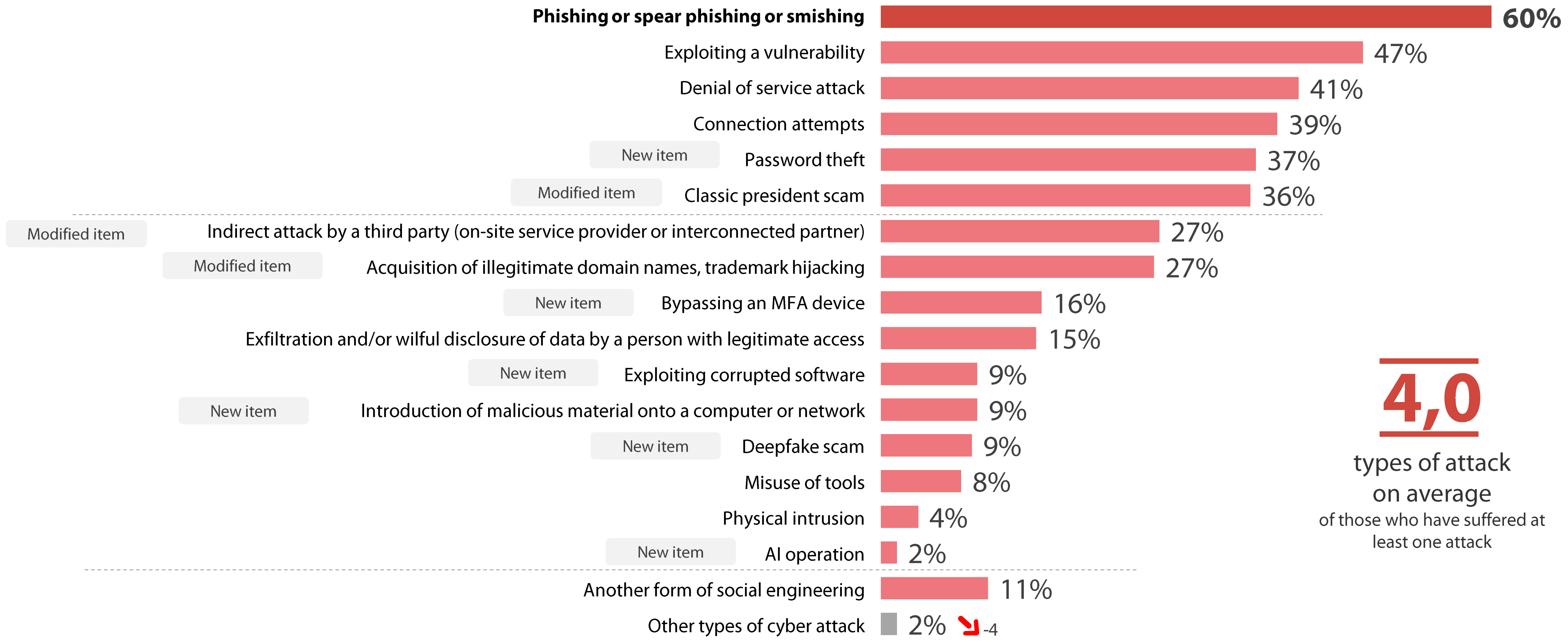
With an average of 4 vectors, phishing remains at the top of the attack list, followed by the exploitation of an existing vulnerability. Attack strategies are similar to last year.

190 people

Q5A. Which of the following attack vectors have impacted your company in the last 12 months?

Base: Experienced an attack - multiple answers possible

47% of companies suffered at least one cyber attack in 2024



Statistically significant change from previous wave

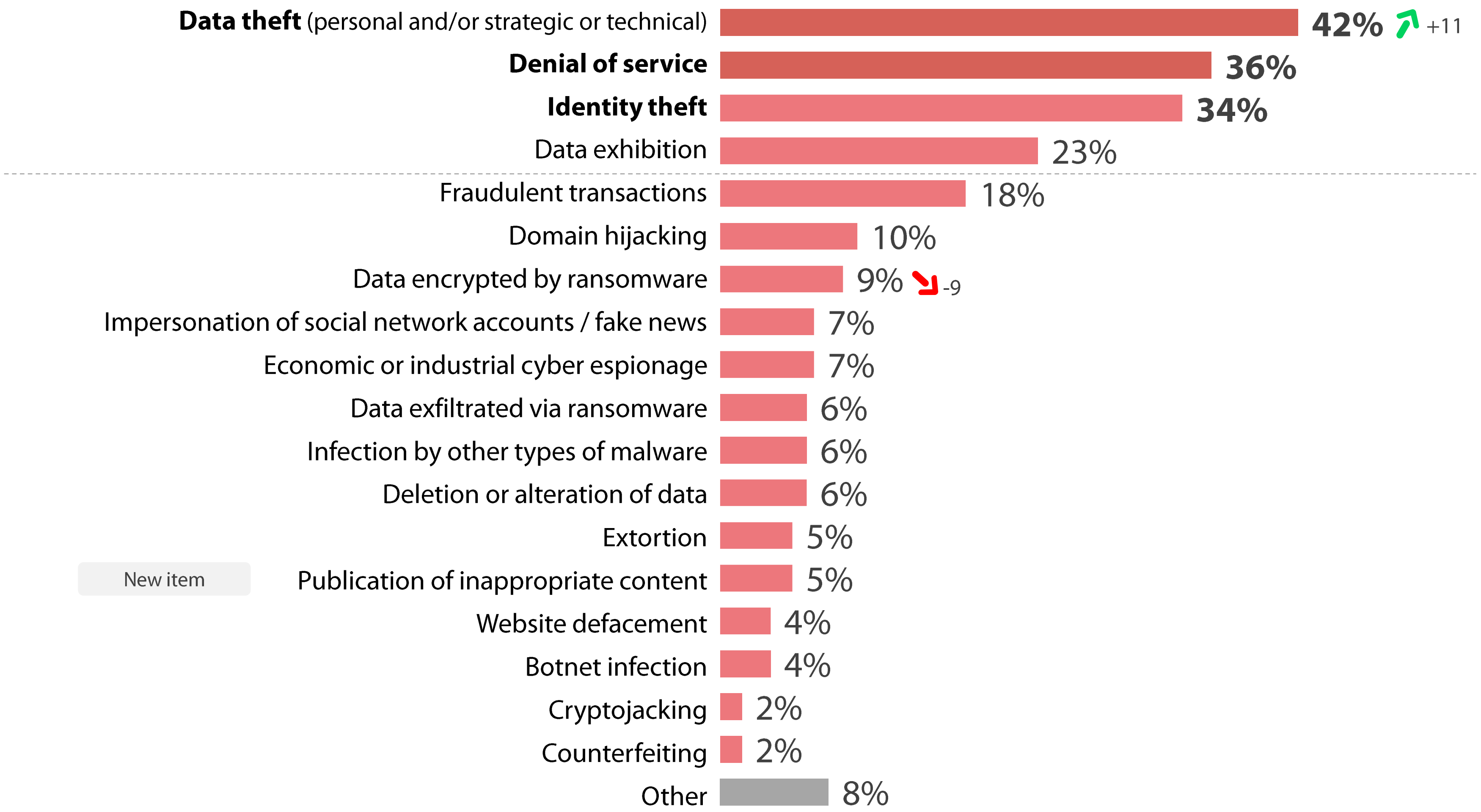
Data theft remains at the top of the list of consequences of these attacks, and is even gaining ground. Denial of service and identity theft are next in importance for over 1/3 of companies. Data encrypted by ransomware is on the decline.

190 people

Q5B. And what were the consequences of this/these attack(s)?

Base: Experienced an attack - multiple answers possible

47% of companies suffered at least one cyber attack in 2024



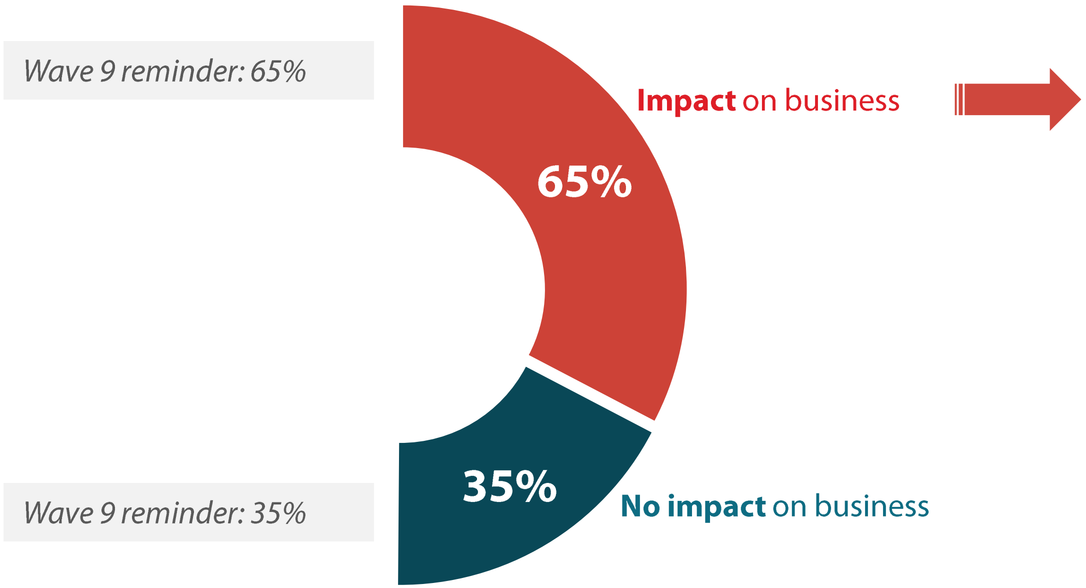
Statistically significant change from previous wave

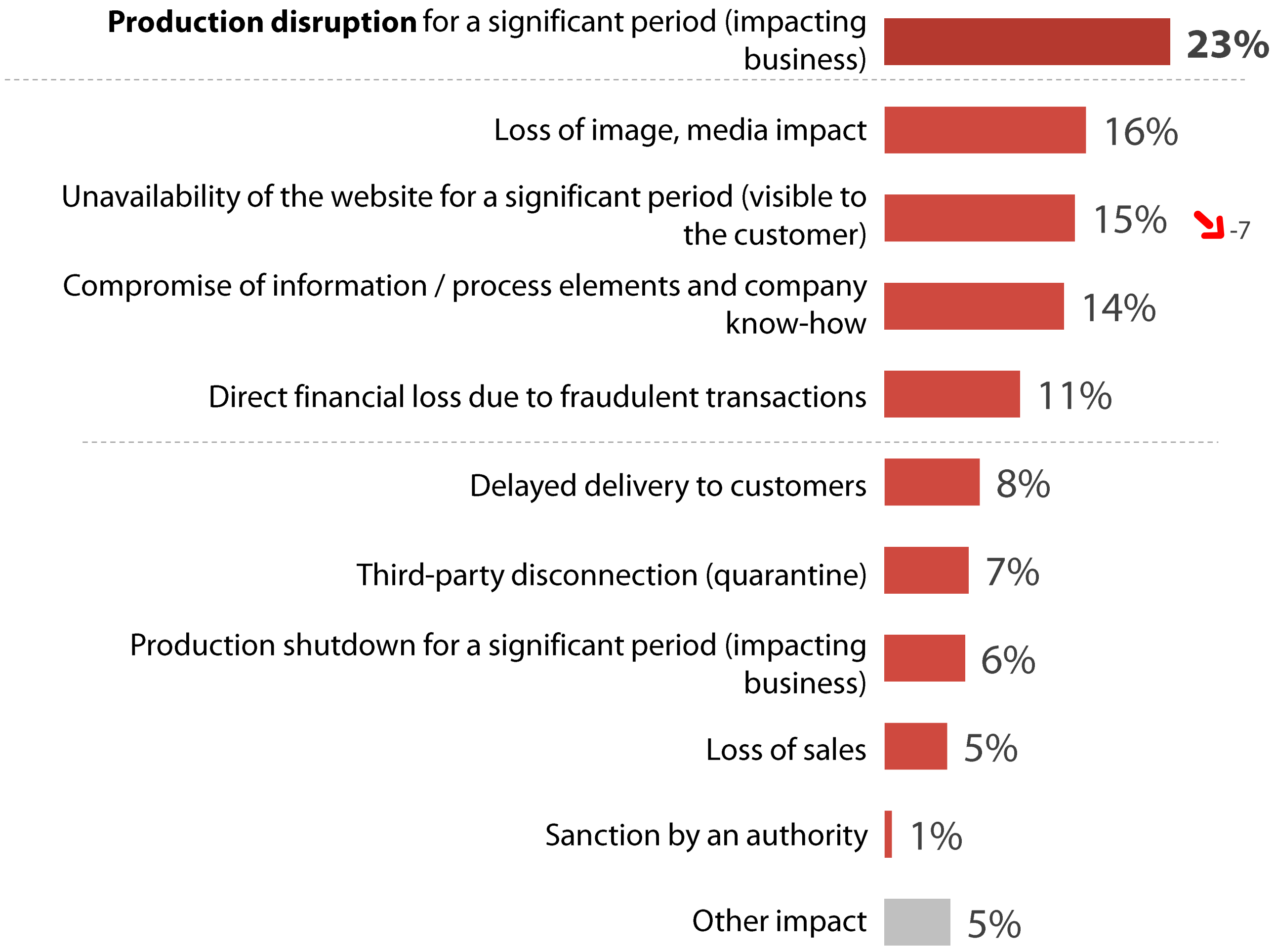
The impact of cyber attacks on business remains stable this year: 2/3 are affected. While production disruption is still the most frequently mentioned consequence, website unavailability for a significant period is declining.

351 people

Q7. What impact have cyber attacks had on your business?

Base: have observed an attack and/or a cause of security incidents - Multiple answers possible





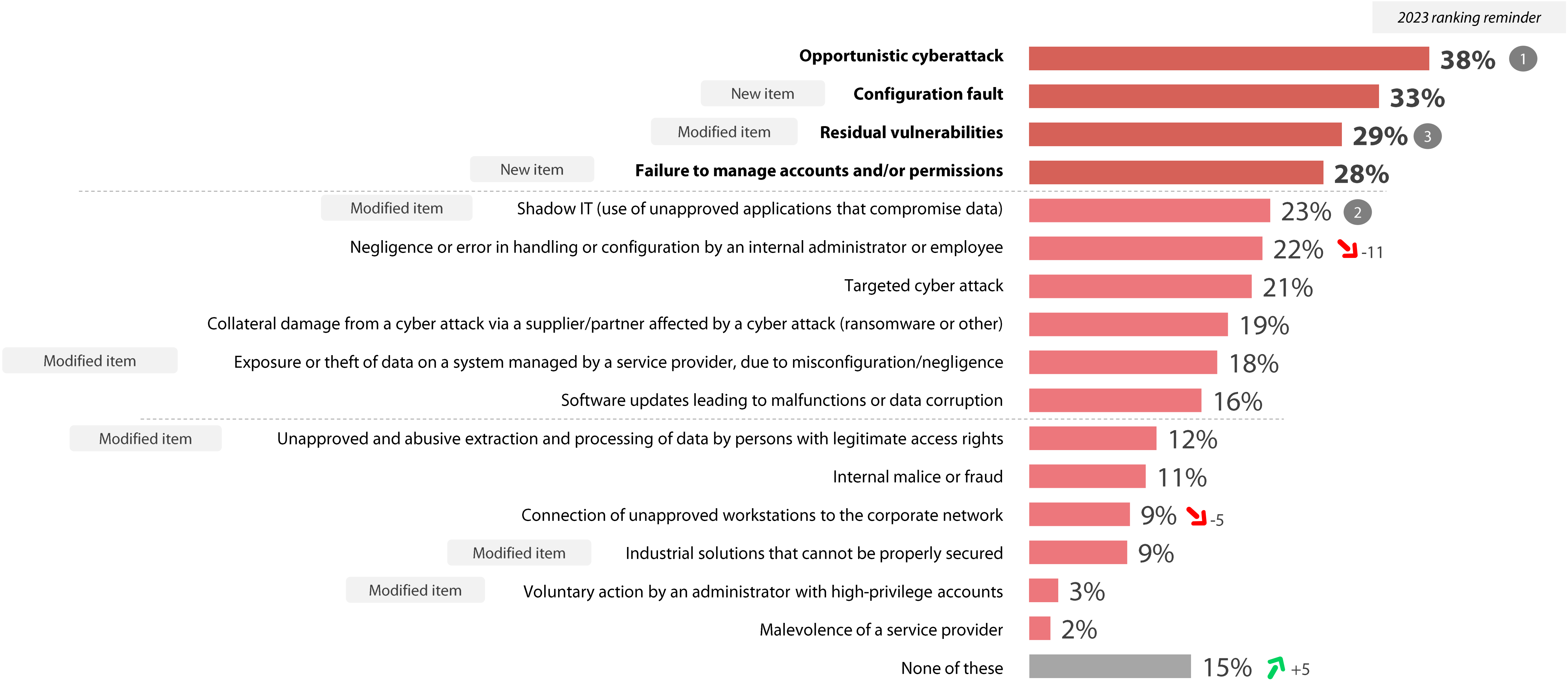
Statistically significant change from previous wave

The majority of security incidents are caused by opportunities left open to attack: opportunistic cyber-attacks, misconfigurations, residual vulnerabilities and account management failures, relegating Shadow IT to 5th this year (vs. 2nd the previous year).

