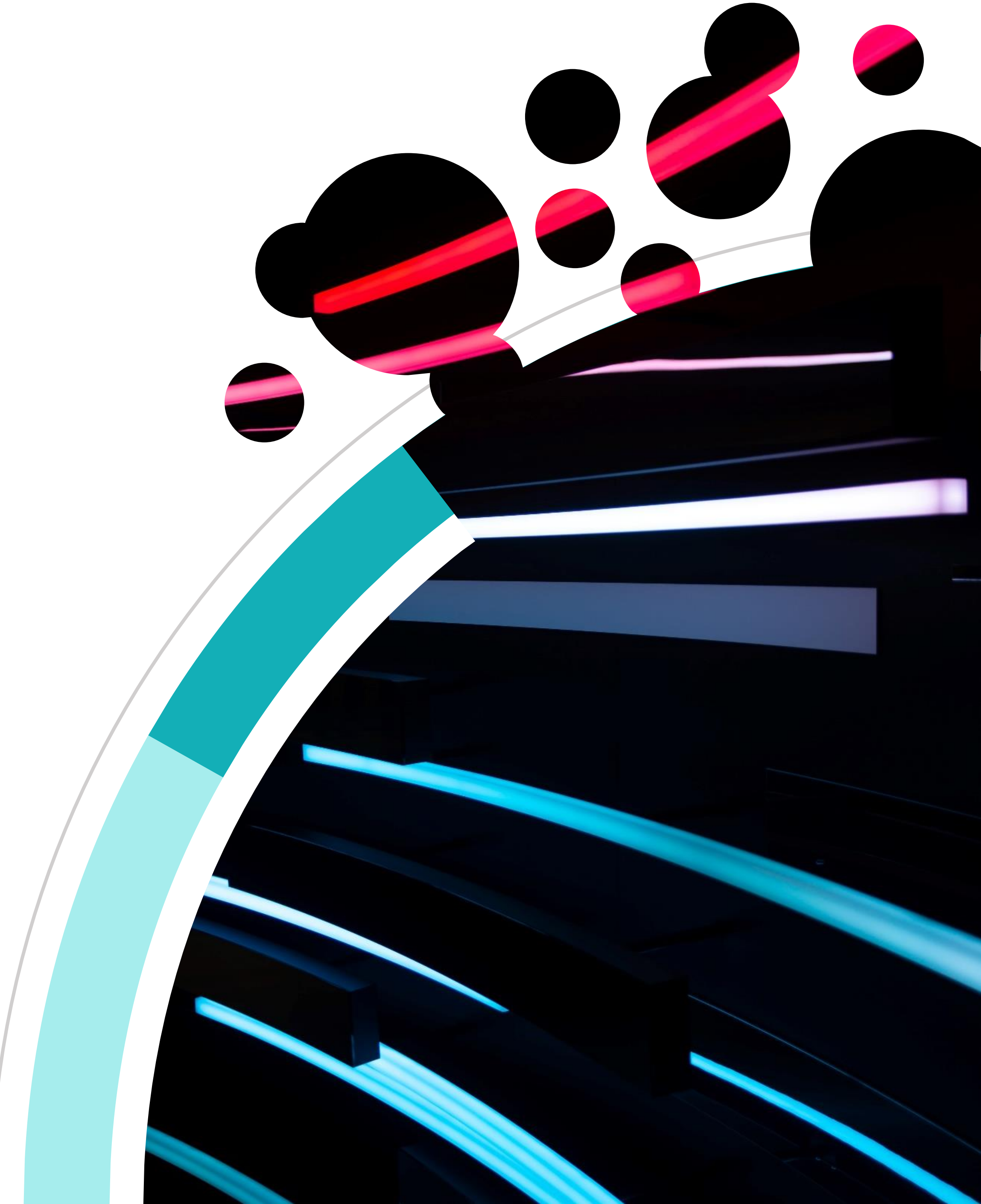
“opinionway for CESIN

Corporate cybersecurity barometer

Wave 9 - January 2024



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

afaq ISO 20252 Étude marketing et d'opinion AFNOR CERTIFICATION

ESOMAR 24 Corporate

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 **456 CESIN members, drawn** from the CESIN membership file.

Questionnaire

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

The interviews were conducted **between November 27 and December 22, 2023**.

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: 4.6 points at most for a sample of 450 respondents.

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

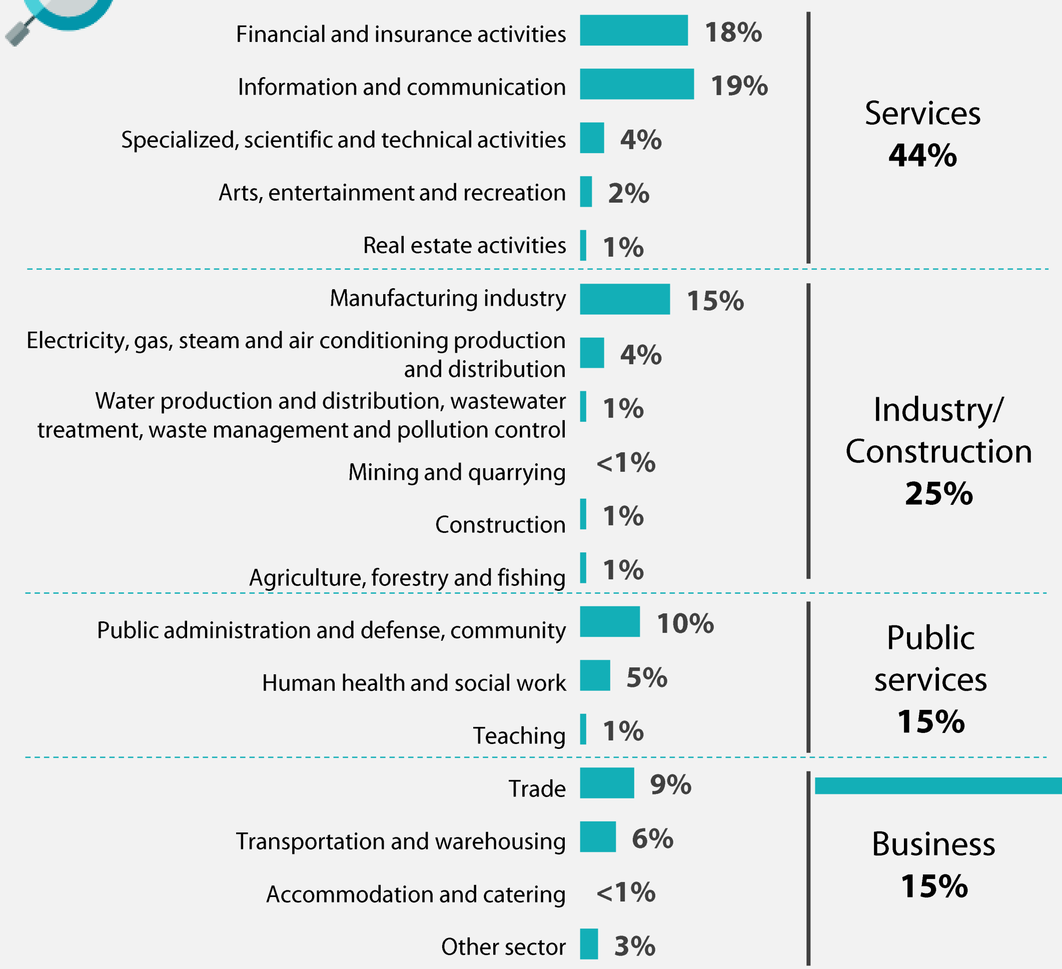
"OpinionWay survey for CESIN".

***and no survey can be dissociated from this title*.**

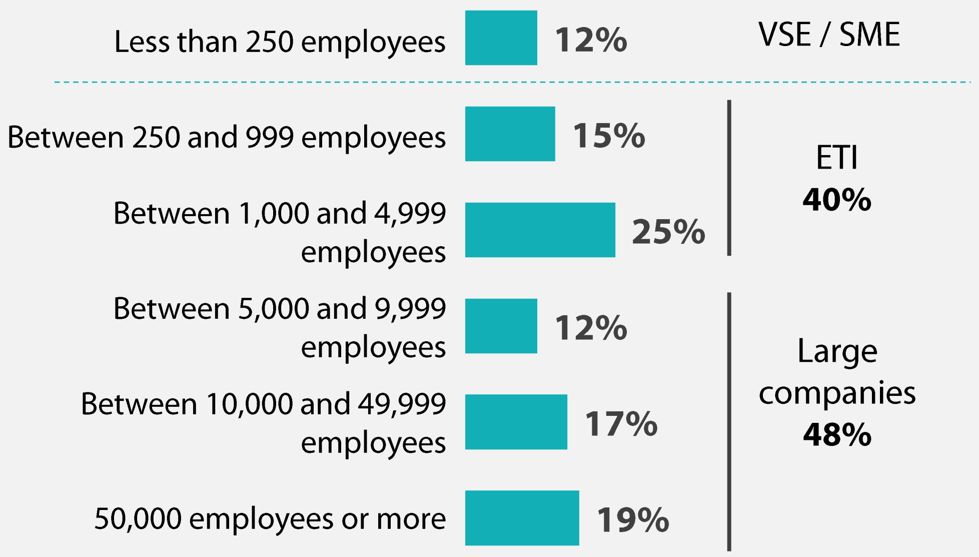
Sample

A sample that perfectly reflects the diversity of the population surveyed

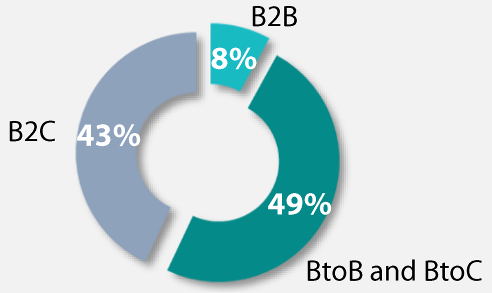
Company sector



Number of company employees



Business



Analyse

01

The number of successful cyberattacks in 2023 remains stable

Denial-of-service attacks take on greater importance this 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 defence efforts to contain and deal with the attack. This does not include attempted attacks that have been stopped by your prevention systems."

***Definition in wave 6**: A cyberattack, for the purposes of this survey, is when a malicious act is performed against a computer device that significantly affects the confidentiality and/or integrity of the company's information or the availability of the information system, resulting in significant financial losses and/or damage to the company's image.*

Half of all companies have suffered a successful cyberattack this year; while the proportion is trending upwards compared to 2022, the number of companies having suffered 15 or more cyberattacks is decreasing.

456 people

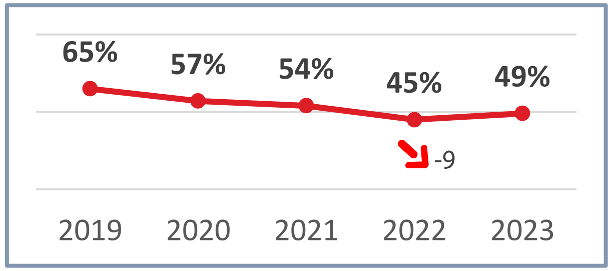
Q4. In total, how many significant cyberattacks has your company suffered in the last 12 months?

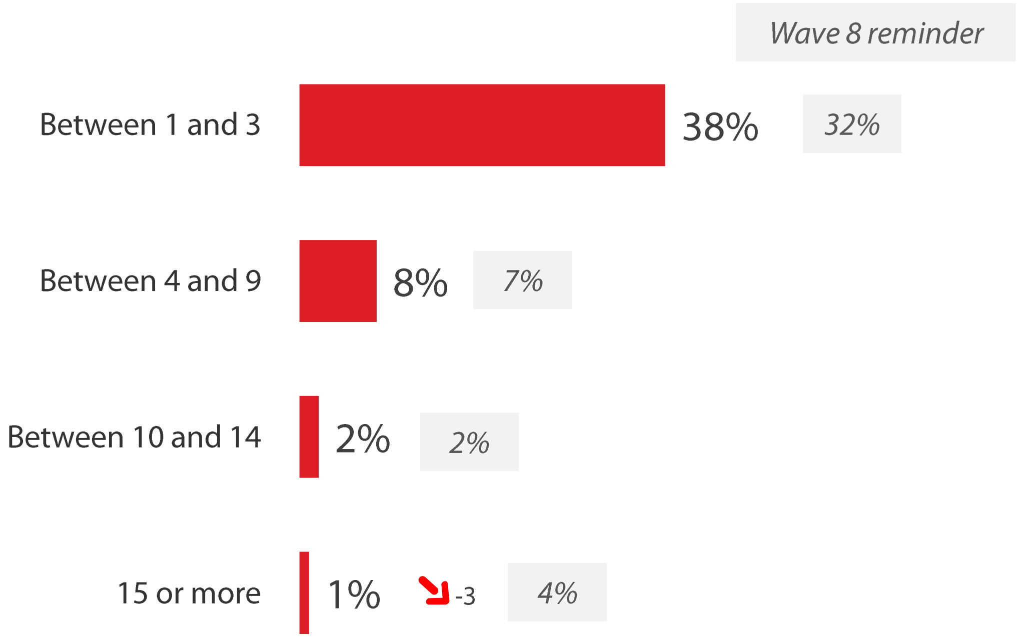
Base: all

49%

of companies have experienced at least a cyberattack

Previous waves reminder





↗ ↘ Statistically significant change from previous wave

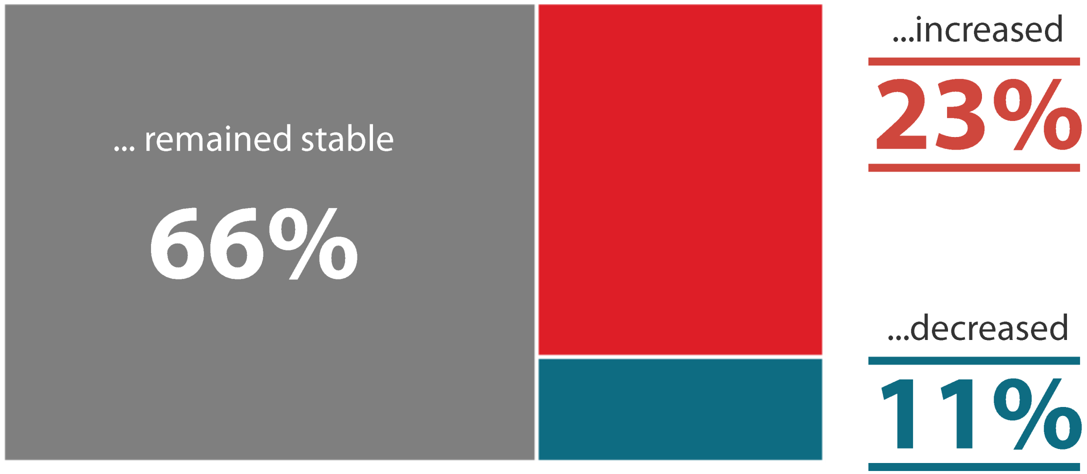
The number of attacks seems to be stabilizing, but continues to grow year on year, even if this growth remains limited.

456 people

Q4bis. Compared with last year, the number of attacks in your company...?

Base: all

In one year, the number of attacks...



