

---

# Club des Experts de la Sécurité de l'Information et du Numérique

## Barometer of the cyber- security in companies

Wave 4 - January 2019

Media contact information:

Véronique Loquet, AL'X COMMUNICATION

+33 6 68 42 79 68 / [vloquet@alx-communication.com](mailto:vloquet@alx-communication.com)

*“opinionway*



OpinionWay: 15 place de la République, 75003 Paris, France

# Table of contents

1. Context and objectives
2. Methodology
3. Key learnings
4. Findings
  1. An increasingly decisive impact of cyberattacks
  2. Cloud and IoT: increased risks on account of the digital transformation
  3. Developing cyber resilience to address cybersecurity risks
  4. Three challenges for the future, mainly focusing on human dimension: awareness, governance and resources
5. Appendices

# Context and objectives

---

- **CESIN** provides a forum for **experts in security and digital technology** within large companies.
- CESIN and OpinionWay launched in 2015 their first major survey to assess, to get the opinion of CESIN members :
  - the **perception of cyber-security and its challenges**
  - the **practical reality** of the IT security in large companies.
- The survey is renewed every year. This last one, conducted at the end of 2018, provides updates of the results and new data on the impact of the digital transformation in companies.

---

# METHODOLOGY

# Methodology



## Sample

Quantitative study carried out by OpinionWay among **174 members of CESIN** from the CESIN member file (498 members).



## Data collection

**Online** data collecting via CAWI (Computer Assisted Web Interview) system



## Fieldwork

From **November 23<sup>rd</sup>** to **December 26<sup>th</sup>** 2018.



## Certification

OpinionWay conducted this survey respecting the **ISO 20252** standard.

**Any total or partial publication must imperatively quote the following mention:**

**“OpinionWay Survey for CESIN”**

**And no resumption of the survey can be dissociated from this mention.**

---

# KEY LEARNINGS

# Key learnings (1/2)

---

## 1. An increasingly decisive impact of cyberattacks

*While the number of cyberattacks tends to remain stable, 8 out of 10 companies continue to be affected each year.*

- The **impact of these attacks on the business** is up to 59%, **10 points higher** than last year.
- **Phishing** is the most common mode of attack (73% were victims), while **“Fake President” fraud** touches this year half of the companies, more than one could expect.
- **Shadow IT** is the **most common cybersecurity risk**, quoted by 64% of respondents as a cybersecurity risk to be treated.

## 2. Cloud and IoT: increased risks on account of the digital transformation

Nearly all companies (98%) believe that the digital transformation has an impact on the security of information systems and data.

Top issues: the **massive use of Cloud**, used by 87% of companies including 52% in public Clouds. A storage mode that raises **problems of non-control**, whether in relation to the **access to the company data** by the hosts (via the administrators or others) or with respect to the **subcontracting chain** practiced by the supplier. Regarding IoT, the most striking feature is the **security vulnerabilities** present in these objects.

These issues imply for CISOs **not to be content with security solutions offered by Cloud service providers** and to have **additional security tools** (versus those offered by the service provider), according to 89% of them.

# Key learnings (2/2)

---

## 3. Developing cyber resilience to address cybersecurity risks

To counter these cybersecurity risks, the CISOs deploy a panoply of **technical solutions**, globally considered **adapted to their needs** (75%), even if some progress remains to be made in their adaptation to the digital transformation. Note the **importance of AI**: 56% of respondents have implemented or plan to use AI-based solutions; however, 55% believe that **AI will not replace human expertise** in safety.

Yet, CISOs are less confident than last year about the ability of their company to cope with cybersecurity risks (51% are confident, -12 points); and **less than half in particular considers that their company is prepared to handle a large cyberattack**. In this context, subscriptions for cyber-insurance are on the rise (+10 points), but **only 1 in 10 companies has set up a genuine cyber resilience program**.

## 4. Three issues for the future, mainly focusing on human dimension

According to the CISOs, the main issue for the future of cyber security is **training and user awareness** (61%). Employee usage brings its share of risks, especially via shadow IT. And if employees are sensitized, they remain little involved as they do not necessarily follow the recommendations. A significant pedagogical work remains to be done.

**Governance of cyber security** must also be at the right level for 60% of CISOs. Despite a positive impact of GDPR compliance on governance (59% of companies), confidence in the ability of the Executive Committee to take into account the issues of cyber-security is very uneven according to the sectors of activity.

**Human resources** are likely to be problematic, with a **shortage of profiles** observed by 91% of CISOs... At a time when 50% of respondents plan to increase the number of staff allocated to the protection against cyber-risks.

---

# FINDINGS

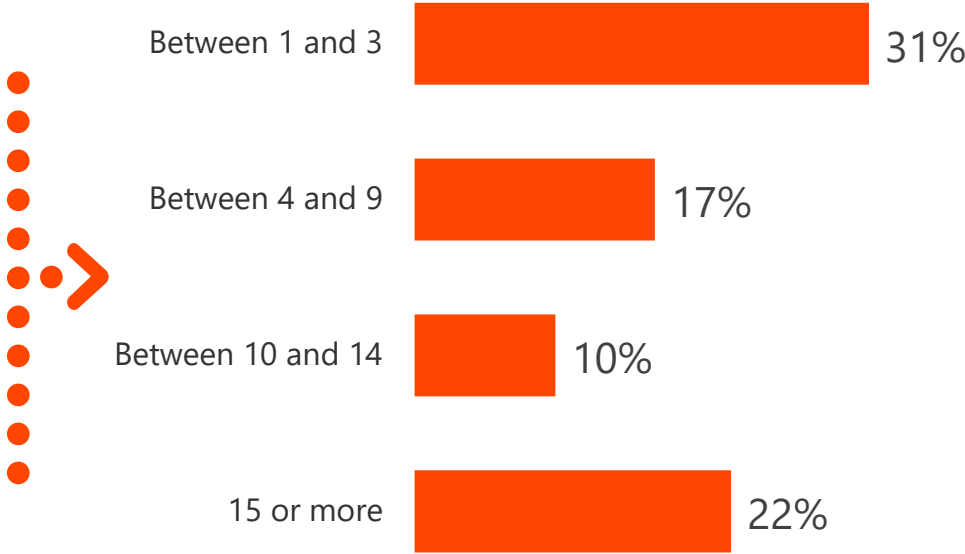
---

# **1. AN INCREASINGLY DECISIVE IMPACT OF CYBERATTACKS**

# The rate of companies affected by a cyberattack remains very high

Q5. How many cyberattacks have occurred in your company in the past 12 months?  
Base: total sample (174)

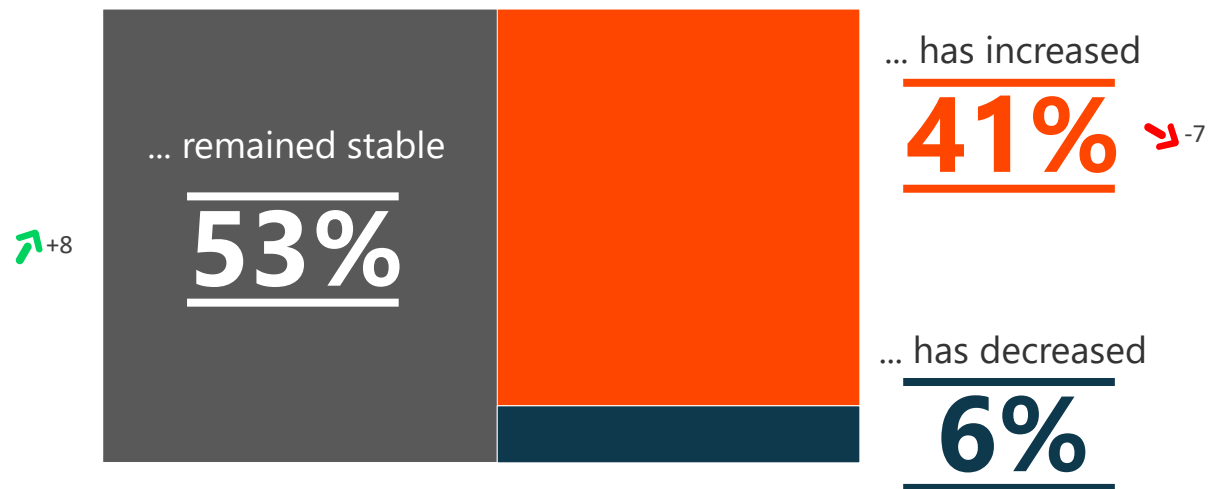
**80%**  
of companies have detected at least one cyberattack



# However, the number of cyberattacks per company tends to stabilize

Q5BIS. And compared to last year, this number of attacks found in your company... ?  
Base: total sample (174)

In one year, the number of attacks...