401 people

Q6. Which of the following causes of security incidents, including cyber-attacks, has your company had to face in the last 12 months?

Base: all - multiple answers possible



“opinionway for CESIN

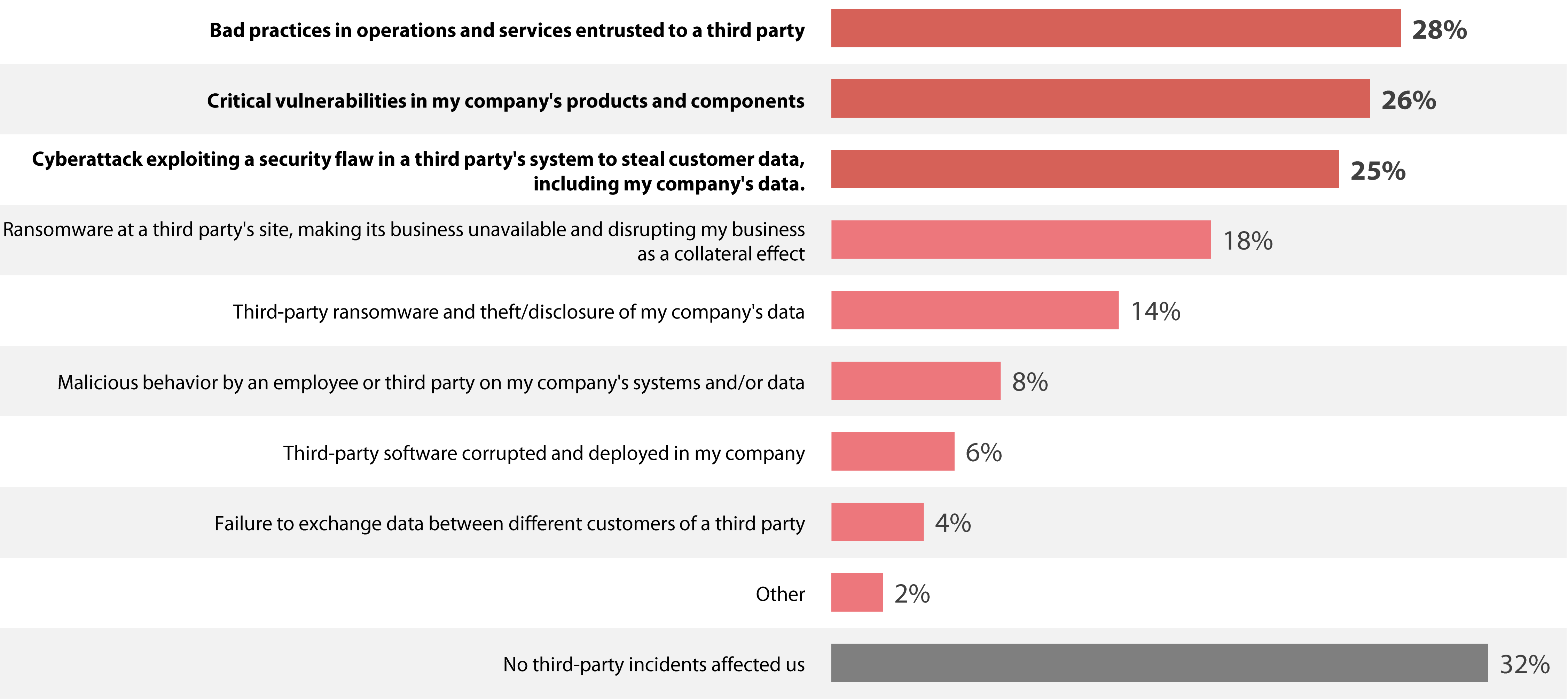
With regard to third-party incidents, ¼ of companies have noted poor practices in operations entrusted to third parties, critical product vulnerabilities or a cyber attack linked to a third-party security flaw.

401 people

New question in 2024

Q40: What third-party incidents have affected you?

Base: all - multiple answers possible



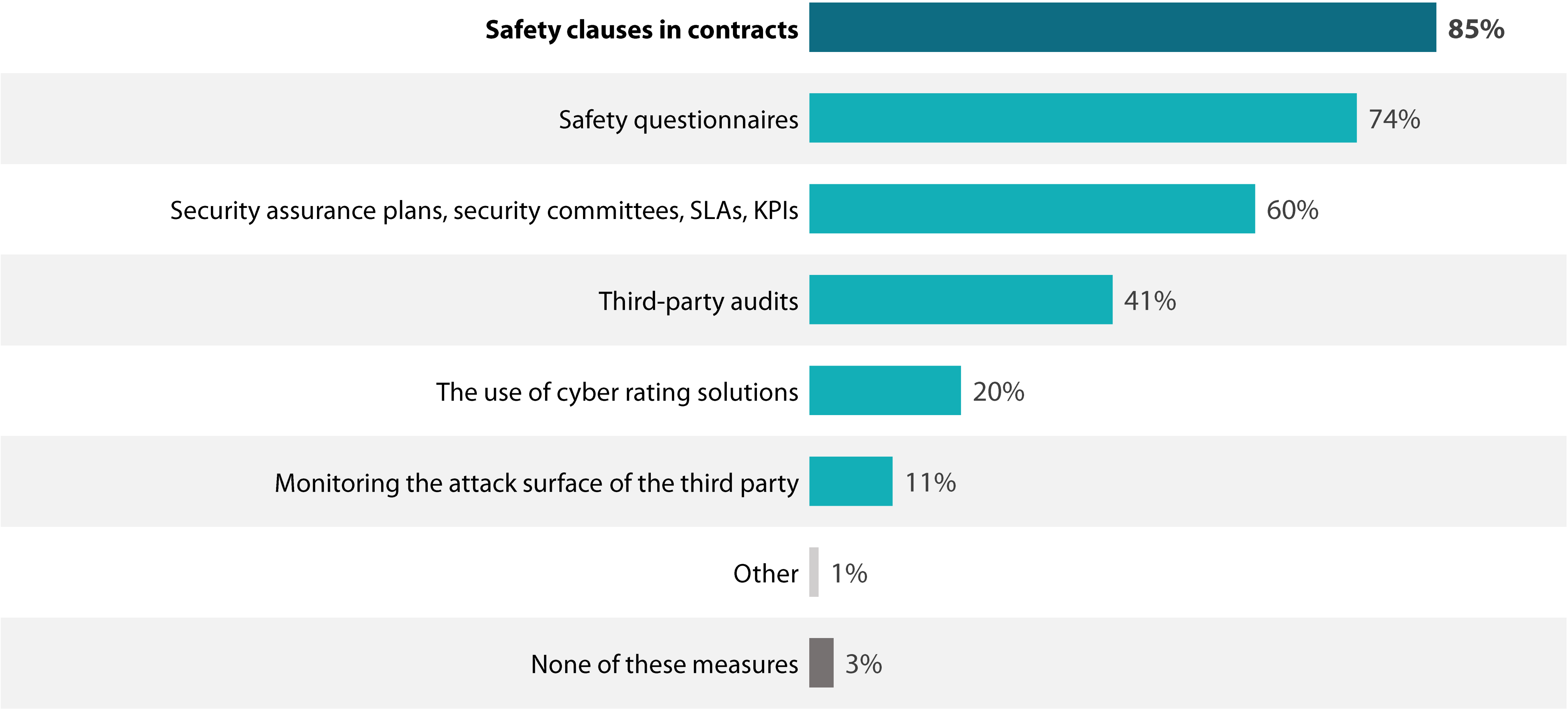
To address this third-party risk, companies rely first on safety clauses in contracts, then on safety questionnaires, and finally on safety insurance plans.

401 people

New question in 2024

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

Base: all - multiple answers possible



Nearly 4 out of 10 companies rate the risk of cyberespionage as high, which is an important factor given that some companies, by virtue of their activity, are not very concerned by this type of risk.

401 people

Q9. Today, how would you assess the level of cyberespionage threats to your company?

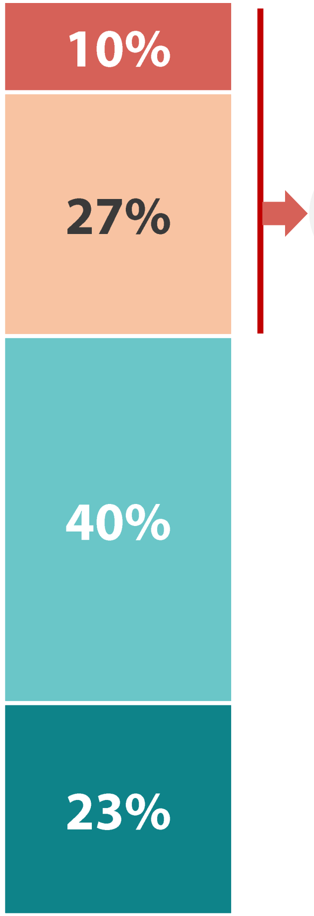
Base: all

Modified item — **Very high : one of the top 3 cyber risks identified**

Modified item — **Quite high : one of the top 10 cyber risks identified**

Modified item — **Fairly low : present in cyber risk mapping**

Modified item — **Very low : not included in cyber risk mapping**



37% **Estimate a high level of threat on cyber espionage**

Industry/Public Works: 46%

02

High-performance defenses that have proven their effectiveness over the years (notably firewalls, EDR and MFA).

In the same proportions as last year, companies are still satisfied with the adequacy of security solutions and services available on the market.

401 people

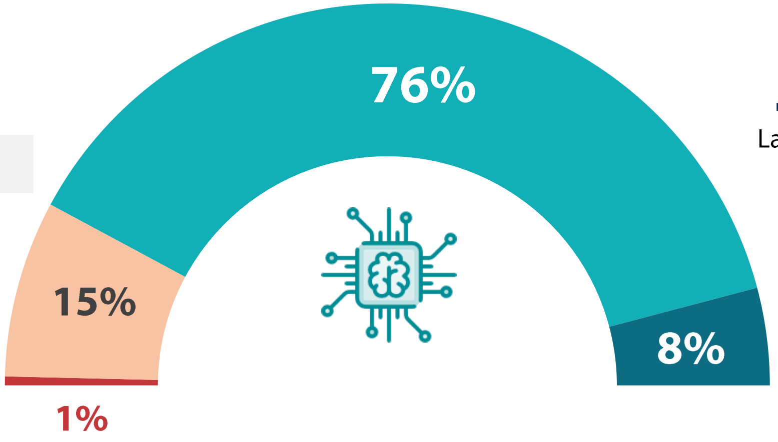
Q25. Do you think that the security solutions and services available on the market are completely, somewhat, rather not or not at all adapted to your company?
Base: all

Not at all suitable | Rather unsuitable | Rather adapted | Perfectly suited

% Unsuitable

16%

Wave 9 reminder: 13%

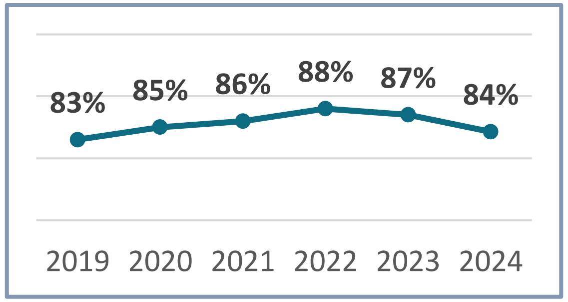


% Adapted

84%

Large companies: 90%

Previous waves reminder

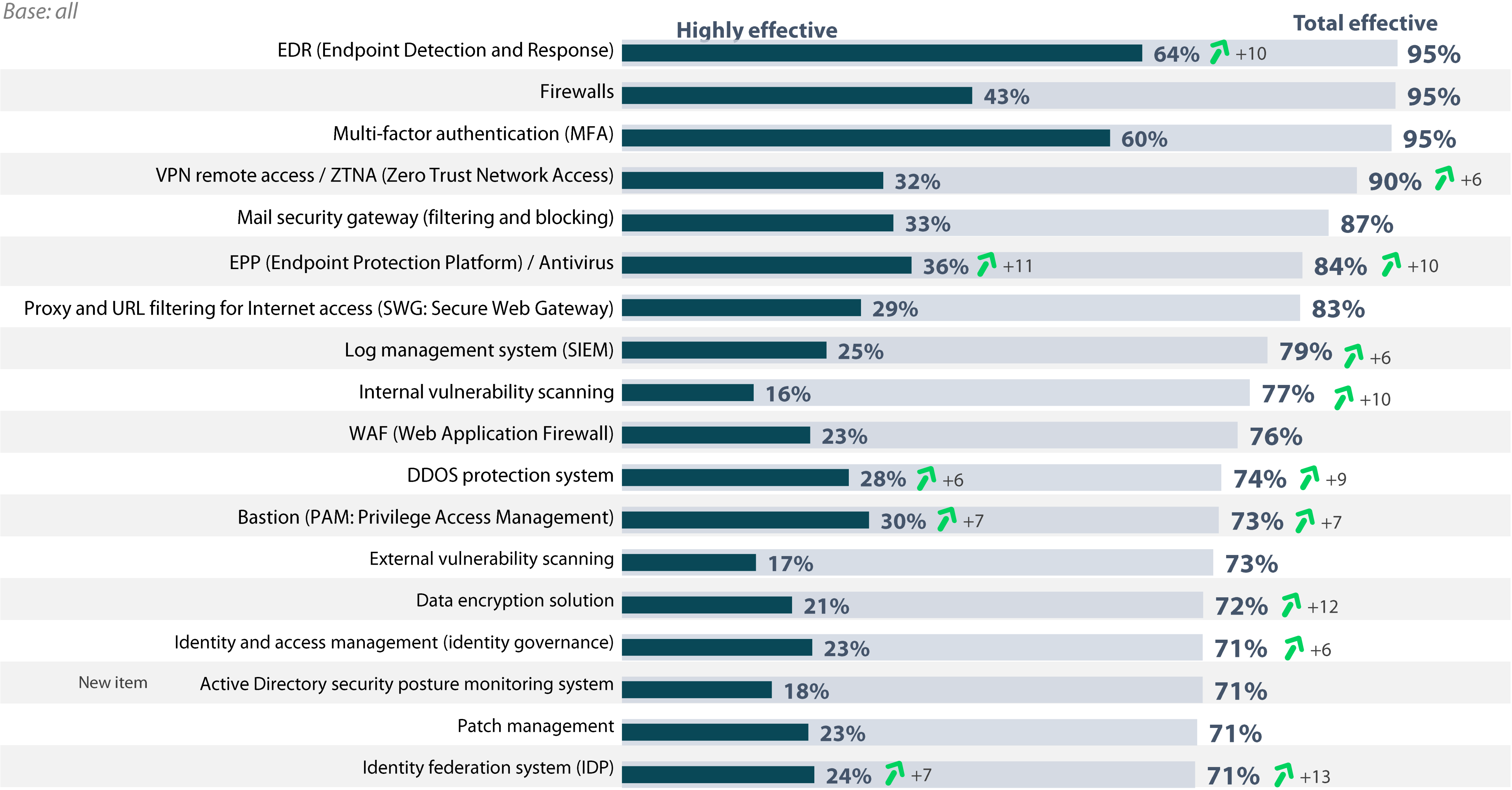


In detail, EDR, firewalls and MFA are considered the most effective solutions, with EDR even gaining points in the "very effective" category.

401 people

Q13. For each of the following solutions, do you consider it to be very effective, rather effective, rather not effective or not at all effective?

Base: all

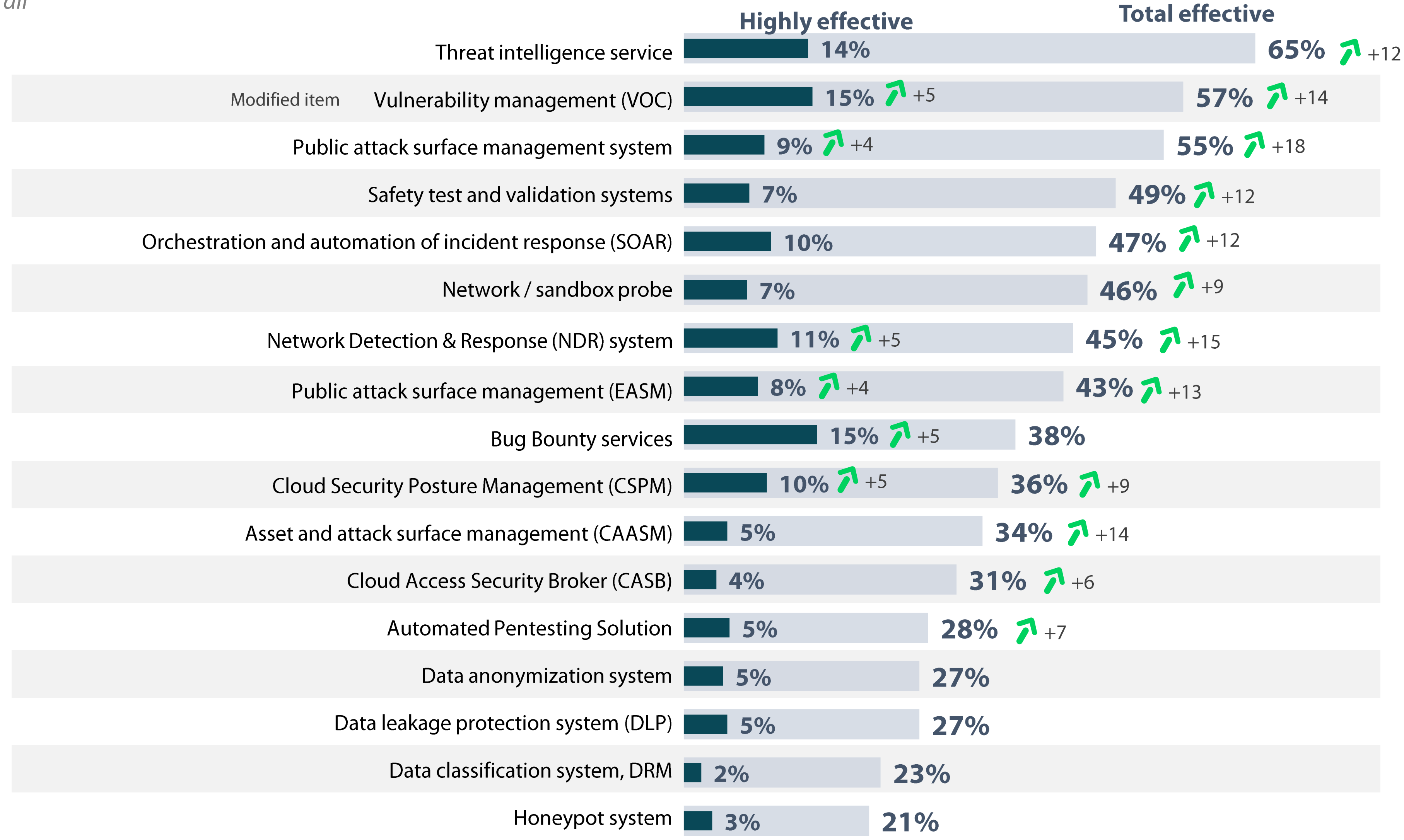


The effectiveness of most other solutions also improved this year.

401 people

Q13. For each of the following solutions, do you consider it to be very effective, rather effective, rather not effective or not at all effective?

Base: all



Firewalls, EDR and MFA continue to top the list of solutions deployed in companies. Mail security gateways are also on the rise, joining the podium. Overall, companies are protecting themselves more.

401 people

Q13. For each of the following solutions, do you consider it to be very effective, rather effective, rather not effective or not at all effective?

Base: all - multiple answers possible

Solution deployed

Solution	Deployed	Change
Firewalls	**100%**	
EDR (Endpoint Detection and Response)	**96%**	
Multi-factor authentication (MFA)	**96%**	
Mail security gateway (filtering and blocking)	**96%**	↗ +4
VPN remote access / ZTNA (Zero Trust Network Access)	95%	
EPP (Endpoint Protection Platform) / Antivirus	94%	↗ +9
Proxy and URL filtering for Internet access	91%	
Patch management	91%	↗ +6
Internal vulnerability scanning	88%	↗ +9
Log management system (SIEM)	87%	
External vulnerability scanning	85%	↗ +7
WAF	84%	
Data encryption solution	83%	↗ +16
Identity and access management (identity governance)	82%	↗ +8
DDOS protection system	80%	↗ +8
Bastion (PAM: Privilege Access Management)	79%	↗ +5
Active Directory security posture monitoring system*	79%	
Threat intelligence service	78%	↗ +13

Solution	Deployed	Change
Identity federation system (IDP)	76%	↗ +12
Vulnerability management (VOC)**	71%	↗ +19
Public attack surface management system	67%	↗ +21
Safety test and validation systems	60%	↗ +13
Network / sandbox probe	57%	↗ +9
Orchestration and automation of incident response (SOAR)	57%	↗ +13
Public attack surface management (EASM)	54%	↗ +16
Network detection and response system (NDR)	52%	↗ +16
Data leakage protection system (DLP)	49%	↗ +10
Data classification system, DRM	47%	↗ +11
Asset and attack surface management (CAASM)	46%	↗ +18
Data anonymization system	45%	↗ +8
Cloud Security Posture Management (CSPM)	45%	↗ +12
Bug Bounty services	42%	
Cloud Access Security Broker (CASB)	40%	↗ +7
Automated Pentesting Solution	37%	↗ +7
Honeypot system	31%	

*New item
** Item modified

↗ ↘ Statistically significant change from previous wave

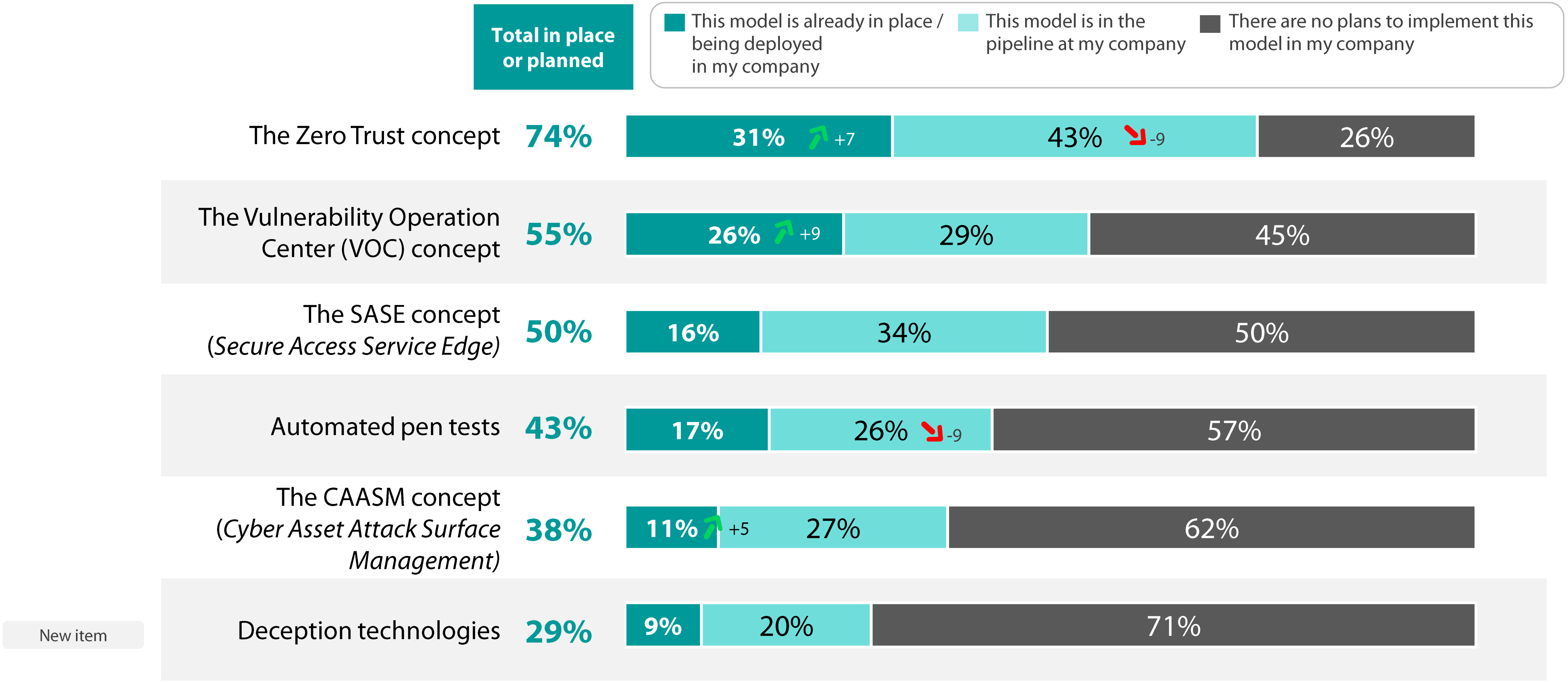
Evolution to be interpreted with caution in view of the addition of items

Zero Trust and VOC are more widely implemented or in the process of being deployed this year, as is CAASM to a lesser extent, which had already begun its ascent last year.

401 people

Q28b. What is your vision of the following concepts?

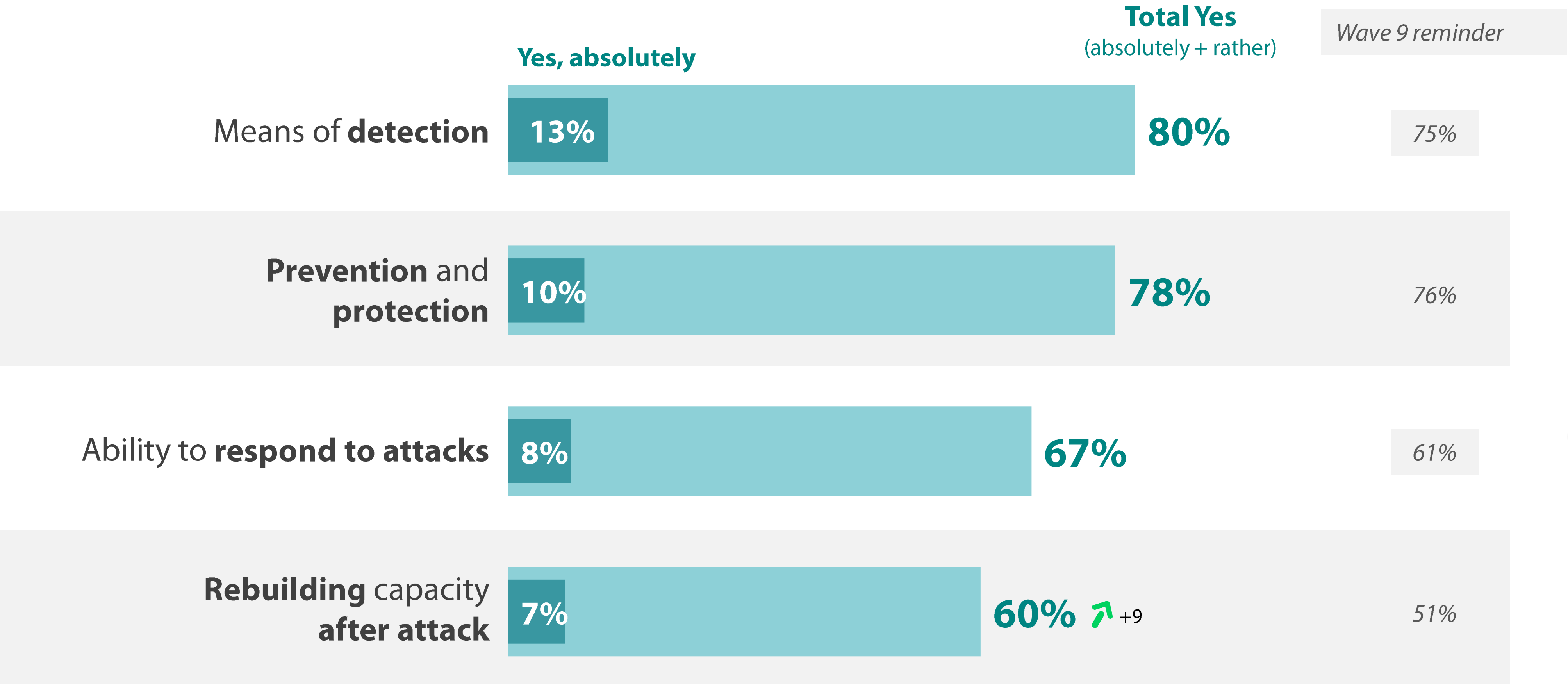
Base: all



While companies are still more confident in their ability to detect and prevent attacks than to respond to them and rebuild, they are nonetheless more confident this year about their ability to rebuild.