Wave 8 reminder: 64%

Wave 8 reminder: 24%

Wave 8 reminder: 12%

40% of companies reporting an attack in 2023

↗ ↘ Statistically significant change from previous wave

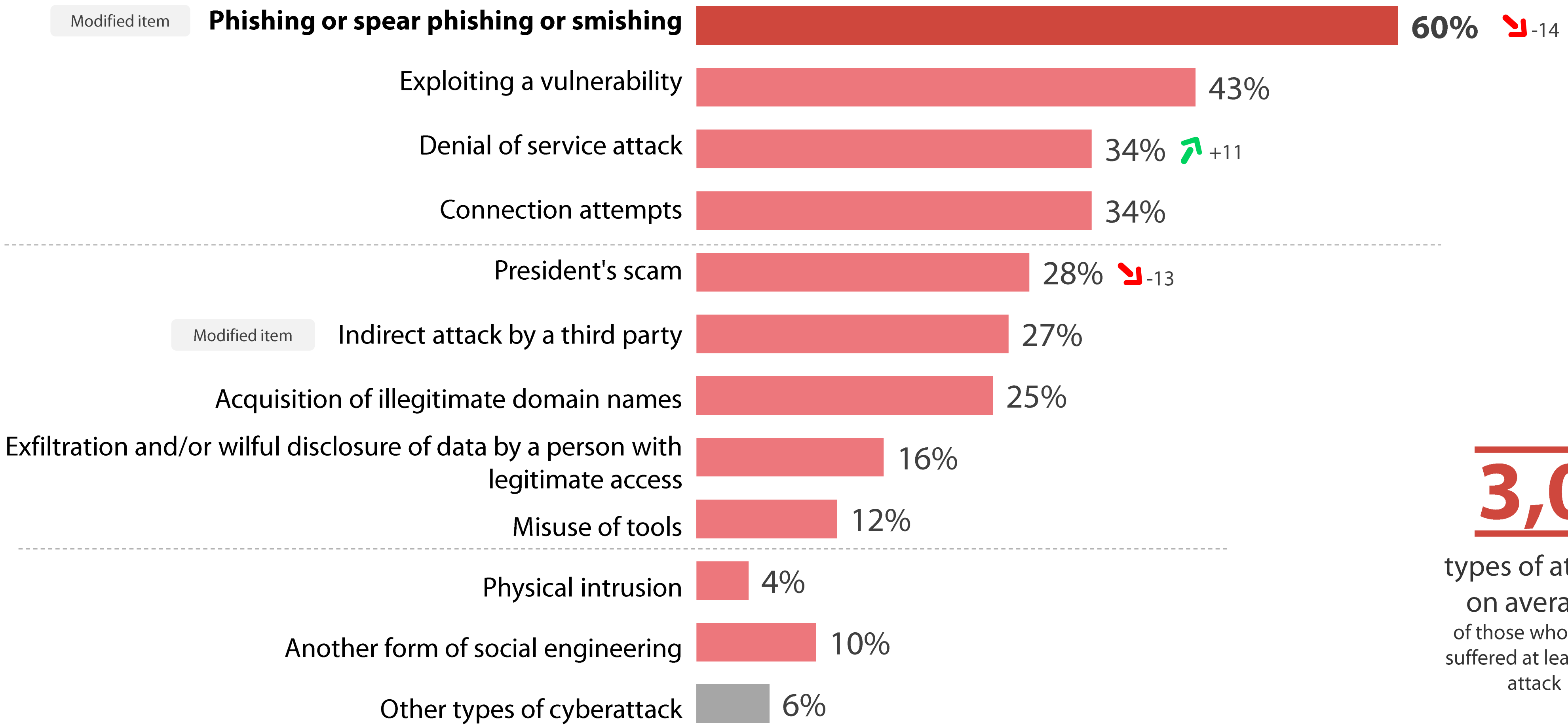
Companies that reported at least one attack suffered an average of 3. Although phishing, spear phishing or smishing remains the main vector, it is declining this year. Note the sharp increase in denial-of-service attacks.

225 people

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

Base: Experienced an attack - multiple answers possible

49% of companies suffered at least one cyberattack in 2023



3,0

types of attack on average

of those who have suffered at least one attack

↗↘ Statistically significant change from previous wave

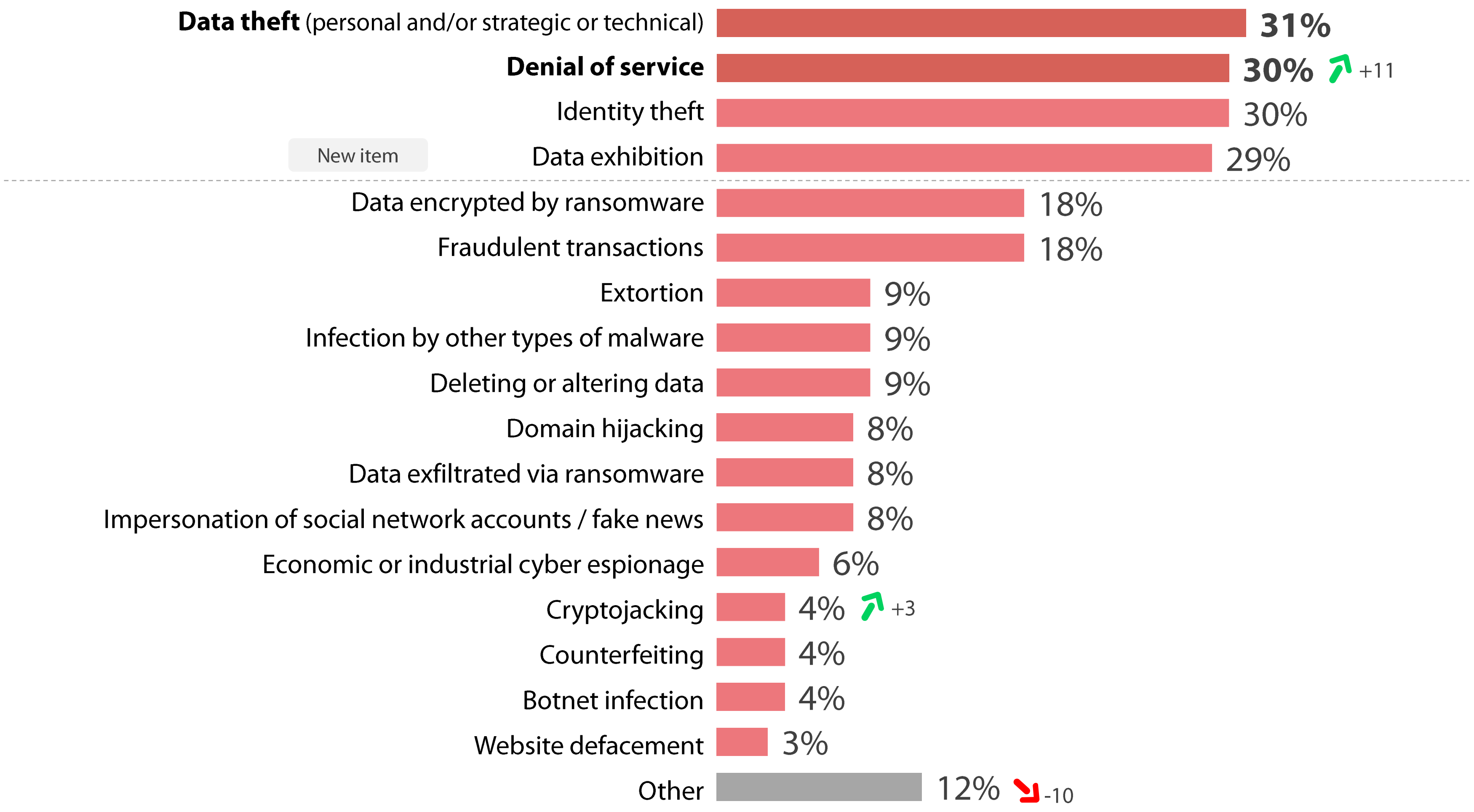
Data theft, denial of service, identity theft and data exposure are the main consequences of these attacks.

225 people

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

Base: Experienced an attack - multiple answers possible

49% of companies suffered at least one cyberattack in 2023



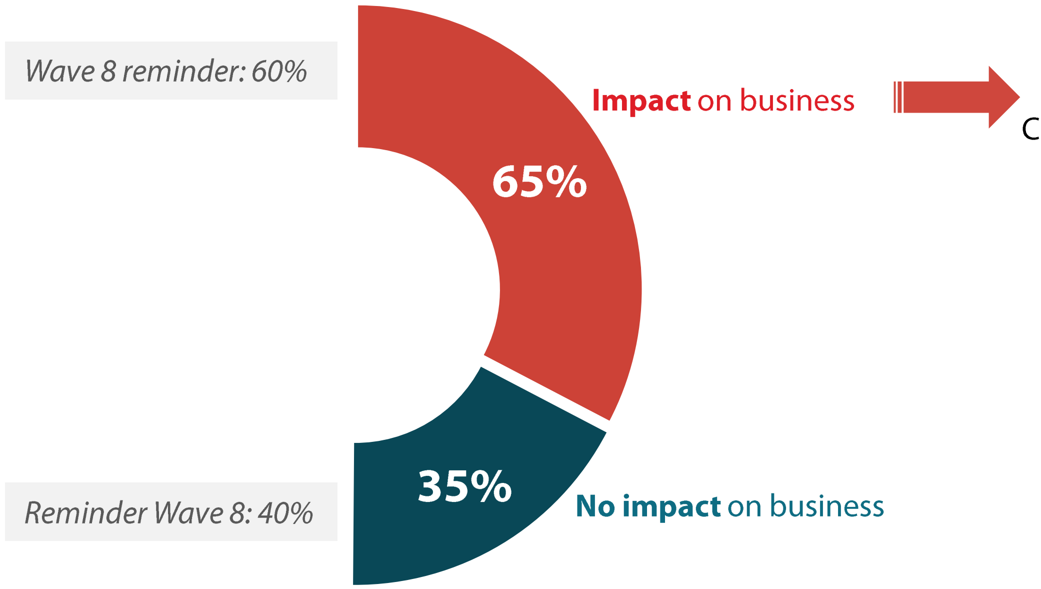
↗ ↘ Statistically significant change from previous wave

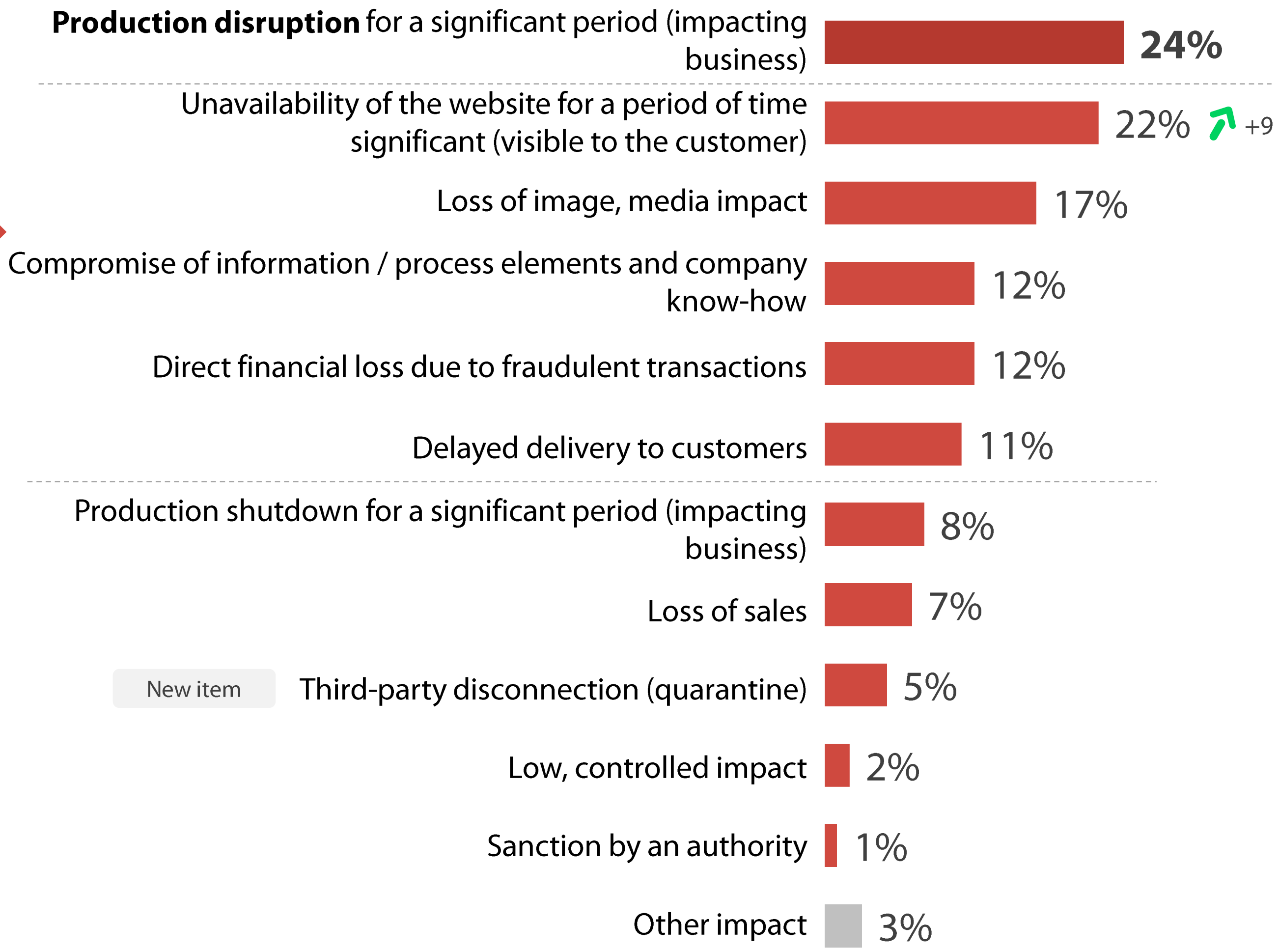
The impact of cyberattacks on business is slightly greater this year: in addition to disrupting production, website unavailability for a significant period is on the rise, in line with the increase in denial-of-service attacks.

420 people

Q7. What impact have cyberattacks had on your business?

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





“opinionway for CESIN

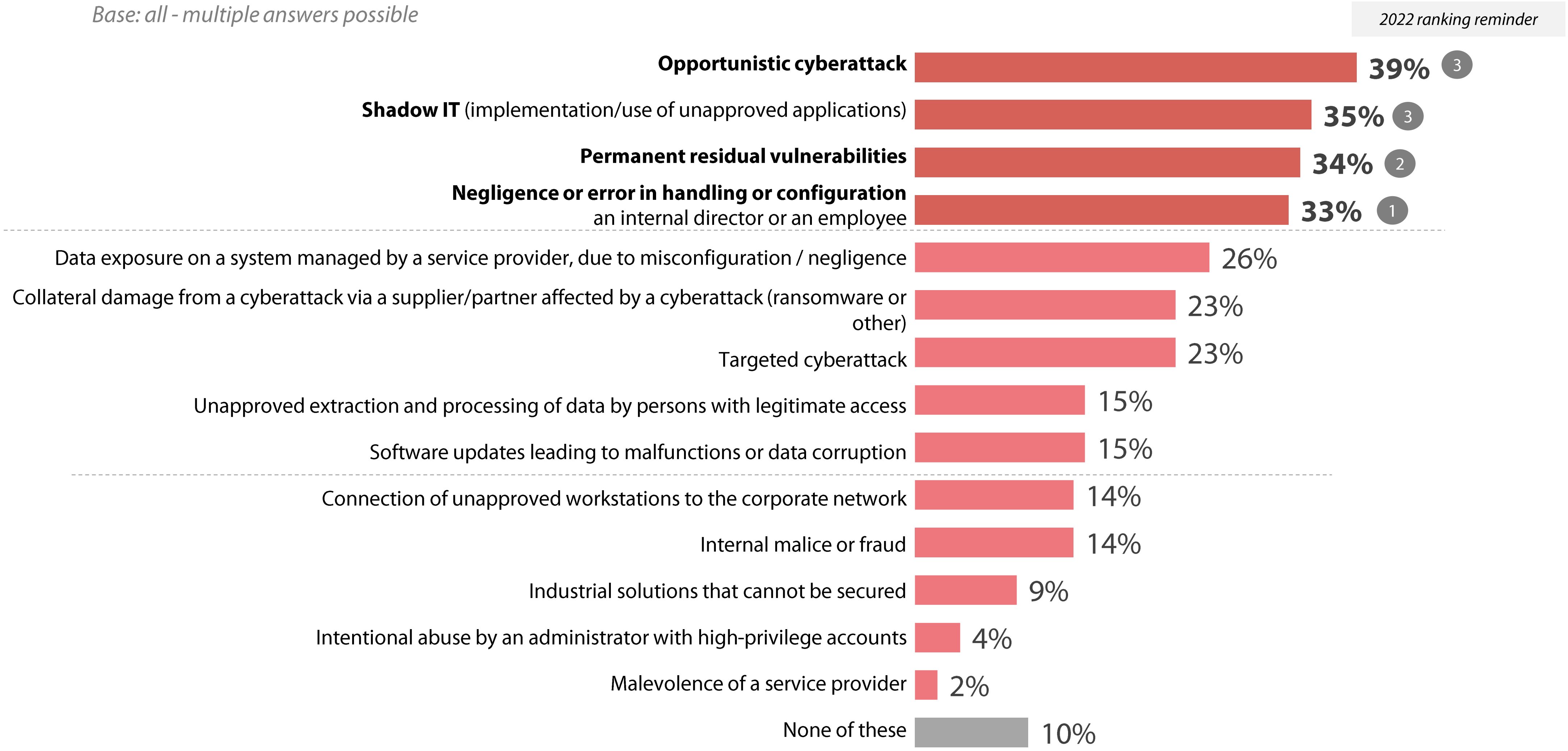
↗↘ Statistically significant change from previous wave

The role of bad practices, including IT operations and Shadow IT, in the source of incidents is still significant. The origins of attacks are better understood, and opportunistic attacks play a relatively important role.

456 people

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

Base: all - multiple answers possible



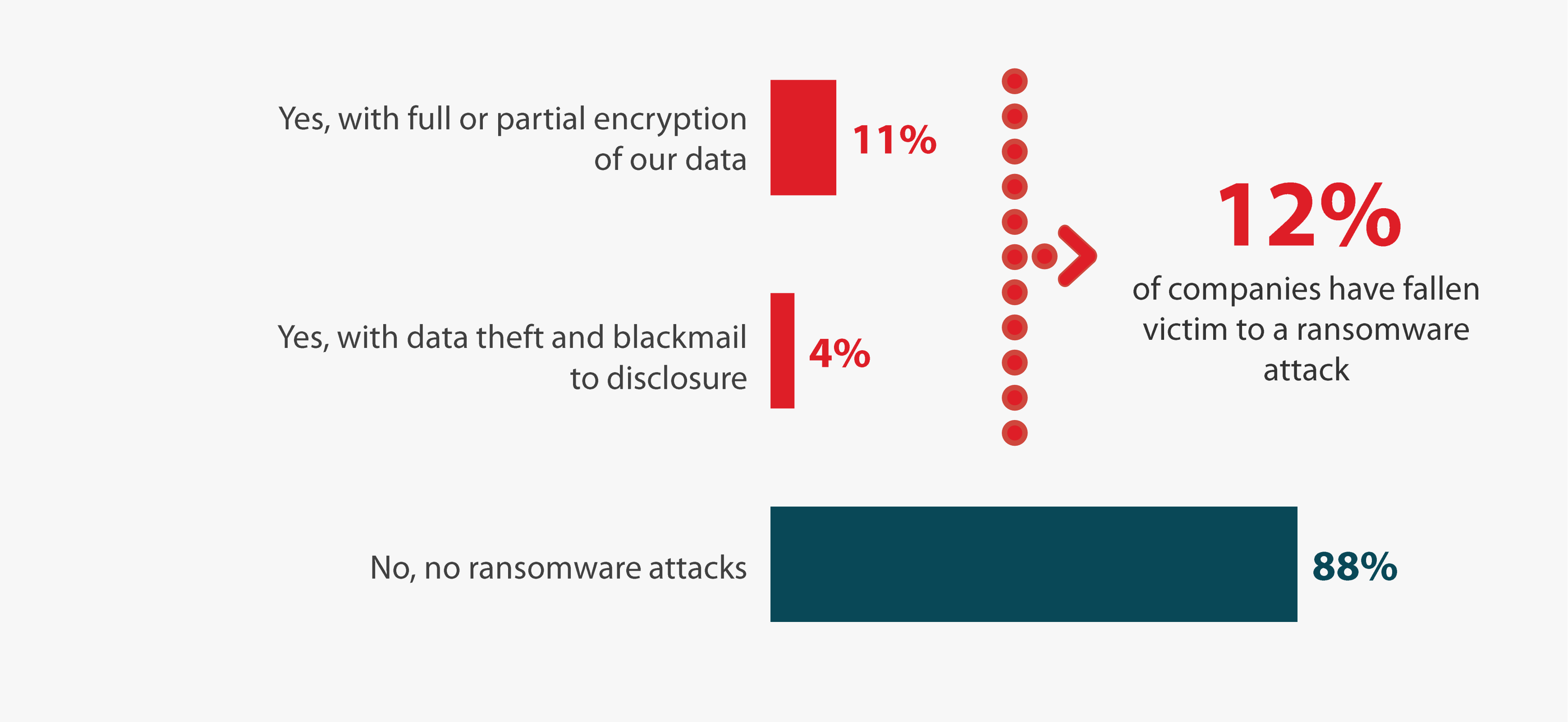
Ransomware attacks stabilize, affecting around 10% of businesses

456 people

Last year was once again marked by an increase in the ransomware threat. In addition to a wave of successful attacks in some cases, attackers have been blackmailing us into disclosing data.

Q10. Have you been a victim of a ransomware attack?

Base: all - Multiple answers possible



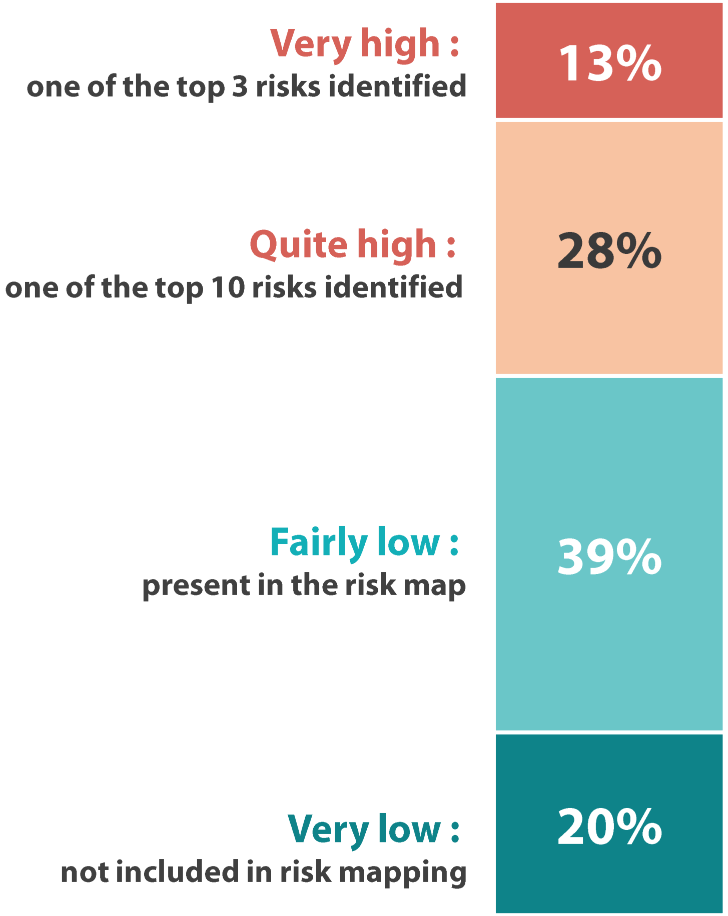
Wave 8 reminder: 14%

The risk of cyber espionage is a high risk for 2 out of 5 companies, which is an important factor given that some companies are not very concerned by this type of risk because of their activity.

456 people

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

Base: all



41% Estimate a high level of threat on cyber-espionage

“opinionway for CESIN

Modified items, no evolution calculation

02

Business protection remains stable. EDR effectiveness and use confirmed again this year

Confidence in the security solutions and services available on the market remains as high as last year

456 people

Q25. Do you think that the security solutions and services available on the market are very suitable, rather suitable, rather unsuitable or not at all suitable to your company?

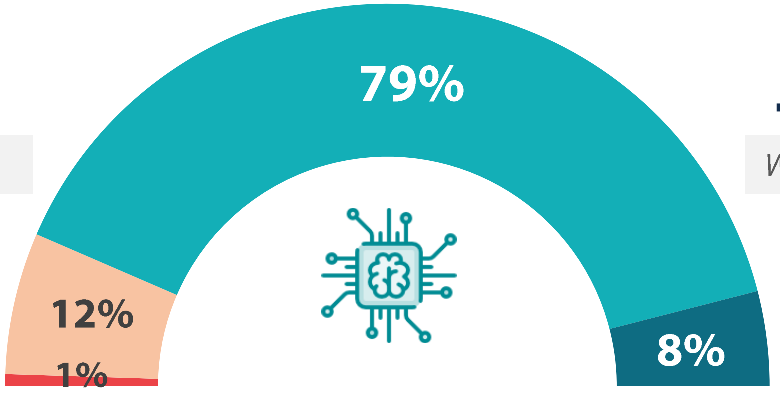
Base: all

🟥 Not at all suitable ▨ Rather unsuitable 🟦 Rather suitable ■ Very suitable

% Unsuitable

13%

Wave 8 reminder: 12%

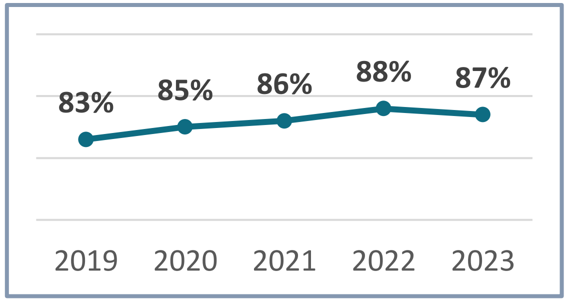


% Adapted

87%

Wave 8 reminder: 88%

Previous waves reminder

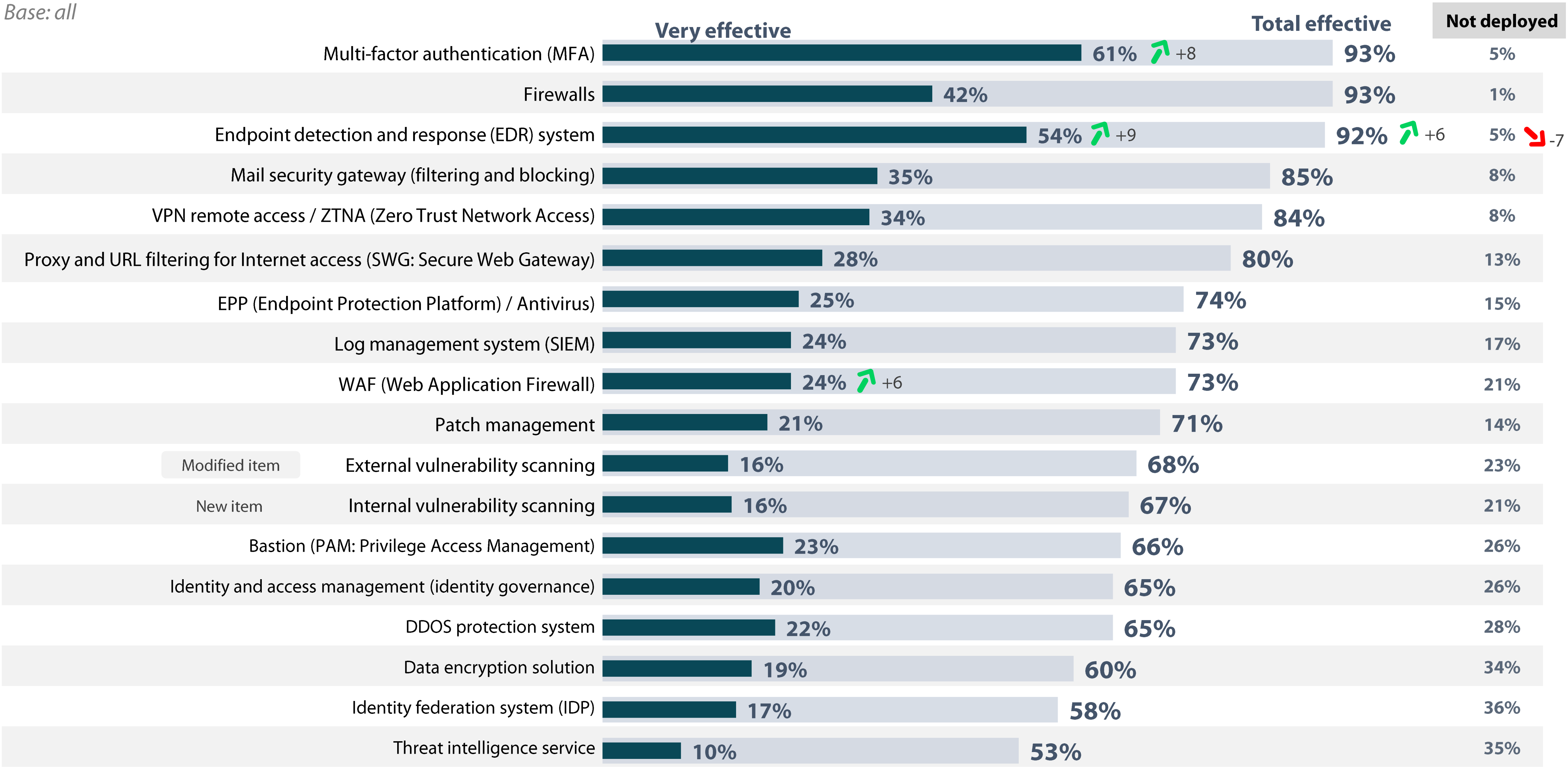


In detail, confidence in the MFA/EDR pairing is growing, with very effective levels approaching 60%.

456 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



↗↘ Statistically significant change from previous wave

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

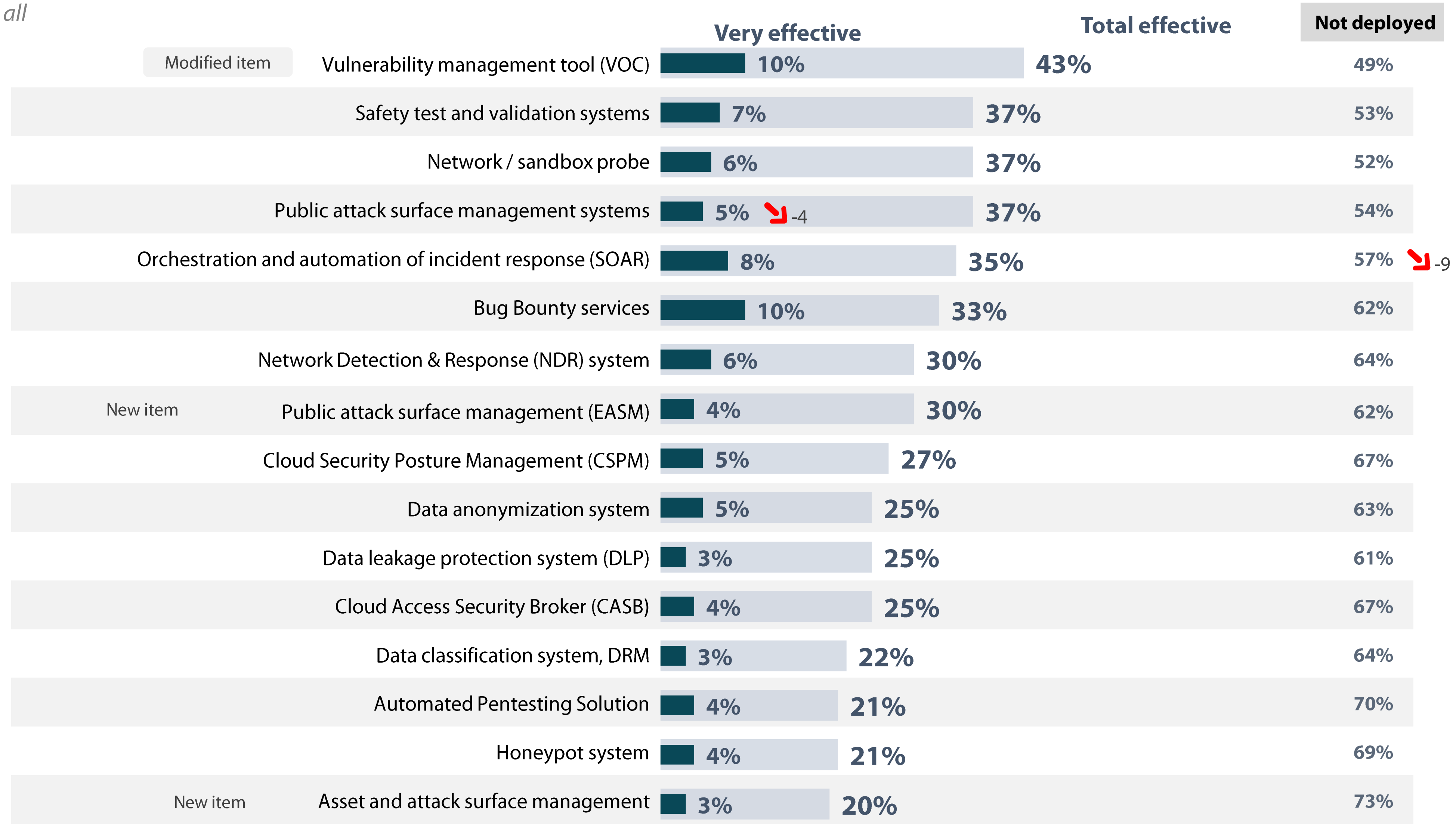
"opinionway for CESIN

Other solutions are less widely deployed in companies

456 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



↗ ↘ Statistically significant change from previous wave

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

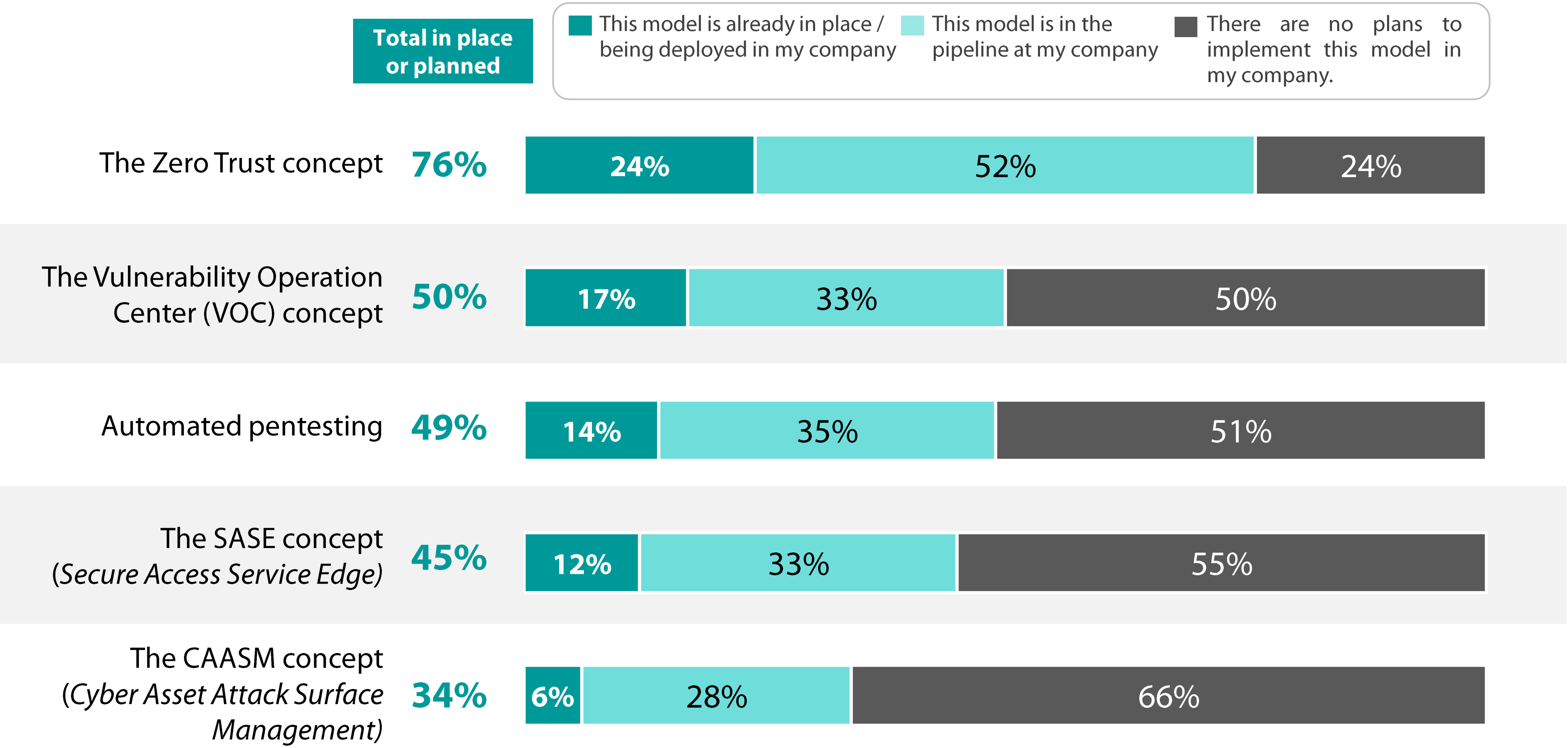
Zero Trust is beginning to gain a certain maturity, while the more recent CAASM concept is just beginning to be spotted in companies but is making a small breakthrough to follow.

456 people

New question in 2023

Q28b. What is your vision of the following concepts?

Base: all

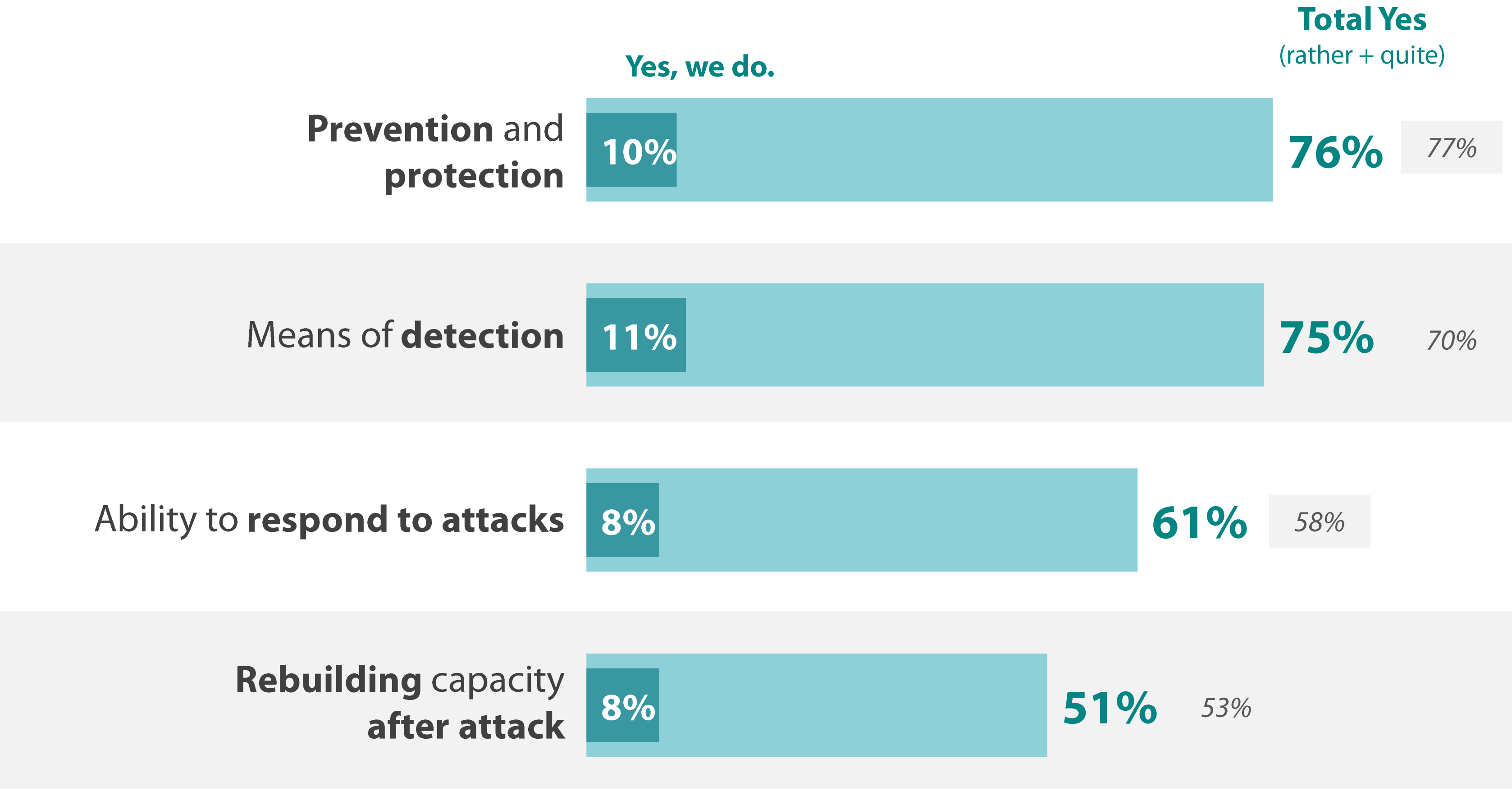


Similar to last year, companies are more confident in their attack preparedness than in their attack response.

456 people

Q14. In your opinion, is your company prepared to handle a large-scale cyberattack in terms of...?

Base: all



“opinionway for CESIN

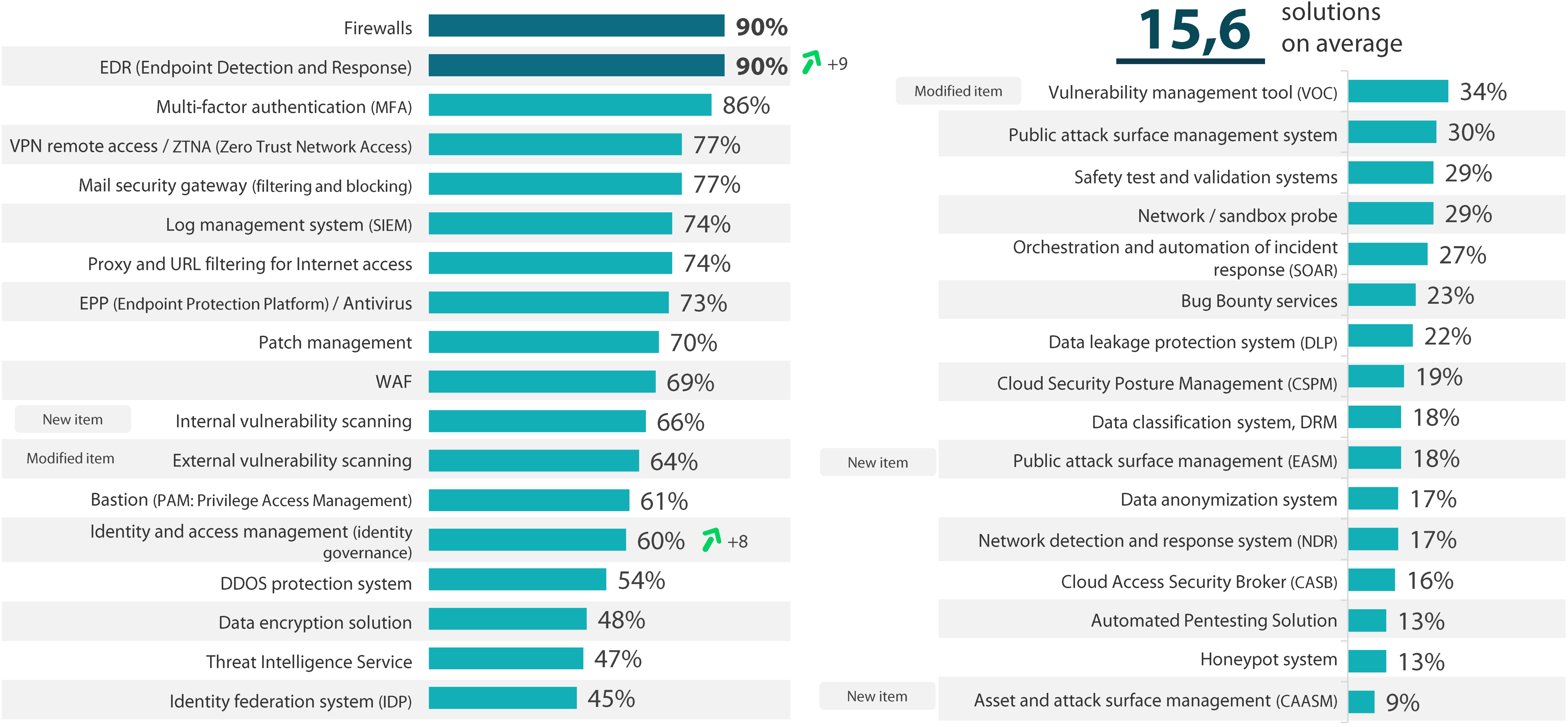
↗↘ Statistically significant change from previous wave

On average, more than 15 solutions or services are deployed in companies. EDR joins firewalls at the top of the list of solutions deployed, with MFA complemented by strong growth in identity management.

456 people

Q12. More generally, which of the following solutions and services are in place in your company?

Base: all - multiple answers possible



15,6 solutions on average

*New item
** item modified

↗ ↘ Statistically significant change from previous wave
Evolution to be interpreted with caution in view of the addition of items

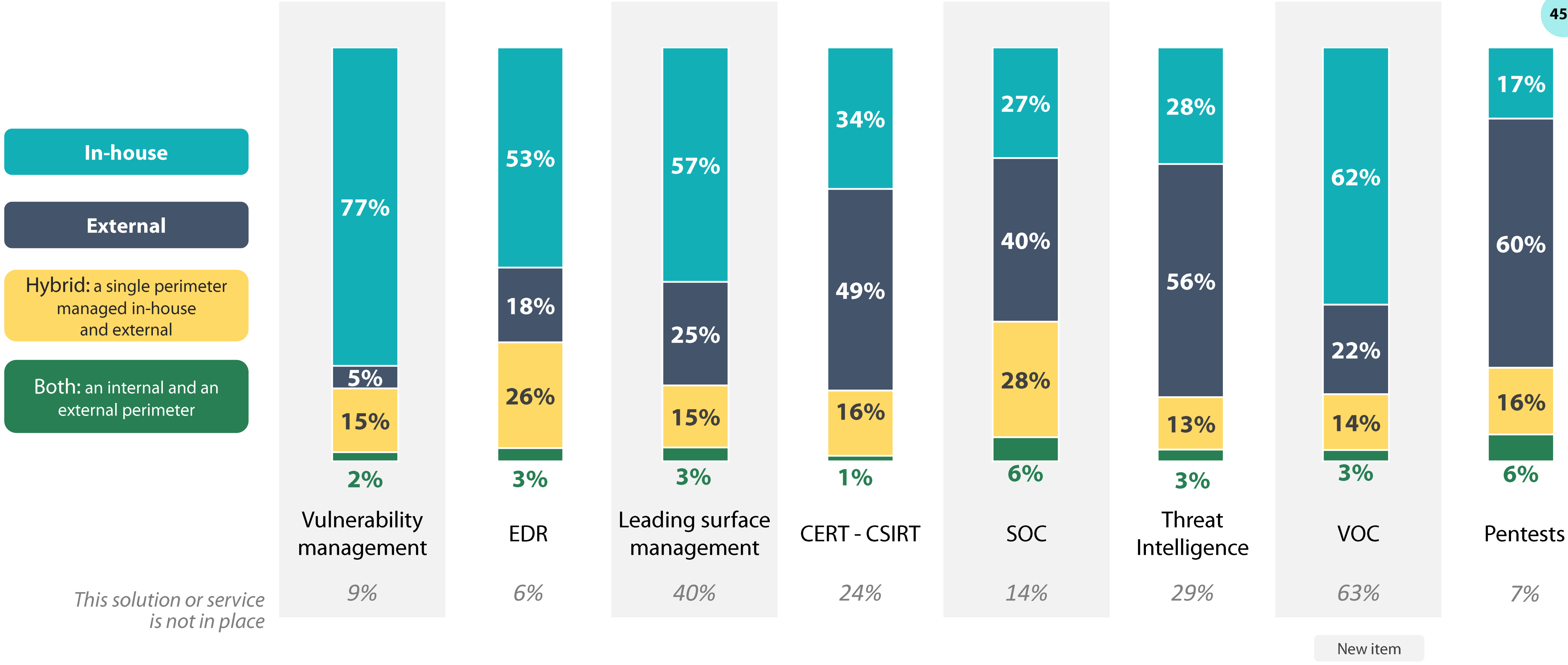
“opinionway for CESIN

Vulnerability management, VOC and attack surface management are mostly handled in-house, unlike Pentests, Threat Intelligence or CERT-CSIRT. It should be noted that a significant proportion of EDR and SOC are handled on a hybrid basis.

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

Base: all - results excluding solutions not implemented

456 people



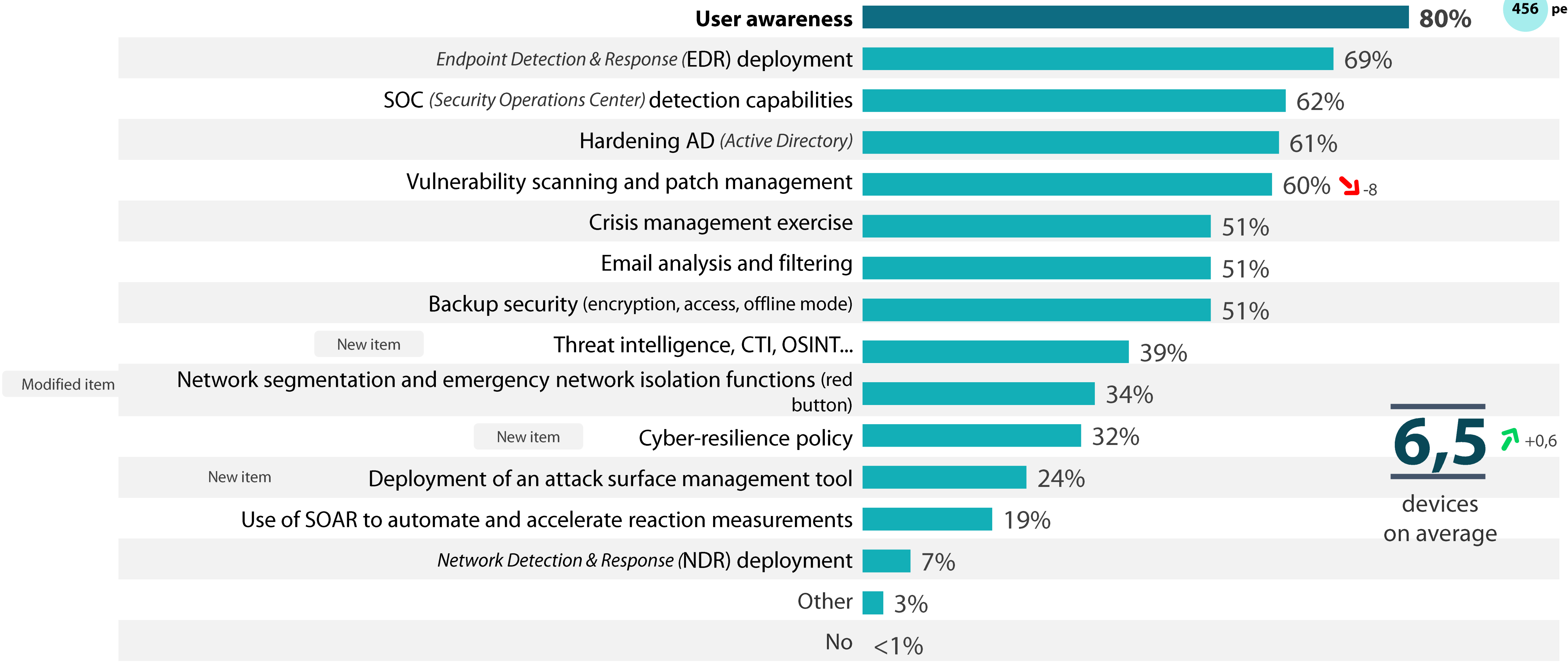
Hybrid item added, no evolution calculation

This year, companies have reinforced more systems (more than 6 on average). User awareness and EDR still predominate

Q11. In response to this wave of cyberattacks dominated by ransomware, what measures have you reinforced?

Base: all - multiple answers possible

456 people



6,5 ↗ +0,6

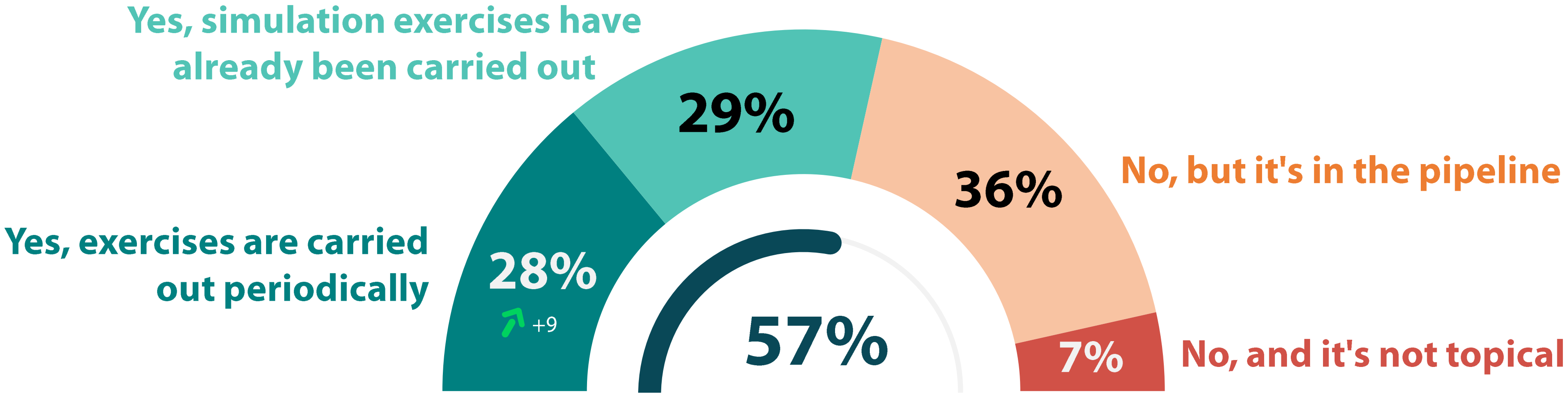
devices on average

↗ ↘ Statistically significant change from previous wave

The proportion of companies having set up a cyber-crisis training program is on the rise. Exercises are also taking place more frequently

456 people

Q15. Does your company have a cyber crisis training program in place?
Base: all



HAVE SET UP A CYBER-CRISIS TRAINING PROGRAM

Wave 8 reminder: 51%

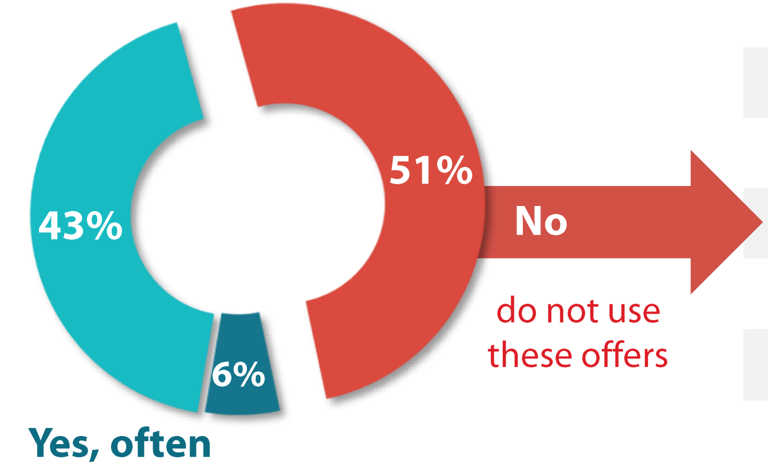
↗ ↘ Statistically significant change from previous wave

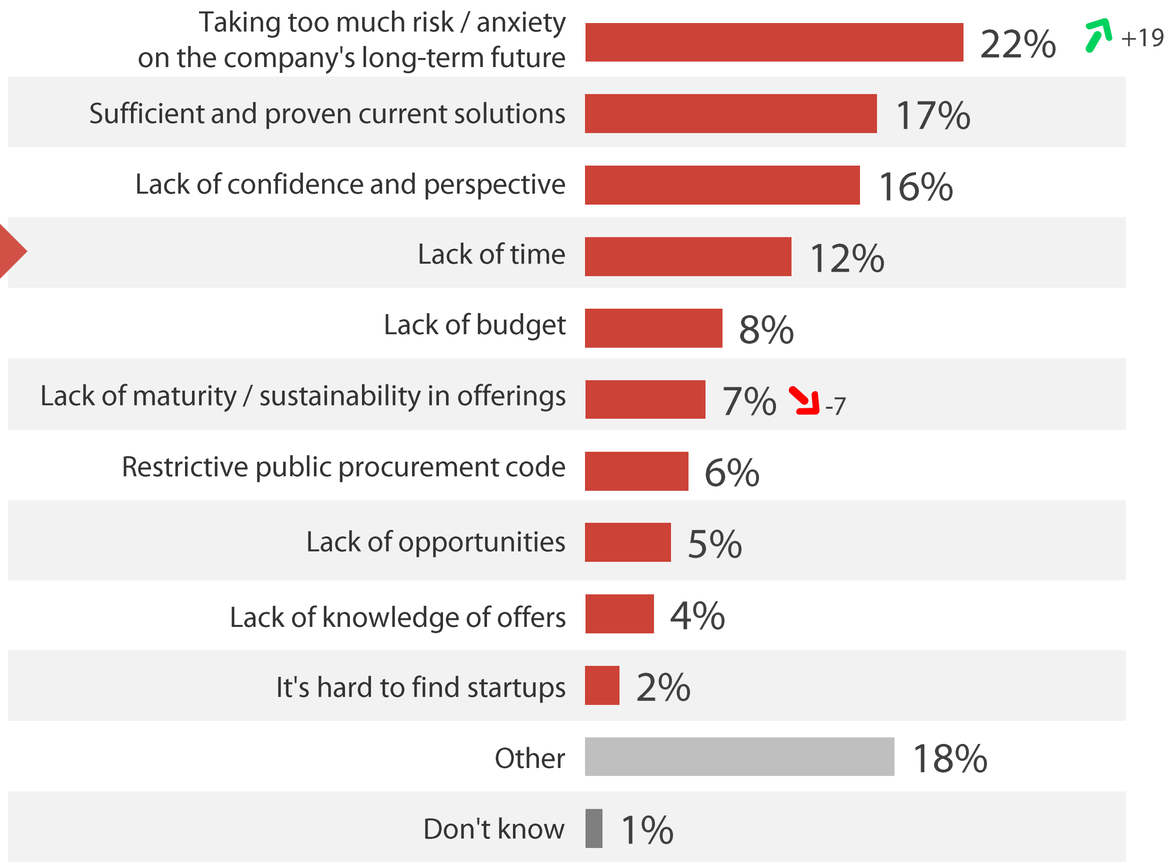
Half of companies use innovative offerings from startups, while those that don't cite excessive risk-taking as the main reason.

456 people

Q26. In terms of cybersecurity, do you make use of innovative offers from start-ups? *Base: all*
Q26bis. Why not? *Base: don't use offers from start-ups (153)*

49% use innovative offers from startups





Modification of Q26 items, no calculation of evolution

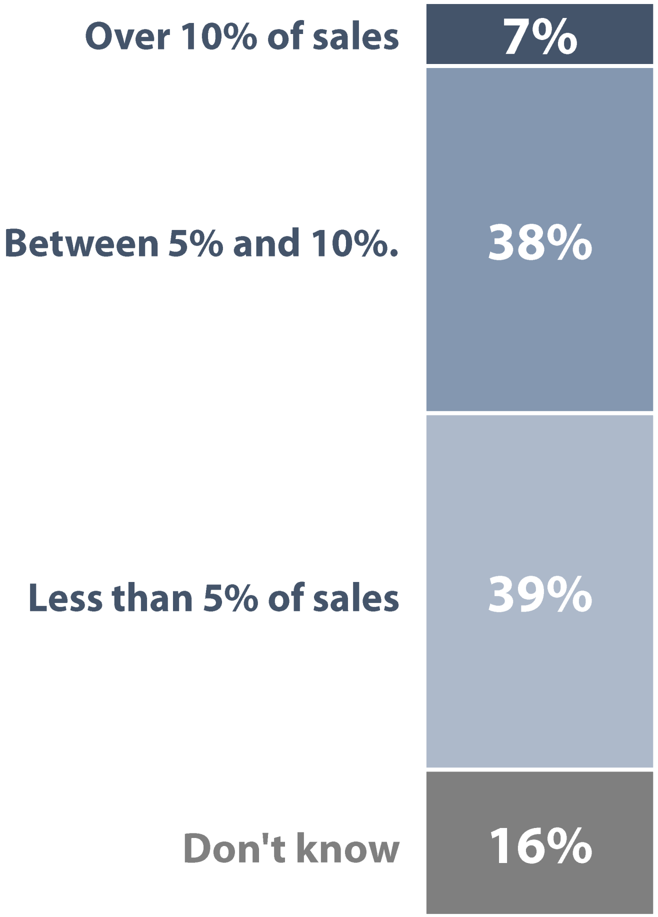
↗ ↘ Statistically significant change from previous wave

All in all, cyber budgets remain at the same level as last year

456 people

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

Base: all



5% or more of the IT/digital budget is spent on security: 45%

Wave 8 reminder: 45%

Focus on…

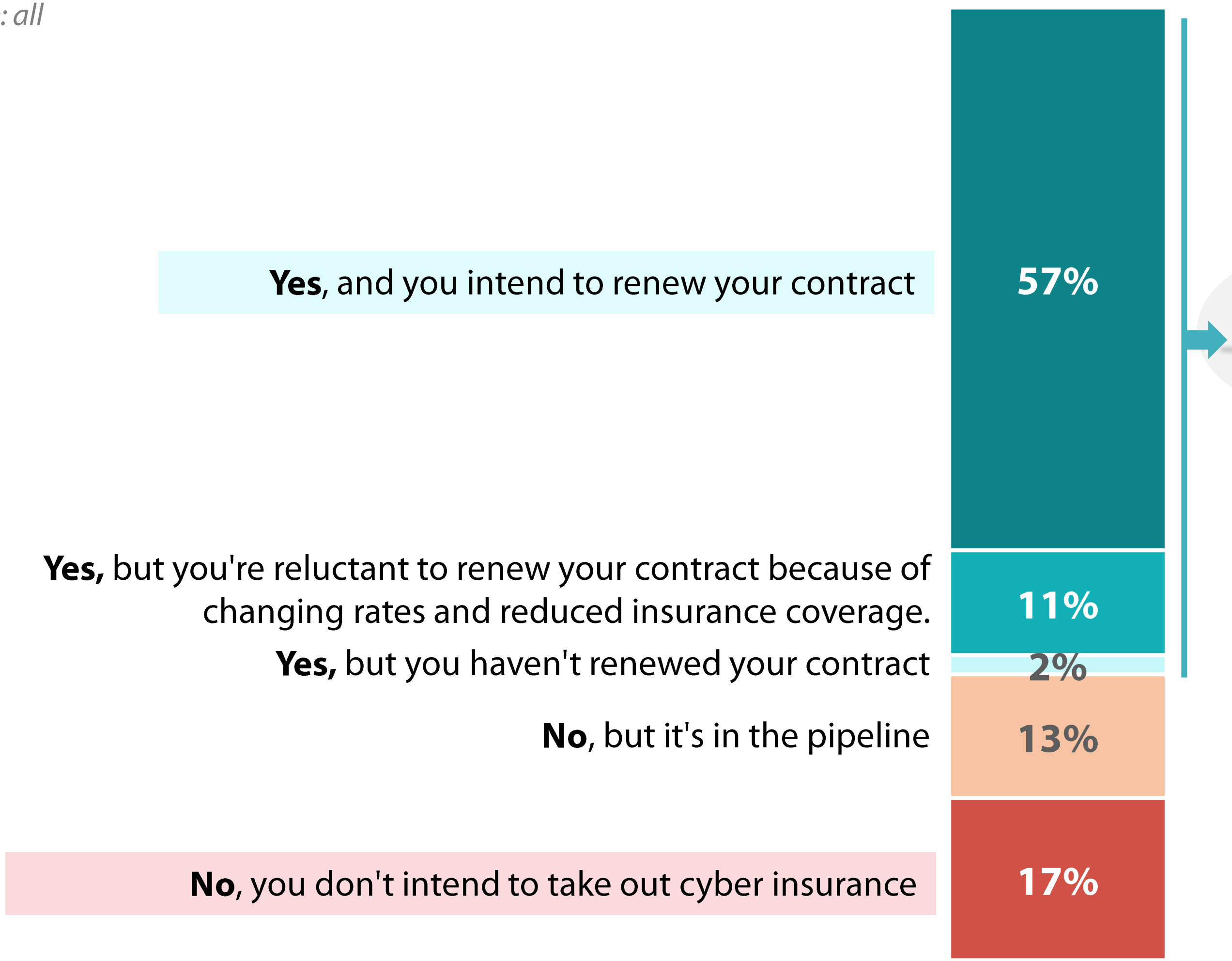
Cyber insurance

7 out of 10 companies have taken out cyber insurance, and the majority intend to renew their policy, while the number of companies insured is stabilizing

456 people

Q31. Do you have cyber insurance?

Base: all



70% **Have taken out cyber insurance**

Wave 8 reminder: 67%

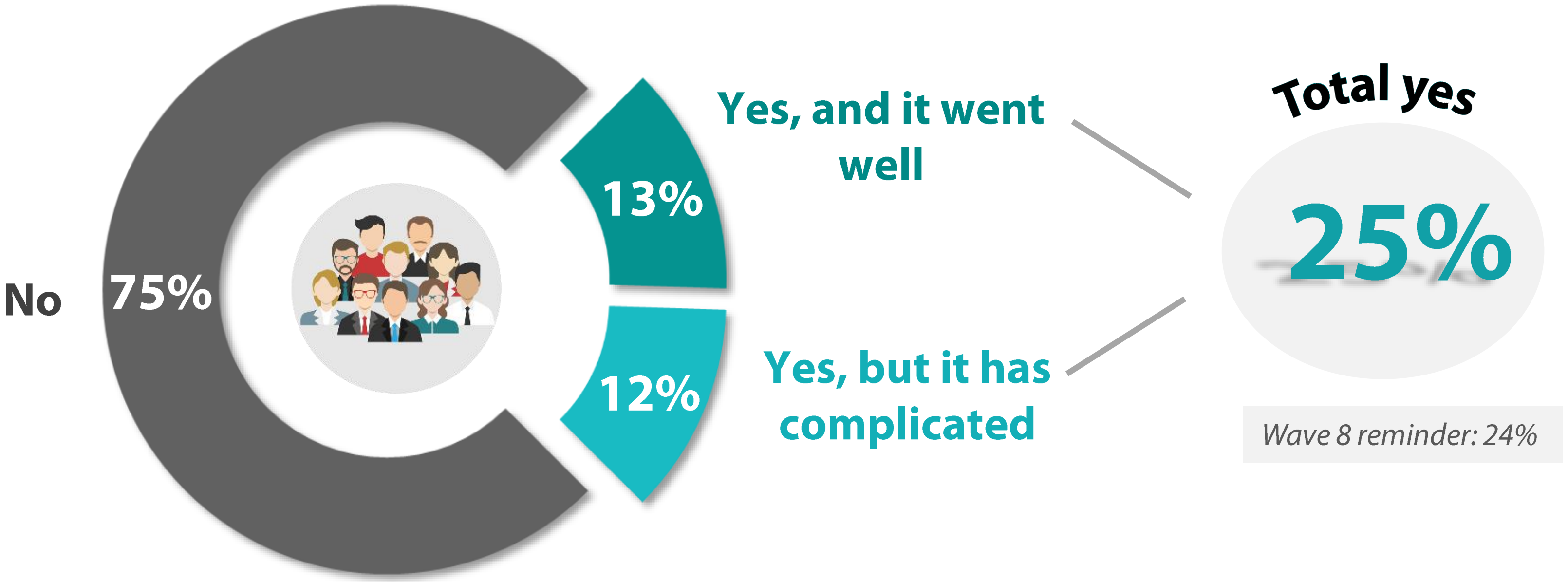
Similar to last year, three quarters of insured companies have never called on their cyber insurance.

320 people

Q32. Has your company ever called on its cyber insurance in the event of a cyberattack?

Base: have or plan to have cyberinsurance

Using cyberinsurance



Wave 8 reminder: 24%

More than half of companies believe that the use of rating agencies by cyber-insurers is not a good thing, considering that the analysis remains very partial.

456 people

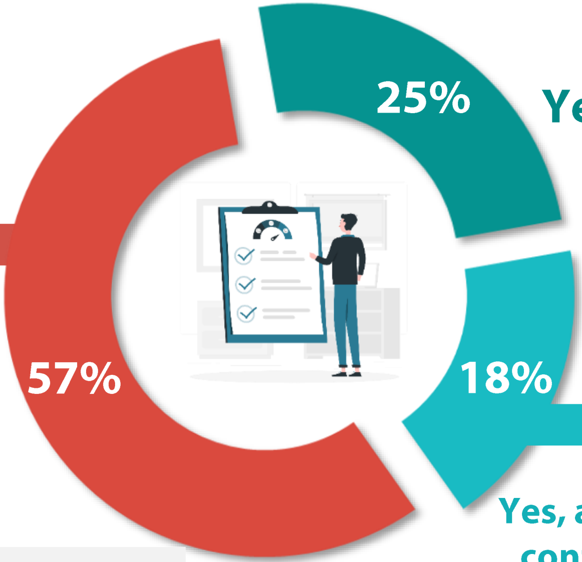
New question in 2023

Q33. E-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 (81)*

Q33bis. What are the reasons for this? *Base: not a good thing (259)*

Using the service rating agencies



Yes — 25% — *Wave 8 reminder: 29%*

Yes, and I myself have contracted services cyber-rating — 18% — *Wave 8 reminder: 21%*

No — 57% — *Reminder Wave 8: 50%*

Modified item	Because, by design, these platforms only provide a very partial analysis of the level of security. and provide a score by extrapolation	71%
	Because the results are unreliable in identifying and assigning assets	58% ↗ +15
Modified item	Because the criteria and method of calculating scores are questionable from the point of view of defined priorities	69%
	Because these services are a form of forced solution selling	37%
	For another reason	3%

64%	Complementing my cyber risk management
30%	To understand and improve the note that was imposed on me
6%	Other reasons

↗ ↘ Statistically significant change from previous wave

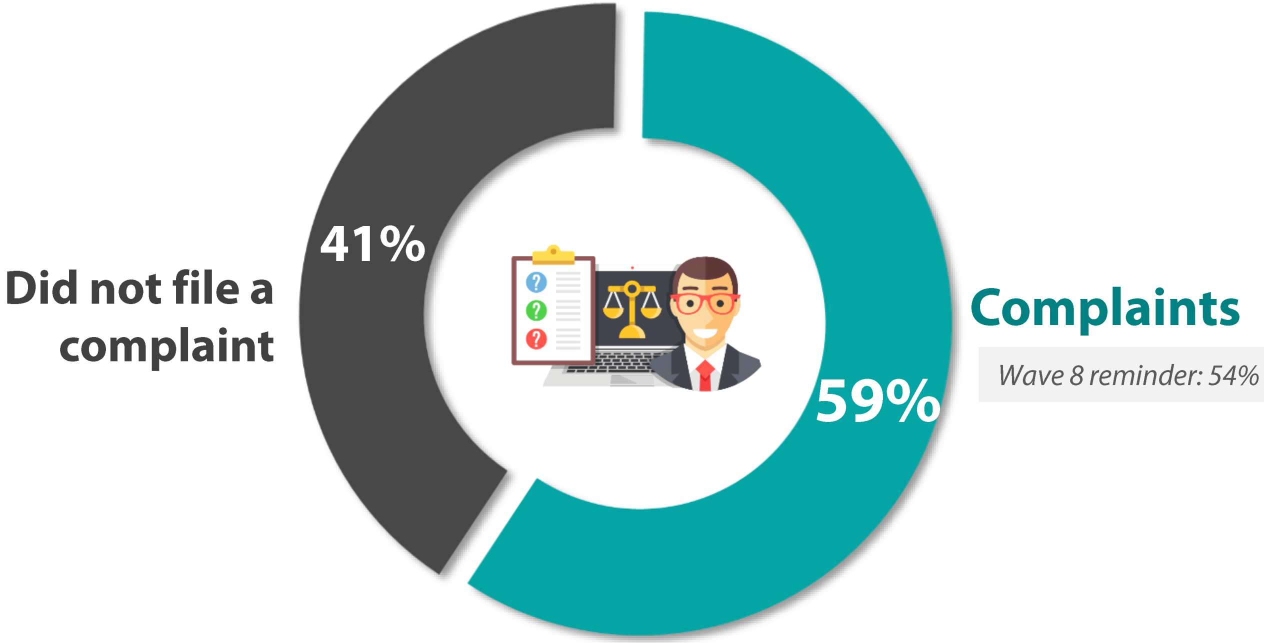
Nearly 6 out of 10 companies have already filed a complaint following a cyberattack...

225 people

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

Base: observed an attack

49% of companies suffered at least one cyberattack in 2023



Wave 8 reminder: 54%

for **all attacks**: 32

for **certain attacks**: 27

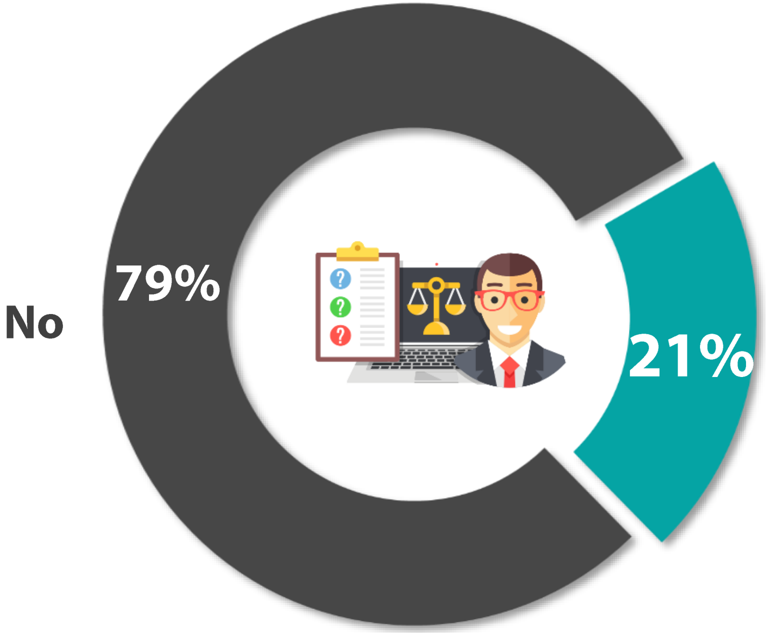
...and the identification/interrogation of the attackers occurred 1 time out of 5, a score which is tending to increase

132 people

Q8bis. Following your complaint(s), did the investigation lead to the identification and/or arrest of the attacker(s)?

Base: filed a complaint

59% of companies have filed a complaint



Yes, the investigation led to identification

Wave 8 reminder: 16%

for **all complaints**: 5%.

for **certain complaints**: 16

03

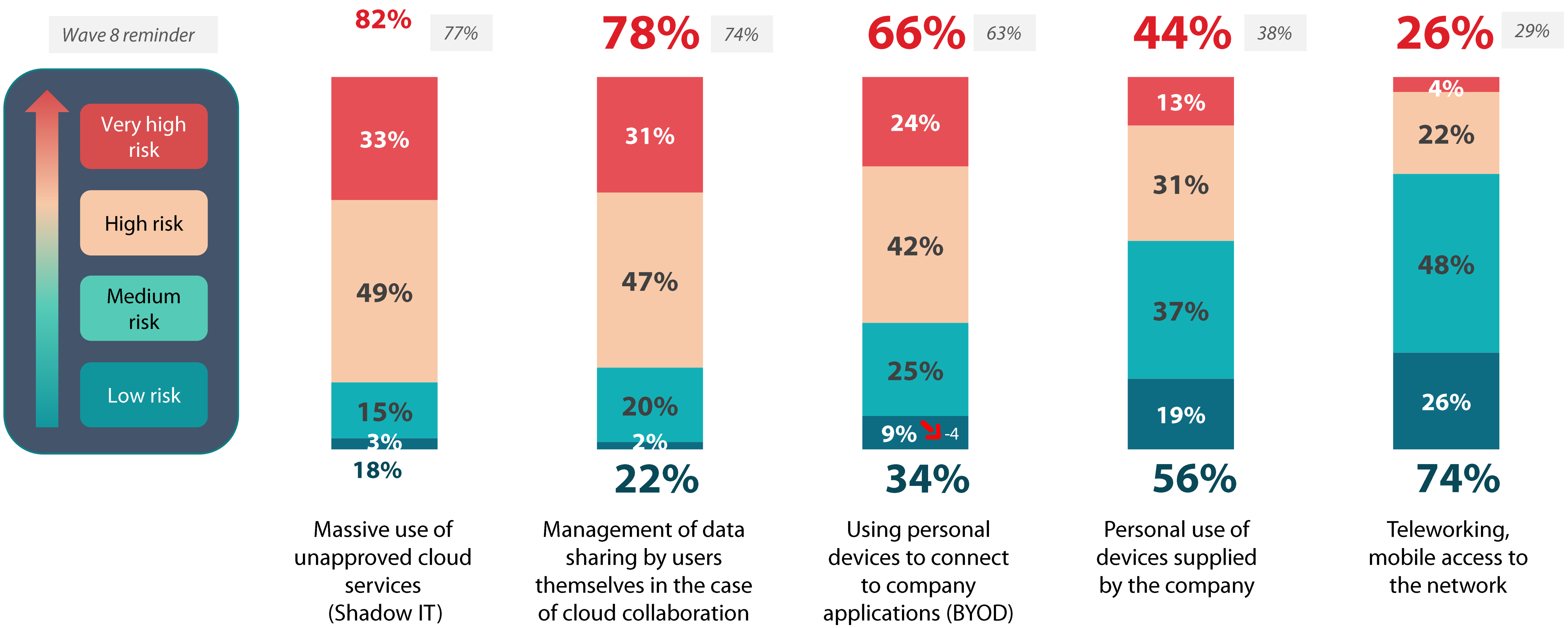
Digital uses still present as many risks, even though employees are more aware of the issues at stake

With the exception of the risks associated with teleworking, CISOs are seeing an upward trend in the level of risk associated with employees' digital habits, particularly in the use of the illegitimate cloud or Shadow IT.

456 people

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

Base: all



↗↘ Statistically significant change from previous wave

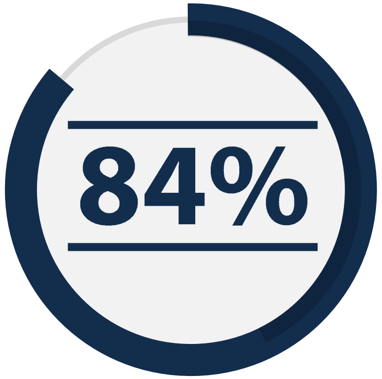
While the metrics used to measure employee participation in training/awareness sessions are widely deployed in companies, this is much less the case for measuring employee knowledge of cybersecurity.

456 people

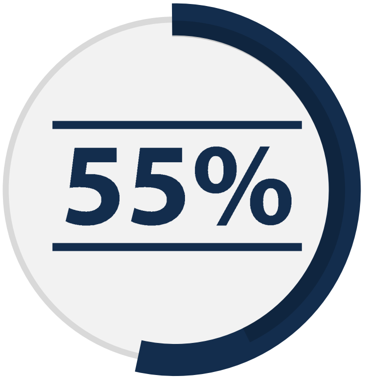
New question in 2023

Q19b. And still with regard to cybersecurity awareness and training, have you implemented the following metrics?
Base: all

Metrics to **measure participation in training courses awareness-raising**



Metrics to measure **knowledge of employees in cybersecurity**

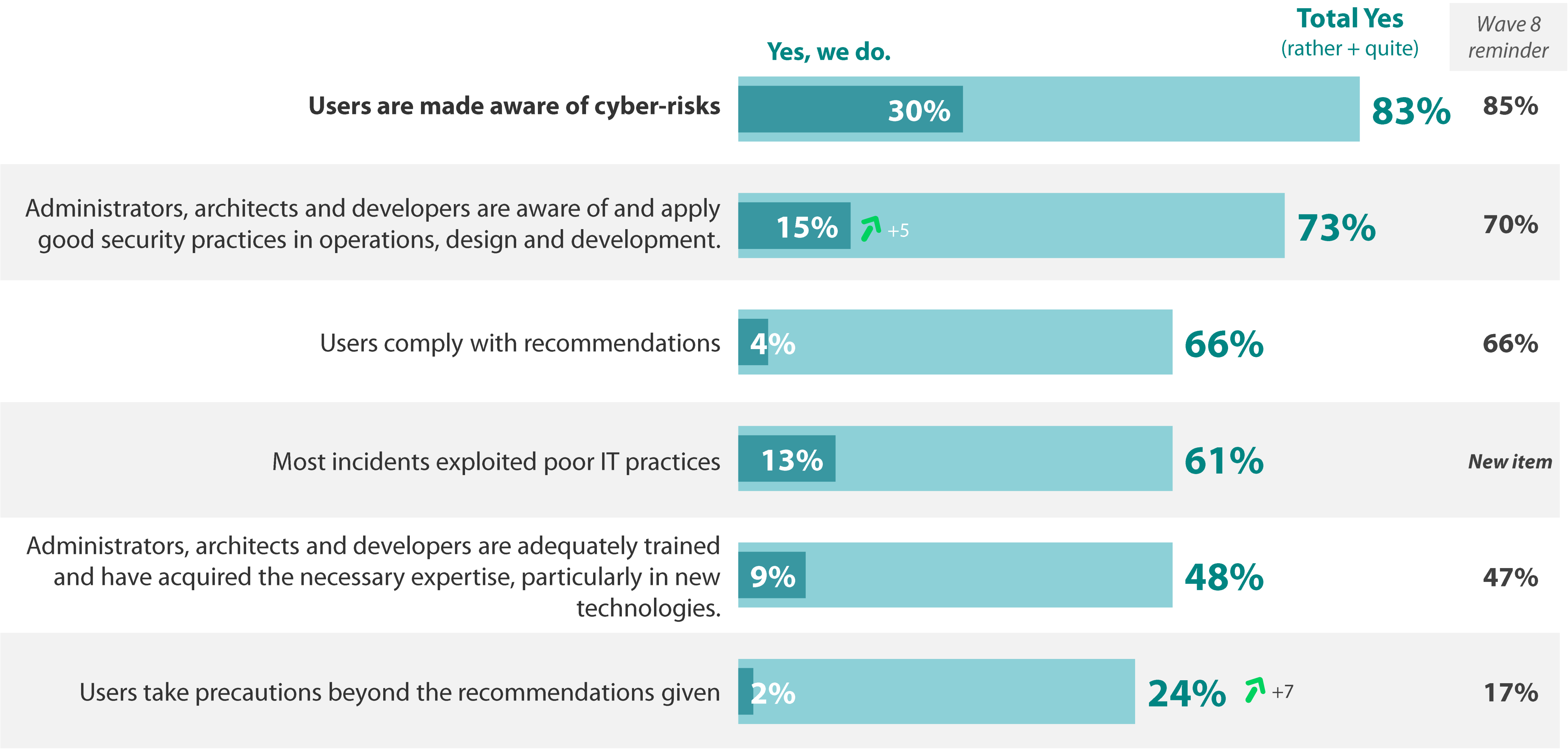


Employee awareness and training in cybersecurity is equivalent to 2022 according to CISOs, and it should be noted that users are taking more precautions, even if this is not always sufficient.

456 people

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

Base: all



“opinionway for CESIN

↗ ↘ Statistically significant change from previous wave

Focus on…

The Cloud

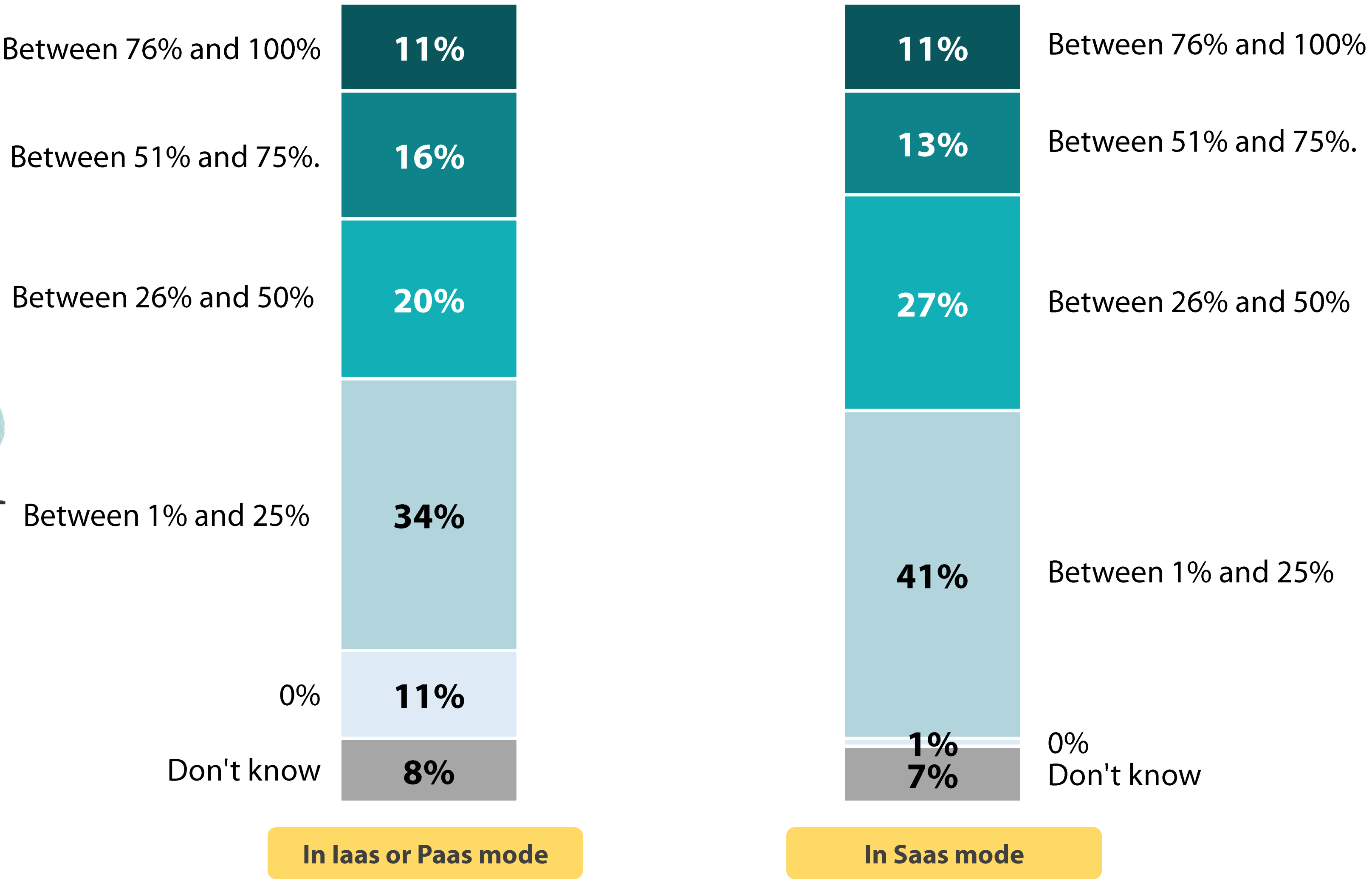
Whether in Iaas/Pass or Saas mode, the cloud represents less than 50% of the IS in the majority of companies (65% for Iaas/Pass mode and 69% for Saas mode).

456 people

New question in 2023

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

Base: all



Risks relating to the control of subcontractors and access by administrators remain the most important, while the lack of compartmentalization between the different customers of the hosting provider is becoming increasingly problematic. Fortunately, the level of expertise is increasing.

456 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

2022 ranking reminder		% High risk	
	1	48%	**No control over the hosting provider's subcontracting chain**
	2	43%	**Difficulty of controlling access by host administrators**
		40%	Poor visibility of the inventory of resources in the cloud
	4	39%	Data stored in France/Europe but provided and/or operated by foreign service providers where the law of the country of origin also applies
		37%	Data storage in foreign datacenters, outside French law
↗ +10		37%	Lack of compartmentalization between the host's different customers
	5	36%	Difficulty of carrying out audits (penetration testing, configuration control, on-site visits)
Modified item		36%	Non-control of security parameters / weak encryption on the part of the host (the host manages the decryption keys)
↘ -9	3	34%	Expertise still too rare, expected from architects and administrators
		33%	Unavailability of data/application due to an attack on the hosting provider
		33%	Failure by the hosting provider to delete data at the end of the contract (normal or early) when contractually required to do so.
		32%	Data confidentiality vis-à-vis the hosting provider
		32%	Difficult to control how your employees use it
		30%	High frequency of new online versions with potential uncontrolled changes to safety principles or parameters
		30%	Bounce attack from host
		29%	Failure to erase data during use, as deletions and purges carried out by the customer are not really effective.
		27%	Systemic propagation of attacks and human errors at the host level
		27%	Difficulty or impossibility of feeding cloud logs into SIEM
		25%	Non-restitution of data by the hosting provider at the end of the contract (normal or early) when contractually agreed.
		23%	Data processing and use by the host without the customer's knowledge
		16%	Trapping a hosted application

↗ ↘ Statistically significant change from previous wave

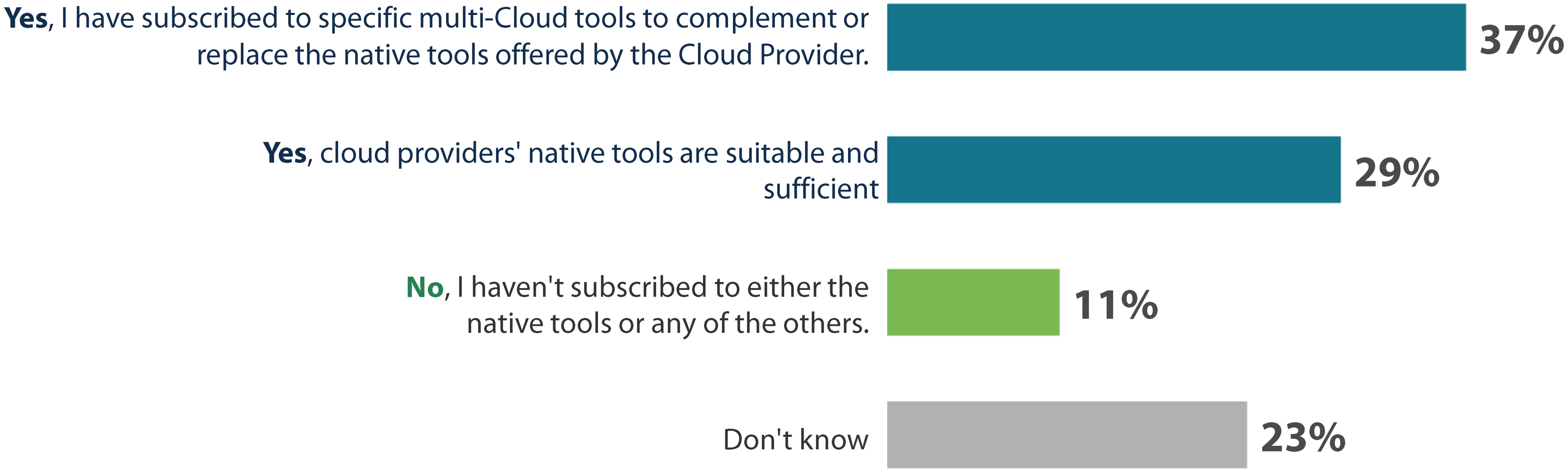
Two-thirds of CISOs believe that securing data in the cloud requires specific tools

New question in 2023

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

456 people

... 66% believe that securing data stored in the cloud requires specific tools



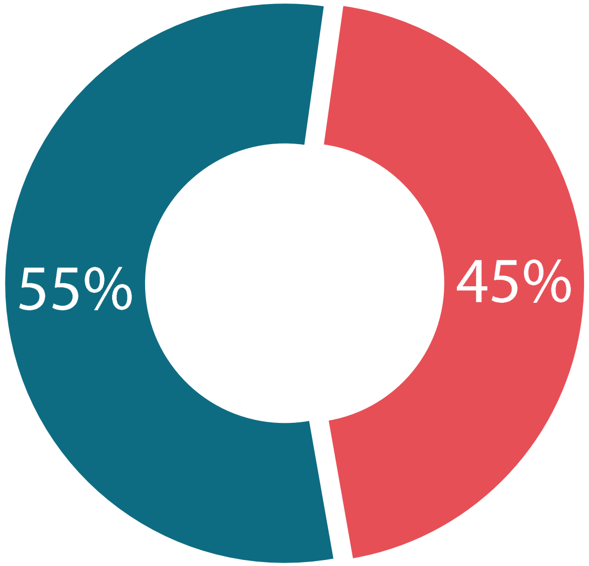
One company in two (55%) is interested in sovereignty and Trusted Cloud initiatives

456 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.

No, my company is not concerned by these issues

04

The development of AI and tightening regulations are forcing companies to adapt

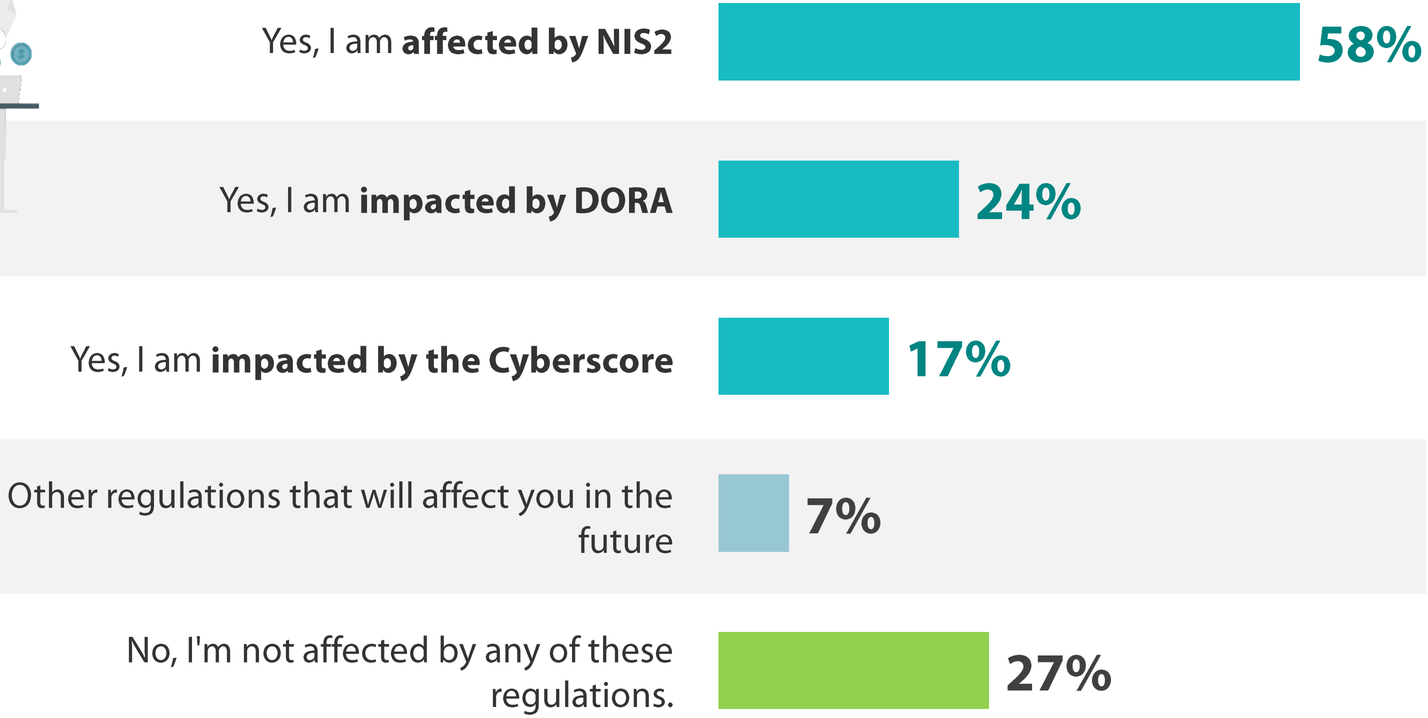
The vast majority of companies are affected by the tightening of regulations, and more specifically by the NIS2 directive.

456 people

New question in 2023

Q37. Regulations are tightening. Are you affected?

Base: all - Multiple answers possible


Yes, I am **affected by NIS2**
58%
Yes, I am **impacted by DORA**
24%
Yes, I am **impacted by the Cyberscore**
17%
Other regulations that will affect you in the future
7%
No, I'm not affected by any of these regulations.
27%

72%

Impacted by at least one regulation

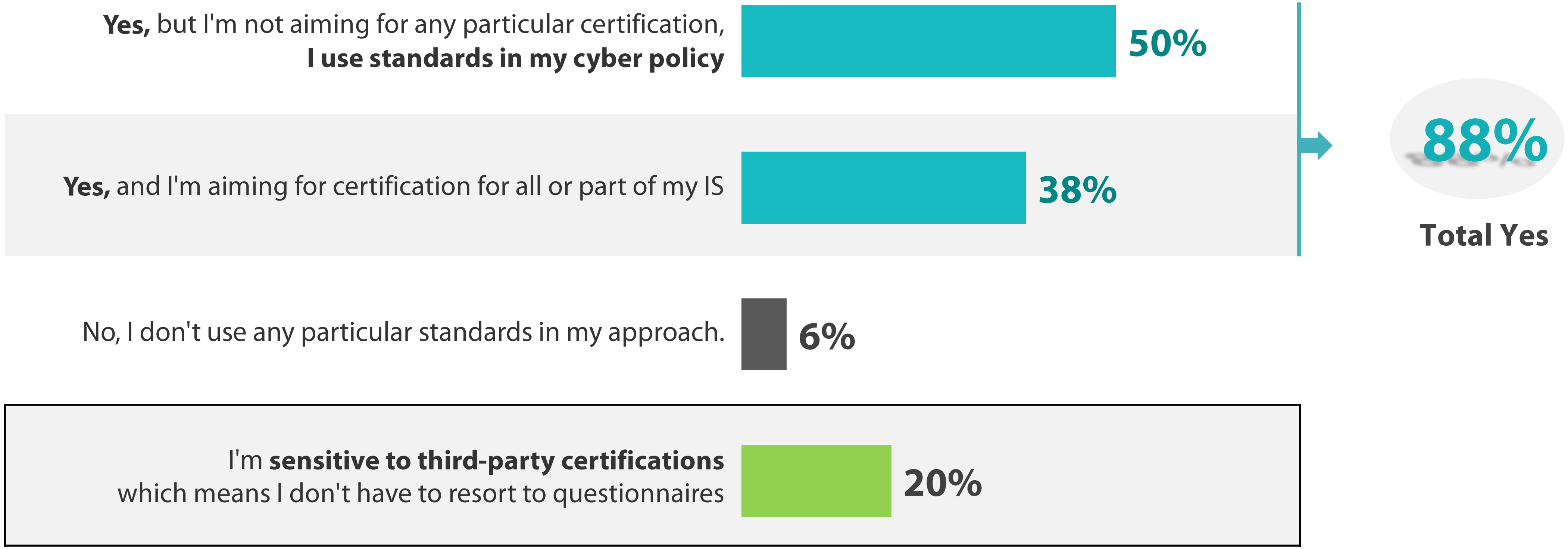
The vast majority of companies integrate standards into their day-to-day business, and certifications are relatively sought-after both internally and by third parties.

456 people

New question in 2023

Q38. Standards are an integral part of the cyber landscape. Are you sensitive to them?

Base: all



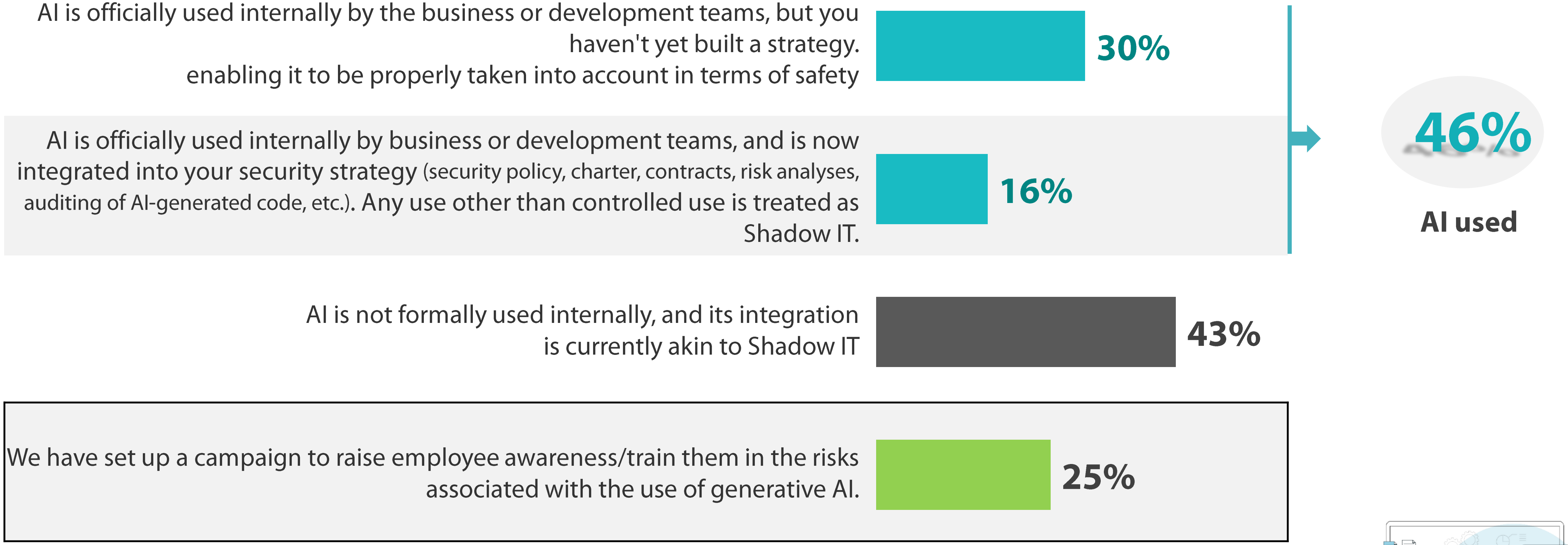
AI is now used in half of all IS, yet the integration of AI into security strategy is still underdeveloped (16%).

456 people

New question in 2023

Q39. AI, already more or less used in certain cyber solutions, has made a dramatic entry 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



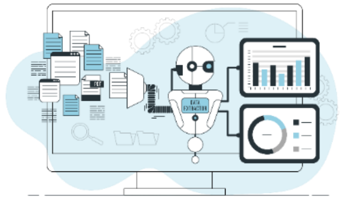
AI is officially used internally by the business or development teams, but you haven't yet built a strategy. enabling it to be properly taken into account in terms of safety — 30%

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. — 16%

46% AI used

AI is not formally used internally, and its integration is currently akin to Shadow IT — 43%

We have set up a campaign to raise employee awareness/train them in the risks associated with the use of generative AI. — 25%

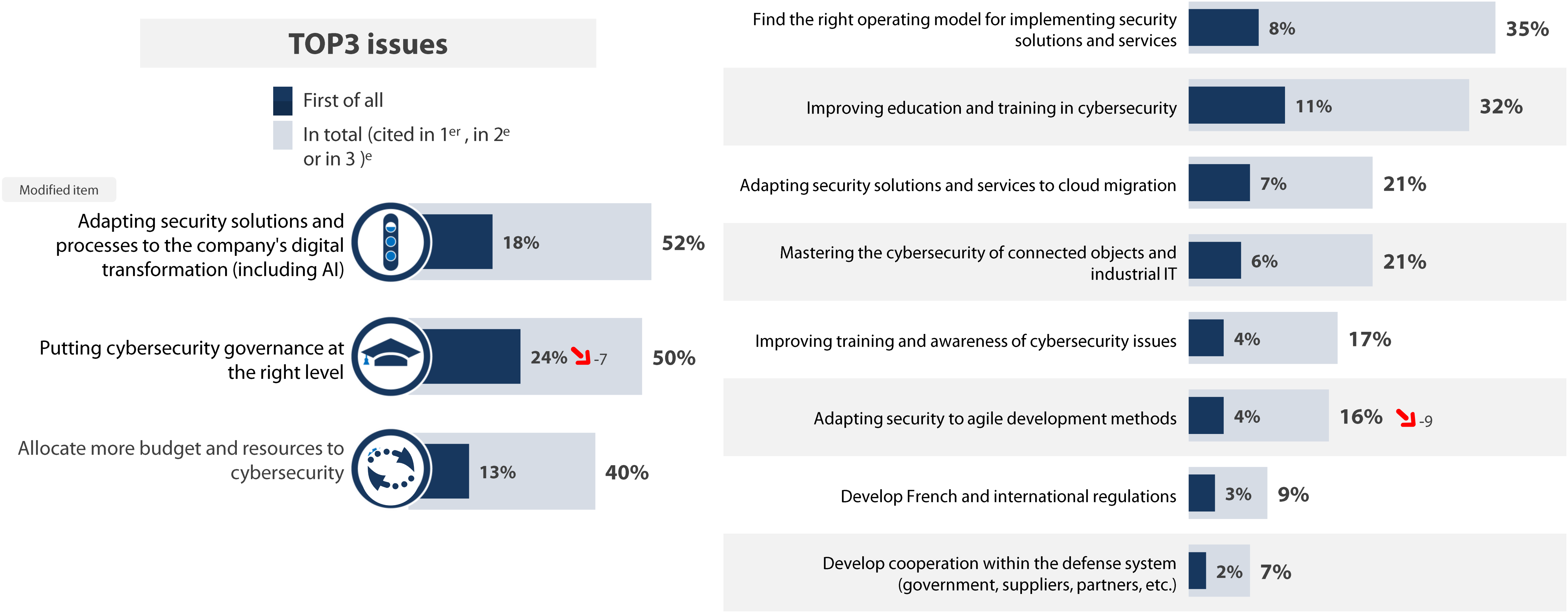


The development of AI makes adapting security solutions and processes the number one challenge for companies

456 people

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

Base: all



↗ ↘ Statistically significant change from previous wave

Cybersecurity is perceived as an important issue, and is taken into account by the COMEX at the same level as in 2022.

456 people

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

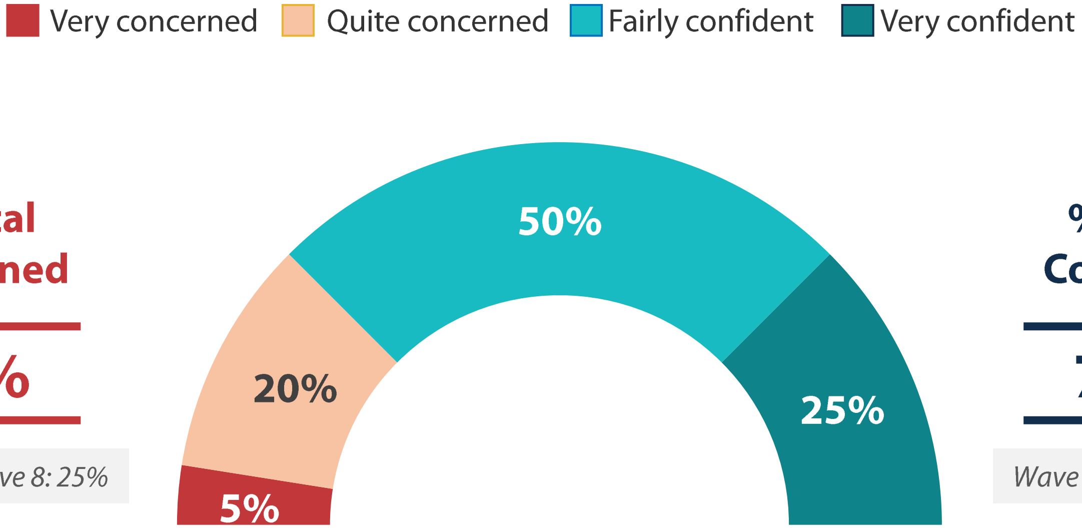
Base: all

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

% Total Concerned

25%

Reminder Wave 8: 25%



% Total Confident

75%

Wave 8 reminder: 75%.

“opinionway for CESIN

Companies feel better prepared to face cyber-risks, with the proportion of "very worried" declining this year

456 people

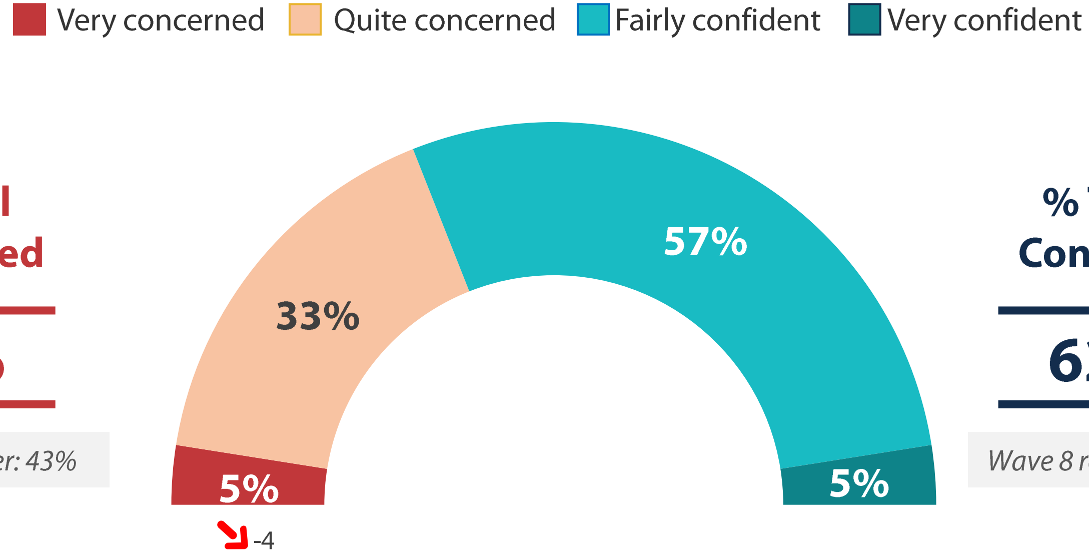
Q24. For the future, would you say you are very confident, fairly confident, fairly worried or very worried about...?
Base: all

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

% Total Concerned

38%

Wave 8 reminder: 43%



% Total Confident

62%

Wave 8 reminder: 57%

Statistically significant change from previous wave

More than half of companies plan to increase staffing levels to combat cyber-risks, with the bulk of these to be devoted to operational cybersecurity.

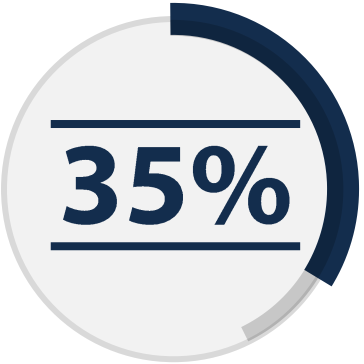
456 people

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

Base: all

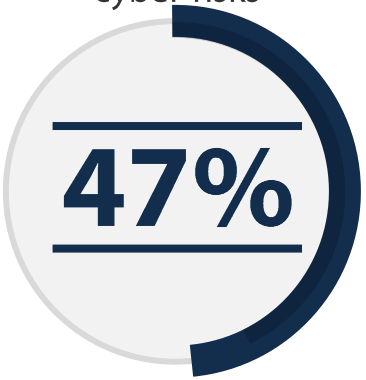
53% plan to increase the number of staff allocated to cyber-crime protection

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



Modified item

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



New item

↗↘ Statistically significant change from previous wave

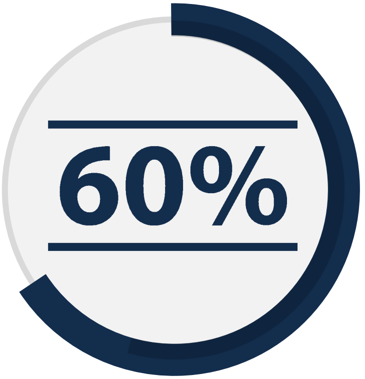
And while the vast majority of companies intend to acquire new technical solutions for cybersecurity, fewer intend to increase their budgets.

456 people

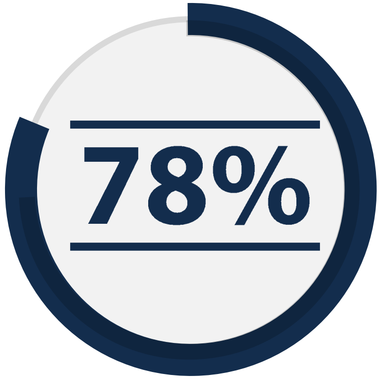
Q17. Over the next 12 months, does your company plan to...?

Base: all

increase budgets allocated to protection against cyber-risks



acquire new technical solutions for cybersecurity



Conclusion

Summary (1/3)

Number of cyberattacks on the rise, boosted by an increase in denial-of-service attacks

For the first time in 4 years, the number of companies having experienced a cyberattack is on the rise (49%, +4 points).

Manipulation-based scenarios are on the decline. Phishing, spear phishing and smishing combined remain the main attack vector, but are declining significantly (60%, -14 pts), as is the president scam (28%, -13 pts).

Conversely, it is worth noting the increase in denial of service attacks this year (34%, +11 pts), making denial of service (30%, +11 pts) one of the main consequences of cyberattacks, along with data theft (31%). Related to this, website unavailability was one of the main impacts of cyberattacks on companies' business (22%, +9 pts), along with production disruption (24%).

Ransomware has stabilized, and the risk of cyberespionage is considered significant.

EDR and, more generally, market solutions deemed effective by companies that are also developing their incident response preparedness.

87% of CISOs feel that the security solutions available on the market are appropriate for their company. On average, more than 15 security solutions or services are deployed in companies, with operating models varying between internal, external or hybrid.

At the same time, 57% of companies have set up a cyber-crisis training program, with exercises carried out periodically (28%, +9 pts).

EDR is the most widely deployed security solution in companies (90%, +9 pts), along with firewalls, whose effectiveness is confirmed more strongly this year by CISOs (92%, +6 pts).

Companies remain open to cyber innovation.

Summary (2/3)

Risky digital uses, despite employees more aware of the issues at stake

According to CISOs, employees' various digital uses still represent a risk, particularly Shadow IT (82%) and the management of data sharing by users themselves (78%).

The implementation of metrics to measure participation in training/awareness-raising sessions (84%) is widely deployed, but we still don't know how to measure its effectiveness and assess employees' maturity on the subject of cybersecurity, even though they seem to take more precautions than those recommended a minima (24%, +7 pts).

A quarter of insured companies have already called on their cyberinsurance

7 out of 10 companies have now taken out cyber insurance, and a quarter of them have already used it in the event of a cyberattack.

In addition, 59% of companies have already lodged a complaint following a cyberattack, and 1 in 5 of these complaints led to the identification and/or arrest of the attackers (a slight increase of 5%).

Confidence in the rating agencies, whose results are considered to be very partial, has declined.

Securing cloud data

According to CISOs, digital uses of the cloud represent a major risk, even if the proportion of IT systems adopting the cloud is still in the minority, but is starting to become significant, whether in Iaas / Paas or Saas mode. Fortunately, expertise in cloud security is growing.

Two-thirds of CISOs believe that securing data stored in the cloud requires specific tools.

Summary (3/3)

Regulation, standards and the use of AI push companies to act

7 out of 10 companies say they are currently affected by at least one regulation (NIS2, DORA, Cyberscore).

88% of companies believe that standards are an integral part of the cyber landscape, and are happy to turn to in-house or third-party certifications.

Almost half (46%) of CISOs see AI being used internally, but only 16% have already integrated it into their security strategy. This use of AI has prompted them to define the adaptation of their solutions to the company's digital transformation as the main challenge for the future (52%).

Companies are slightly less worried about their ability to cope with cyber-risks (38%, - 5 pts), with the proportion of "very worried" almost halved from 9% to 5%.

In the end, more than half of companies plan to increase the number of staff allocated to protection against cyber-risks, and the vast majority (78%) intend to acquire new technical solutions. Lastly, budgets for dealing with cyber-risks are likely to remain stable.

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