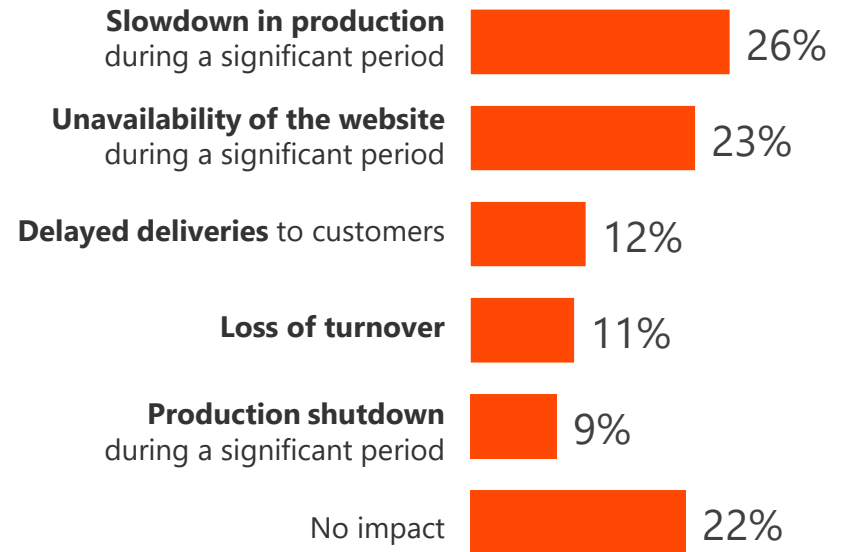
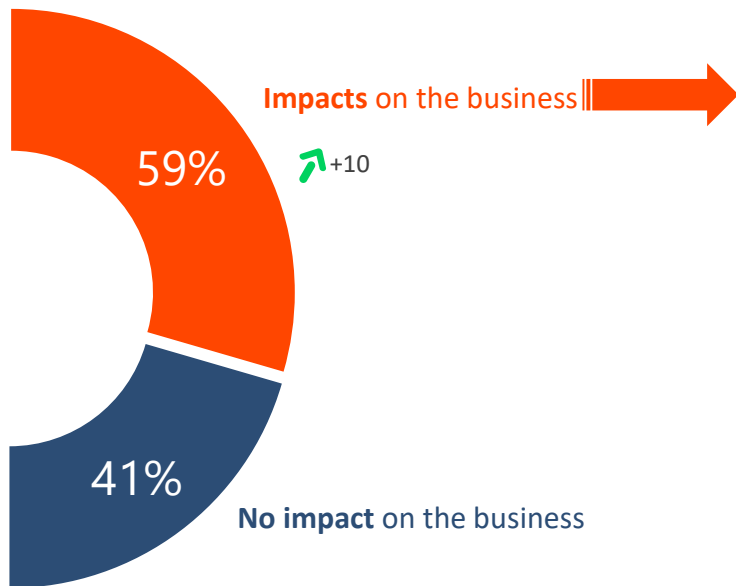


However, the number of cyberattacks per company tends to stabilize

# On the other hand, cyberattacks have a greater impact on the business of targeted companies

Q30. What has been the impact of cyberattacks on your business?

Base: total sample (174) / Several possible answers



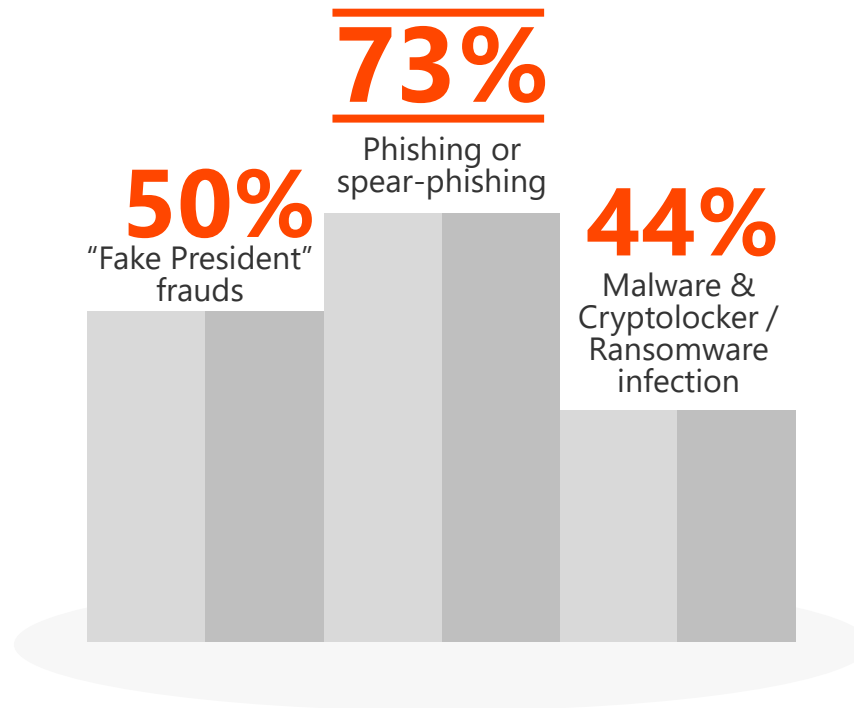
Impacts spontaneously mentioned by respondents:  
Increased workload, lower productivity of employees, bad reputation of the company

# In 2018, phishing becomes the most widespread attack and contrary to what one might think, the "Fake President" frauds affect one in two companies

Q6. What types of cyberattacks has your business seen in the past 12 months?  
Base: have detected an attack (139) / Several possible answers

## Cyberattacks suffered

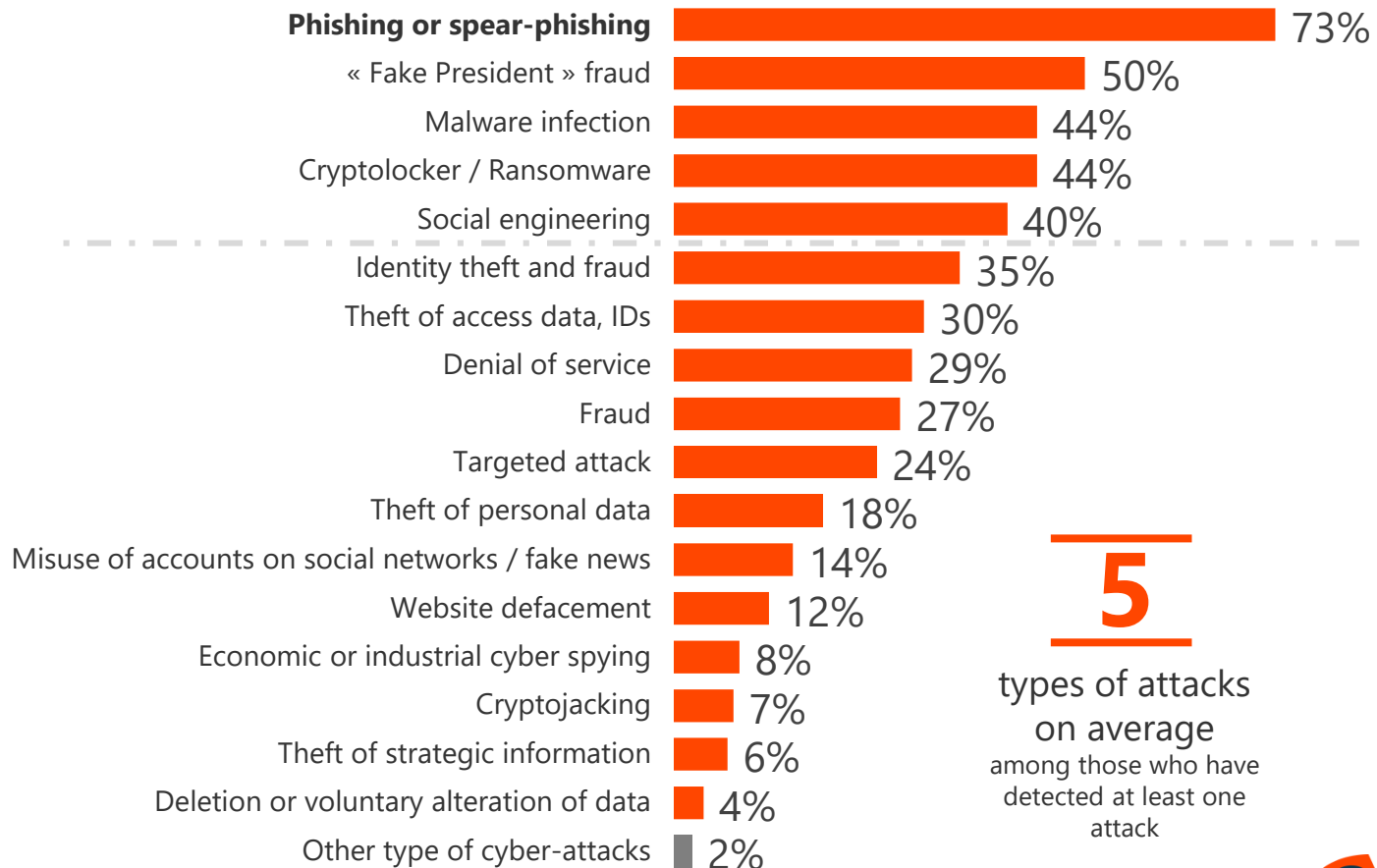
TOP3



# On average, companies face five different types of attacks each year

Q6. What types of cyberattacks has your business seen in the past 12 months?