401 people

Q14. In your opinion, is your company prepared to handle a large-scale cyber attack in terms of...?
Base: all



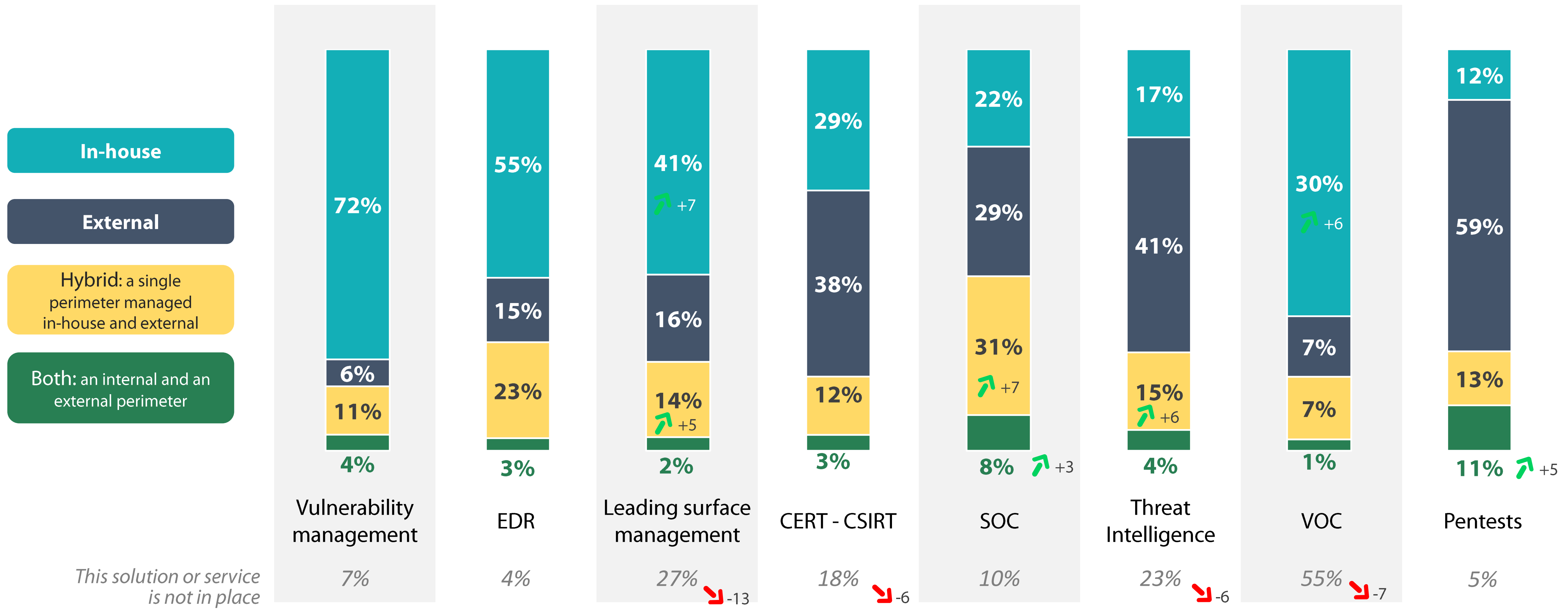
Statistically significant change from previous wave

Management varies depending on the solution: while vulnerabilities, EDR, attack surface and VOC are mainly managed in-house, pentests, threat intelligence and CERT-CSIRT are mostly outsourced, while SOC combines hybrid internal and external management.

401 people

Q30b. How do you operate the solutions and services below?

Base: all - results excluding solutions not implemented



6 out of 10 companies have set up a cyber crisis training program, a proportion that has remained stable since last year.

401 people

Q15. Has your company set up a cyber crisis training program?
Base: all

Wave 9 reminder: 57%

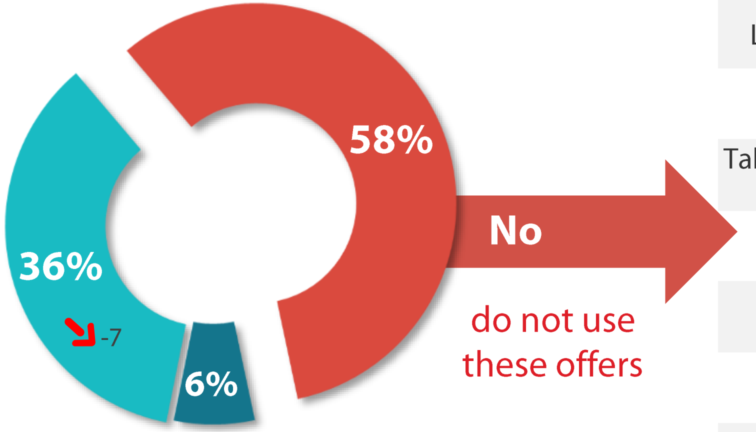
The use of innovative offers from startups concerns 4 out of 10 companies. For the others, lack of budget explains their reluctance, as does the lack of maturity of the offers, which is on the increase this year. On the other hand, fewer and fewer companies see this as a risk.

401 people

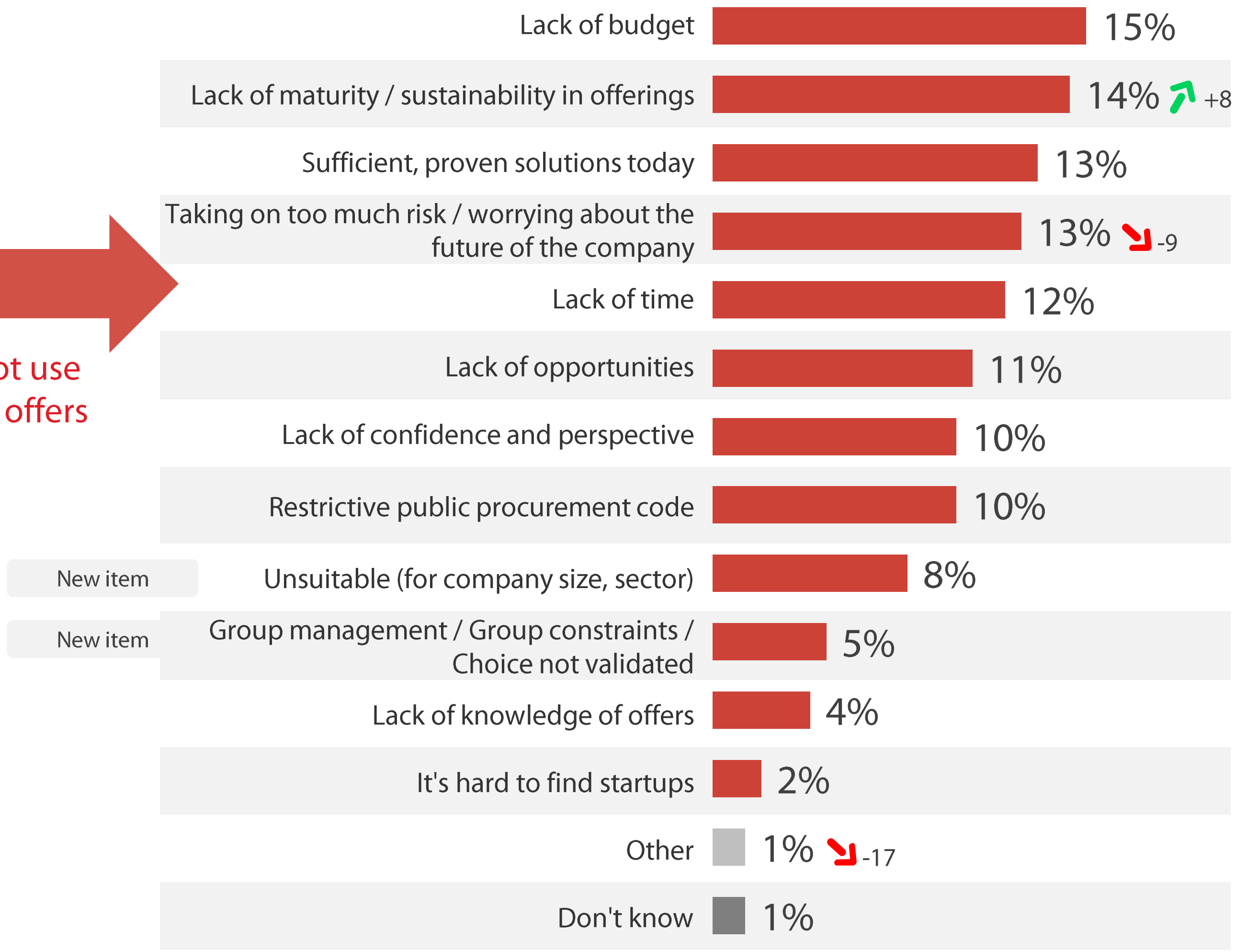
Q26. When it comes to cybersecurity, do you use innovative offers from startups? *Base: all*
Q26bis. Why don't you? *Base: do not use offers from start-ups - excluding non-respondents (152)*

Yes, occasionally

42% use innovative offers from startups



Yes, often



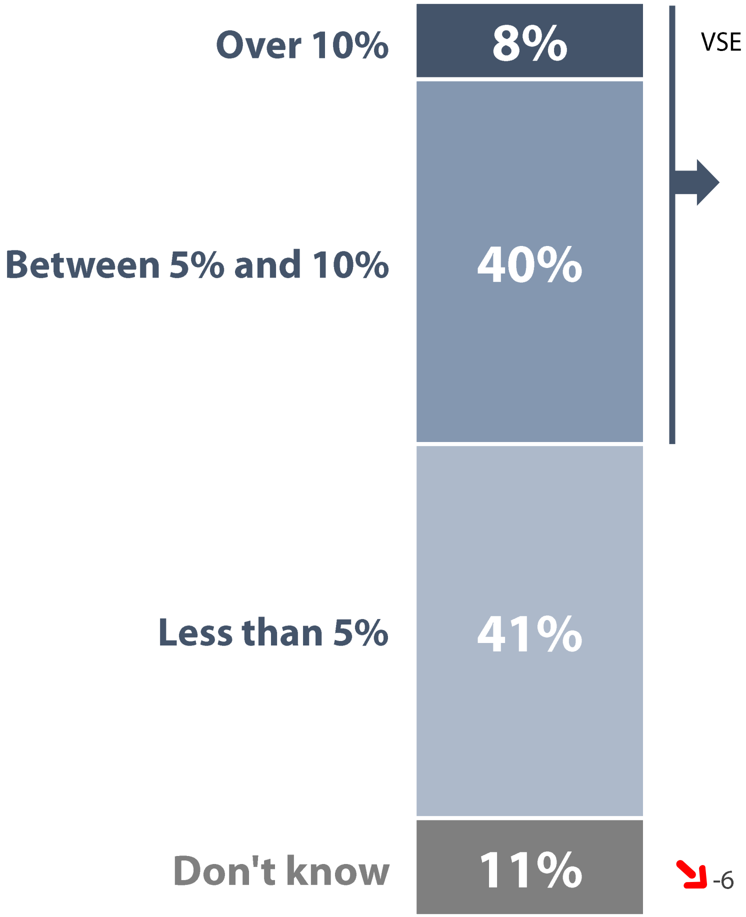
Statistically significant change from previous wave

IT security budgets remain stable for the 3rd consecutive year.

401 people

Q18. In your company, how much of the IT/digital budget is devoted to security?

Base: all

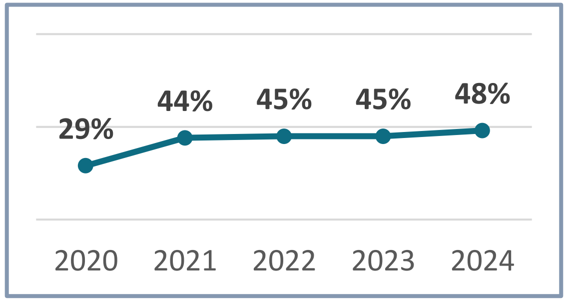


VSE / SME: 16%

5% or more of the IT/digital budget is spent on security: 48%

Wave 9 reminder: 45%

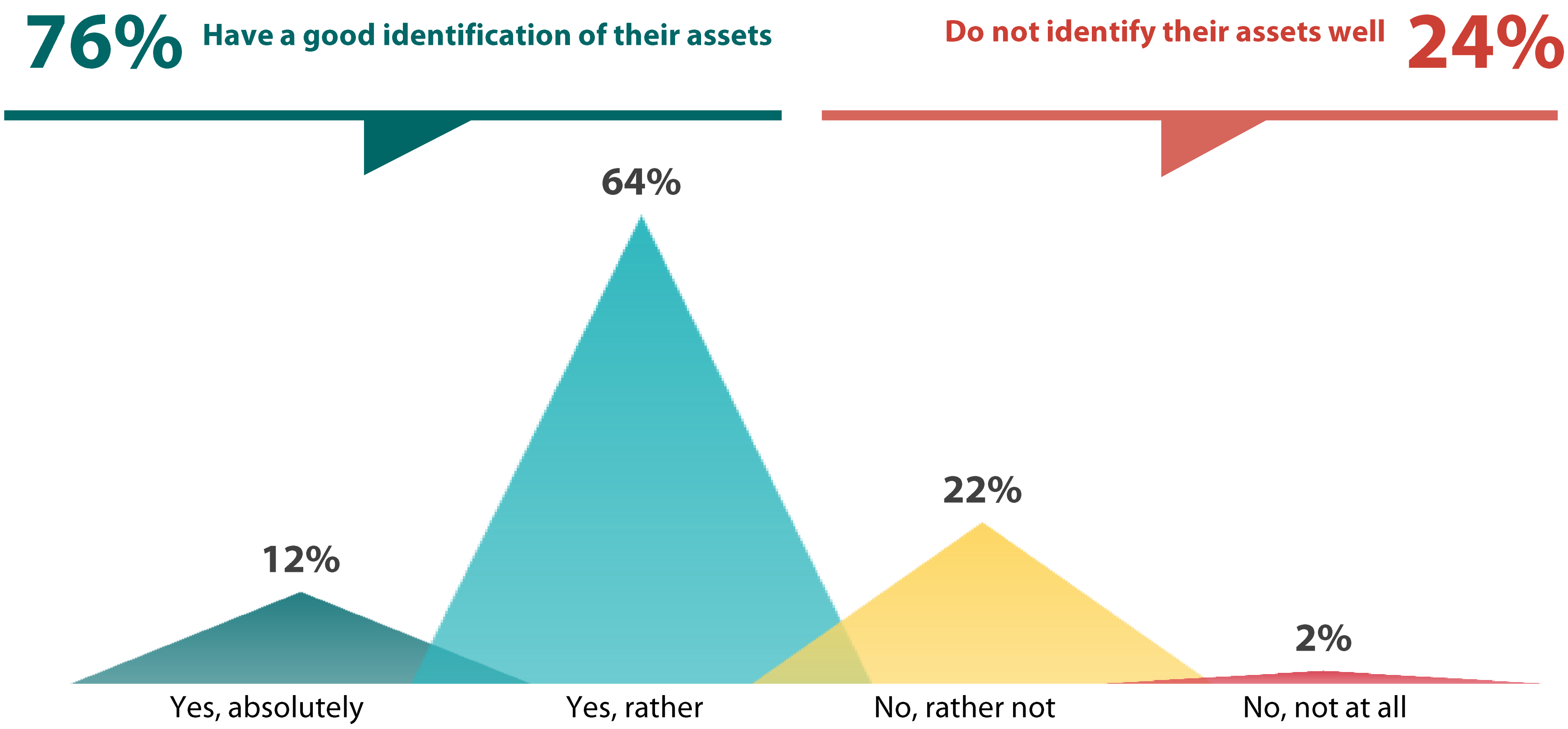
Previous waves reminder



¾ of companies correctly identify their assets.

New question in 2024

Q41: How well do you identify your assets?
Base: all



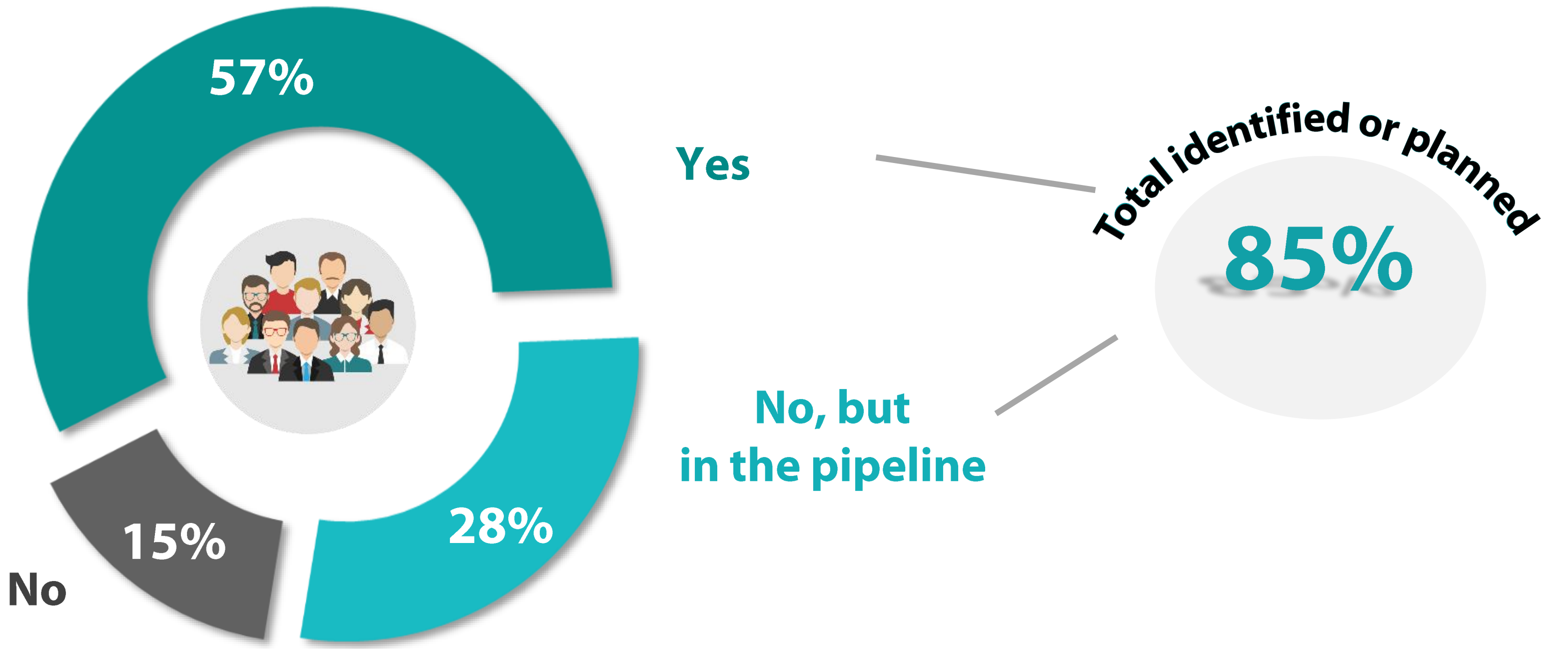
The same applies to the identification of critical assets for the vast majority of companies: while more than half already identify them, ¼ plan to do so.

401 people

New question in 2024

Q42: Have you clearly identified and marked crown jewels?

Base: all

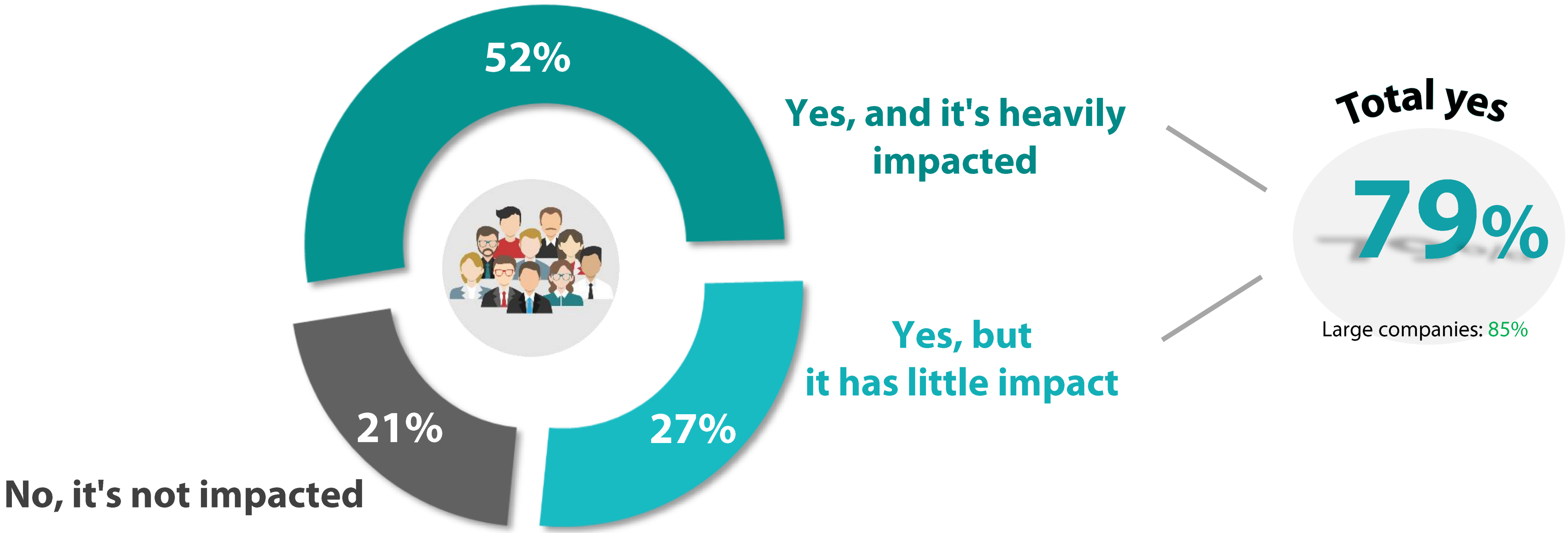


Cyber regulations (excluding GDPR) are of great importance to businesses: the majority are impacted, half of them heavily.

401 people

New question in 2024

Q46: Is your company impacted by one or more cyber regulations (excluding GDPR)?
Base: all



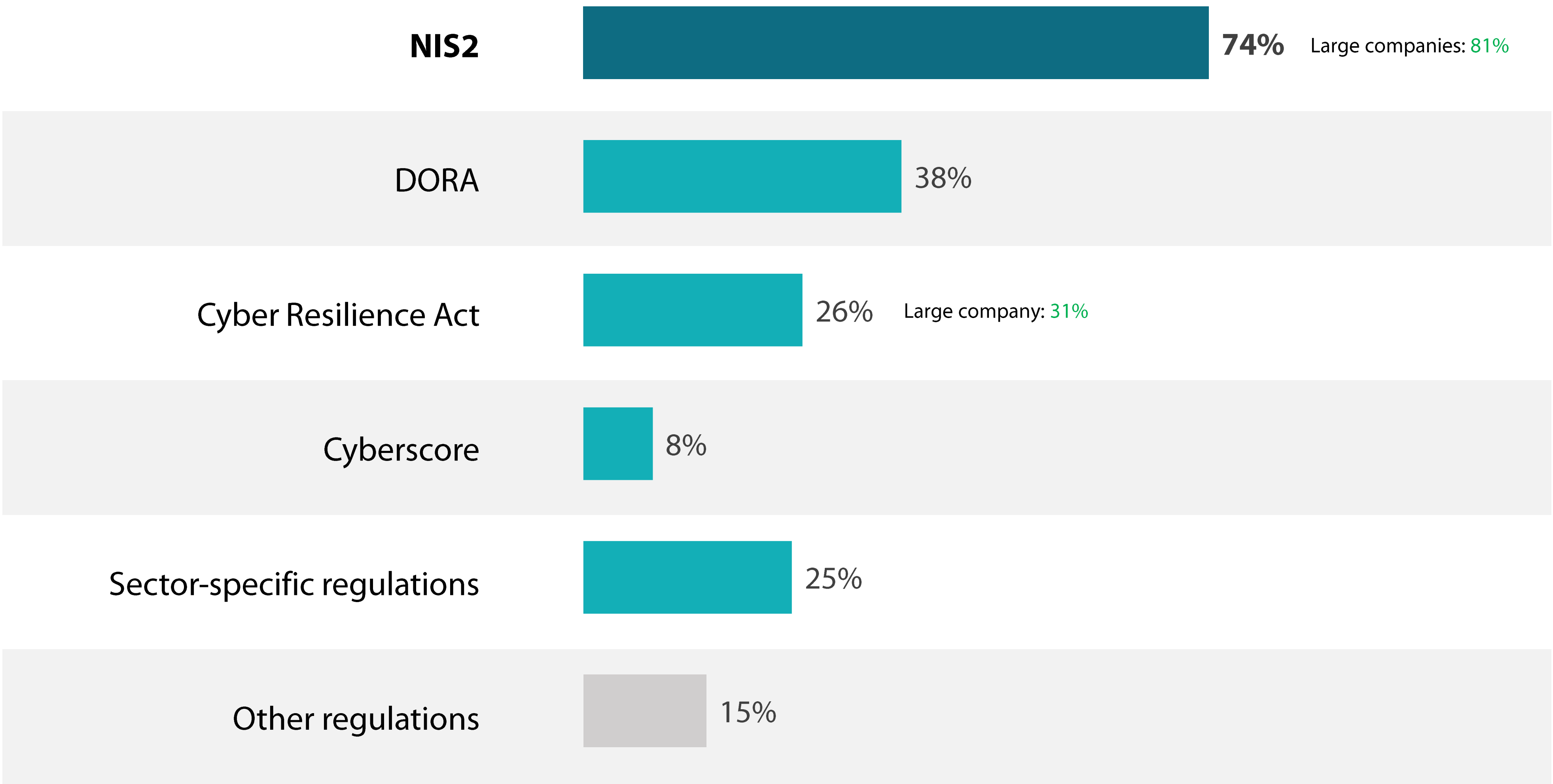
In detail, it is the NIS2 regulation that has the greatest impact on businesses, far ahead of DORA and the Cyber Resilience Act. Meanwhile, Cyberscore remains in the minority.

317 people

New question in 2024

Q47: What cyber regulations does your company have to comply with?

Base: your company is impacted by one or more cyber regulations (excluding RGPD) - multiple answers possible



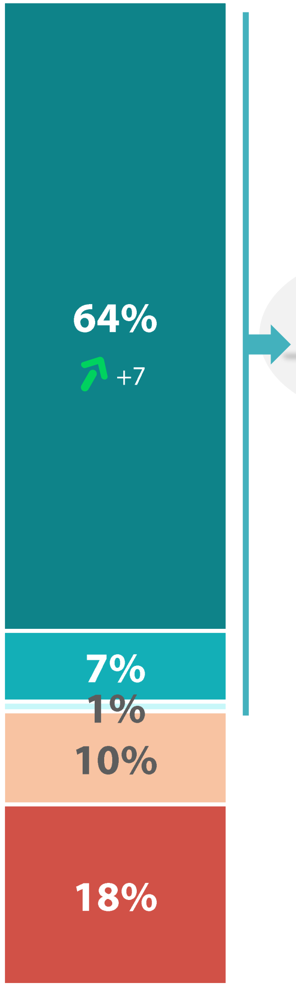
Focus on…

Cyber insurance

While the proportion of companies with cyber insurance remains stable in 2024 (7/10), more and more are planning to renew their contracts.

401 people

Q31. Do you have cyber insurance?
Base: all



Yes, and you intend to renew your contract

Large companies: 74%

Yes, but you're reluctant to renew your contract because of changing rates and reduced insurance coverage

Yes, but you haven't renewed your contract

No, but it's in the pipeline

No, you don't intend to take out cyber insurance

72% Have taken out cyber insurance

Wave 9 reminder: 70%

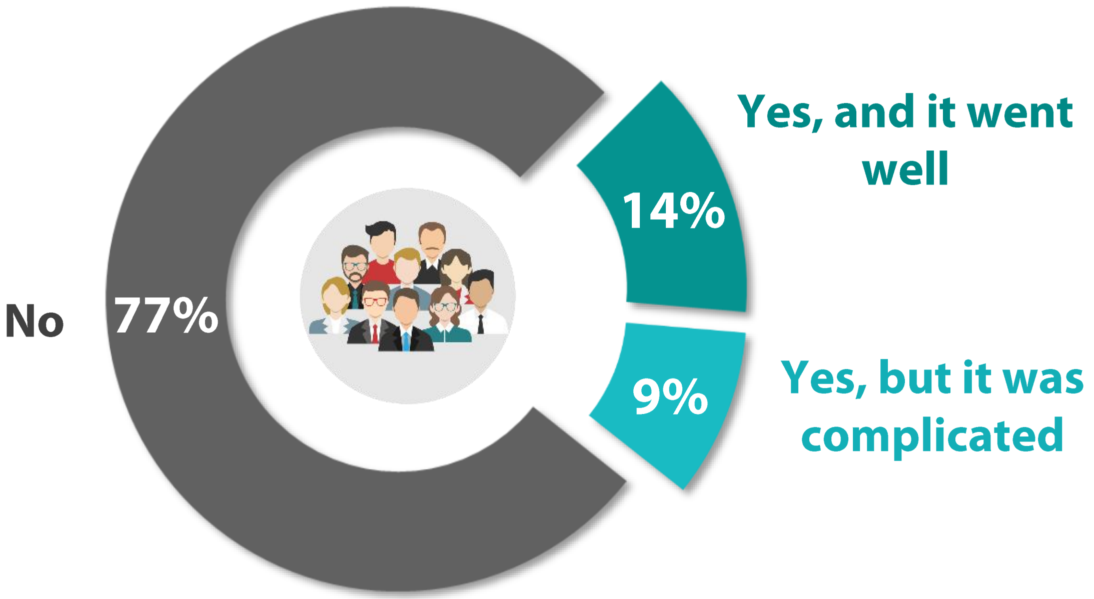
Large companies: 80%

Even so, only a quarter of companies have ever called on their cyber insurance in the event of an attack.

289 people

Q32. Has your company ever called on its cyber insurance in the event of a cyber attack?
Base: have or plan to have cyberinsurance

Using cyberinsurance



Total yes

23%

Reminder Wave 9: 25%

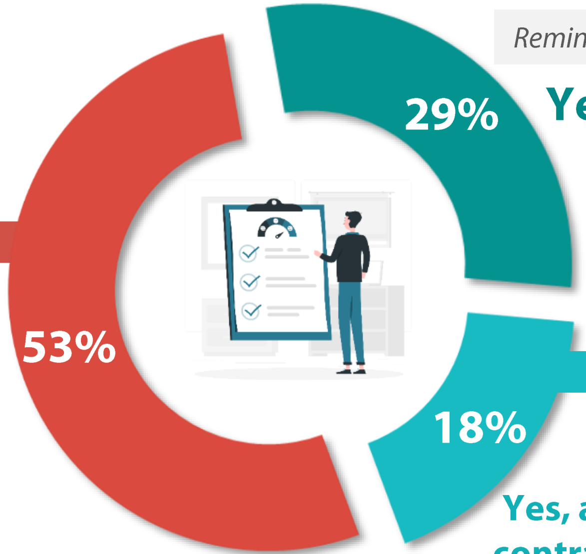
Large companies: 30%

The perception of the use of rating agencies by cyber insurers divides companies: half think it's a good idea, mainly because it gives them the opportunity to find out how third parties view their company. The others are not convinced by the analysis and scores produced by these agencies.

401 people

Q33. Cyber insurers are increasingly using the services of rating agencies. Do you think this is a good thing? *Base: all*
Q33b. And why did you contract cyber-rating services? *Base: have contracted cyber-rating services (72)*
Q33bis. For what reasons? *Base: don't think it's a good thing (212)*

Using the service rating agencies



Yes – 29% — *Reminder Wave 9: 25%*

No – 53% — *Wave 9 reminder: 57%*

Yes, and I have myself contracted the services of cyberrating – 18% — *Wave 9 reminder: 18%*

No – reasons

Reason	%	
Because, by design, these platforms only provide a very partial analysis of the level of security, and provide a score by extrapolation.	68%	
Because the criteria and method of calculating scores are questionable from the point of view of defined priorities	63%	
Because there's too much opacity and instability in score calculations	55%	New item
Because the results are unreliable in identifying and assigning assets	53%	
Because these services are a form of forced solution selling	38%	
For another reason	3%	

Yes, and I have myself contracted the services of cyberrating – reasons

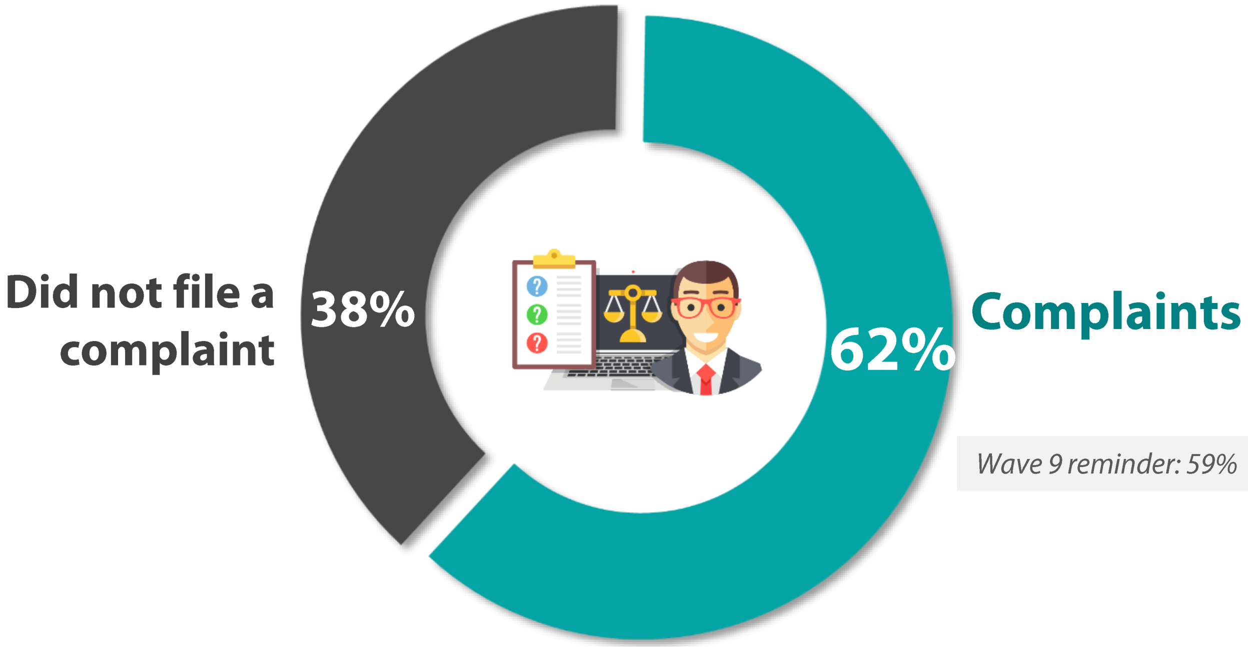
%	Reason	
65%	To find out how others view my company online	New item
57%	I consider it useful for my surveillance	New item
49%	To improve my rating, as this is an indicator requested/monitored by my Executive Committee.	New item
42%	To assess the safety level of my third parties	New item
6%	Other reasons	

Almost 2/3 of companies file a complaint in the event of a cyber-attack, including almost 1/3 for all attacks.

190 people

Q8. Did you file a complaint following the cyber attack(s) your company suffered?
Base: observed an attack

47% of companies suffered at least one cyber attack in 2024



Wave 9 reminder: 59%

for **all attacks**: **29%**

for **certain attacks**: **33%**

03

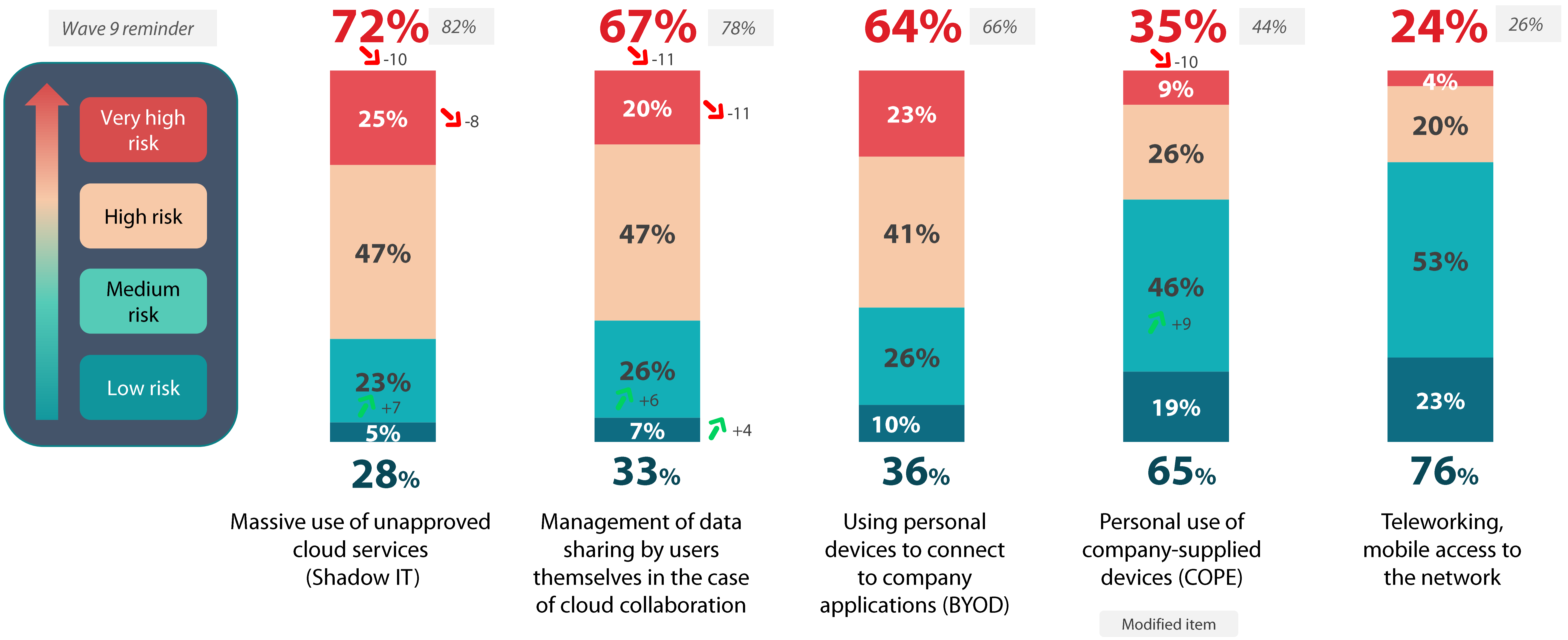
Reduced digital risks thanks to effective awareness-raising and training of employees

The level of risk associated with employees' digital practices has fallen this year, with regard to Shadow IT and data sharing via cloud collaboration (although the risk remains high), as well as personal use of company devices.

401 people

Q23. How do you assess the level of risk induced by the following uses of digital technology by employees?

Base: all



Cybersecurity awareness and training for all employees (users, administrators, architects and developers) remains stable this year, with companies particularly confident in cyber risk awareness.

401 people

Q19. With regard to raising awareness and training employees in cybersecurity, do you think that?

Base: all

	Yes, absolutely	Total Yes (absolutely + rather)	*Wave 9 reminder*
Users are made aware of cyber-risks	29%	85%	83%
Administrators, architects and developers are aware of and apply good security practices in operations, design and development	13%	73%	73%
Users comply with recommendations	3%	70%	66%
Most incidents exploited poor IT practices	13%	67%	61%
Administrators, architects and developers are adequately trained and have acquired the necessary expertise, particularly in new technologies	9%	52%	48%
Users take precautions that go beyond the recommendations given	2%	25%	24%

Focus on…

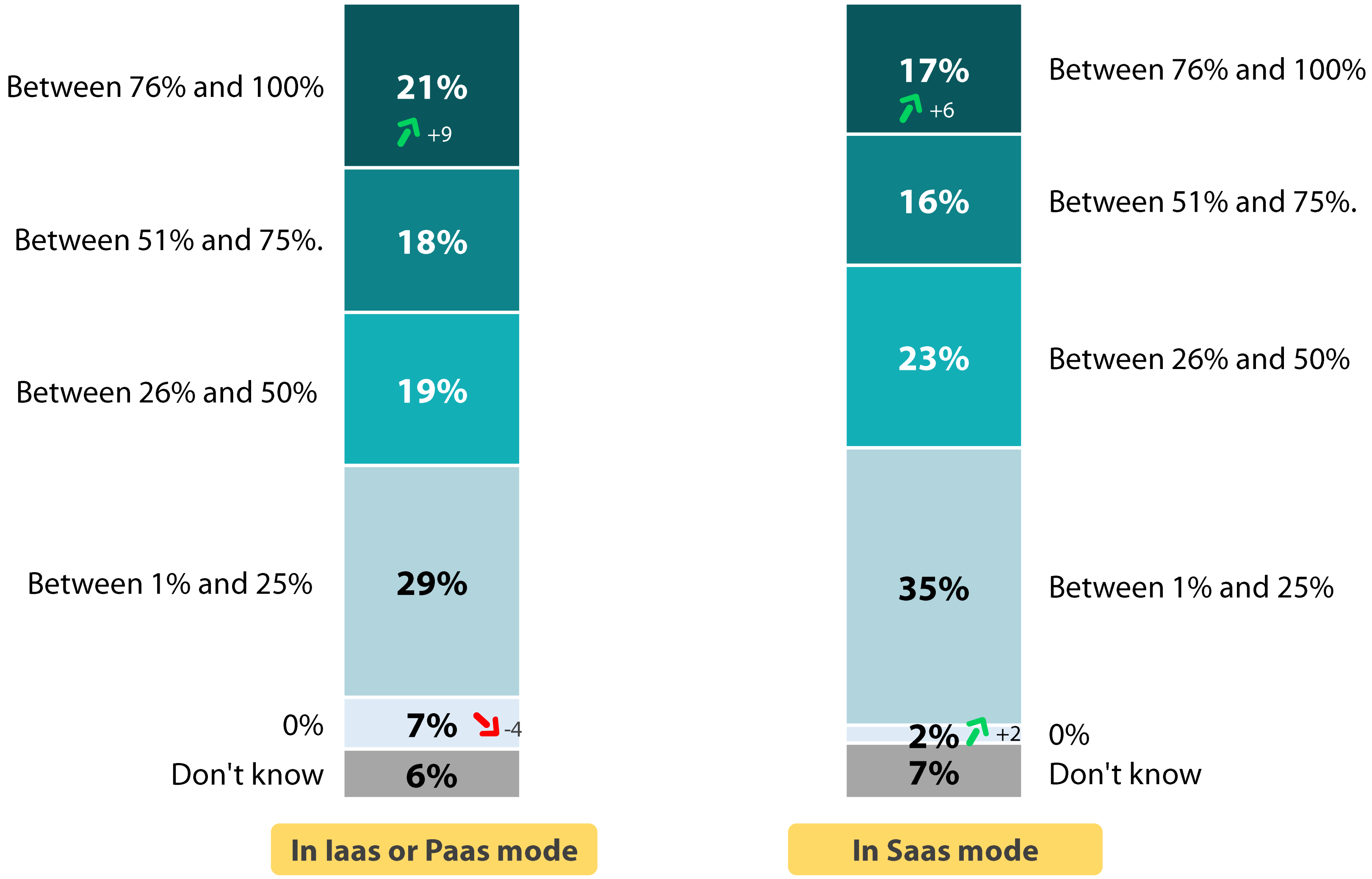
The Cloud

For both Iaas/Pass and Saas modes, the cloud has been adopted by less than 50% of the IS in the majority of companies. However, there has been an increase in adoption to over 75%.

401 people

Q20b. How much of your IS is in the Cloud, whether in Iaas, Paas or Saas mode?

Base: all



The risks of using the Cloud lie mainly in the control of subcontractors (although in decline since 2023), the difficulty of carrying out audits, and access control by administrators (also in decline). Poor visibility of Cloud resource inventory is less of a risk for companies this year (whereas it was the 3rd risk in 2023).

401 people

Q21. In your opinion, do the following factors represent a low, moderate or high risk when it comes to using the Cloud?

Base: all

2023 ranking reminder	% High risk	
↘ -9 / 1	40%	**No control over the hosting provider's subcontracting chain**
	37%	**Difficulty of carrying out audits (penetration testing, configuration control, on-site visits)**
↘ -7 / 2	36%	**Difficulty of controlling access by host administrators**
	34%	Expertise still too rare, expected from architects and administrators
5	34%	Data storage in foreign datacenters, outside French law
4	34%	Data stored in France/Europe but provided and/or operated by foreign service providers where the law of the country of origin also applies
	33%	Difficult to control how your employees use it
	32%	Lack of compartmentalization between the host's different customers
	31%	Unavailability of data/application due to an attack on the hosting provider
↘ -10 / 3	31%	Poor visibility of the inventory of resources in the cloud
	29%	Data confidentiality vis-à-vis the hosting provider
↘ -7	29%	Non-control of security parameters / weak encryption on the part of the host (the host manages the decryption keys)
	26%	High frequency of new online versions with potential uncontrolled changes to safety principles or parameters
	25%	Systemic propagation of attacks and human errors at the host level
	25%	Difficulty or impossibility of feeding logs from the cloud into the SIEM system
↘ -10	23%	Failure by the hosting provider to delete data at the end of the contract (normal or early) when contractually required to do so
↘ -7	23%	Bounce attack from host
↘ -7	22%	Failure to erase data during use, as deletions and purges carried out by the customer are not really effective
	22%	Data processing and use by the host without the customer's knowledge
	21%	Non-restitution of data by the hosting provider at the end of the contract (normal or early) when contractually agreed
	15%	Trapping a hosted application

↗ ↘ Statistically significant change from previous wave

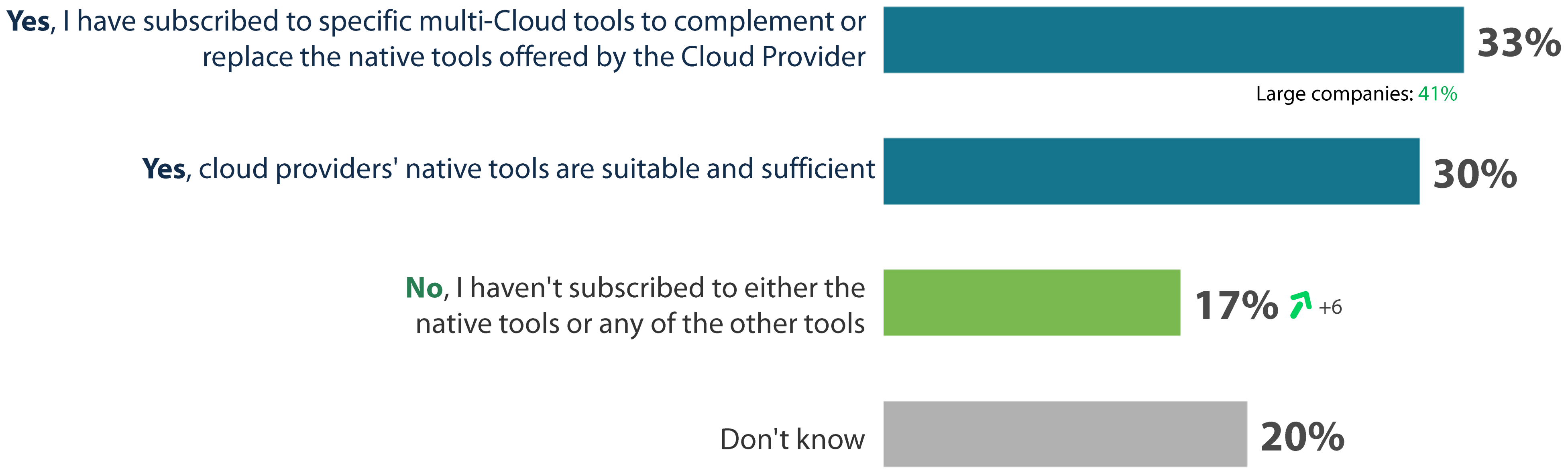
Nearly 2/3 of companies believe that securing data stored in the cloud requires specific tools, with 1/3 having subscribed to additional tools for this purpose.

401 people

Q22b. In your opinion, does securing data stored in the Cloud require any specific tools or devices?
Base: all

... 63% believe that securing data stored in the Cloud requires specific tools

Large companies: 70%



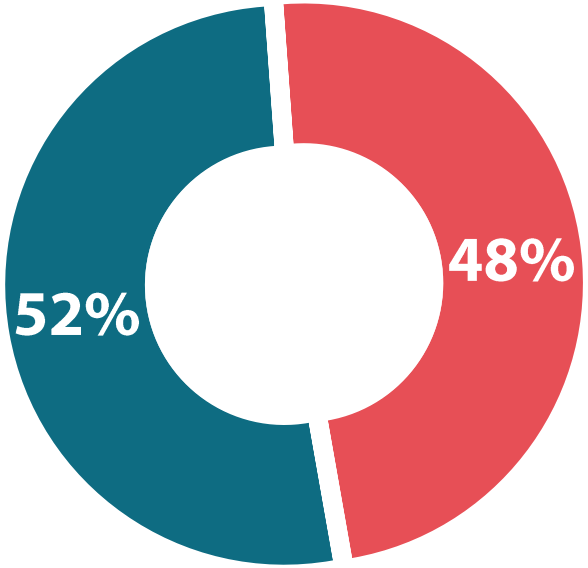
Half of companies feel concerned by the subject of sovereignty and the Trusted Cloud, in the same proportions as last year.

401 people

Q35. A number of initiatives have recently been launched in the field of sovereignty and the Trusted Cloud. Do you feel concerned by these issues?

Base: all

Sovereignty and Trusted Cloud



Yes, it's a concern for my company

VSE / SME: 71%

No, my company is not concerned by these issues

04

Companies need to adapt to digital transformations, including the rise of AI

The use of AI has risen sharply since 2023, and now concerns 7 out of 10 companies, 1/3 of which have officially integrated it into their security strategy.

401 people

Question modified in 2024

Q39. AI, already used to a greater or lesser extent in certain cyber solutions, has made its way into our IS, with a large number of initiatives around generative AI in particular. What role does AI play in your organization today?

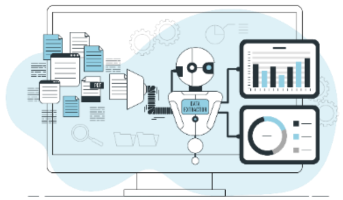
Base: all

AI is officially used internally by business or development teams, and is now integrated into your security strategy (security policy, charter, contracts, risk analyses, auditing of AI-generated code, etc.). Any use other than controlled use is treated as Shadow IT	35%	↗ +18
AI is officially used internally by the business or development teams, but you haven't yet built a strategy enabling it to be properly taken into account in terms of safety	34%	
We have set up a campaign to raise employee awareness/train them in the risks associated with the use of generative AI	29%	
AI is not formally used internally, and its integration is currently akin to Shadow IT	19%	↘ -23

69% ↗ +23

AI used

Large companies: 79%



↗↘ Statistically significant change from previous wave

Adapting security solutions and processes to digital transformations remains essential in this context of AI development, the first challenge identified for the future of cybersecurity.

401 people

Q27. Which of the following issues do you consider to be the three most important for the future of corporate cybersecurity?
Base: all

TOP3 issues

First of all
In total (cited in 1er , in 2e or in 3)e

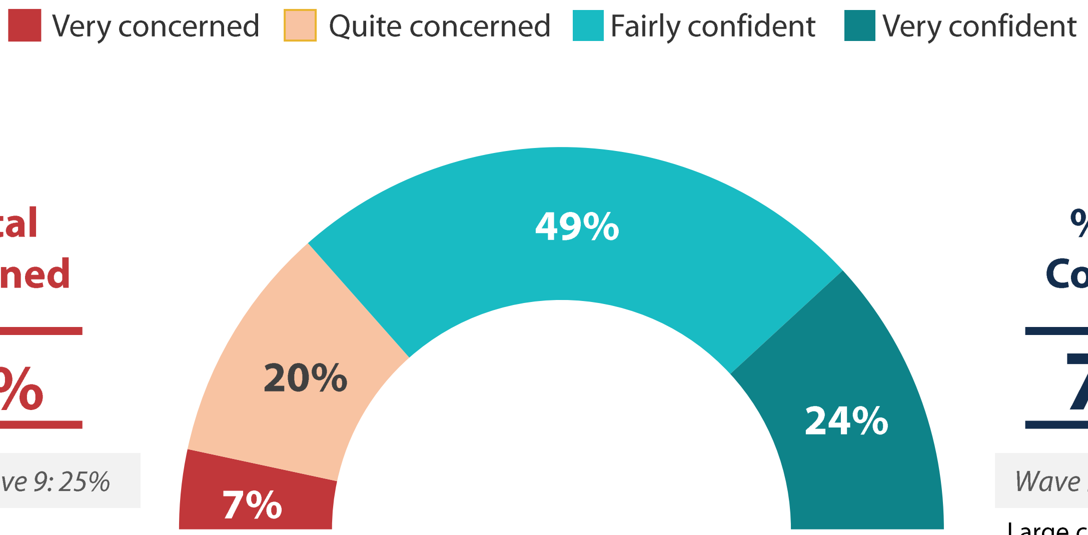
Issue	First of all	In total
Adapting security solutions and processes to the company's digital transformation (including AI) (Modified item)	20%	55%
Putting cybersecurity governance at the right level	25%	50%
Find the right operating model for implementing security solutions and services	9%	38%
Allocate more budget and resources to cybersecurity	11%	35%
Improving education and training in cybersecurity	10%	28%
Mastering the cybersecurity of connected objects and industrial IT	5%	23%
Raising awareness of cybersecurity issues	6%	19%
Adapting security solutions and services to cloud migration	6%	19%
Adapting security to agile development methods	4%	16%
Develop cooperation between the various public and private players in the defense sector	2%	8%
Develop French and international regulations	2%	7%

¾ of companies trust their COMEX to measure the scale of cybersecurity challenges, in the same measures as in 2023.

401 people

Q24. For the future, would you say you are very confident, fairly confident, fairly worried or very worried about...?
Base: all

Ensuring that your company's COMEX takes cybersecurity **issues into account**



% Total Concerned

27%

Reminder Wave 9: 25%

% Total Confident

73%

Wave 9 reminder: 75%

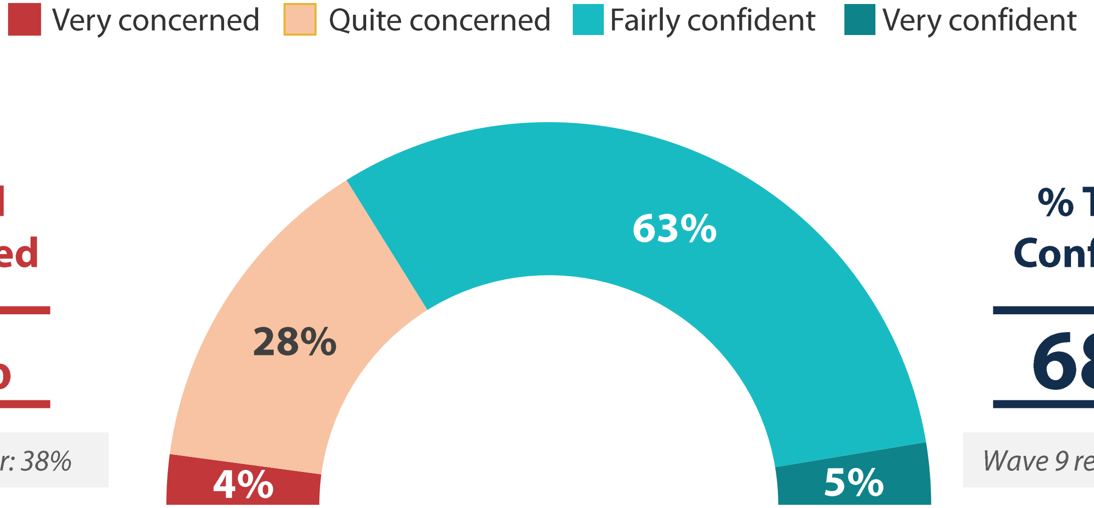
Large companies: 80%

As well as being aware of the challenges, 7 out of 10 companies are confident in their ability to cope with cyber risks.

401 people

Q24. For the future, would you say you are very confident, fairly confident, fairly worried or very worried about...?
Base: all

Your company's **ability to cope with cyber-risks**



% Total Concerned

32%

Wave 9 reminder: 38%

% Total Confident

68%

Wave 9 reminder: 62%

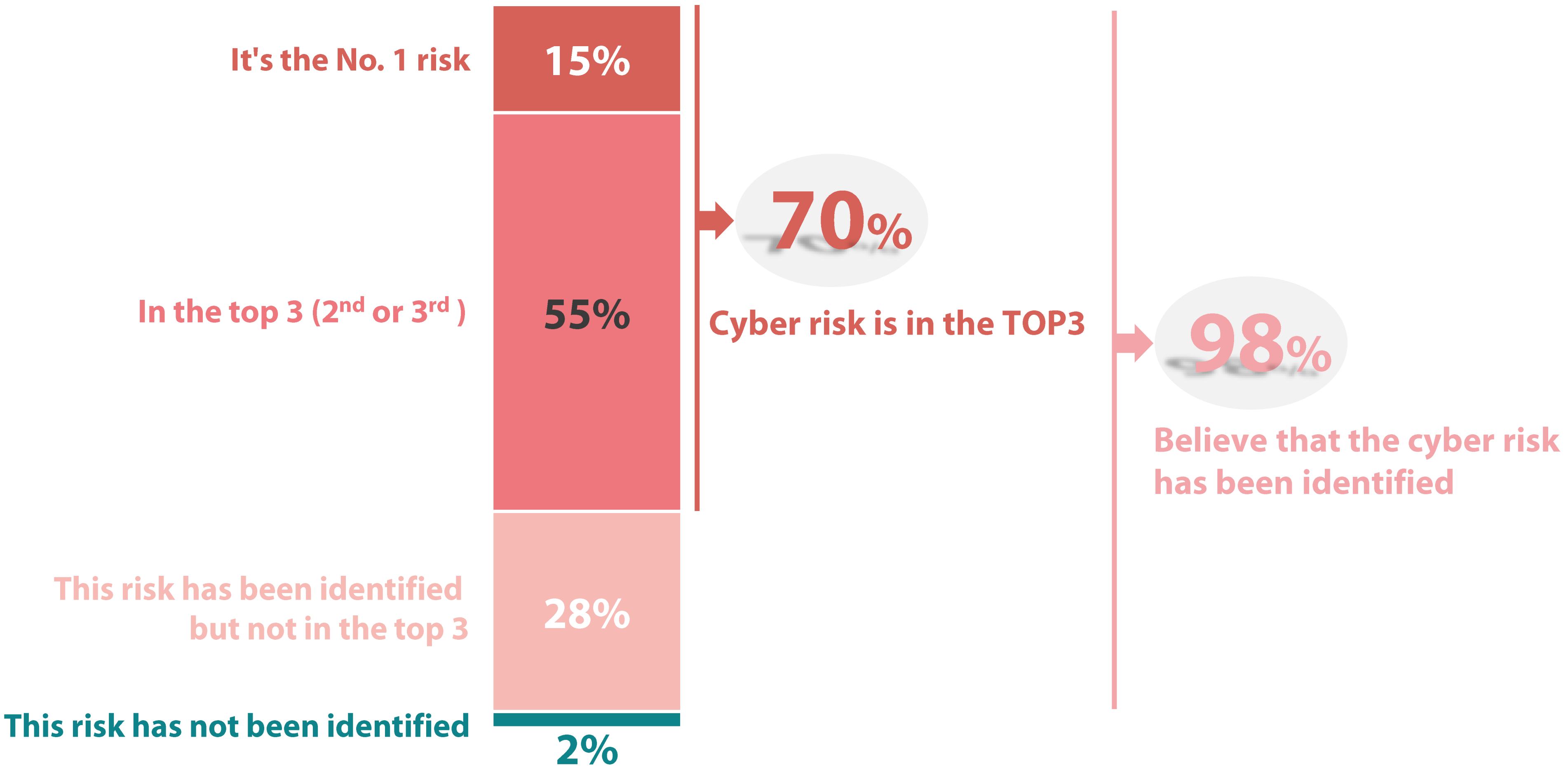
Large companies: 75%

Almost all companies identify cyber risk in their risk mapping, with 7/10 even ranking it in the TOP3.

401 people

New question in 2024

Q48: How is cyber risk positioned in your company's risk map?
Base: all



Modified item

To address cyber risk, almost half of all companies are planning to increase the number of staff dedicated to cybersecurity, although fewer are planning to do so than in 2023.

401 people

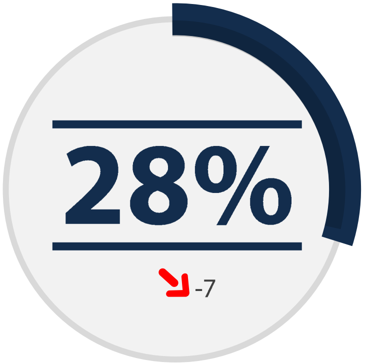
Q17. Over the next 12 months, does your company plan to...?

Base: all

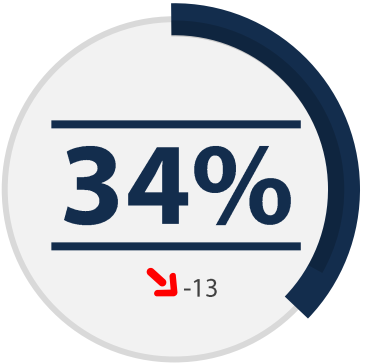
45% plan to increase the number of staff allocated to cyber risk protection

Large companies: 52%

increase the number of staff allocated to the governance of protection against cyber-risks



increase the number of staff allocated to operational cybersecurity to protect against cyber-risks



New item

increase the number of staff allocated to safety culture, awareness-raising and training

Similarly, the desire to acquire new solutions and increase budgets is down this year.

401 people

Q17. Over the next 12 months, does your company plan to...?

Base: all

increase budgets allocated to protection against cyber-risks

acquire new technical solutions for cybersecurity

Statistically significant change from previous wave

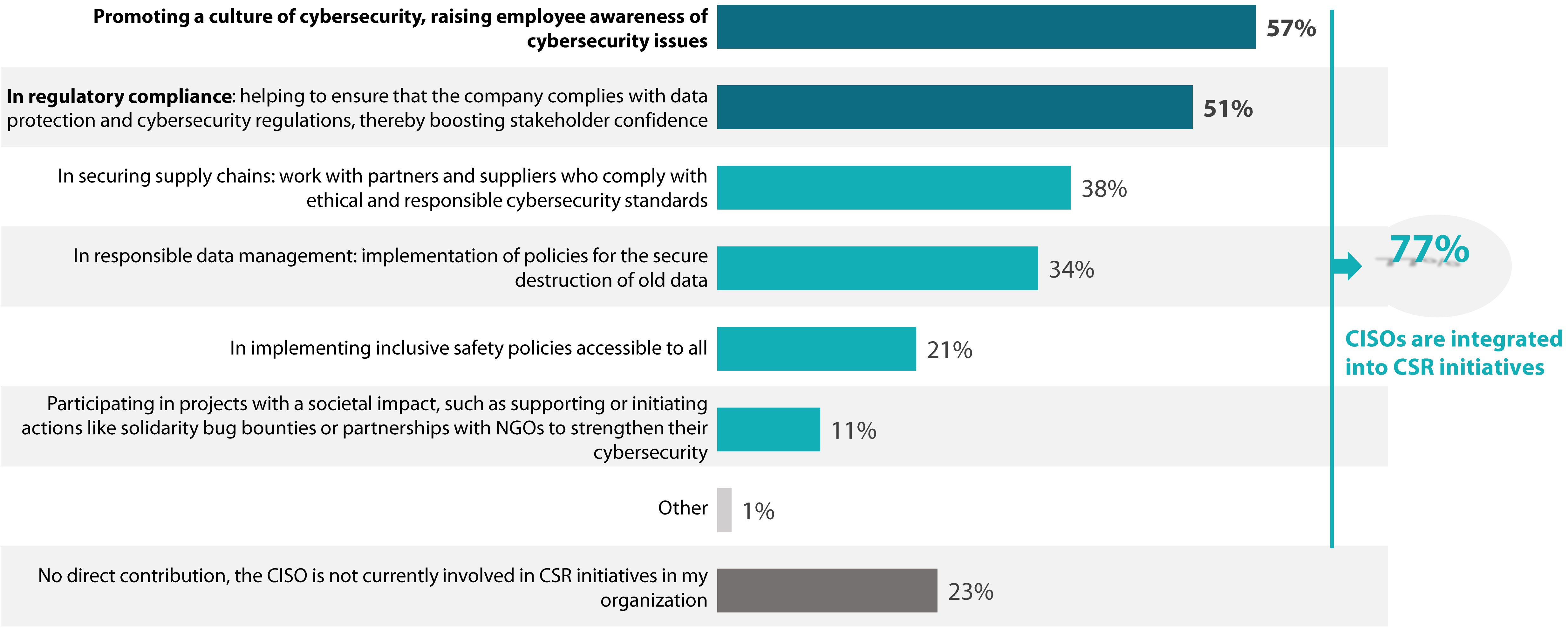
¾ of CISOs are integrated into their company's CSR initiatives, notably via the promotion of a culture of cybersecurity and regulatory compliance.

401 people

New question in 2024

Q49: To what extent does, or could, your role contribute to your organization's CSR objectives?

Base: all - multiple answers possible



Conclusion

Summary (1/4)

Number of cyberattacks stable since 2023, with little innovation in attack methods or impact

In the same proportions as last year, one company in two suffered at least one successful cyber attack in 2024 (47%).

Strategies remain similar to last year, with phishing, spear phishing and smishing again the main attack vectors (60%), followed by vulnerability exploitation (47%) and denial of service (41%).

As a result of these attacks, data theft has increased in 2024 (42%, +11 points), while denial of service remains stable (36%). Identity theft (34%) completes the trio of main impacts. At the same time, data encrypted by ransomware is declining (9%, -9 points).

Third parties are also sources of incidents, mainly through bad practices (28%). To protect themselves, companies rely mainly on security clauses in contracts (85%), as well as on security questionnaires (74%).

The risk of cyberespionage remains important for companies, with 37% considering it to be high.

Summary (2/4)

Renewed confidence in emblematic defensive systems: firewalls, EDR and MFA.

For 84% of CISOs, security solutions and services are still adapted to business needs. While most of the solutions measured are becoming more effective this year, the three most popular solutions are consolidating their position: firewalls, EDR and MFA, both in terms of effectiveness and deployment within companies.

The Zero Trust and Vulnerability Operation Center (VOC) concepts are more widely implemented in companies (respectively 31%, +7 points and 26%, +9 points), as is Cyber Asset Attack Surface Management (CAASM) (11%, +5 points).

Companies have a good understanding of their assets (76%) and crown jewels (57%).

The vast majority of companies are impacted by cyber regulations (79%, of which 52% strongly), notably by NIS2 (74% of companies concerned).

Cyber insurers well established in the cybersecurity market

The majority of companies have taken out cyber insurance (72%), with 64% planning to renew (+7 points). Nearly a quarter (23%) used their cyber insurance following an attack.

The use of rating agencies by cyber insurers continues to divide companies. 47% think it's a good thing, particularly as it gives them an insight into the cyber view of their company held by third parties (65% of companies concerned), while 53% say it's not a good idea, as they are sceptical about the agencies' analyses and scores.

At the same time, 62% of companies have filed a complaint following a cyber attack, a figure stable compared to 2023.

Summary (3/4)

Less risky individual behavior thanks to ongoing employee training and awareness campaigns

While the digital uses of employees still represent a risk for companies, this risk decreases in 2024 for Shadow IT (72%, -10 points), the management of data sharing by users in cloud collaboration (67%, -11 points) and the personal use of company-supplied devices (COPE) (35%, -10 points).

Improved risk management has been achieved by raising awareness and training all employees in cybersecurity (85% of users have been trained).

The Cloud: a real security challenge for businesses

The adoption of Cloud in IS concerns less than 50% of IS in the majority of companies, whether in Iaas / Paas or Saas mode.

The use of the Cloud represents a risk for companies, mainly due to a lack of control over the hosting provider's subcontracting chain, although this risk has been declining since 2023 (40%, -9 points). The difficulty of carrying out audits (37%) and the difficulty of controlling access by the host's administrators (36%, -7 points) are also among the priority risks of the Cloud.

Securing data stored in the Cloud also requires specific tools for 63% of CISOs, 33% of whom have subscribed to specific tools in addition to the Cloud Provider's native tools.

Summary (4/4)

Digital transformations necessarily imply an adaptation of companies, in particular to take into account the rise of AI

The use of AI is democratizing in companies. 69% of companies now use it (an increase of +23 points since 2023), including 35% (+18 points) who have formally integrated it into their security strategy.

Adapting security solutions and processes to digital transformations remains the main challenge for the future of cybersecurity (55%).

CISOs continue to show confidence in their companies' ability to take into account cybersecurity issues (73%) and to face cyber risks (68%).

In fact, cyber risk is included in the risk mapping of almost all companies (98%), 70% of which rank it among the TOP3 risks.

Despite these risks being very much on companies' minds, forecasts of increases in the number of staff allocated to protection against cyber risks are in decline this year (28%, -7 points for an increase in the budget allocated to governance of protection against cyber risks, and 34%, -13 points for operational cybersecurity of protection against risks). Similarly, the desire to acquire new technical solutions and increase budgets is in decline this year.

At the same time, 77% of CISOs are involved in their company's CSR initiatives, notably through the promotion of a culture of cybersecurity (57%) and regulatory compliance (51%).

Appendices

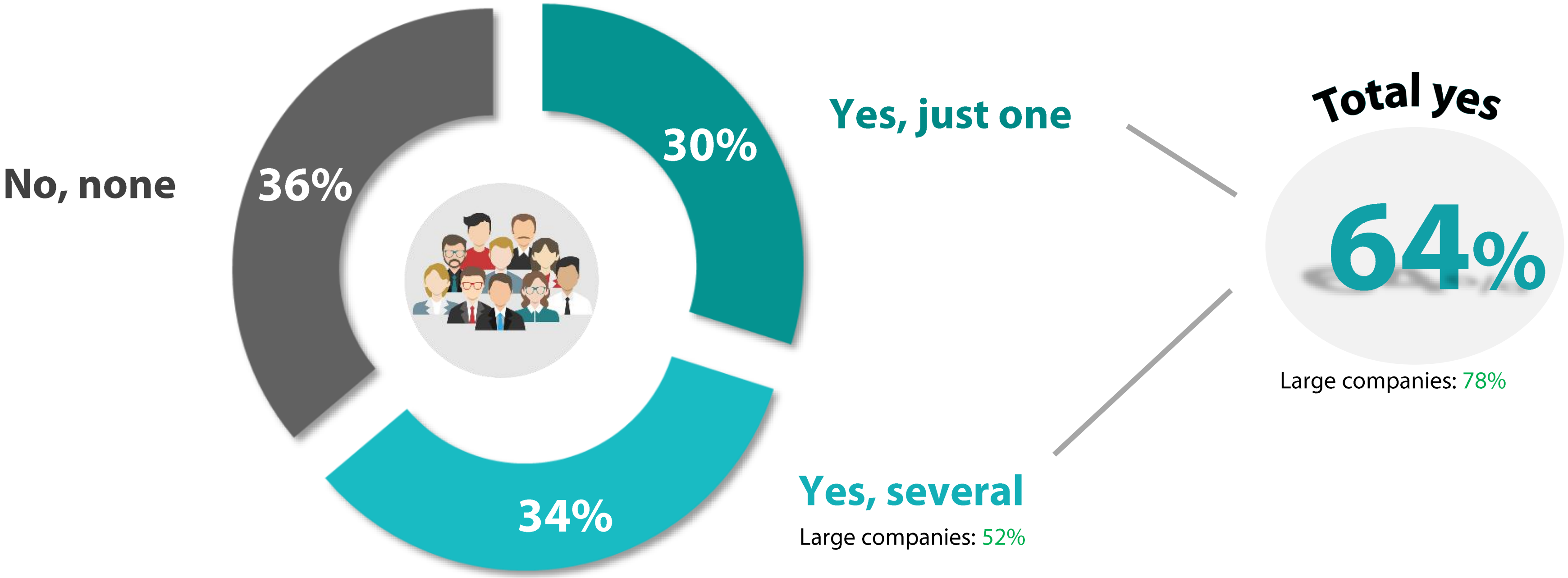
2/3 of companies have integrated work-study students this year, including 1/3 who recruited several.

401 people

New question in 2024

Q44: In the last 12 months, have you integrated any work-study students?

Base: all



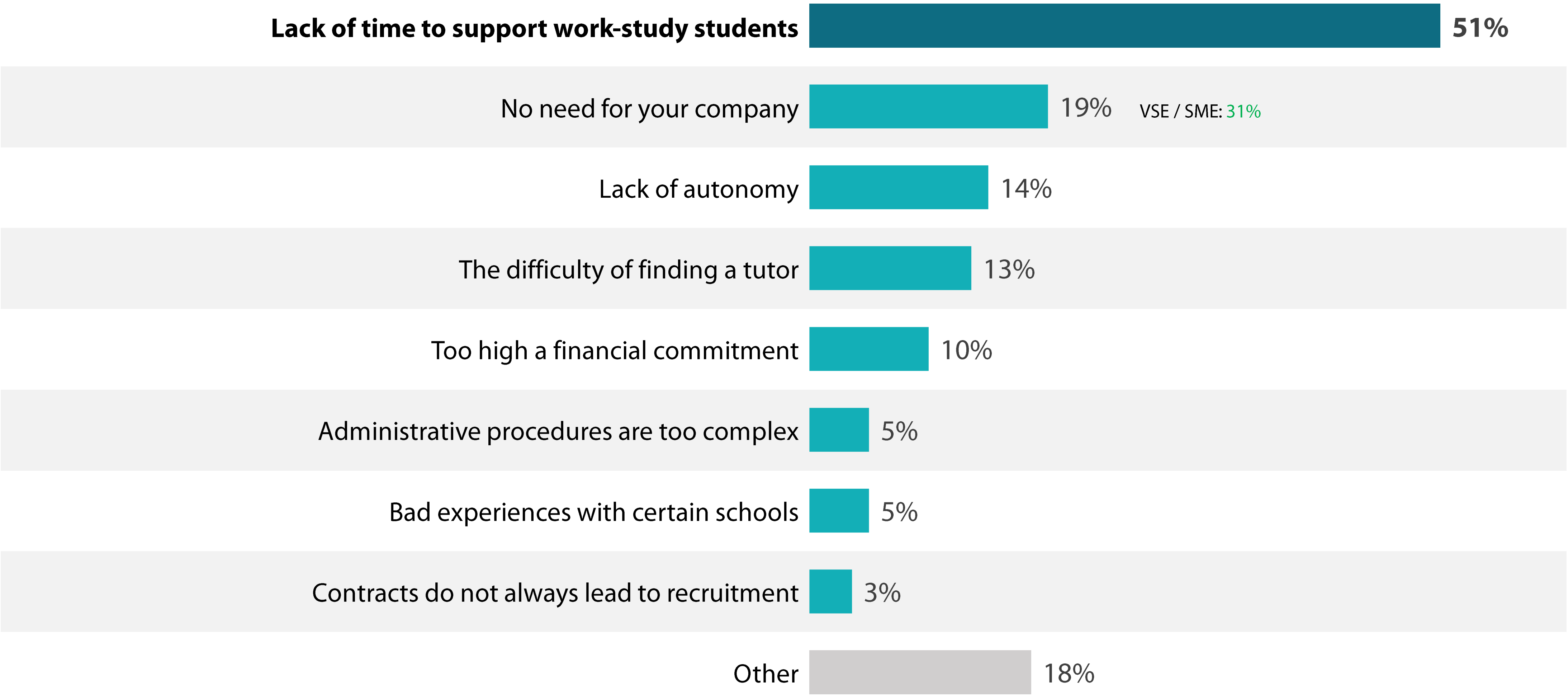
For those who have not recruited alternants, lack of time is the main obstacle to taking action.

145 people

New question in 2024

Q45: Why haven't you recruited any work-study students?

Base: have not recruited any work-study students - multiple answers possible



MAKE THE WORLD EASY TO UNDERSTAND SO WE CAN ACT NOW AND IMAGINE THE FUTURE.

WE ARE DIGITAL !

Founded in 2000 on this radically innovative idea at the time, OpinionWay was a forerunner in renewing the practices of the marketing and opinion researches.

With continuous growth since its creation, the company has constantly opened up to new horizons to better address all marketing and societal issues, by integrating Social Media Intelligence, smart data exploitation, creative co-construction activities, online communities approaches and storytelling into its methodologies.

Today OpinionWay continues its dynamic growth by expanding geographically in high-potential regions such as Eastern Europe and Africa.

This is the mission that drives OpinionWay's employees and the foundation of the relationship they build with their clients.

The pleasure they derive from providing answers to the questions they ask themselves, reducing uncertainty about the decisions to be made, tracking relevant insights and co-constructing solutions for the future, feeds all the projects they work on.

This enthusiasm, combined with a genuine taste for innovation and transmission, explains why our customers express a high level of satisfaction after each collaboration - 8.9/10, and a high recommendation rate – 3,9/4.

Pleasure, commitment and intellectual stimulation are the three mantras of our interventions.

LET'S STAY CONNECTED !

www.opinion-way.com

Let's go further together !
Receive our latest market researches results each week in your mailbox by subscribing to our newsletter !

opinionway

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN