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

Baromètre de la cyber-sécurité des entreprises

Janvier 2016

À : Alain Bouillé
De : Emmanuel Kahn, Agathe Martini
OpinionWay, 15 place de la République, 75003 Paris

opinionway CESIN

Sommaire

CONTEXTE ET OBJECTIFS

Contexte et objectifs

- Le **Club des Experts de la Sécurité de l'Information et du Numérique** (CESIN) offre un lieu d'échanges aux **experts de la sécurité et du numérique** au sein de grandes entreprises.
- Le CESIN a souhaité lancer auprès de ses membres **une grande enquête** qui a vocation à être renouvelée chaque année.
- L'objectif de cette enquête et de connaître
  - la **perception de la cyber-sécurité et de ses enjeux** au sein des entreprises membres du CESIN
  - **la réalité** concrète de la sécurité informatique des grandes entreprises.

MÉTHODOLOGIE

Méthodologie

Méthodologie

Étude quantitative réalisée auprès de **125 membres du CESIN**, à partir du fichier membre du CESIN (235 contacts)

Mode d'interrogation

L'échantillon a été interrogé par Internet sous système **CAWI** (*Computer Assisted Web Interview*)

Dates de terrain

Du **8** au **22 décembre 2015**

Certification

OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la norme **ISO 20252**

Toute publication totale ou partielle doit impérativement utiliser la mention complète suivante :

« Sondage OpinionWay pour le CESIN »

et aucune reprise de l'enquête ne pourra être dissociée de cet intitulé.

MESSAGES CLÉS

Messages clés (1/2)

Les enseignements à retenir

1. Le **digital** et la **SSI** sont des **enjeux importants** et **stratégiques** dans la plupart des entreprises. À la croisée de ces enjeux, **la gestion des cyber-risques est souvent confiée à la DSI** ou à la direction risques lorsqu'elle existe.
2. **Toutes les entreprises sont jugées exposées** aux cyber-risques et font effectivement l'objet d'attaques.
3. En matière d'attaques, les entreprises se sentent particulièrement exposées au **vol ou à la fuite d'information ou de données et aux attaques virales**. Mais dans les faits, **l'attaque la plus fréquente est la demande de rançon.** Concernant les autres risques, **la dépendance humaine et les vulnérabilités résiduelles** sont les plus préoccupantes et celles qui affectent le plus souvent les entreprises en matière de sécurité.
4. Les **nouveaux usages du numérique au travail** posent de nouveaux défis en matière de cyber-sécurité. Le **Cloud** en particulier, en plus de nécessiter des outils spécifiques, inquiète pour des raisons de **confidentialité des données**. Le **BYOD** et les **objets connectés** sont aussi des nouveaux enjeux de la cyber-sécurité.

Messages clés (2/2)

Les enseignements à retenir

5. Les entreprises ont généralement mis en place de nombreuses **solutions techniques** pour assurer leur cyber-sécurité, en structurant leurs dispositif le plus souvent selon une **typologie de sensibilité des données**. Elles optent aussi quasiment toutes pour une **limitation des usages** des salariés – incluant parfois du filtrage web – qui ne se révèle efficace qu'à la marge. D'autant que **les salariés sont jugés trop peu sensibilisés aux cyber-risques**, et **peu enclins à respecter scrupuleusement les recommandations**.

6. Pour autant, les **moyens alloués à la cyber-sécurité semblent peu satisfaisants actuellement**, en particulier les **moyens humains.** Nombre d'entreprises envisagent d'ailleurs **d'augmenter les ressources techniques, financières ou humaines** dédiées à la cyber-sécurité, et elles sont également nombreuses à envisager de **souscrire une cyber-assurance**.

7. Les entreprises estiment que les **outils disponibles actuellement sur le marché sont déjà peu adaptés** à la situation en matière d'usages du numérique comme en matière d'attaques. Même en prenant la cyber-sécurité au sérieux, l'inquiétude demeure quant à la capacité concrète à faire face à l'augmentation pressentie des attaques sur le court et moyen terme.

8. Les enjeux prioritaires à leurs yeux **seront humains plus que techniques** : **donner toute son importance à la cyber-sécurité dans l'entreprise** (en y allouant suffisamment de ressources et en lui donnant sa juste place dans la gouvernance), et à **travailler autour des usages** (sensibiliser les usagers et s'adapter à leurs pratiques).

RÉSULTATS

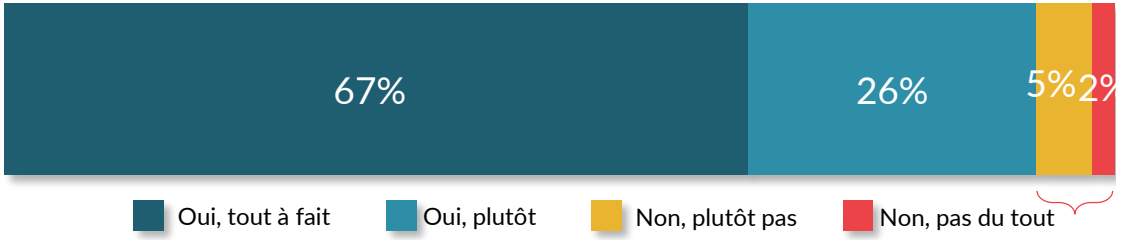
1. PLACE DE LA CYBER-SÉCURITÉ DANS LES ENTREPRISES

Le digital et la SSI, des enjeux pris au sérieux dans l'entreprise

Q1. Dans votre entreprise, diriez-vous que le digital est un enjeu stratégique ?

125 entreprises

93% considèrent que le digital est **un enjeu stratégique dans leur entreprise**



7%

Q2. La sécurité des systèmes d'information et des données est-elle considérée par la direction de votre entreprise comme…

88% considérée que la SSI est **importante** pour la direction de l'entreprise

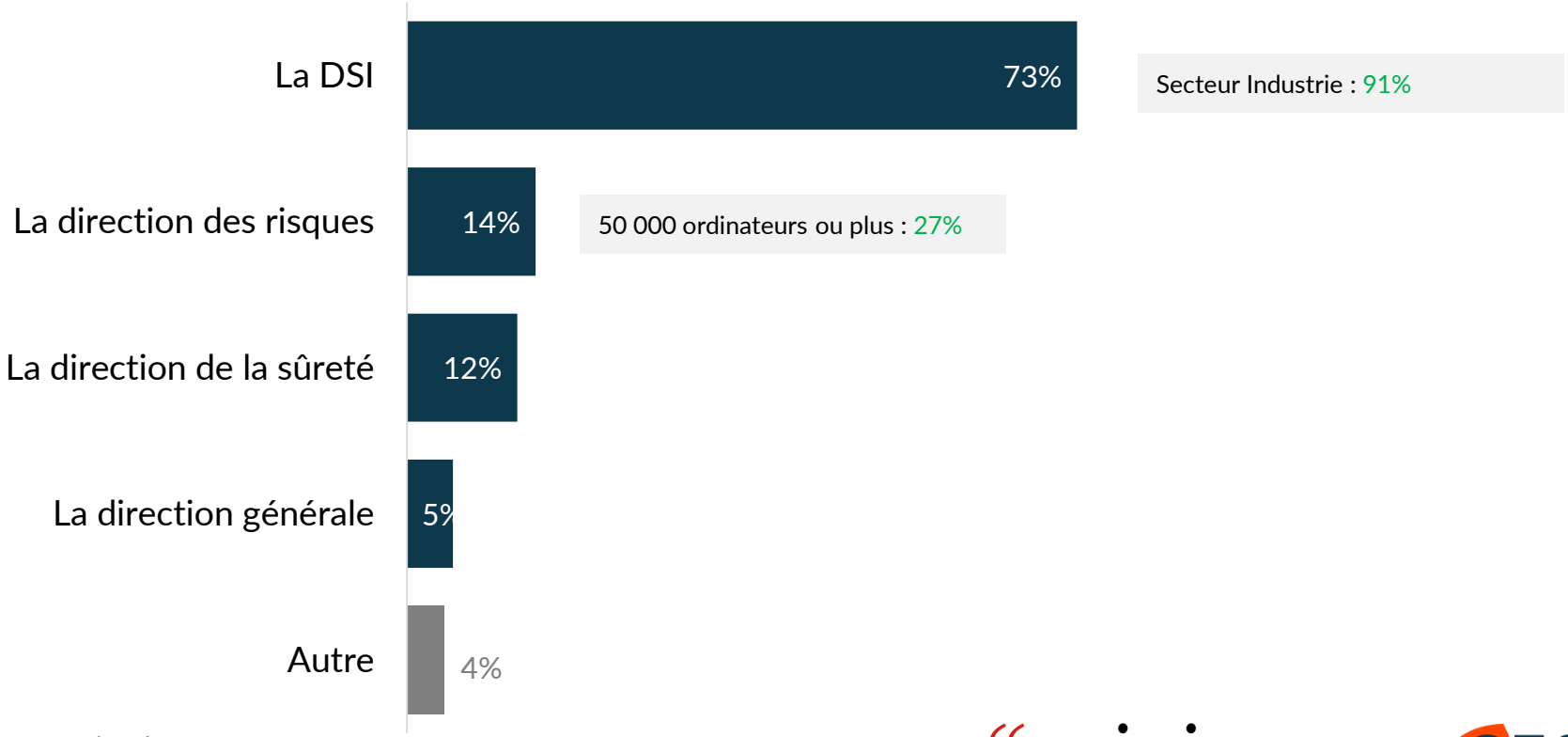
12%

"opinionway CESIN

La gestion des cyber-risques est souvent confiée à la DSI, voire à la direction des risques quand elle existe

Q3. Dans votre entreprise, quelle est l'entité en charge du pilotage de la protection contre les cyber-risques ?

125 entreprises

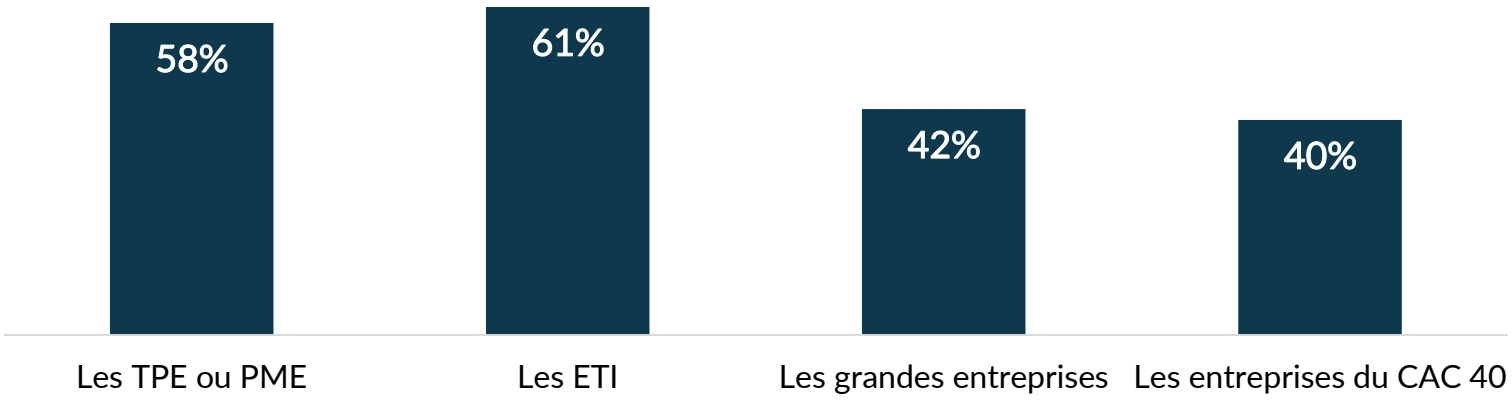


opinionway CESIN

2. RÉALITÉ DES CYBER-ATTAQUES AUXQUELLES SONT EXPOSÉES LES ENTREPRISES

Toutes les entreprises sont jugées exposées aux cyber-risques, même si les plus grandes sont considérées mieux protégées

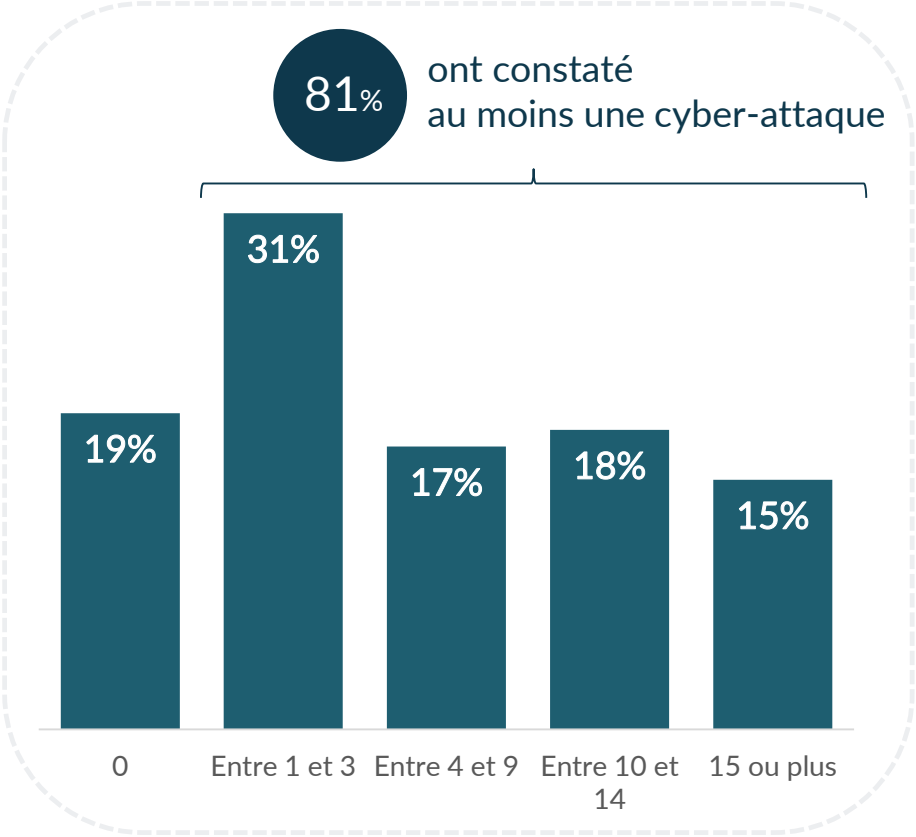
Q27. Selon vous, les entreprises les plus exposées aux cyber-risques sont… (plusieurs réponses possibles)



Dans les faits, un grand nombre d'entreprises a fait l'objet de cyber-attaques au cours de l'année

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?

125 entreprises



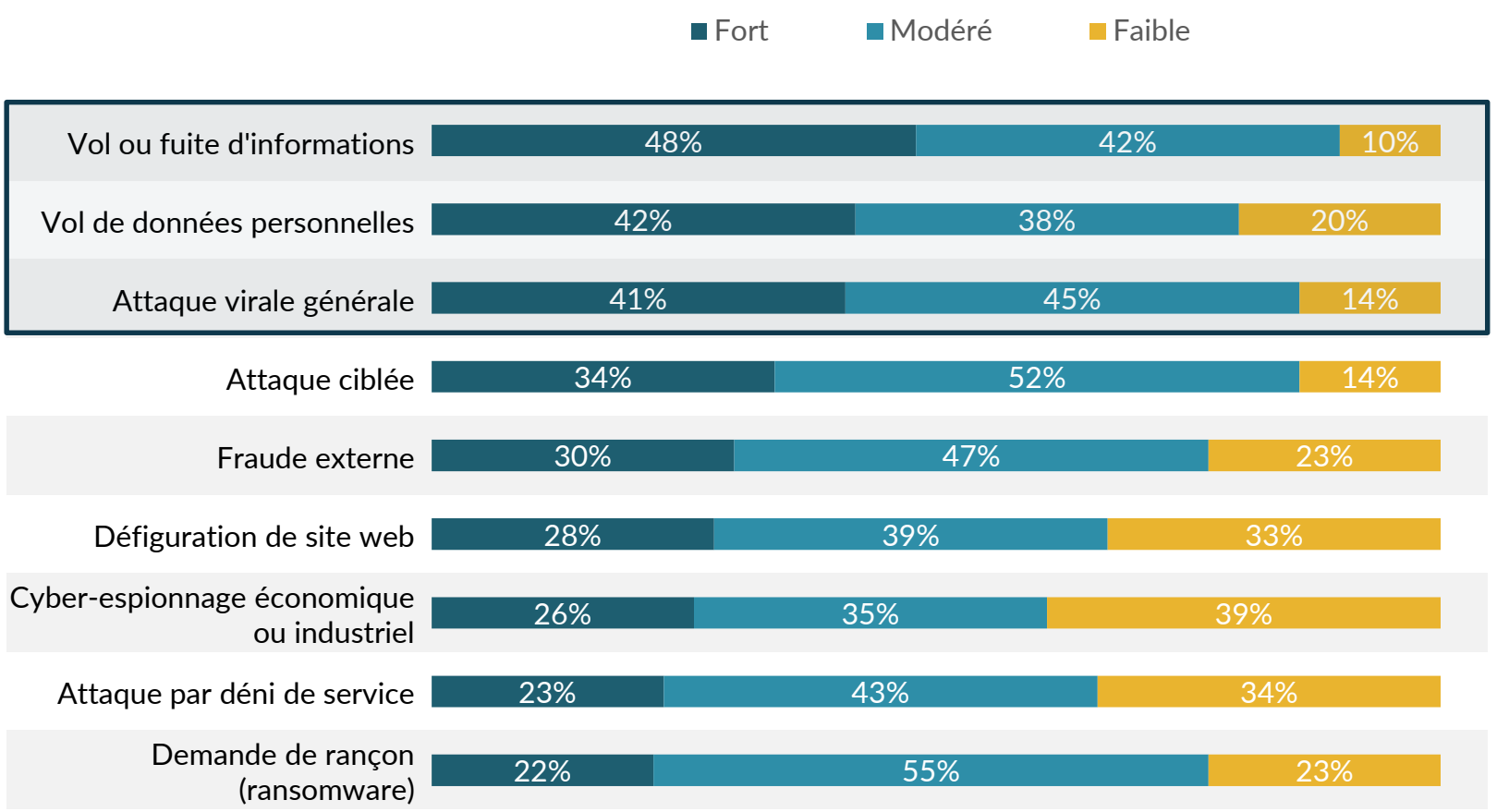
Nombre moyen d'attaques : **13**

Nombre d'ordinateurs	Base	Nb moyen
Moins de 999 ordinateurs	22*	2,2
Entre 1 000 et 9 999 ordinateurs	51*	7,3
Entre 10 000 et 49 999 ordinateurs	26*	14,3
50 000 ordinateurs ou plus	26*	32,1

* Attention, base faible

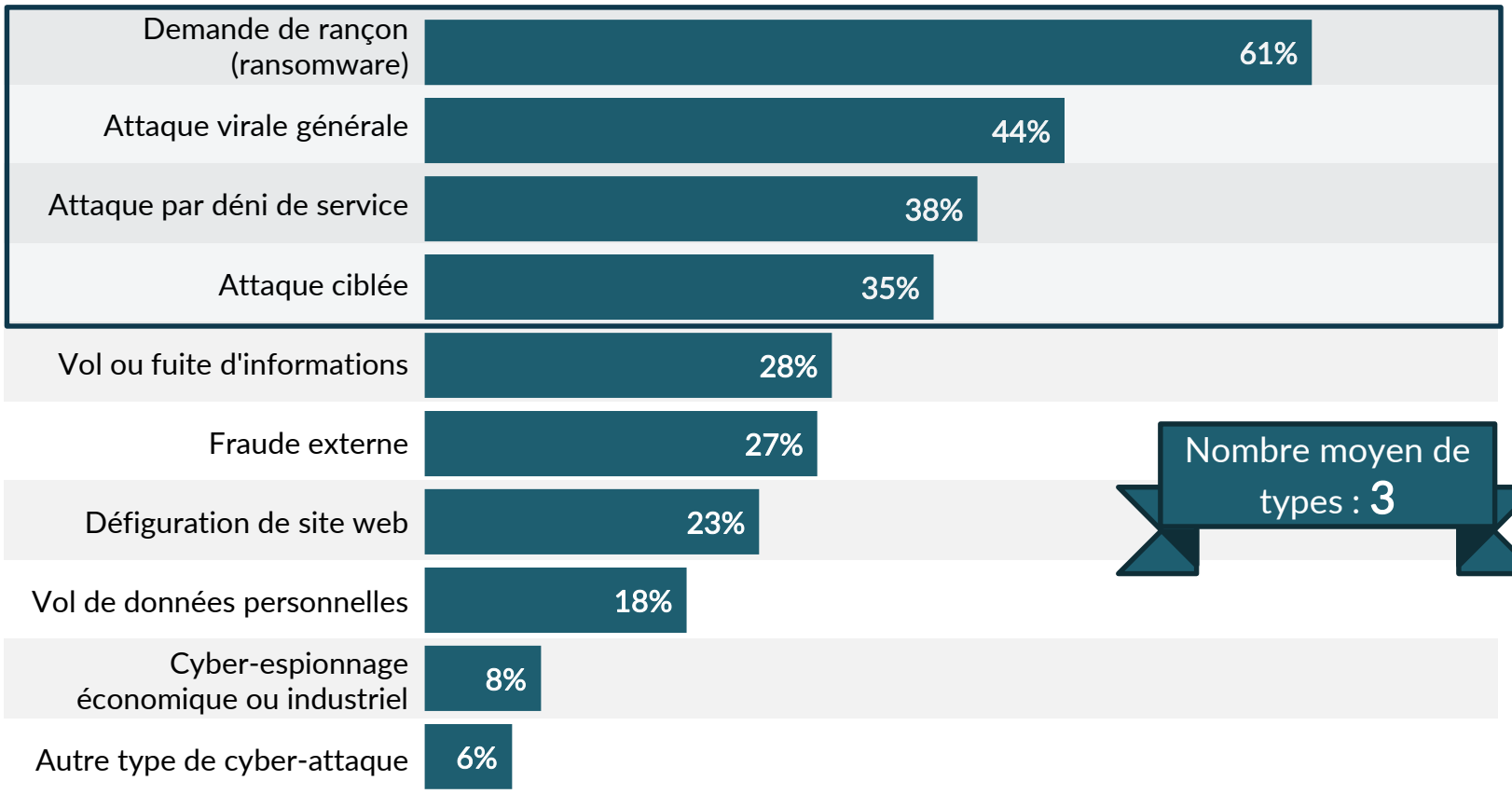
Les attaques qui préoccupent le plus grand nombre d'entreprises sont le vol d'infos ou de données et les attaques virales

Q4. Quel est le niveau d'exposition de votre entreprise aux cyber-risques suivants ?



Dans les faits, les cyber attaques constatées sont surtout le ransomware, les attaques virales, de déni de service et les attaques ciblées.

Q6. Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?

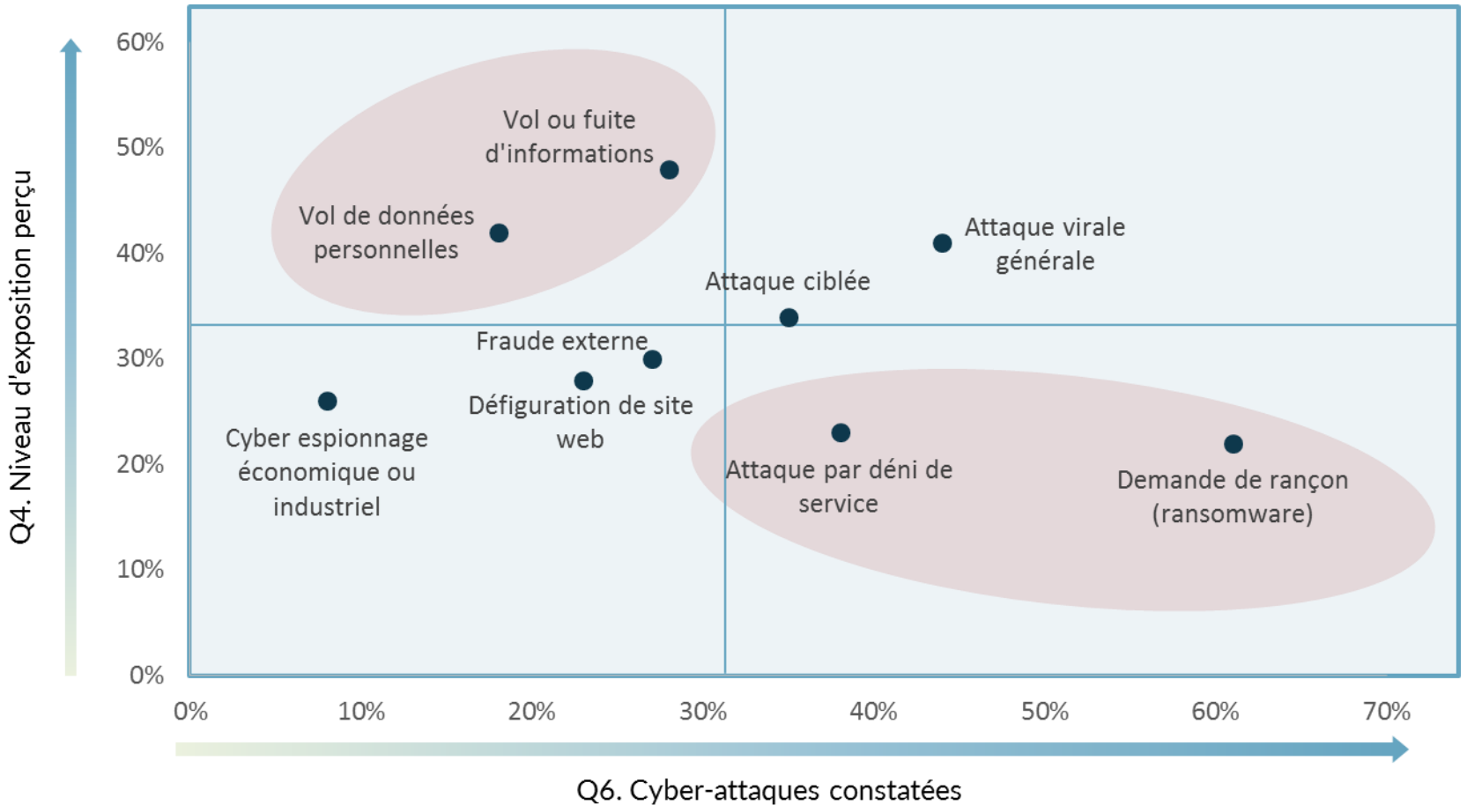


102 entreprises ayant constaté au moins une cyber-attaque au cours des 12 derniers mois

Nombre moyen de types : 3

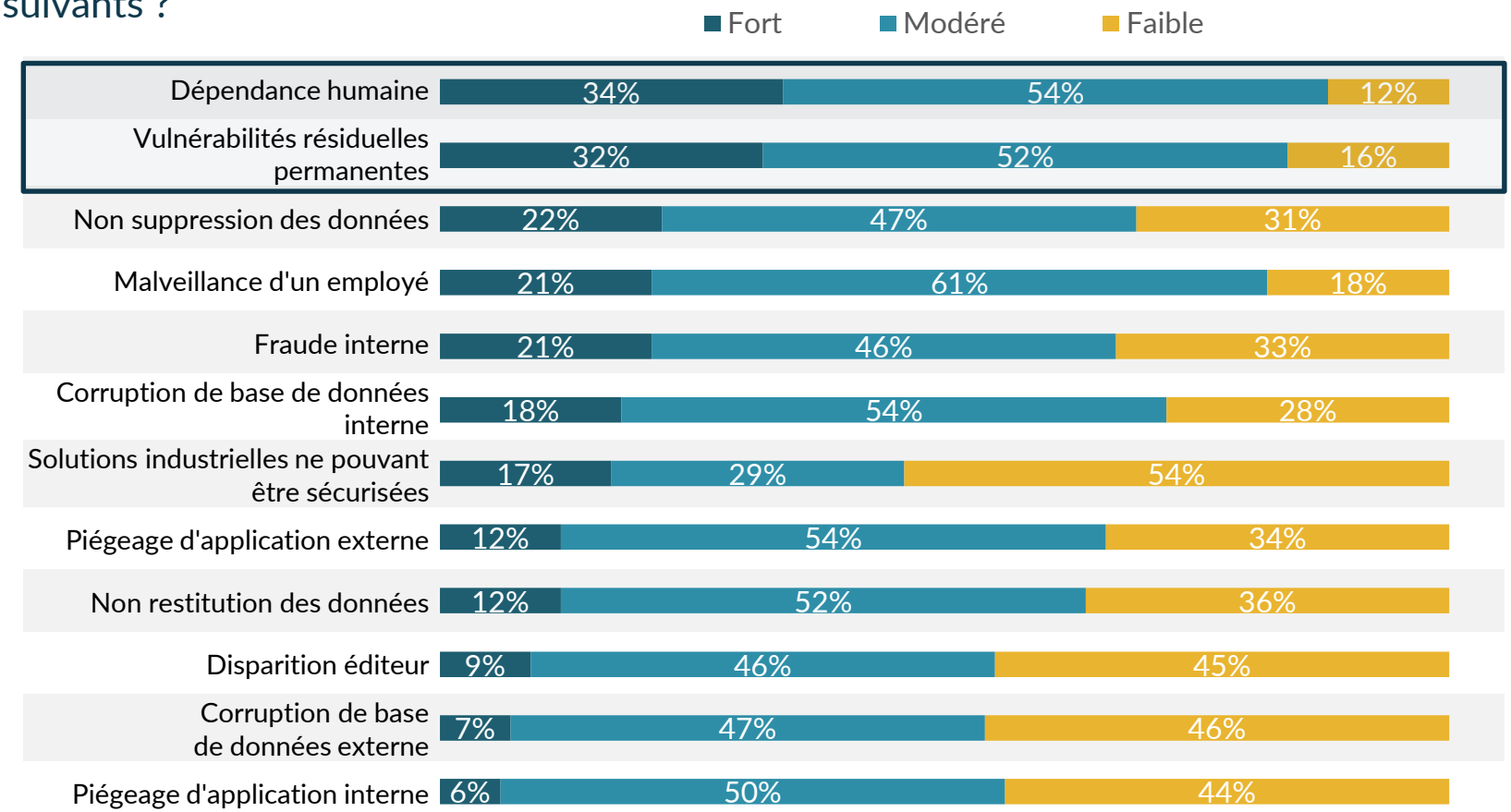
opinionway CESIN

Un sentiment d'exposition pas toujours directement lié aux attaques constatées



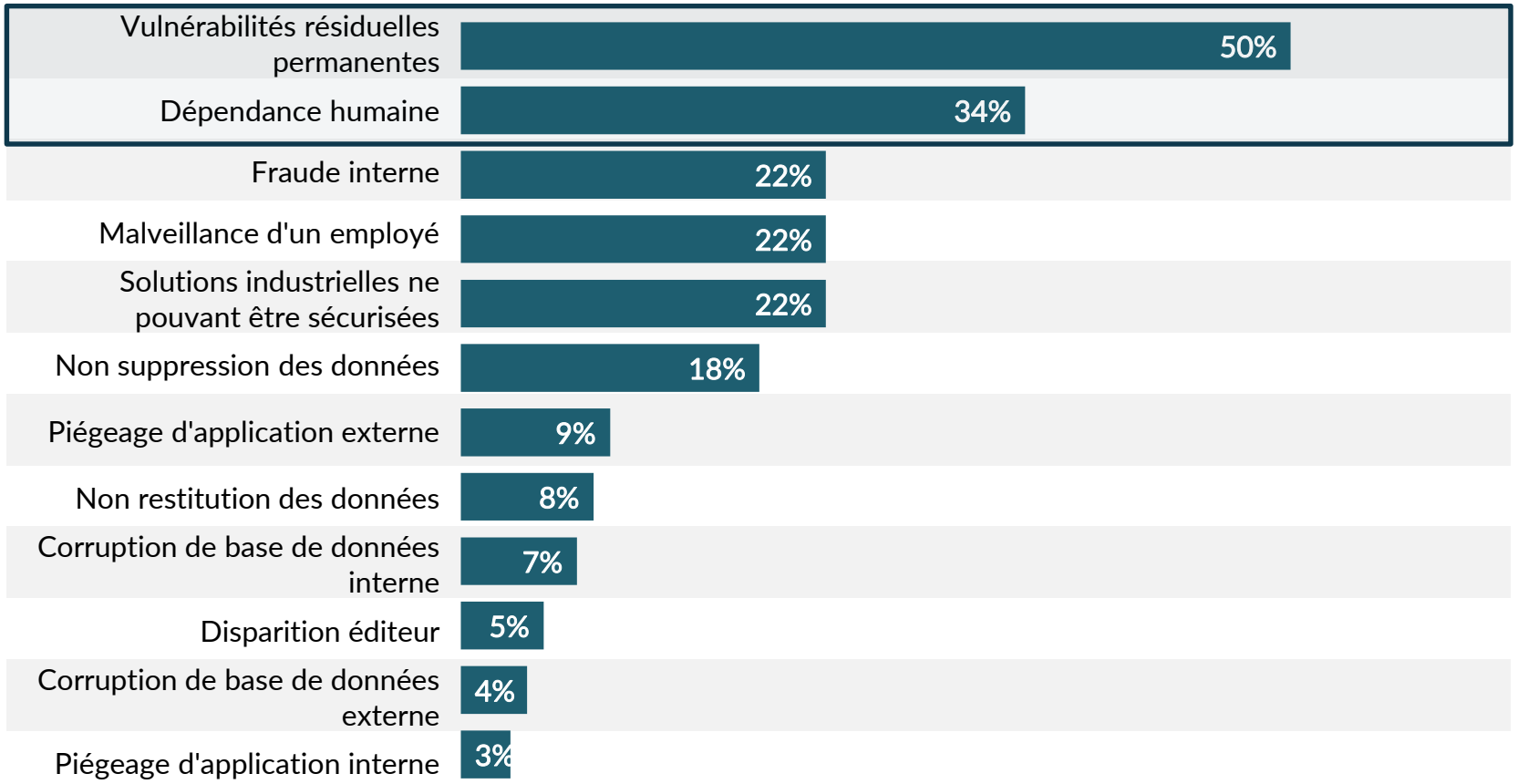
Les risques qui préoccupent le plus grand nombre d'entreprises sont la dépendance humaine et les vulnérabilités résiduelles permanentes

Q4bis. Quel est le niveau d'exposition de votre entreprise aux autres risques suivants ?

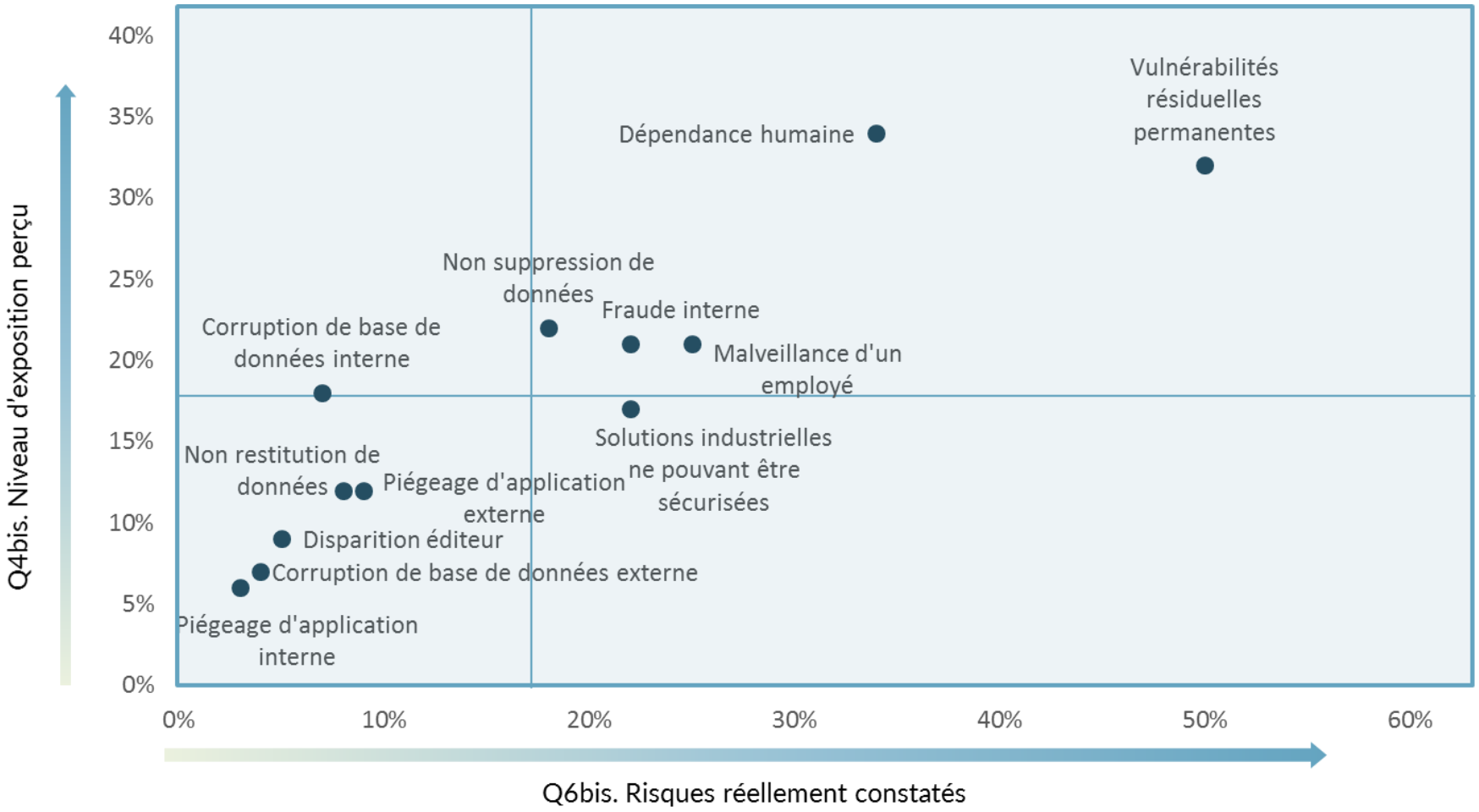


Les risques auxquels font réellement face le plus d'entreprises sont les vulnérabilités résiduelles et la dépendance humaine

Q6bis. Parmi les éléments suivants liés à la cyber-sécurité, quels sont ceux auxquels votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?



Une perception d'exposition aux risques en phase avec la réalité



3. RISQUES LIÉS AUX NOUVEAUX USAGES DU NUMÉRIQUE

Un recours généralisé au Cloud, en particulier à des Clouds publics ou hybrides

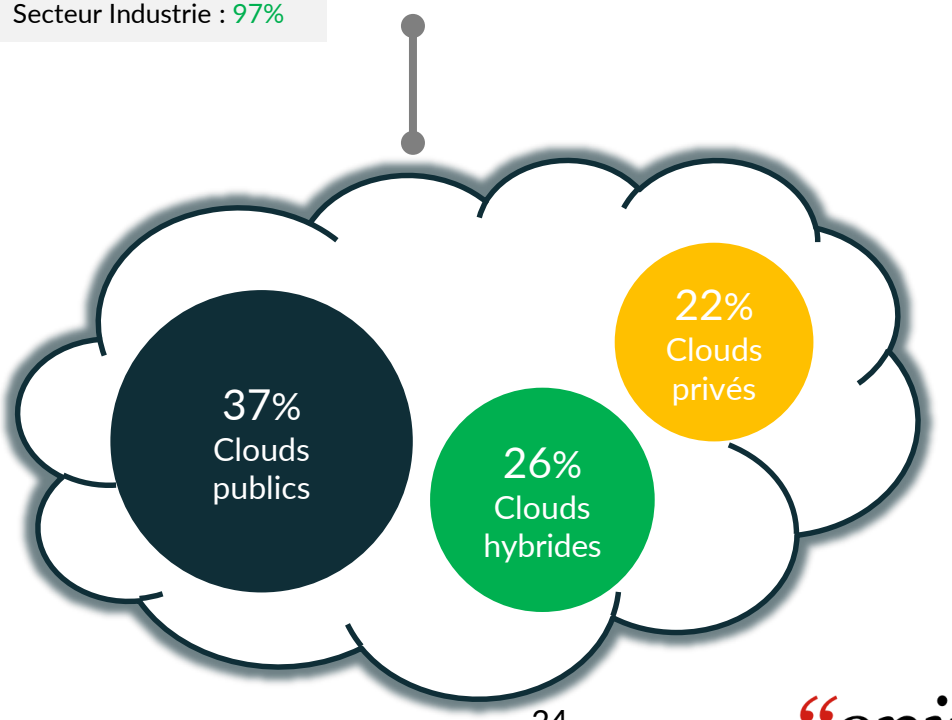
Q20. Certaines données de votre entreprise sont-elles stockées dans un Cloud ?

125 entreprises

85% stockent des données dans un Cloud

Secteur Industrie : 97%

15% ne stockent aucune donnée dans un Cloud



opinionway CESIN

Un recours au Cloud qui entraîne des conséquences en termes d'outils de sécurisation

Q23. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?

125 entreprises

93%

pensent que le Cloud
requiert des outils ou dispositifs spécifiques

opinionway CESIN

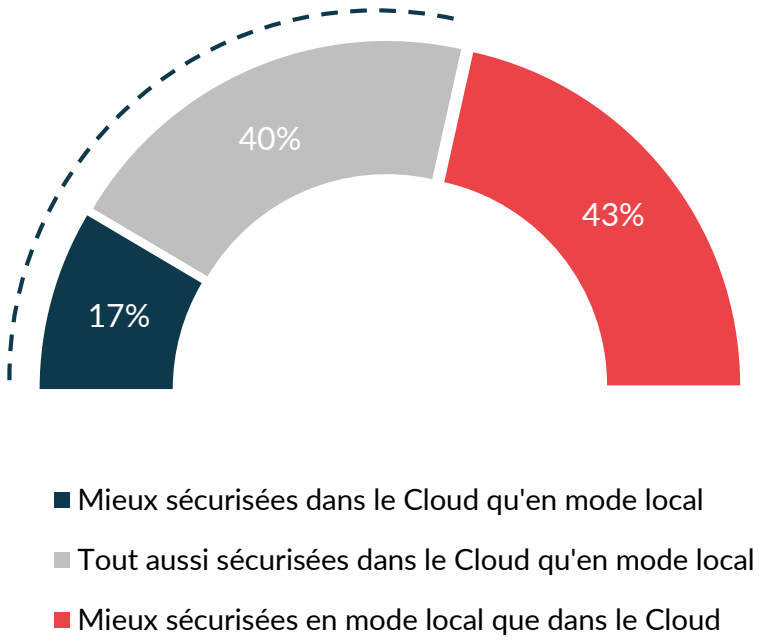
La sécurisation des données en Cloud fait débat

Q21. Pensez-vous que les données de votre entreprise sont / seraient… ?

125 entreprises

57%

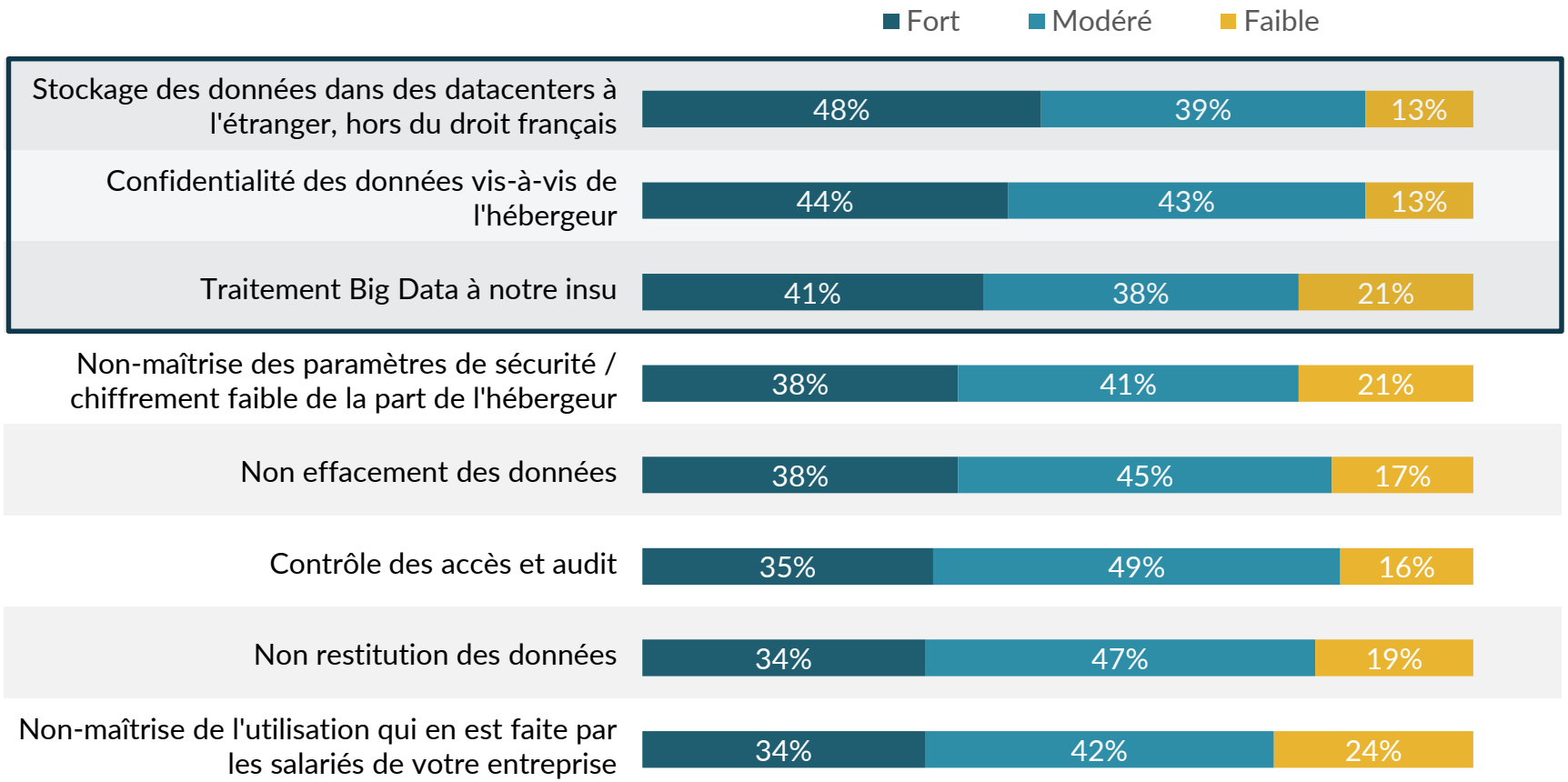
des entreprises pensent le Cloud est autant ou plus sécurisé



opinionway CESIN

Les principaux risques perçus comme associés au Cloud sont l'hébergement hors droit français, la confidentialité vis-à-vis de l'éditeur et la réutilisation des données

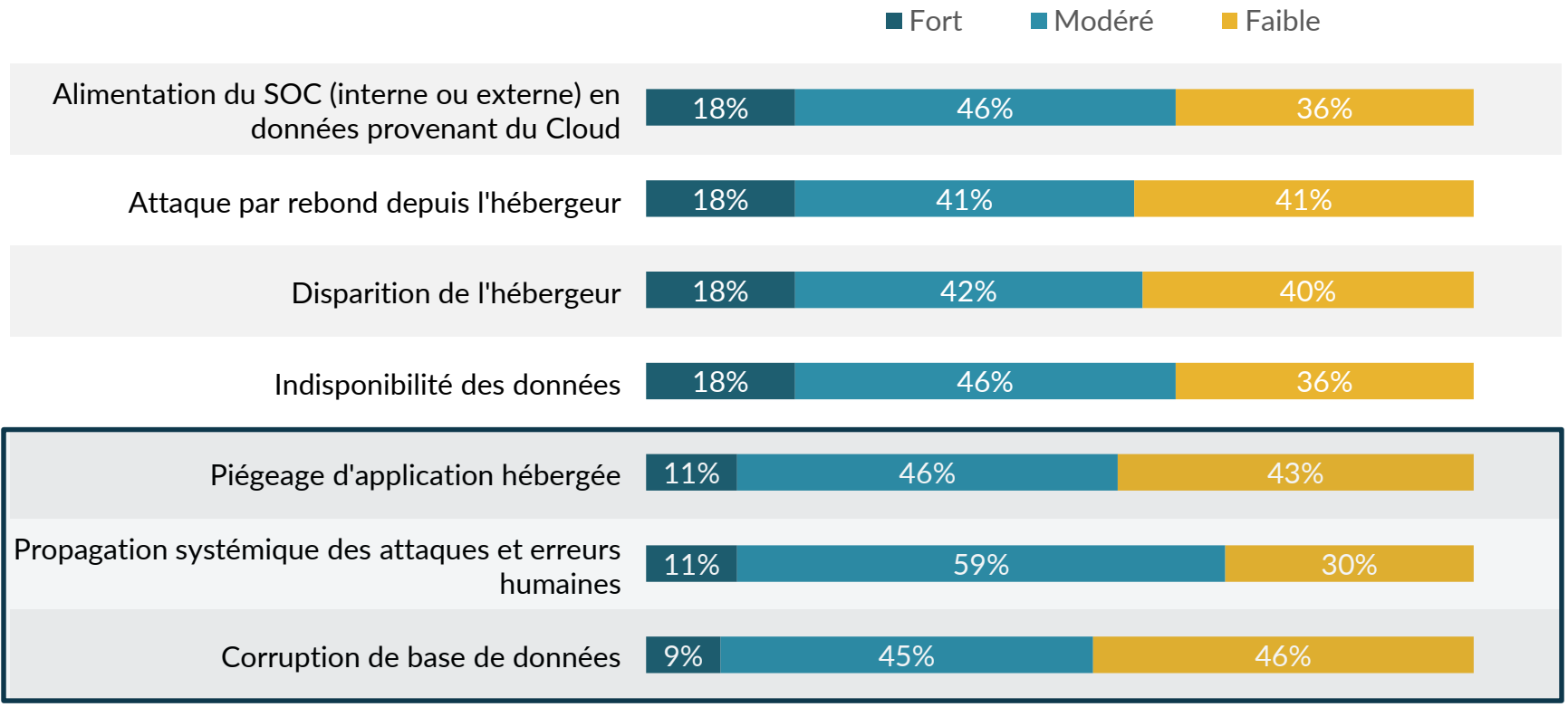
Q22. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ?



Certains risques sont peu associées au Cloud, comme le piégeage d'application, la corruption de BDD, l'indisponibilité des données

Q22. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ?

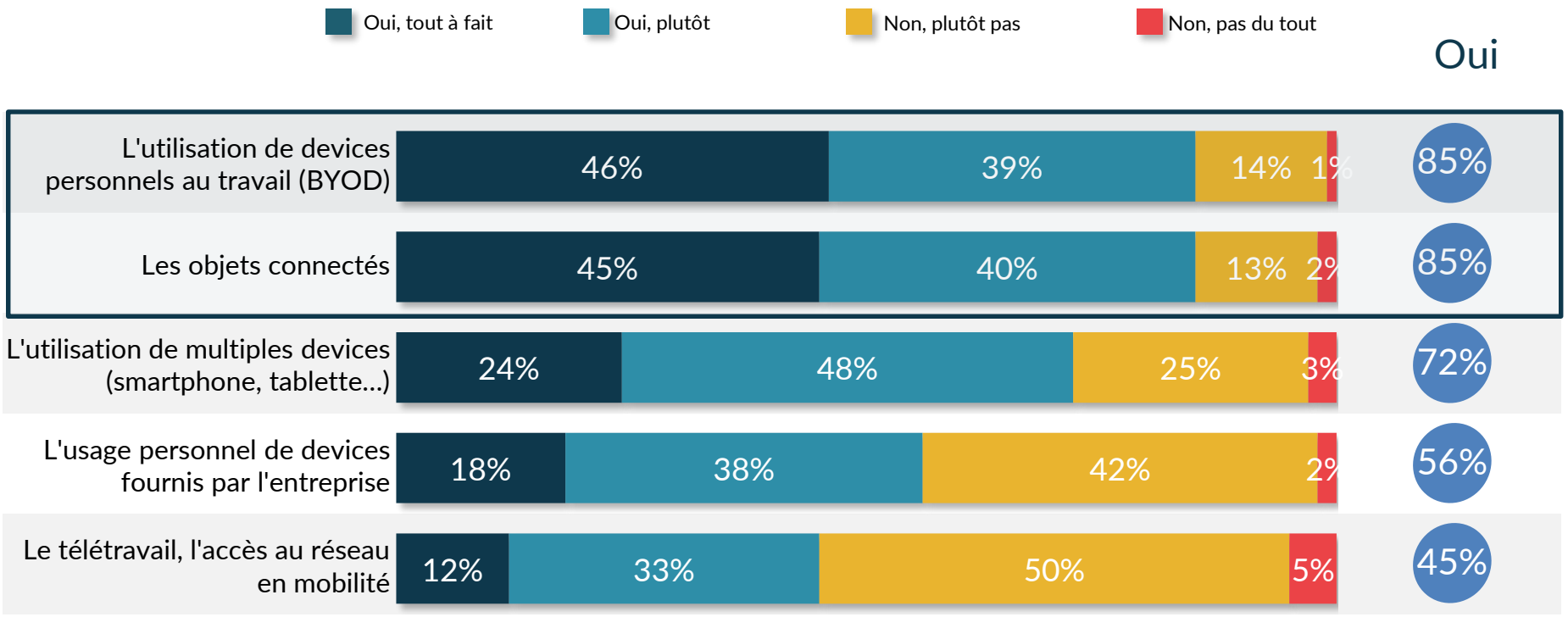
125 entreprises



"opinionway CESIN

BYOD et objets connectés, des nouveaux usages qui présentent des risques

Q24. À vos yeux, les nouveaux usages suivants du numérique au travail représentent-ils un risque pour la cyber-sécurité des entreprises ?



Des entreprises qui estiment leur protection peu adaptée aux nouveaux usages du numérique au travail

Q25. Pensez-vous que les solutions de protection actuelles de votre entreprise sont adaptées à l'évolution des nouveaux usages du numérique au travail ?

125 entreprises

58% considèrent que les solutions de protection actuelles ne sont PAS **adaptées à l'évolution des nouveaux usages** du numérique au travail

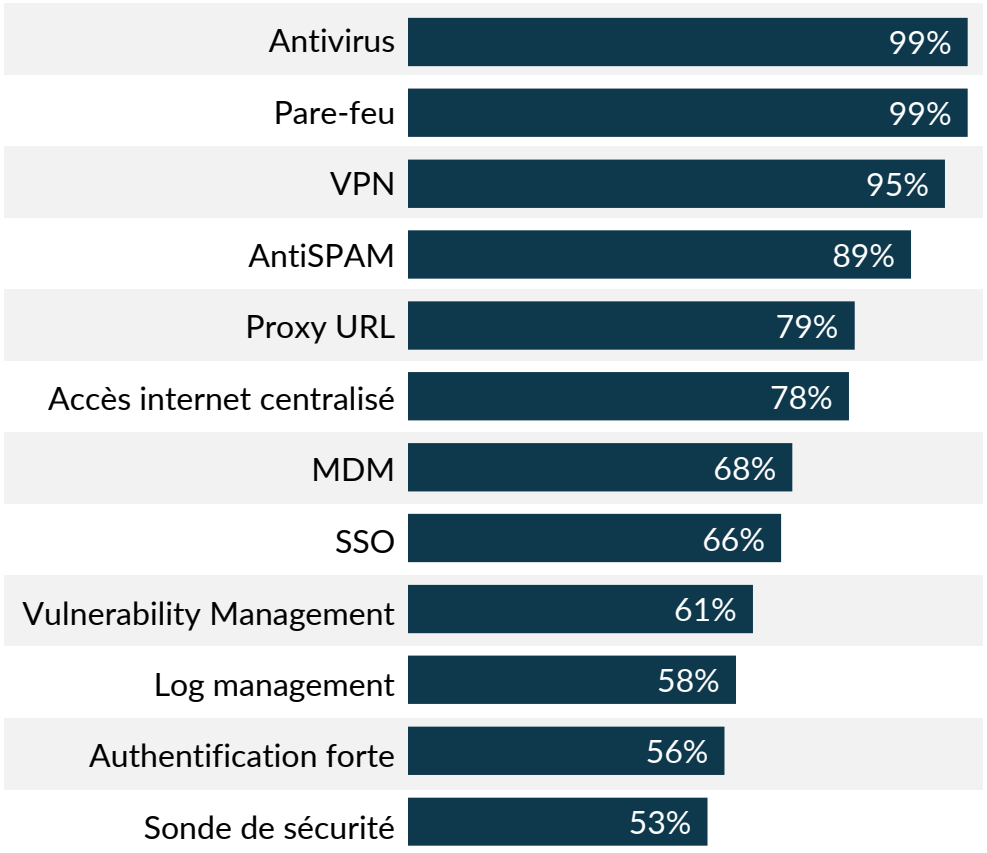
Oui, tout à fait | Oui, plutôt | Non, plutôt pas | Non, pas du tout

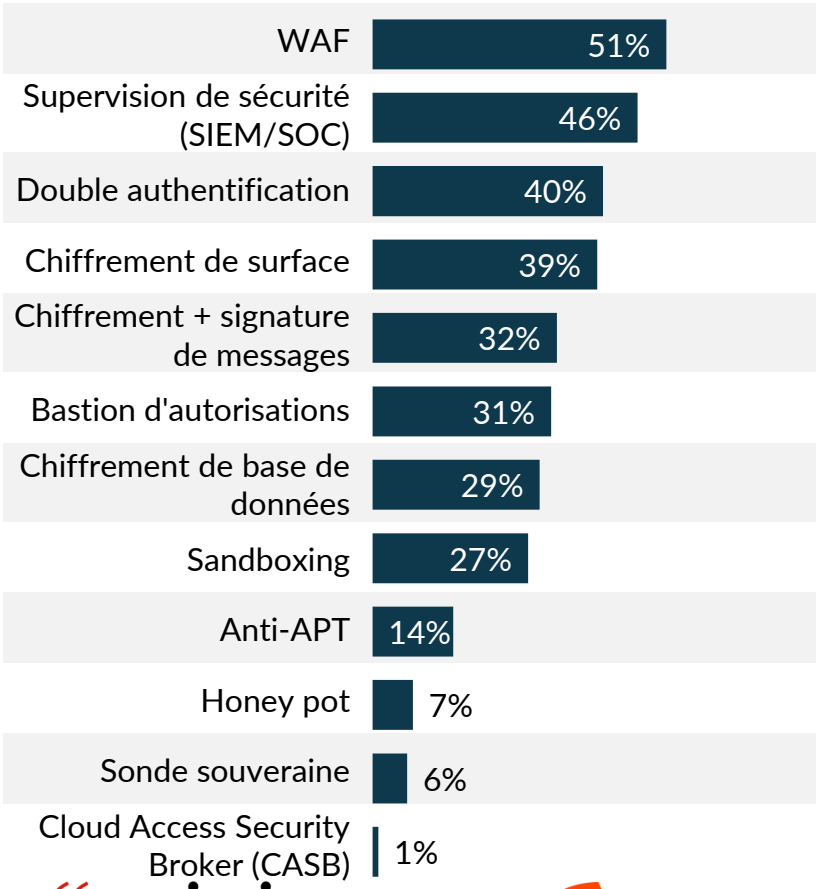
4. MOYENS MIS EN PLACE POUR LUTTER CONTRE LES CYBER-RISQUES

Des solutions de sécurité plus ou moins répandues selon les types

Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise ?

125 entreprises



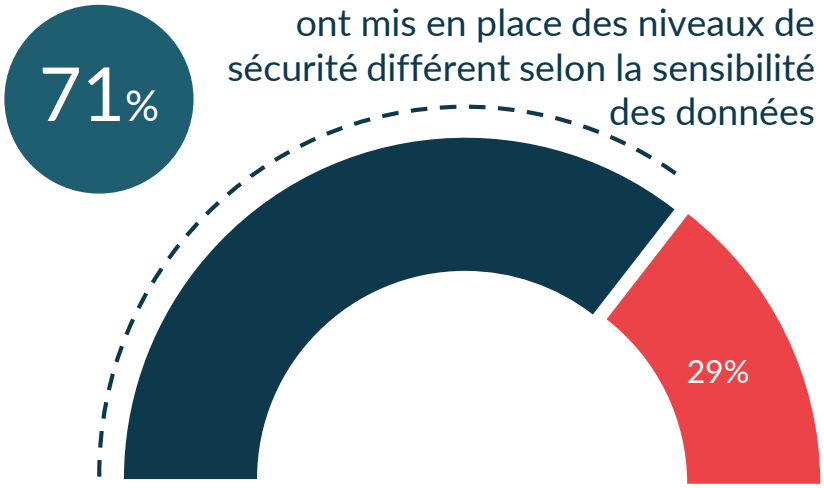


“opinionway CESIN

Des niveaux de sécurité qui diffèrent souvent selon une typologie de sensibilité des données

Q10. Avez-vous mis en place différents niveaux de sécurité selon le degré de sensibilité des données de votre entreprise ?

125 entreprises

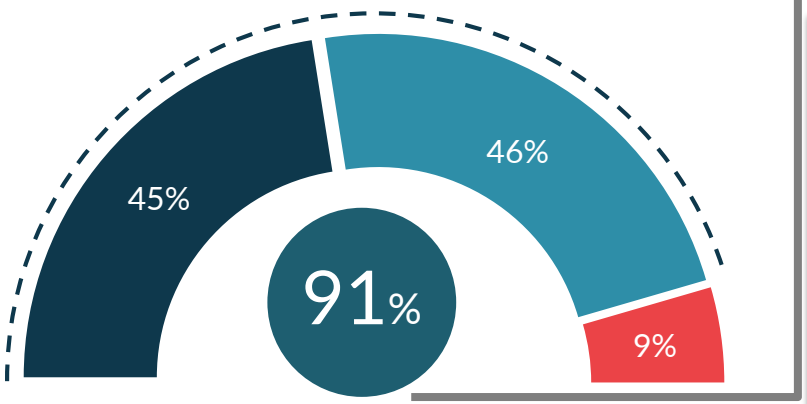


opinionway CESIN

La sécurisation passe le plus souvent par une limitation des usages, globalement acceptée, mais qui n'a d'impact qu'à la marge

Q16. Votre entreprise a-t-elle mis en place des limitations sur les usages des salariés (du type limitation d'usage de sites d'échanges de données, filtrage web, restrictions sur l'utilisation de périphériques…) ?

125 entreprises

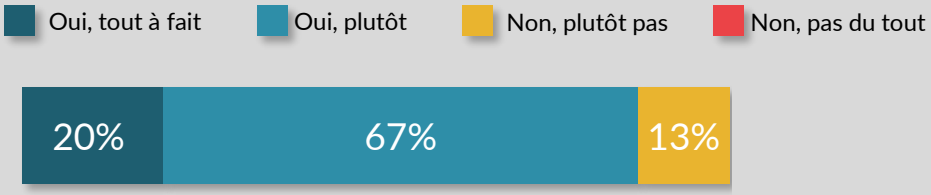


ont mis en place des limitations sur les usages des salariés

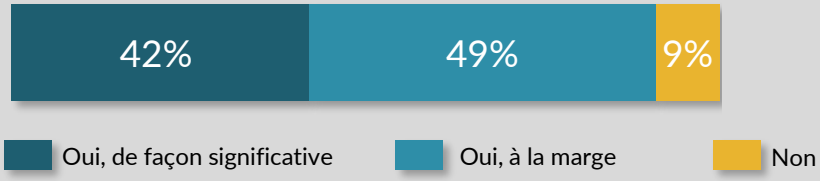
- Oui, ces limitations ont été mises en place
- Oui, mais seulement certaines limitations ont été mises en place
- Non, aucune limitation n'a été mise en place

116 entreprises ayant mis en place des contraintes

Q17. Ces contraintes sont-elles acceptées par les salariés ?



Q18. Et, globalement, la mise en place de ces limitations a-t-elle eu un impact concret sur la cyber-sécurité de votre entreprise ?



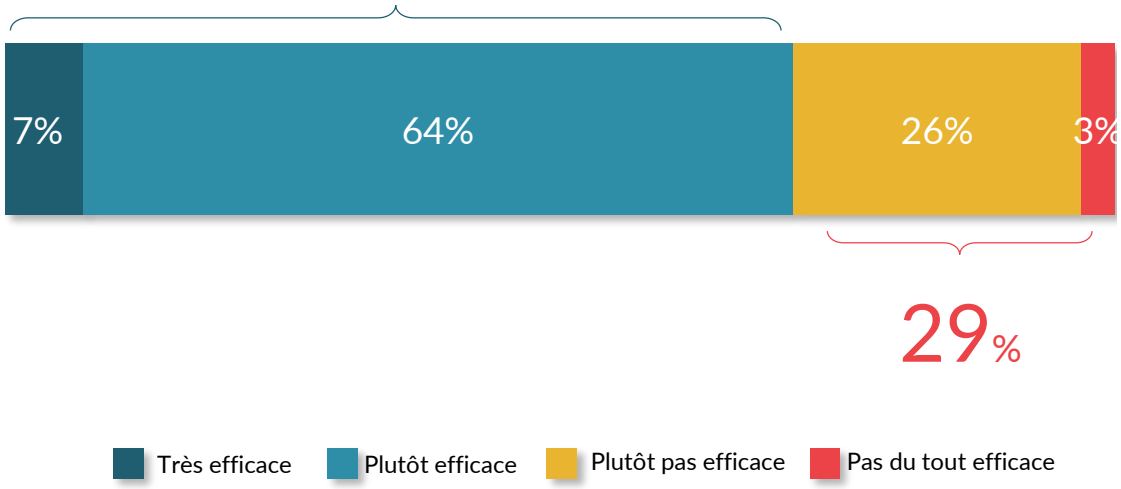
opinionway CESIN

Le filtrage web, une contrainte des usages rarement jugée très efficace pour la sécurité

Q19. Et concernant le filtrage web (c'est-à-dire l'accès refusé à certains sites pour les salariés) en particulier, cette mesure vous semble-t-elle efficace dans la protection des entreprises contre les cyber-attaques ?

125 entreprises

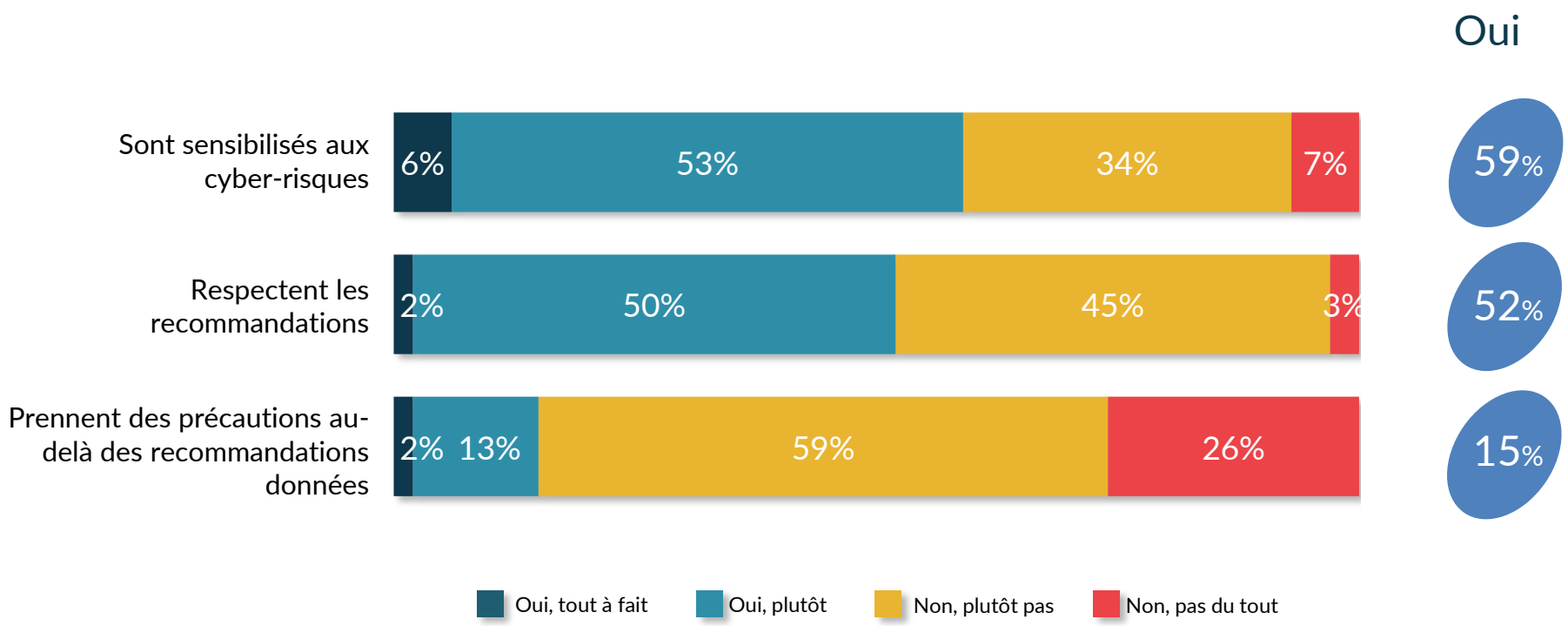
Le **filtrage web** est **efficace** pour 71% des entreprises



opinionway CESIN

Beaucoup de salariés ne sont pas encore sensibilisés ou ne respectent pas les recommandations

Q15. En ce qui concerne la cyber-sécurité, pensez-vous que les salariés de votre entreprise… ?



Des moyens techniques, financiers et humains jugés globalement insuffisants pour faire face aux cyber-risques

Q12. Les **moyens techniques** alloués par votre entreprise à la protection contre les cyber-risques vous semblent-ils suffisants ?

Oui 42%

Q13. Et les **budgets d'investissements** alloués par votre entreprise à la protection contre les cyber-risques vous semblent-ils suffisants ?

36%

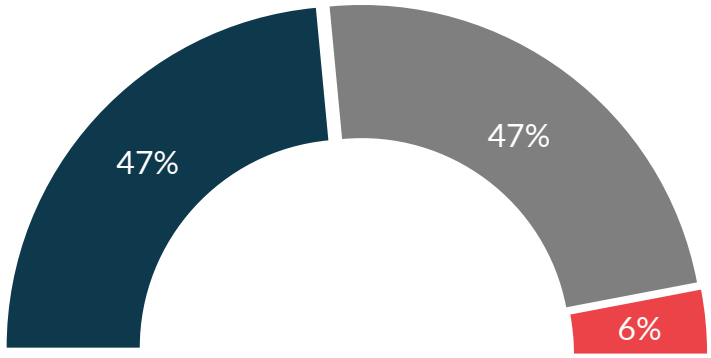
Q11. Les **moyens humains** alloués par votre entreprise à la protection contre les cyber-risques vous semblent-ils suffisants ?

31%

Des prévisions non négligeables d'augmentation des ressources à allouer à la protection contre le cyber-risque

Q14. Au cours des 12 prochains mois, votre entreprise envisage-t-elle de… ?

125 entreprises

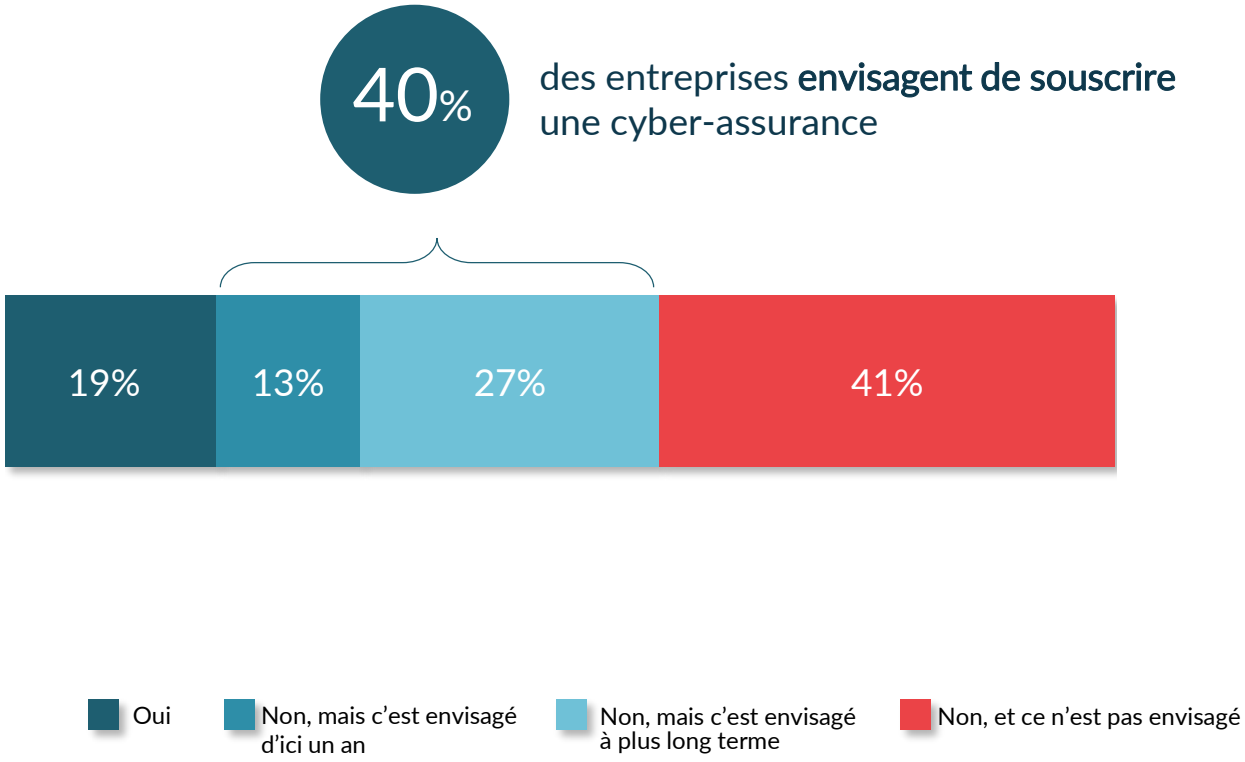


- Augmenter les budgets et ressources dédiés à la cyber-sécurité
- Maintenir les budgets et ressources dédiés à la cyber-sécurité
- Réduire les budgets et ressources dédiés à la cyber-sécurité

Nombre d'entreprises envisagent de se doter dune cyber-assurance

Q9. Votre entreprise a-t-elle souscrit une cyber-assurance ?

125 entreprises

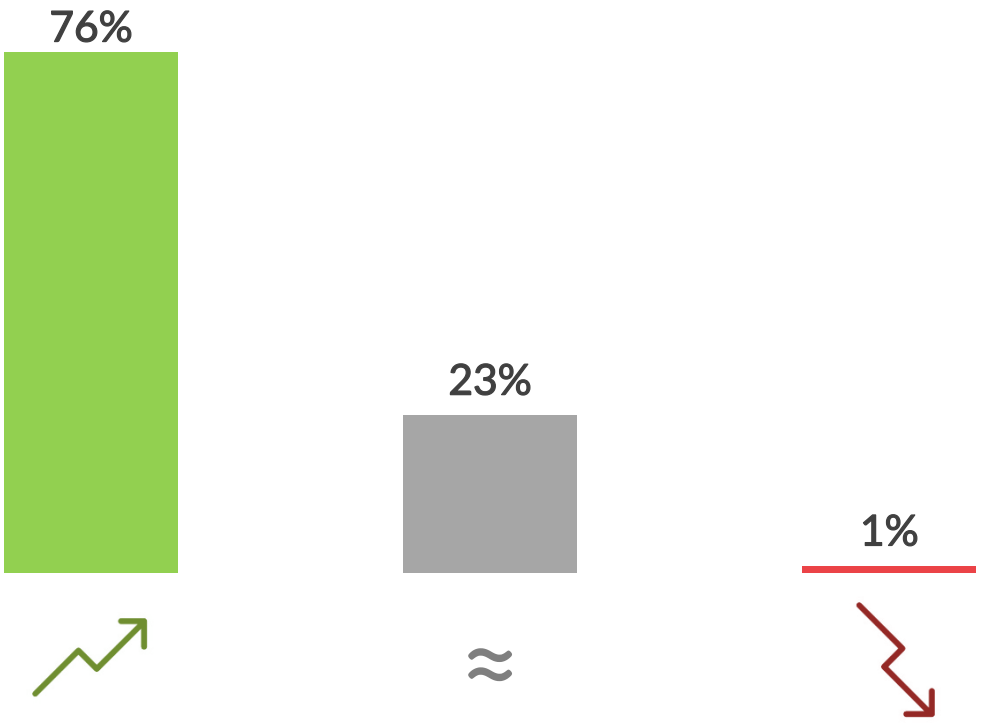


opinionway CESIN

5. PERSPECTIVES SUR LE FUTUR DE LA CYBER-SÉCURITÉ

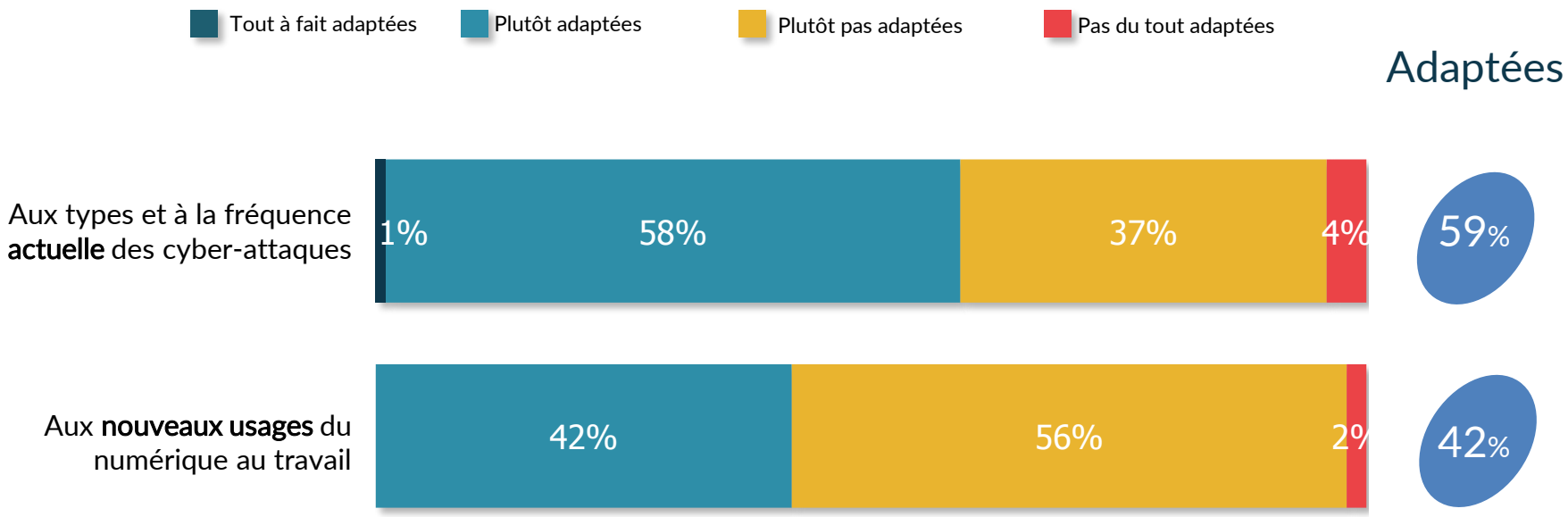
Des entreprises qui s'attendent à une augmentation des attaques cette année

Q7. Selon vous, dans les 12 mois à venir, le nombre d'attaques constatées dans votre entreprise va-t-il… ?



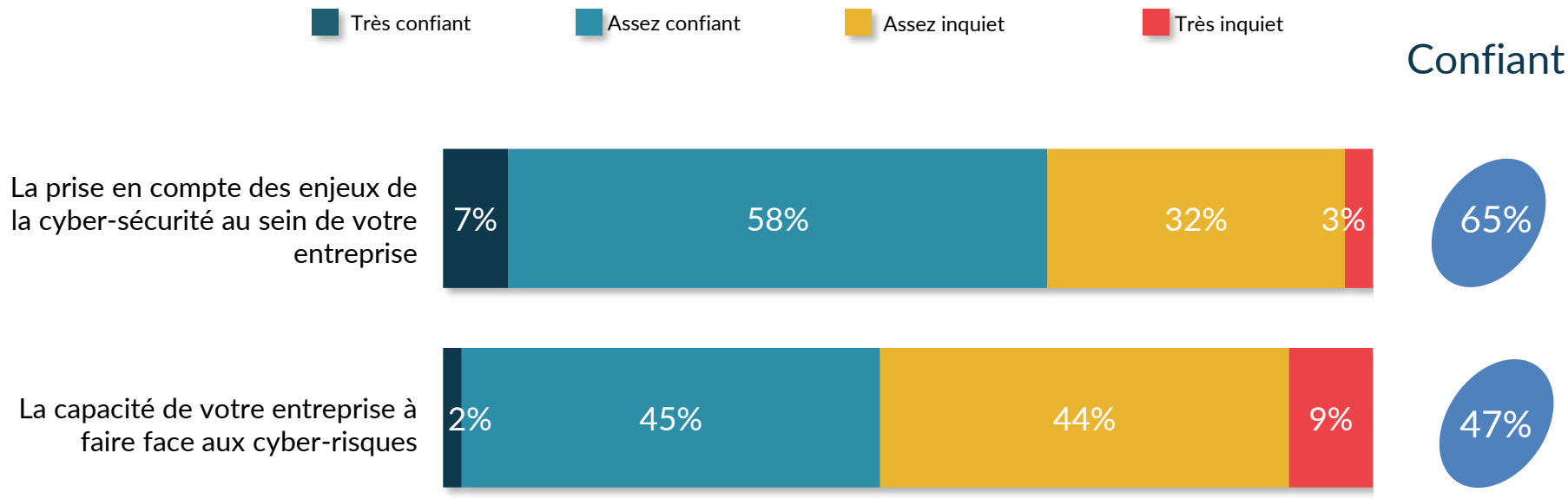
Les solutions proposées par le marché convainquent globalement peu les entreprises

Q29. Pensez-vous que les solutions de protection disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptées… ?



Une confiance dans la volonté de leur entreprise à prendre le cyber-risque au sérieux à l'avenir, mais moins dans sa capacité à y faire face concrètement

Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?

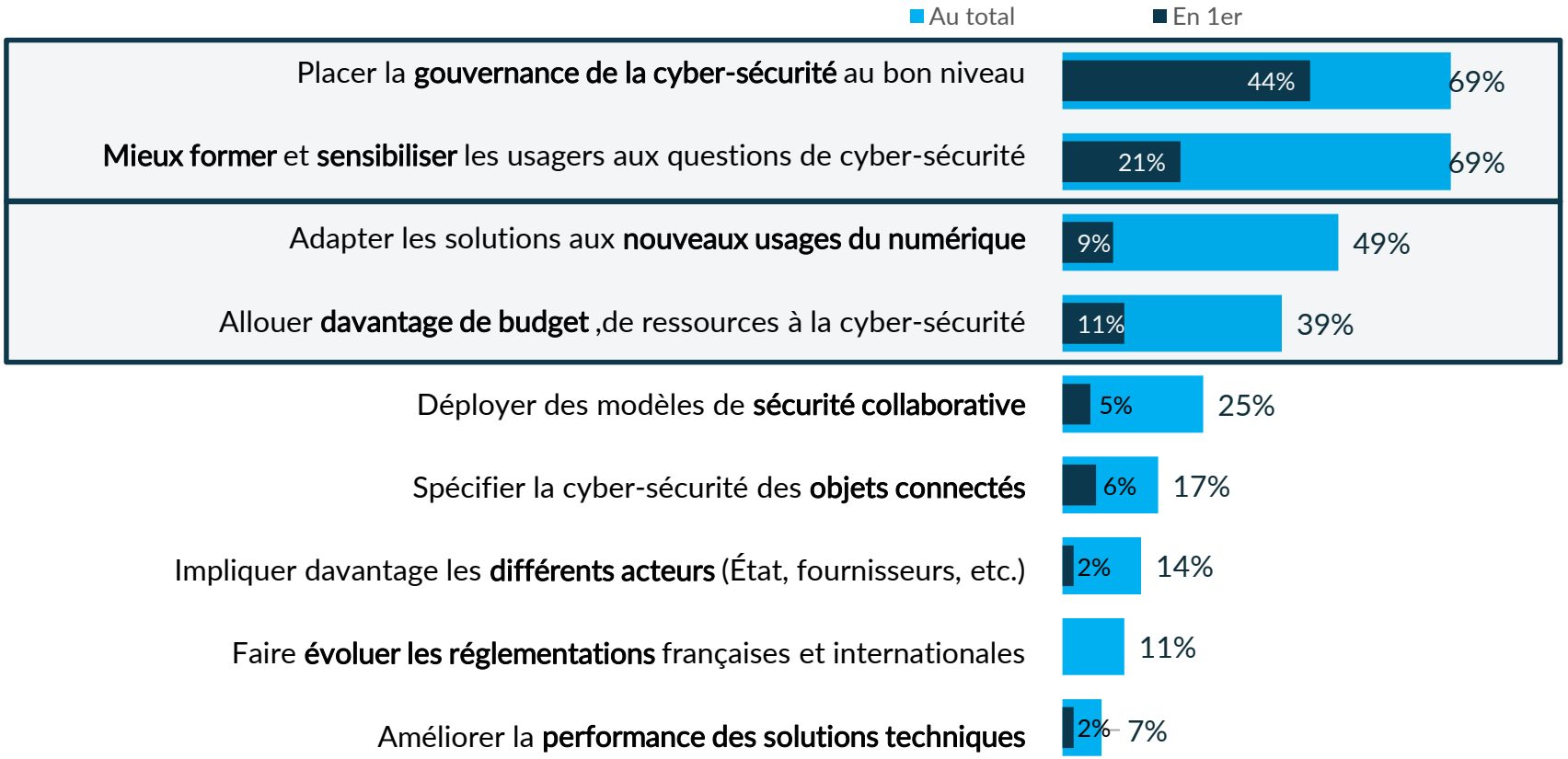


Des enjeux d'avenir plus humains que techniques :

- **L'importance donnée à la cyber sécurité** (par les ressources allouées et la gouvernance)
- **Le travail autour des usages** (pour former les usagers et s'adapter aux pratiques nouvelles)

Q28. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cyber-sécurité des entreprises ?

125 entreprises

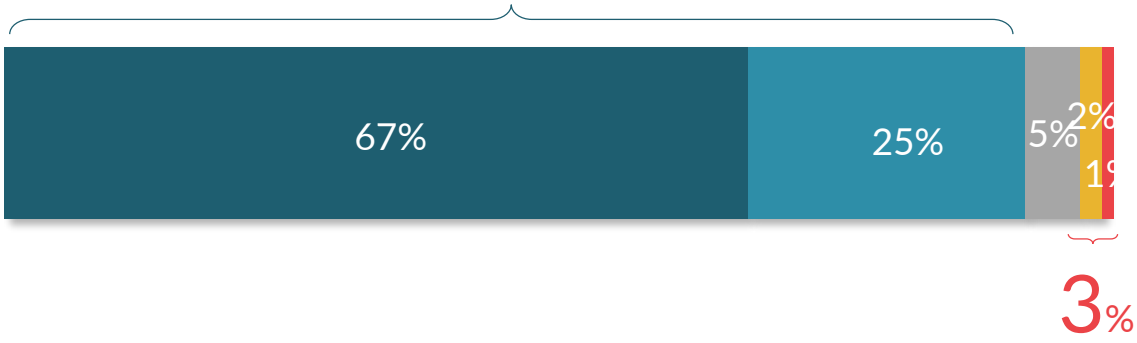


Les DSI font face à des usagers peu habitués à des outils sécurisés dans la sphère personnelle

Q30. Enfin, diriez-vous que, par rapport aux équipements utilisés dans le cadre professionnel, les ordinateurs privés de vos salariés sont…

125 entreprises

Les **ordinateurs privés sont moins bien sécurisés** que les équipements professionnels pour **92%** des entreprises



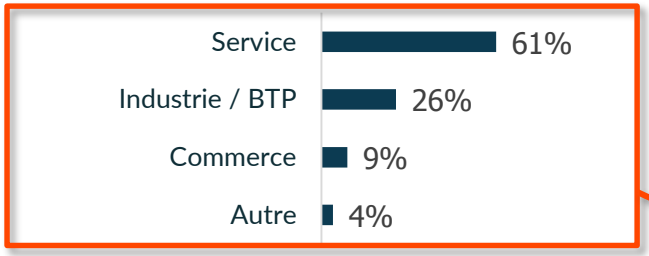
PROFIL DES RÉPONDANTS

Profil des répondants

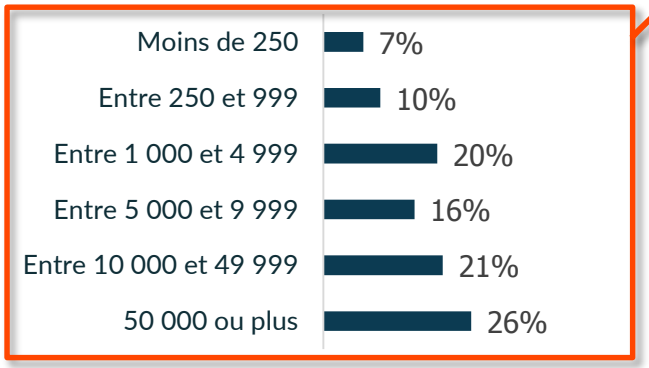
Fonction du répondant

84% de RSSI / CISO / CSO
5% d'experts
5% de DSI
6% autres fonctions

Secteur d'activité de l'entreprise



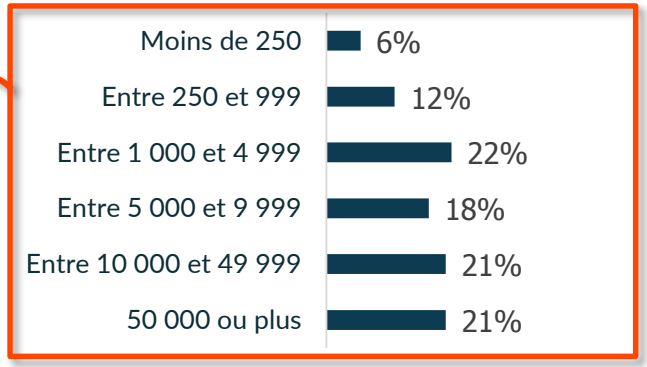
Nombre de salariés de l'entreprise



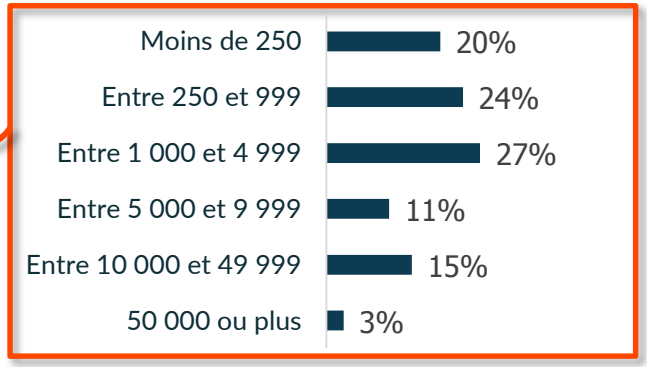
CESIN

125 membres du CESIN

Nombre d'ordinateurs de l'entreprise



Nombre de smartphones & tablettes de l'entreprise



"opinionway CESIN