Base: have detected an attack (139) / Several possible answers

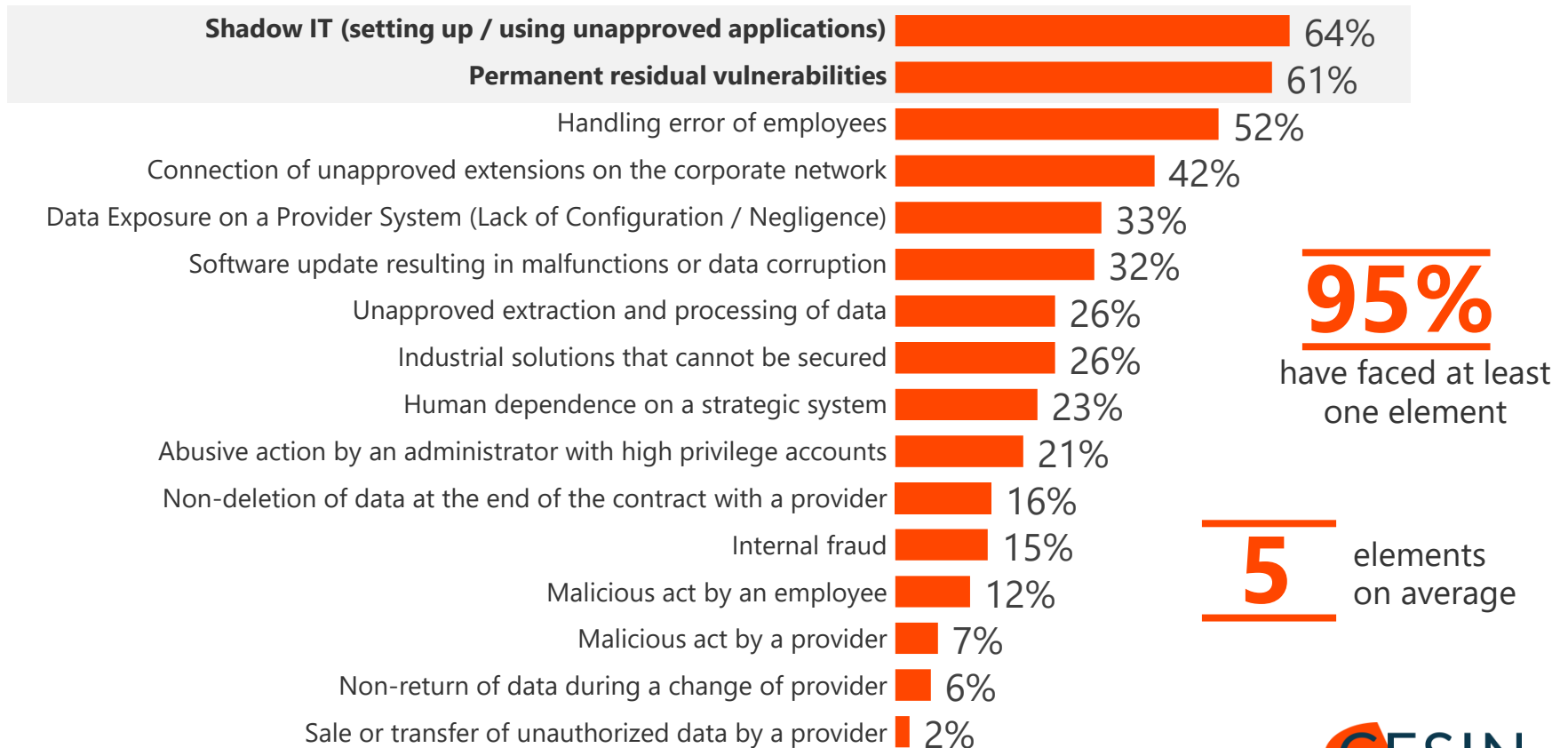


# Shadow IT is the most common cybersecurity risk

Q6BIS. Which of the following cyber security issues did your company face in the past 12 months?

Base: total sample (174) / Several possible answers

## The cybersecurity risks involved



---

## **2. CLOUD AND IOT: INCREASED RISKS ON ACCOUNT OF THE DIGITAL TRANSFORMATION**

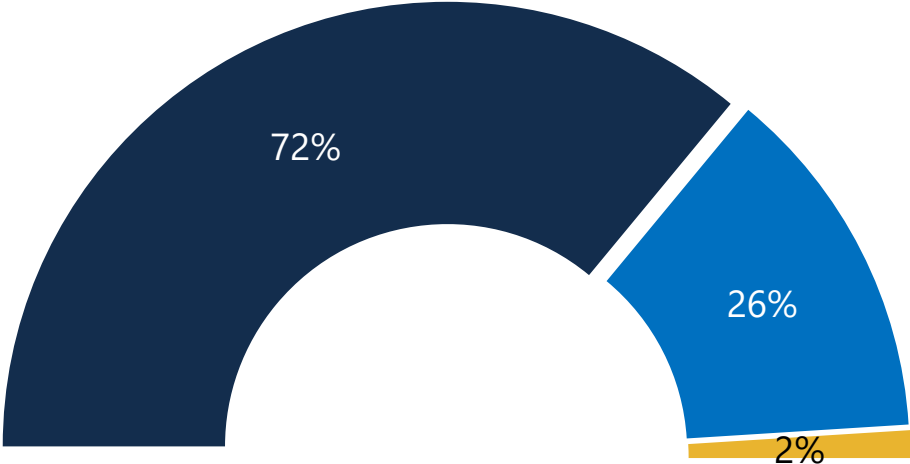
# Digital transformation has an impact on the security of information systems across all companies

Q2BIS. In your company, does digital transformation have an impact on the security of information systems and data?  
Base: total sample (174)

**98%**

consider that digital transformation **has an impact on the security** of information systems and data

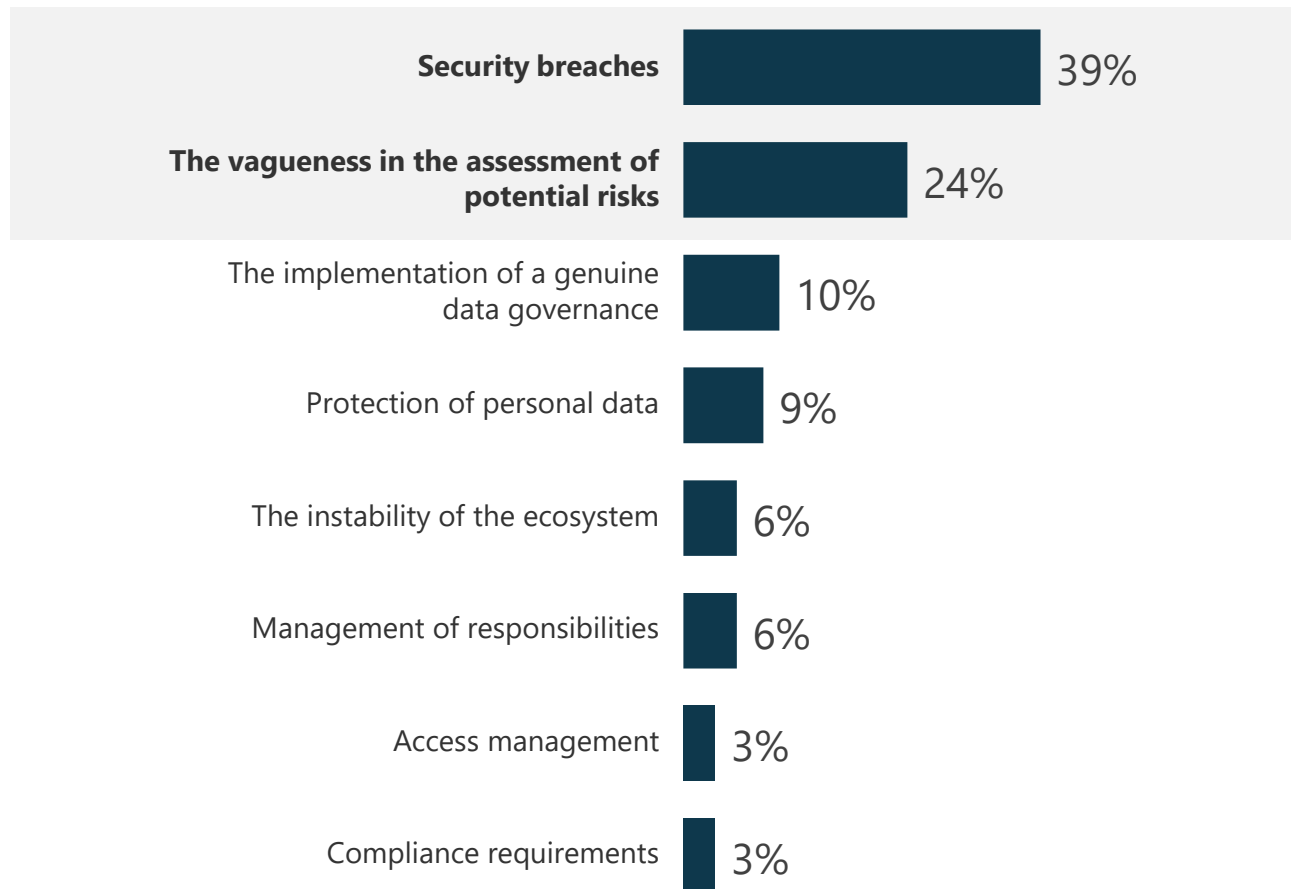
■ Definitely   ■ Probably   ■ Probably not   ■ Definitely not



# Security breaches remain the most prominent feature of IoTs

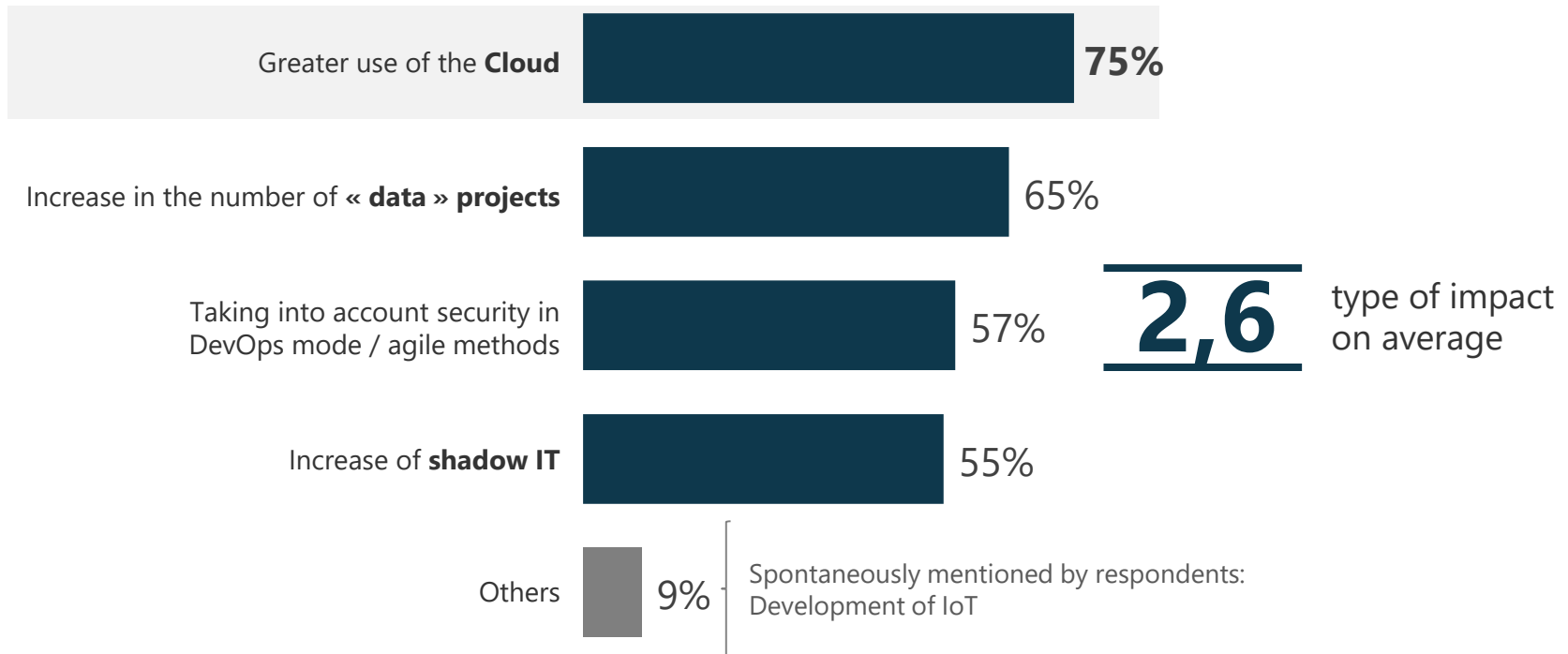
Q36. What do you think is the biggest challenge facing the CISO with regard to Internet of Things (IoT) in business?

Base: total sample (174)



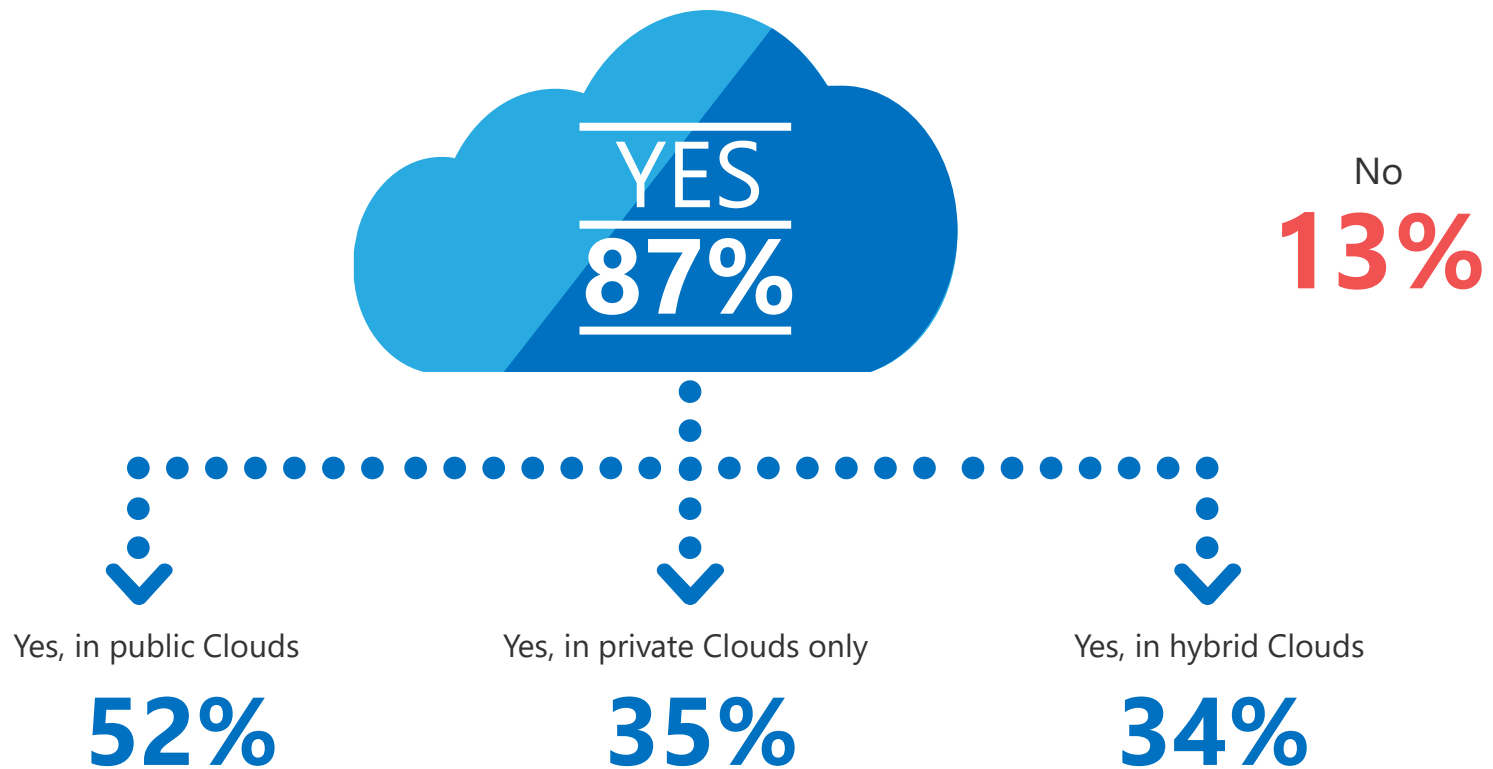
# ... but the most frequent impact of digital transformation within companies is the use of Cloud

Q2BISV4. How does digital transformation impact the security of your company's information systems and data?  
Base: consider that digital transformation has an impact on the security of information systems and data (170)



# Most companies store at least some of their data in a Cloud ... most of them in public clouds

Q20. Are some of your company's data stored in a Cloud?  
Base: total sample (174) / Several possible answers



# In addition, the Cloud exposes companies to different risks, especially due to lack of control

Q22. In your opinion, do the following factors represent a low, moderate, or high risk for Cloud use?

Base: total sample (174)

%  
A strong  
risk

- 52% **Difficulty to control access by administrators of the host**
- 52% **No control of the outsourcing chain of the host**
- 51% **Non-deletion of data**
- 48% Data storage in data centers abroad, outside French law
- 48% Data storage in France but with foreign providers where the law of the country of origin also applies
- 48% Difficulty to carry out audits (pen tests, control of configurations, visit on site)
- 47% No control of the use made of it by the employees of your company
- 45% Confidentiality of data with respect to the host
- 39% No control of the security settings / weak encryption on the part of the host
- 36% Data processing by the host without our knowledge
- 34% Failure of partitioning between the different customers of the host
- 34% Failure of the SOC (internal or external) from the Cloud
- 33% Non-return of data
- 29% Unavailability of data / application due to an attack on the host
- 29% Systemic propagation of attacks and human errors
- 25% Smurf attack from the web host
- 22% Trapping a hosted application
- 21% Low frequency of online versions and lack of security checks

# To secure data stored in a public Cloud, CISOs are not satisfied with the tools offered by the provider...

Q23. In your opinion, does securing data stored in the Cloud require specific tools or devices?

Base: total sample (174)

... **89%** believe that securing data stored in the Cloud requires specific tools or devices

**Yes**, in addition to the tools offered by the provider



80%

**Yes**, replacing the tools proposed by the provider



9%

**No**, the level of security offered is appropriate



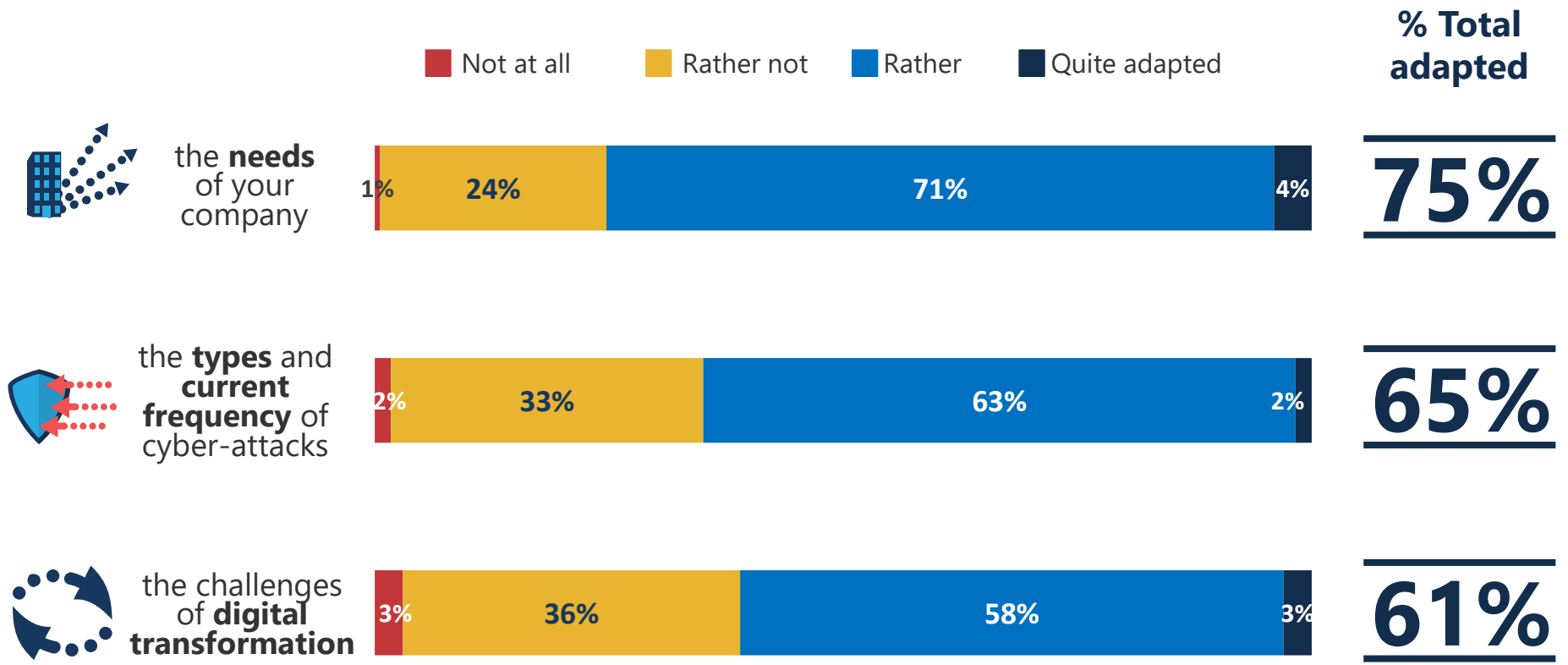
13%

---

## **3. DEVELOPING CYBER RESILIENCE TO ADDRESS CYBERSECURITY RISKS**

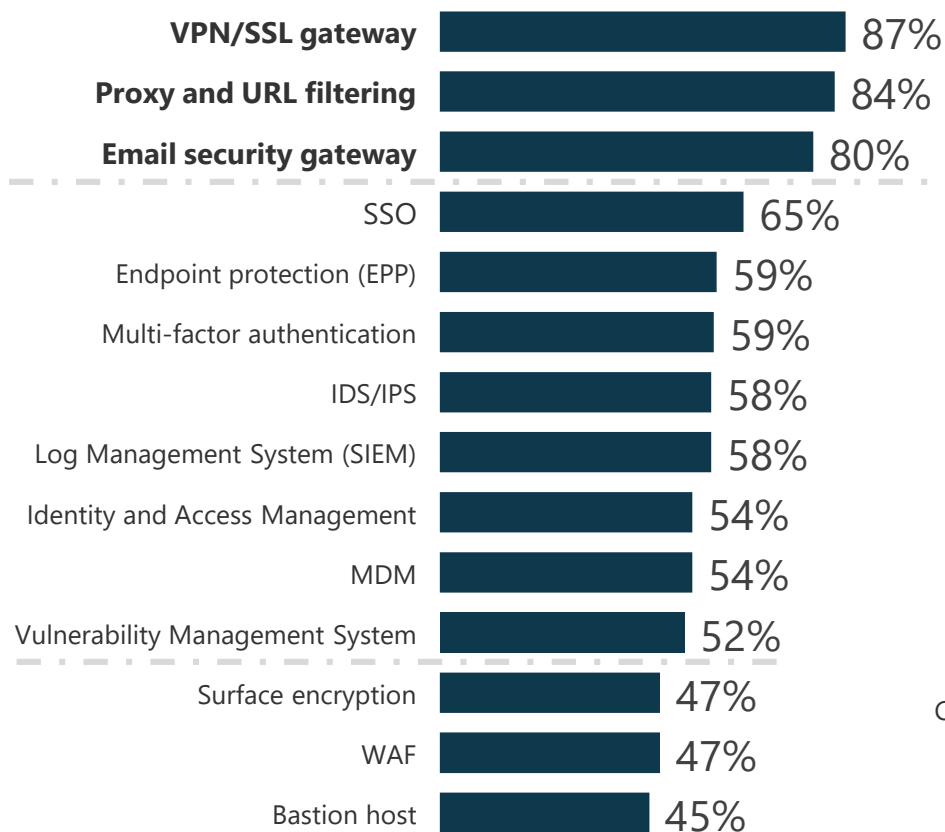
# On a technical level, the proposed solutions seem in line with expectations of the companies but remain challenged by the digital transformation

Q29. To what extent do you think protection solutions available on the market are adapted or not to...?  
Base: total sample (174)

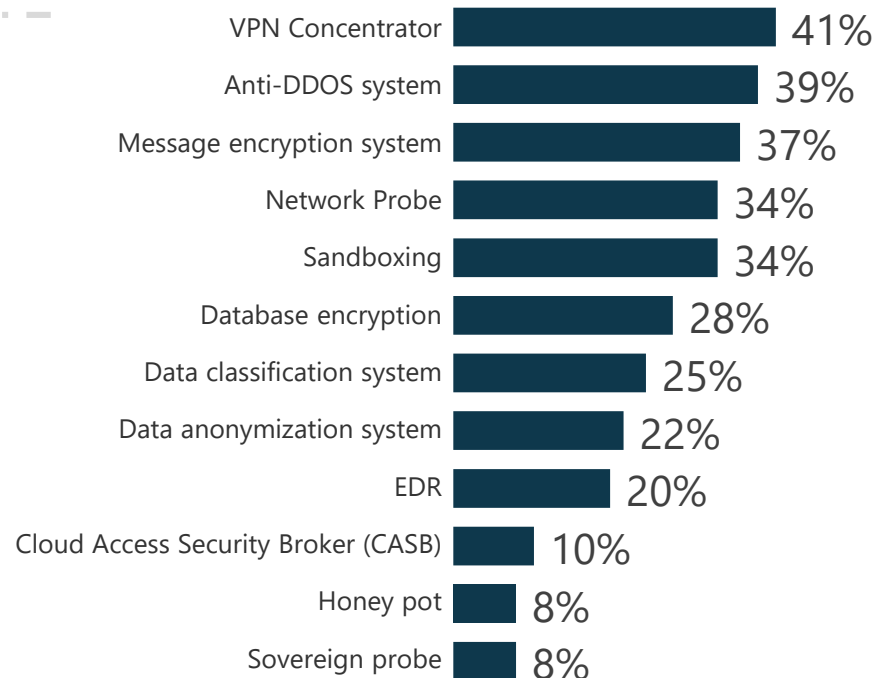


# Concretely, companies deploy nearly a dozen solutions on average...

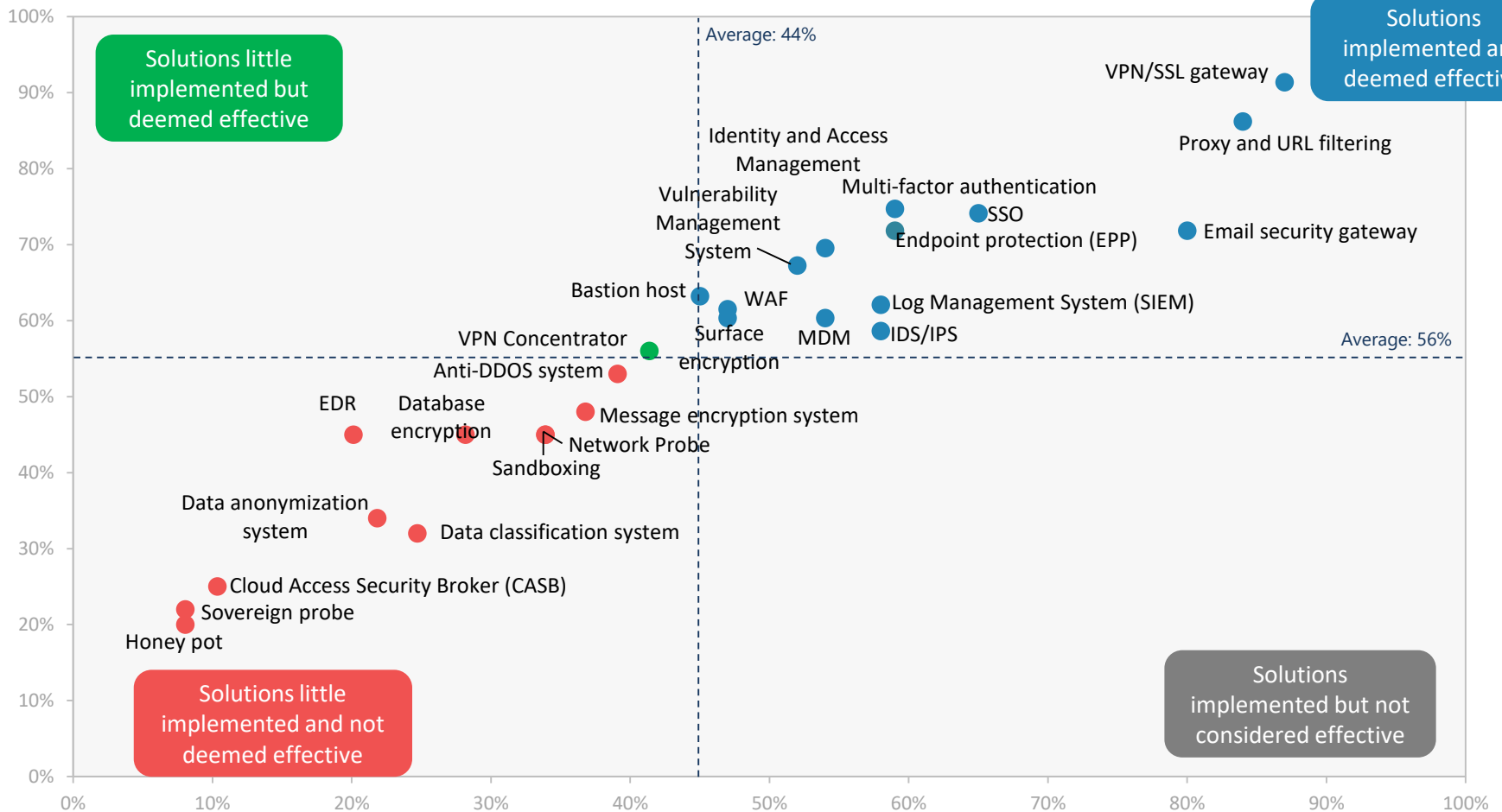
Q8. Which of the following protection solutions have been implemented in your company, in addition to the basics tolls (antivirus, firewall,...) *Base: total sample (174) / Several possible answers*



**11,6** solutions on average



# ... and these implemented solutions are considered effective



Solutions considered effective

Solutions implemented

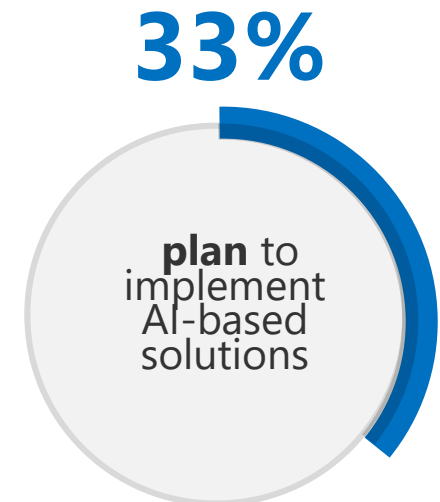


# AI-based protection solutions to face cyber-risks are becoming increasingly popular...

Q40. Let's talk about the potential role of AI in IT security. In your company, have you implemented AI-based protection or detection solutions?

Base: total sample (174)

**56%** have AI-based solutions in place or plan to do so

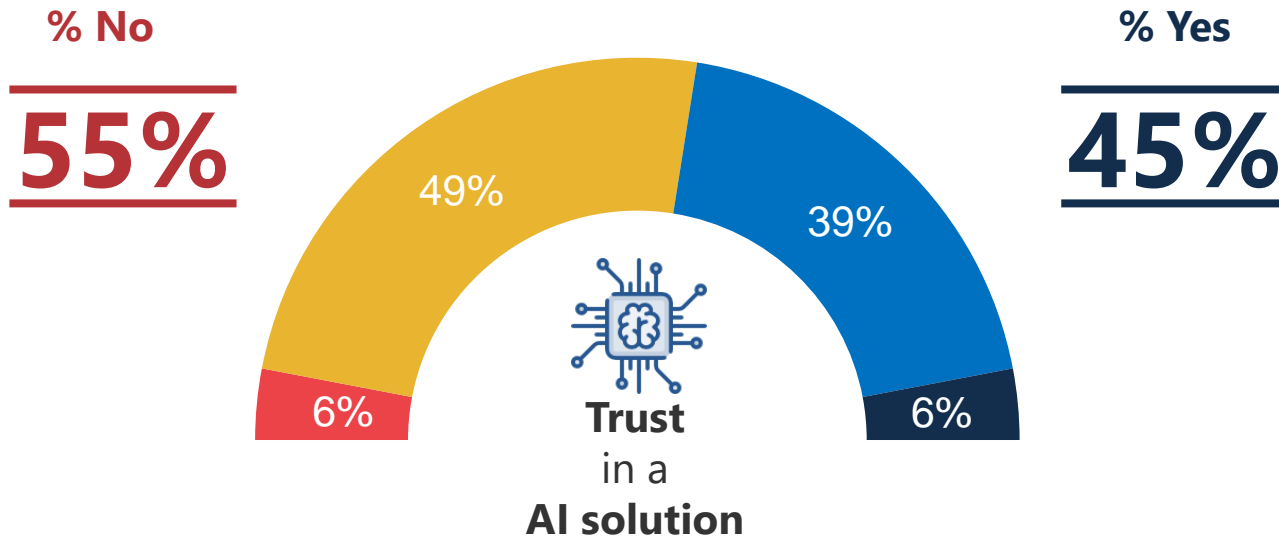


*For 44%, it is not planned.*

# ... even if human intervention remains necessary for CISOs

Q41. Would you be willing to let an AI solution make security decisions regarding detection and/or remediation?  
Base: total sample (174)

■ No, AI will never decide instead of human experts   ■ No, not mature enough yet   ■ Yes, probably   ■ Yes, definitely



# Despite all these solutions, confidence in the ability to cope with cyber risks is decreasing

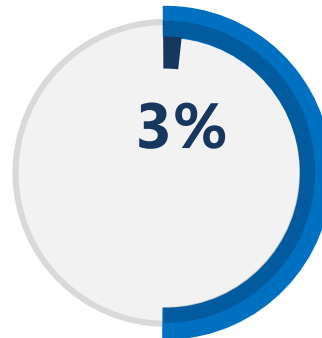
Q26. For the future, would you say that you are very confident, somewhat confident, somewhat worried or very worried about...?

Base: total sample (174)

51% ↘<sup>-12</sup>

Your company's **ability to cope** with cybersecurity risks

- Very confident
- Very + Somewhat confident



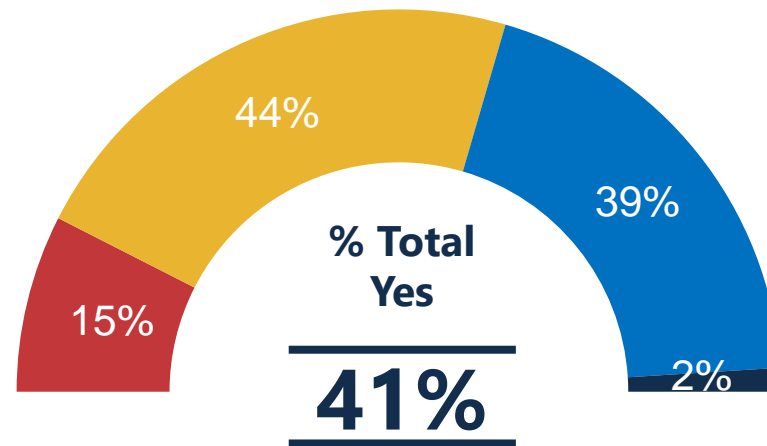
# And less than half of the companies feels capable of handling a massive cyberattack

Q38. In your opinion, is your company prepared to handle a major cyberattack?

Base: total sample (174)

« Is your company prepared to handle a massive cyberattack? »

■ No, not at all ■ No, probably not ■ Yes, probably ■ Yes, definitely



# In this context, more and more companies subscribe to cyber-insurance

Q9. Does your company have a cyber-insurance?

Base: total sample (174)

50%  +10



10%



18%



# Cyber-resilience becomes an issue for two-thirds of companies, which set up a program

Q39. Does your company have a cyber resilience program in place?

Base: total sample (174)

**79%** have a cyber resilience program in place or plan to do so

**12%**

**already have a program of Cyber resilience in place**

**33%**

The implementation of the program is **in progress**

**34%**

**plan to implement a cyber-resilience program**

*For 21%, it is not planned.*

---

## **4. THREE CHALLENGES FOR THE FUTURE**

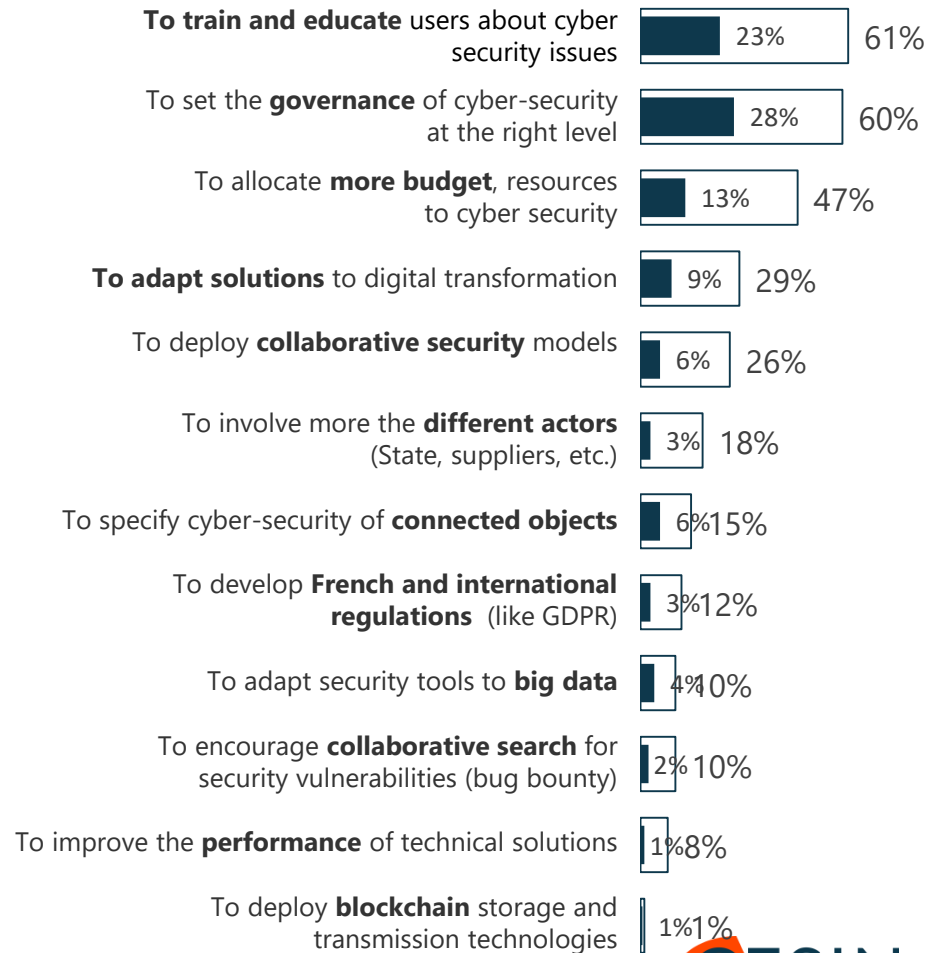
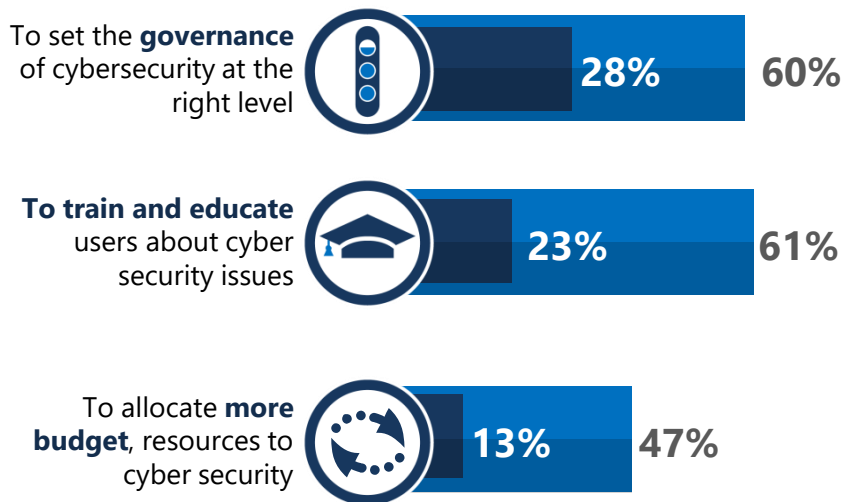
- ▶ AWARENESS**
- ▶ GOVERNANCE**
- ▶ RESOURCES**

# The challenge for the future remains more human than technical

Q28. Among the following issues, what do you think are the 3 challenges for tomorrow, for the future of corporate cybersecurity?  
 Base: total sample (174)

## TOP 3 challenges

■ First  
 ■ Overall (mentioned in 1<sup>st</sup>, second or third)



---

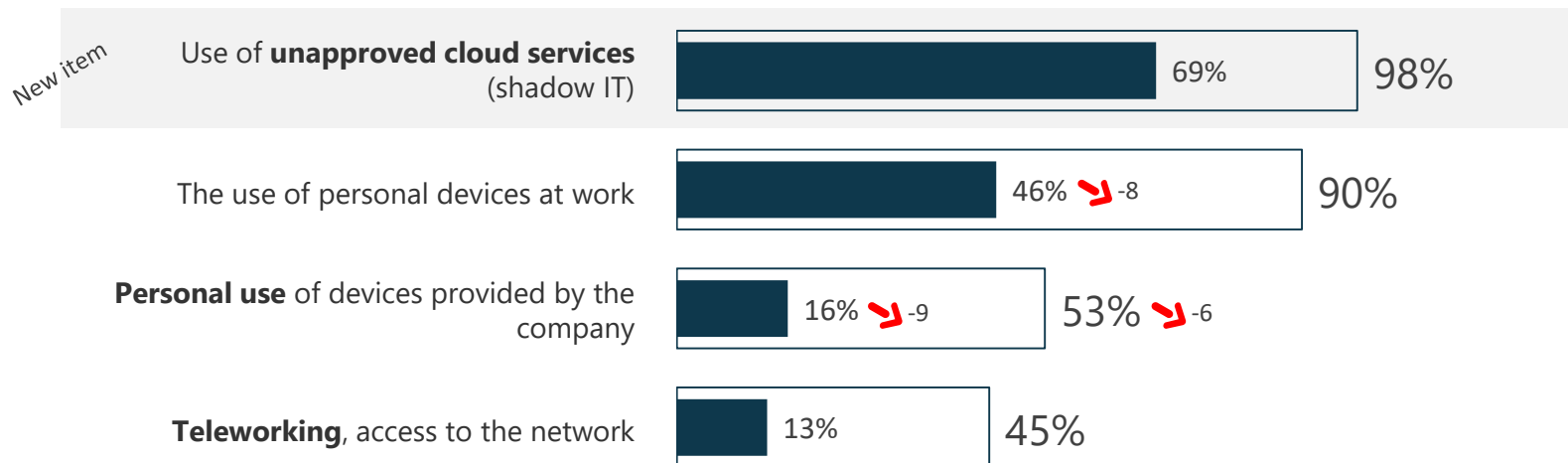
## 4. THREE CHALLENGES FOR THE FUTURE

- ▶ **AWARENESS**
- ▶ GOVERNANCE
- ▶ RESOURCES

# Digital uses by employees represent a real risk, especially shadow IT

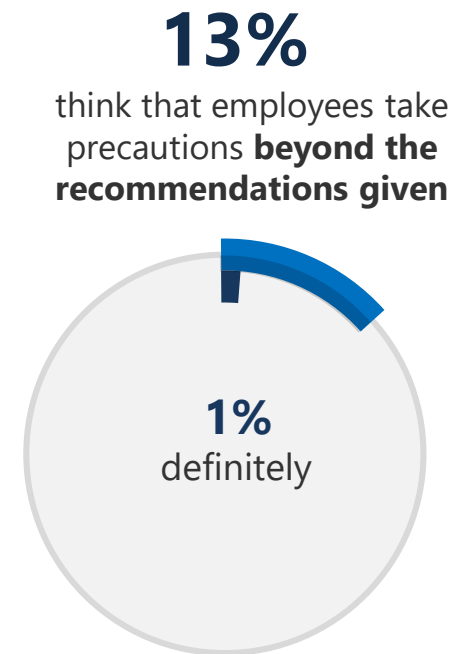
Q24. In your opinion, do the following uses of digital by employees represent a risk for corporate cybersecurity?  
 Base: total sample (174)

Yes, definitely     
  Total Yes  
 (definitely + probably)



# And even if they are aware of cybersecurity, employees are not very involved, according to CISOs

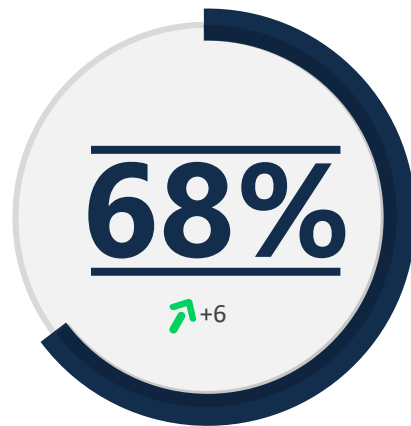
Q15. With regard to cybersecurity, do you think that the employees of your company ...?  
Base: total sample (174)



# In this context, more and more companies set up procedures to monitor the implementation of recommendations

Q15BIS. Have you set up procedures to monitor the implementation of recommendations by employees in specific situations, such as audits, fake phishing campaigns, internal controls, etc.?

Base: total sample (174)



have **set up procedures to monitor** the implementation of recommendations by employees

---

## 4. THREE CHALLENGES FOR THE FUTURE

- ▶ AWARENESS
- ▶ **GOVERNANCE**
- ▶ RESOURCES

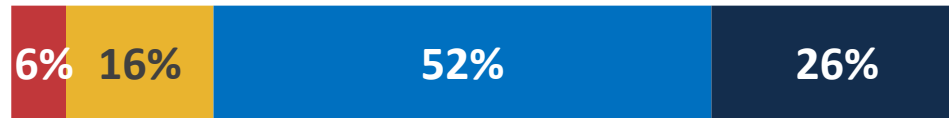
# GDPR compliance has raised awareness of data protection issues

Q32. Regarding compliance with GDPR, would you say that it...?

Base: total sample (174)

■ Not at all ■ Probably not ■ Probably ■ Definitely

Helped raise the **awareness** of the Executive Committee of your company to the **challenges of data protection**



% Total Yes

**78%**

Helped to really **strengthen the protection of personal data** (clients, companies, etc.)



**65%**

Has **changed the governance of the company** in terms of protection of information



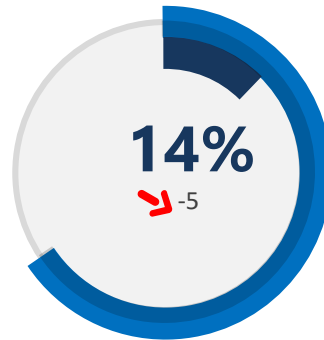
**59%**

# However, the CISOs show little confidence in the ability of their Executive Committee to take into account the issues of cyber-security

Q26. For the future, would you say that you are very confident, somewhat confident, somewhat worried or very worried about...? *Base: total sample (174)*

**66%** ↘<sup>-5</sup>

**Taking into account the issues of cyber security** within the Executive Committee



- Very confident
- Very + Somewhat confident

---

## 4. THREE CHALLENGES FOR THE FUTURE

- ▶ AWARENESS
- ▶ GOVERNANCE
- ▶ RESOURCES

# Most companies plan to invest more in cybersecurity, through solution acquisitions and budget increases

Q11BIS. In the next 12 months, does your company plan to...?

Base: total sample (174)

to acquire **new technical solutions** for protection against cyber risks



to increase the budgets allocated to the protection against cyber-risks

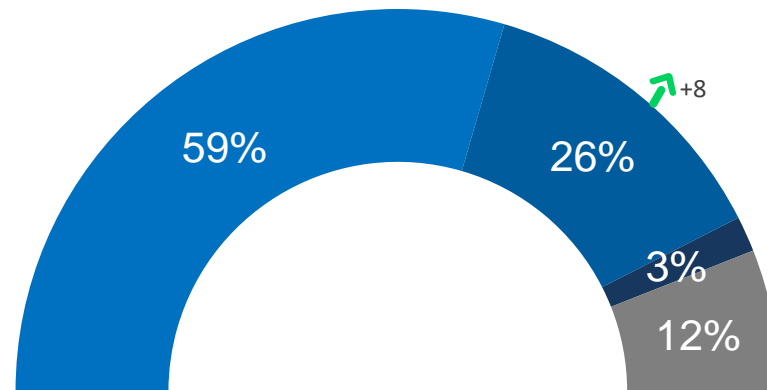


# Investments are slightly more relevant within the IT budget devoted to security, even if it remains low

Q37. In your company, how much of the IT budget is spent on security?

Base: total sample (174)

■ Less than 5% ■ Between 5 and 10% ■ More than 10% ■ Don't know



# On the other hand, the rate of companies planning to increase the workforce is declining

Q11BIS. In the next 12 months, does your company plan to...?

Base: total sample (174)

**increase the workforce**  
dedicated to the protection  
against cyber-risks



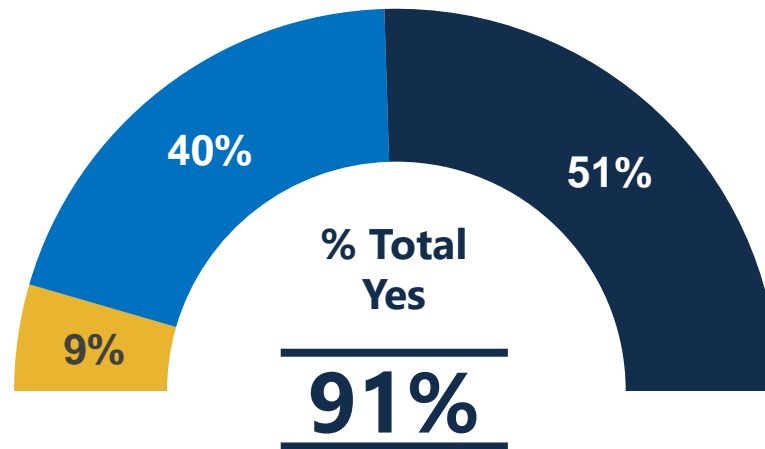
# A situation that echoes a lack of qualified profiles observed by most CISOs

Q43. Finally, here are some questions about recruitment in IT security. Do you see a shortage of IT security profiles leading to recruitment difficulties?

Base: total sample (174)

« There is a **shortage of IT security profiles** on the market, leading to recruitment difficulties »

■ Not at all ■ Not really ■ Yes, somewhat ■ Yes, definitely



# A shortage that primarily affects the business of risk management

Q44. Among the following IT security job, which one is the most affected by a shortage of profiles?

Base: total sample (174)



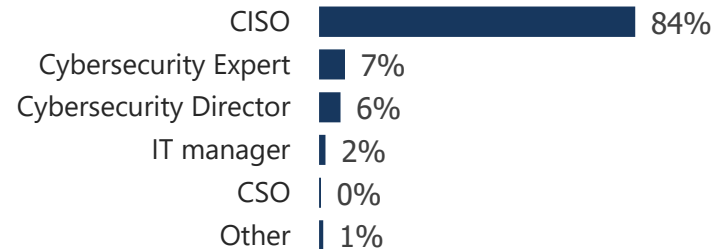
---

# APPENDICES

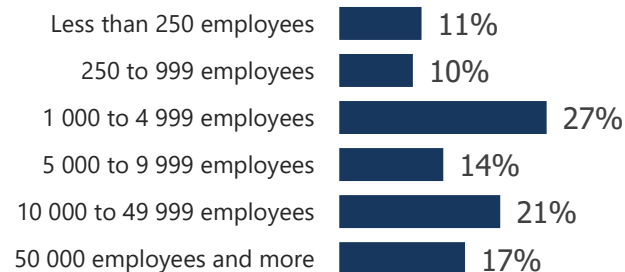
# Respondent profile

174  
members of  
**CESIN**  
participated in  
this survey

## Profession of respondent:



## Number of employees in the company:



## Industry:

