Baromètre de la cyber-sécurité des entreprises

Vague 6 – Janvier 2021

“opinionway

15 place de la République 75003 Paris

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

Rapport

CESIN

Alain BOUILLE - ***Délégué Général du CESIN***

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

De : Diane HION - ***Directrice de clientèle***
Valentin HERITIER - ***Chargé d’études***

Sommaire

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, avec OpinionWay, a lancé en 2015 sa première grande enquête auprès de ses membres pour 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.

- L'enquête, renouvelée chaque année, met à jour les résultats sur la perception et la réalité de la cyber-sécurité, et apporte de nouvelles données sur l'impact de la transformation numérique des entreprises.

- Dans le contexte ou l'actualité cybersécurité évolue en permanence et avec la crise sanitaire de 2020, le baromètre a été mis à jour afin de tenir compte de ces nouvelles réalités. Le but étant d'illustrer aux mieux l'état de la cybersécurité dans les entreprises françaises.

MÉTHODOLOGIE

Méthodologie

- Étude réalisée auprès d'un échantillon de **228 membres du CESIN,** à partir du fichier des membres du CESIN

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

- Mode d'interrogation : L'échantillon a été interrogé **en ligne sous système CAWI** (Computer Assisted Web Interview), avec un questionnaire d'une durée de 15 minutes.

Questionnaire

- Dates de terrain : les interviews ont été réalisées entre le **7 décembre 2020 et le 11 janvier 2021**.

- OpinionWay rappelle par ailleurs que les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 6,5 points au plus pour un échantillon de 230 répondants.

Profil des répondants

Nombre de salariés de l'entreprise

Moins de 250 salariés	9%	TPE / PME
Entre 250 et 999 salariés	14%	ETI **36%**
Entre 1 000 et 4 999 salariés	22%	
Entre 5 000 et 9 999 salariés	14%	Grandes entreprises **55%**
Entre 10 000 et 49 999 salariés	18%	
50 000 salariés ou plus	23%	

Secteur d'activité de l'entreprise

Activités financières et d'assurance	22%	Services **43%**
Information et communication	11%	
Activités immobilières	3%	
Activités spécialisées, scientifiques et techniques	3%	
Entreprise de service du numérique	2%	
Arts, spectacles et activités récréatives	2%	
Industrie manufacturière	18%	Industrie/BTP **22%**
Production et distribution d'électricité, gaz, vapeur, air conditionné	2%	
Industries extractives	1%	
Construction	1%	
Commerce	11%	Commerce **16%**
Transports et entreposage	4%	
Hébergement et restauration	1%	
Administration publique et défense	10%	Services publics **16%**
Santé humaine et action sociale	4%	
Enseignement	1%	
Autre secteur	4%	

MESSAGES CLÉS

Les enseignements à retenir (1/2)

1. Une vulnérabilité des entreprises aux cyber-attaques toujours avérée…

57% des entreprises déclarent avoir connu au moins une cyber-attaque en 2020 : une vulnérabilité toujours présente donc, malgré un taux en légère baisse par rapport à l'année dernière (65%).

1 entreprise sur 5 (19%) a été victime d'une attaque de type ransomware provoquant un chiffrement ou un vol et chantage de données. Les entreprises, conscientes de la recrudescence de la menace ransomware en 2020 renforcent la sensibilisation des utilisateurs (83%) à ce type d'attaque. **Les vecteurs d'attaque par phishing (80%) et exploitation des failles (52%)** restent les plus répandues, menant le plus souvent à un vol de données (30%) ou à un déni de service (29%).

Une des principales causes de cyber-risques est **le Shadow IT pour 44% des entreprises**, suivies par la vulnérabilité résiduelle permanente (36%) et la cyber-attaque opportuniste (36%). **Plus de la moitié des entreprises (56%) estiment que le niveau des menaces relatives au cyber-espionnage est élevé.**

Similairement à l'année dernière, **58% des cyber-attaques ont un impact sur le business**, entraînant le plus souvent une perturbation de la production (27%).

2. …et qui ne peuvent que progresser sur leur capacité à répondre aux attaques

85% des entreprises jugent les solutions de protection disponibles sur le marché plutôt adaptées aux besoins de leur entreprise. Elles sont d'ailleurs 69% à s'estimer prêtes à gérer une cyber-attaque en termes de moyens de prévention , mais moins nombreuses à l'être en termes de moyens de détection (59%).

Pour ce faire, **elles mettent en place en moyenne 10 solutions**, et en priorité le VPN, le proxy & filtrage d'URL et la passerelle de sécurité mail. Toujours dans une démarche de prévention, **29% des entreprises ont mis en place le concept de Zero Trust** et 45% sont en train de l'étudier.

Toutefois, **seules 46% des entreprises se disent confiantes quant à leur capacité de réponse à une cyber-attaque**. 33% des entreprises mettent en place un programme d'entraînement à la cyber-crise et 24% ont déjà fait appel à leur cyber-assurance en cas d'attaque.

47% des entreprises ont porté plainte à la suite d'une ou plusieurs cyber-attaques, mais seulement 15% des enquêtes ont débouché sur une identification ou une interpellation des attaquants.

Les enseignements à retenir (2/2)

3. La crise sanitaire apporte de nouveaux risques

La crise sanitaire provoque 2 changements majeurs dans le cadre de la cybersécurité : la généralisation du télétravail (37%) et l'augmentation des crises cyber liée aux nouveaux risques (35%). 43% des entreprises se disent d'ailleurs prêtes à augmenter les budgets liés à la cybersécurité pour faire face à ces nouveaux risques.

4. Une sensibilisation des salariés en continu

77% des entreprises estiment que leurs salariés sont sensibilisés à la cybersécurité, mais tous ne semblent pas appliquer les recommandations (63%). D'après les RSSI, les usages numériques des salariés présentent de nombreux risques, et plus particulièrement **l'utilisation à des services cloud non approuvés (84%) ou encore la gestion des partages de données à l'initiative des salariés (80%).**

5. Le Cloud, environnement toujours à risques

Les RSSI mettent en avant plusieurs risques à l'utilisation du Cloud, les plus forts étant **la non-maîtrise de la chaîne de sous-traitance de l'hébergeur (51%), la difficulté de contrôler les accès par des administrateurs de l'hébergeur (45%) et la non-maîtrise de l'utilisation qui en est faite par les salariés de l'entreprise (44%).**

86% des entreprises estiment par ailleurs que les outils fournis par les prestataires de solutions Cloud ne permettent pas de sécuriser les données et qu'il est nécessaire d'utiliser des dispositifs et outils spécifiques.

Bilan

Des entreprises inquiètes, mais clairvoyantes sur les enjeux de demain

Au final, une entreprise sur deux est inquiète quant à sa capacité à faire face aux cyber-risques.

Les entreprises identifient 3 principaux enjeux pour demain :

- **Le premier enjeu consiste à placer la cybersécurité au centre de la gouvernance (60%),** les entreprises se disent d'ailleurs confiantes quant à la prise en compte des enjeux de la cybersécurité au sein du COMEX (**72% / +8 points par rapport à 2019**).

- **Le second est la formation et la sensibilisation des usagers à la cybersécurité (56%)**, il s'agit d'un processus déjà mis en place puisque la sensibilisation est le premier dispositif (83%) à avoir été renforcé par les RSSI face à la vague des cyber-attaques.

- **Enfin, le troisième enjeu est l'allocation de davantage de budgets et de ressources à la cybersécurité (46%).** 57% des entreprises comptent augmenter les budgets pour la protection contre les cyber-risques. En termes de ressources, les entreprises souhaitent augmenter les effectifs de cybersécurité (52%). L'augmentation du budget passe également par l'acquisition de nouvelles solutions techniques désirée par 85% des entreprises.

ANALYSE

opinionway

01

Une vulnérabilité des entreprises aux cyber-attaques toujours avérée

Près de 6 entreprises sur 10 ont constaté au moins une cyber-attaque en 2020

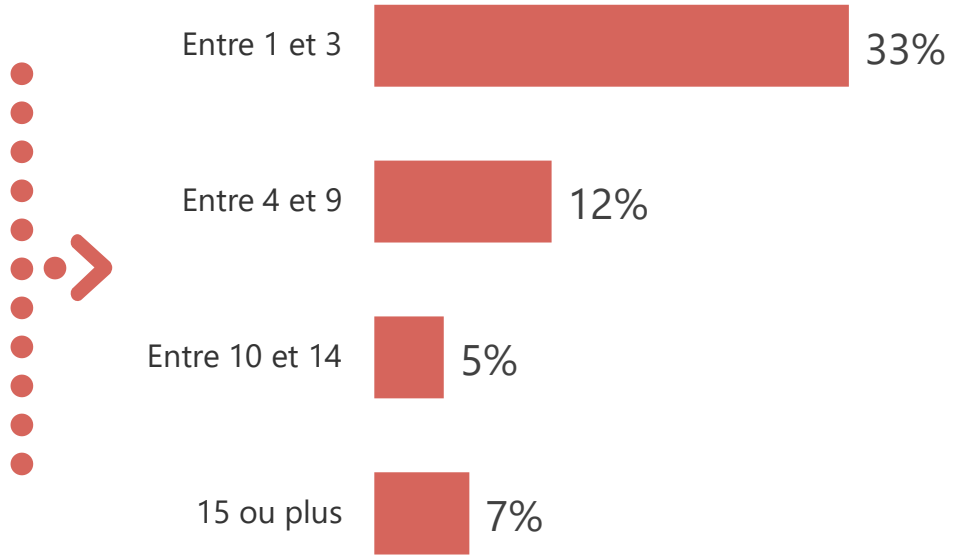
Q4. De façon générale, combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (228)

La cyber-attaque, telle que nous l'entendons dans cette enquête, est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information, entraînant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise.

57%

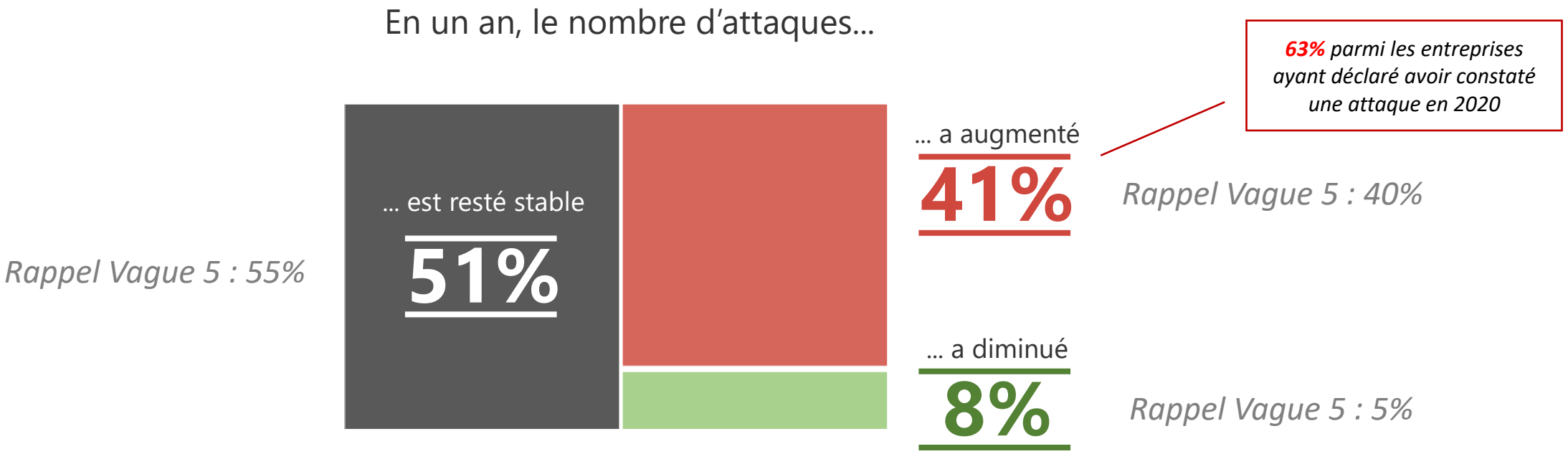
des entreprises ont constaté au moins une cyber-attaque

Rappel vague 5 : 65%
(la définition a été ajustée cette année)



Pour une grande partie des entreprises, le nombre d'attaque a augmenté par rapport à l'année dernière

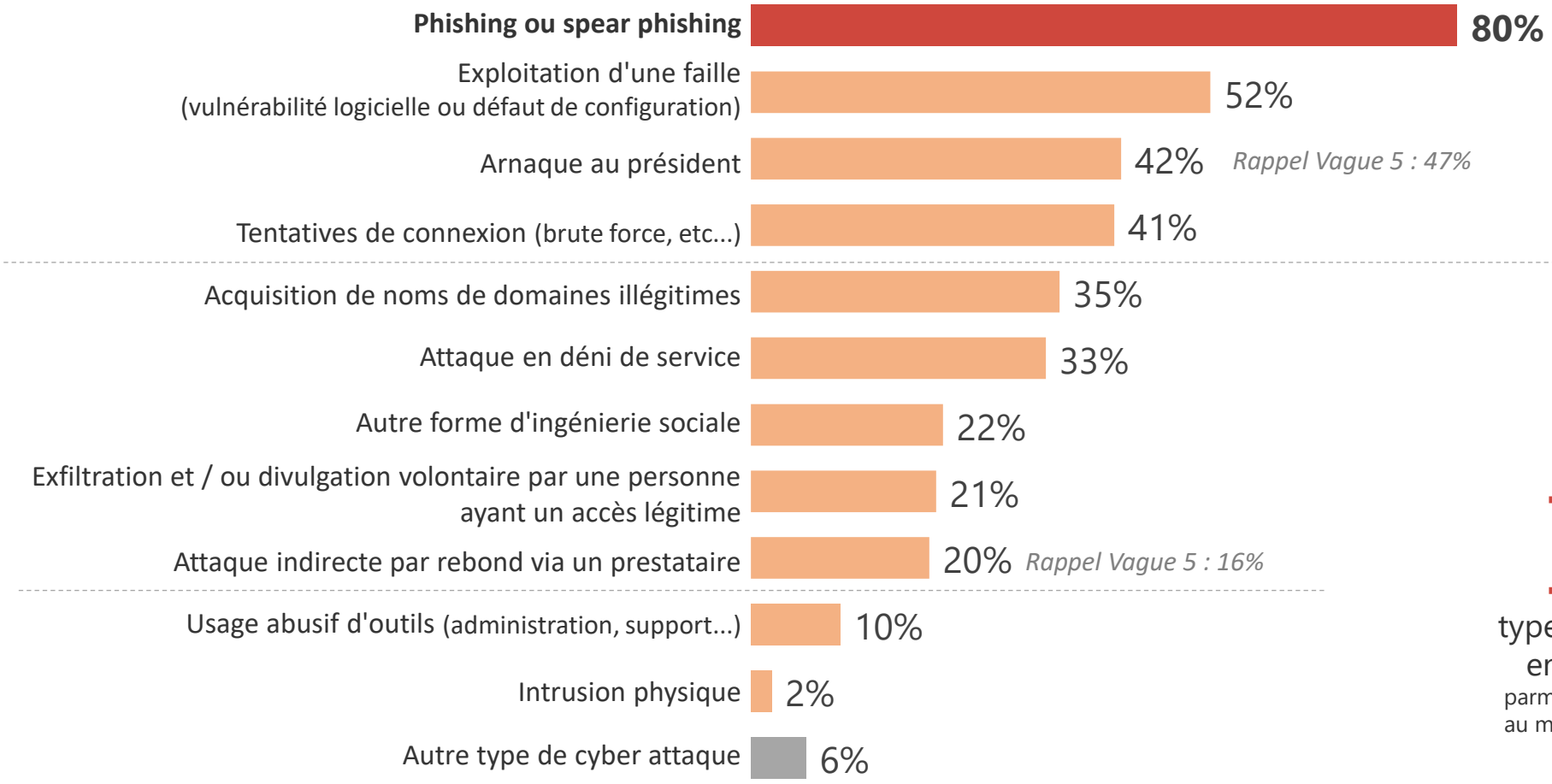
Q4bis. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ?
Base : ensemble (228)



Le phishing, premier vecteur d'attaque dans les entreprises

Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?

Base : ont constaté une attaque (129) / Plusieurs réponses possibles



3,6

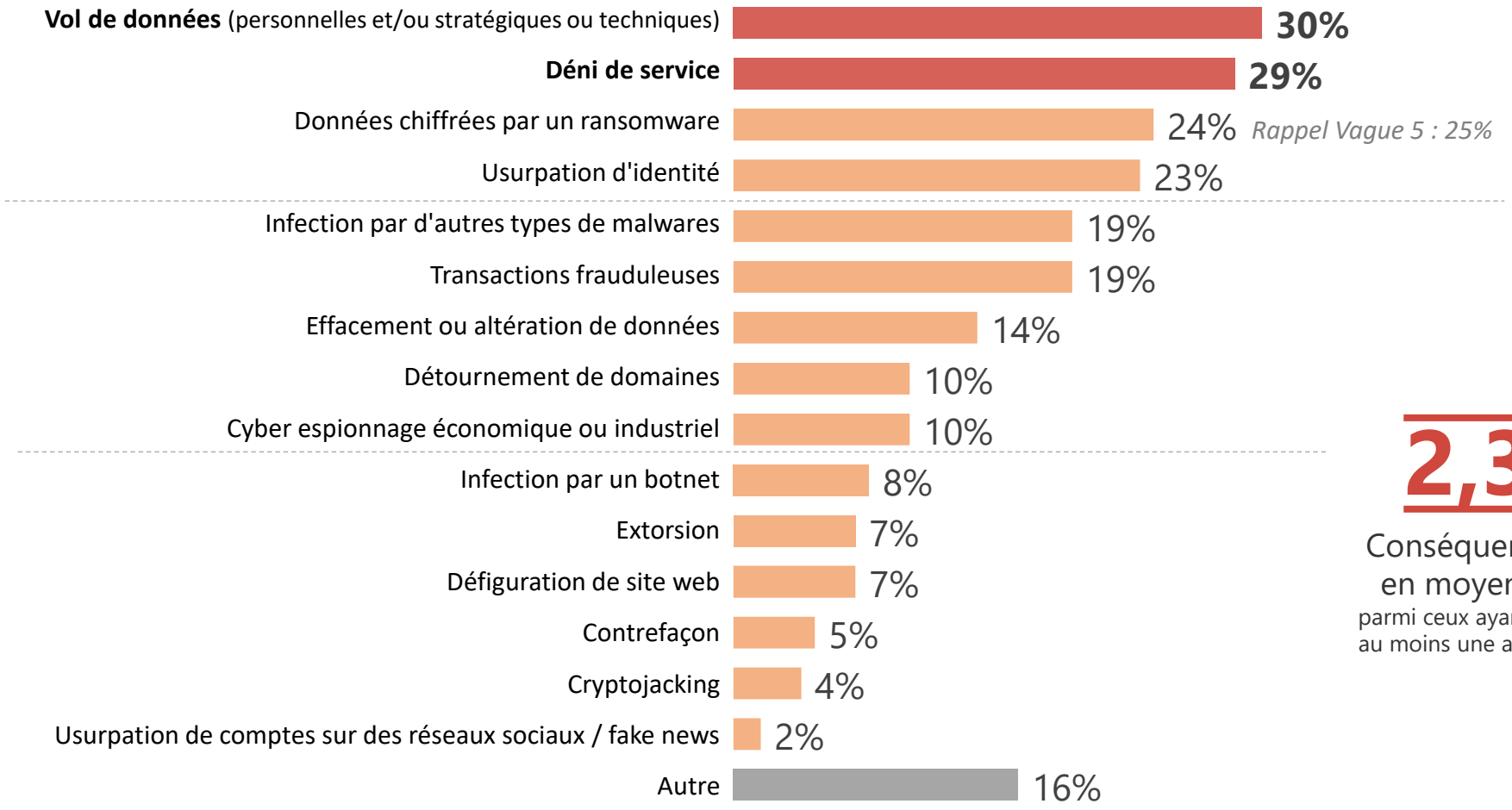
types d'attaques en moyenne

parmi ceux ayant subi au moins une attaque

Le vol de données et le déni de service sont les conséquences directes de ces attaques

Q5B. Et quelles ont été les conséquences de cette/ces attaque(s) ?

Base : ont constaté une attaque (129) / Plusieurs réponses possibles



2,3

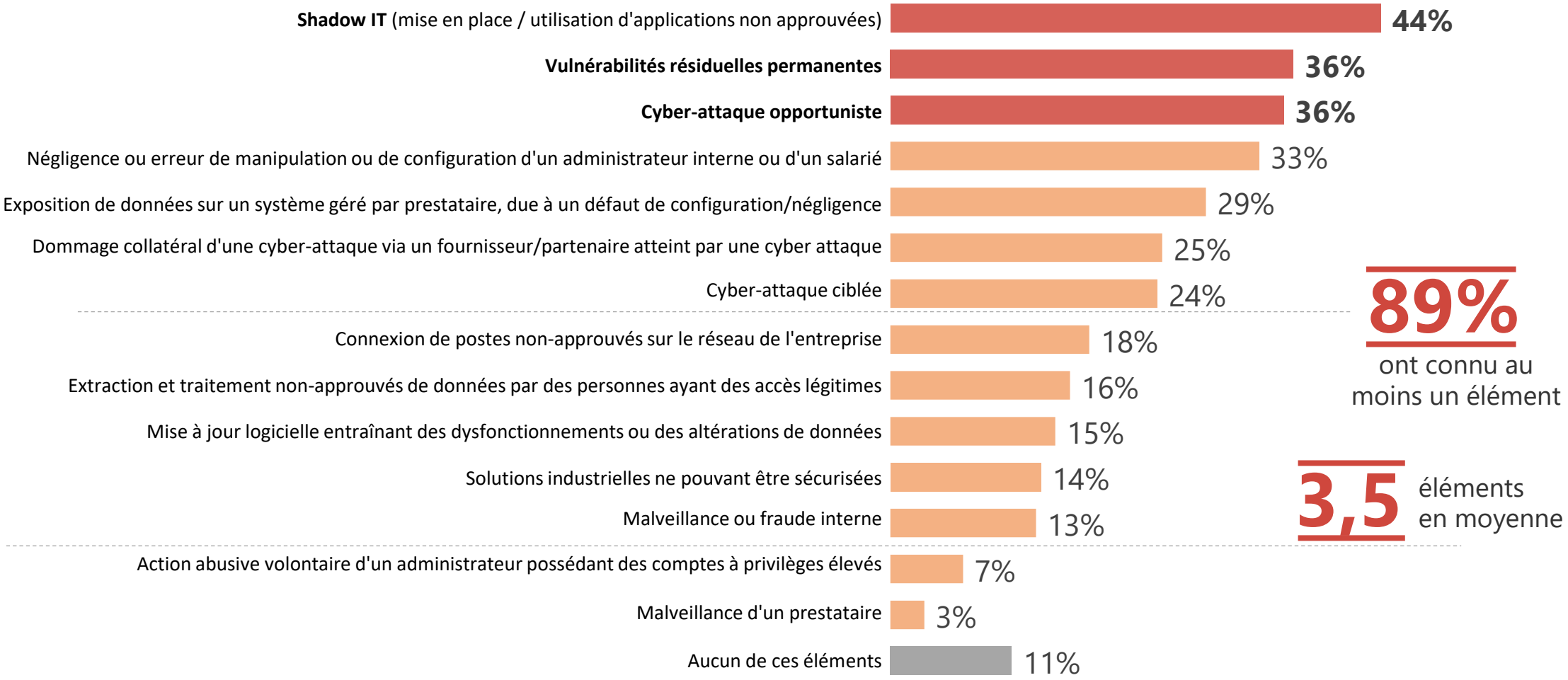
Conséquences en moyenne

parmi ceux ayant subi au moins une attaque

Le Shadow IT est la principale cause des incidents de sécurité rencontrés par les entreprises

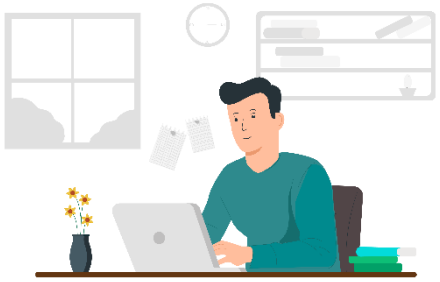
Q6. Parmi les causes des incidents de sécurité rencontrées par l'entreprise, cyber-attaques incluses, quelles sont celles auxquelles votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?

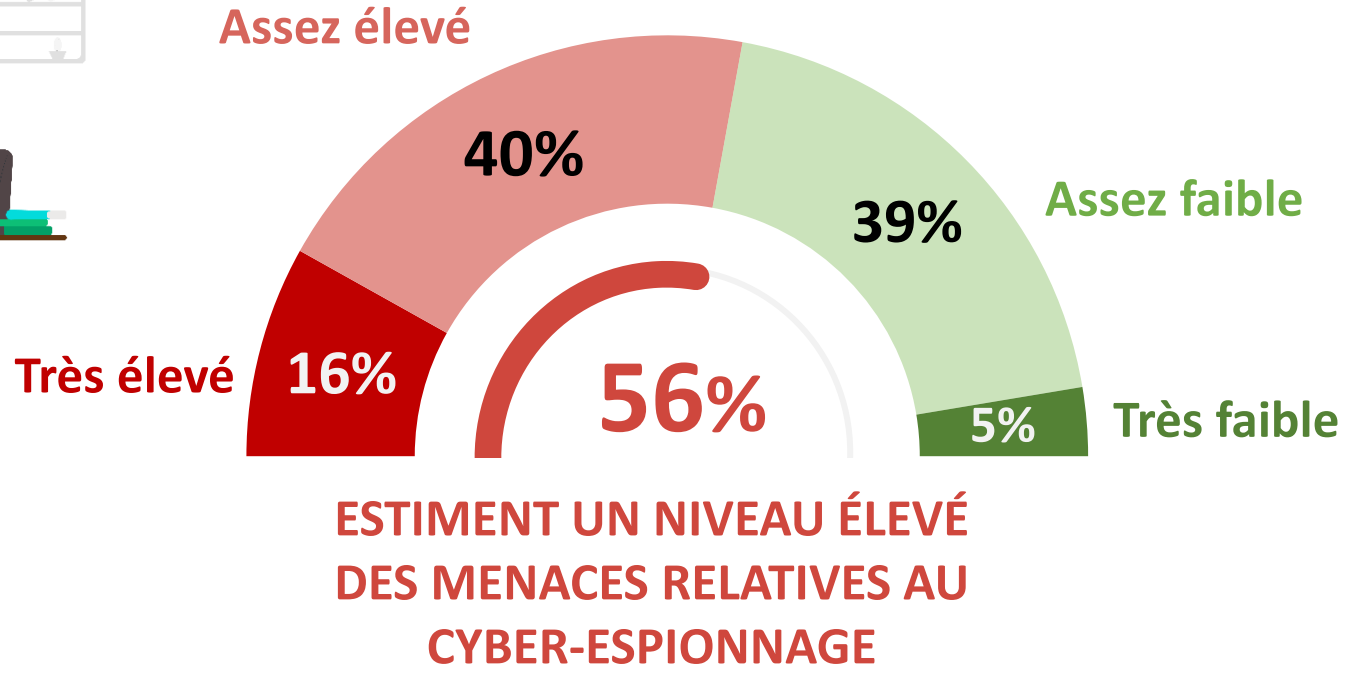
Base : ensemble (228) / Plusieurs réponses possibles



Plus de la moitié des entreprises considèrent que les menaces en lien avec le cyber-espionnage sont élevées

Q9. Aujourd'hui, comment évaluez-vous le niveau des menaces relatives au cyber-espionnage pour votre entreprise ?
Base : ensemble (228)



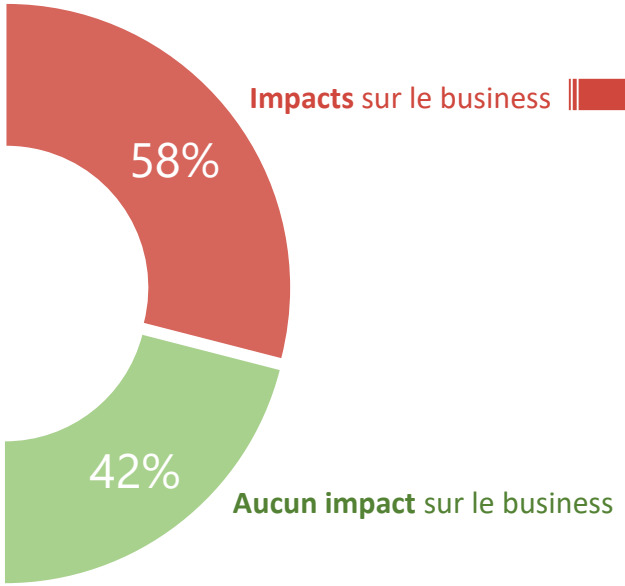


Au final, comme pour l'année précédente, 6 entreprises sur 10 constatent un impact des cyber-attaques sur leurs business, perturbant avant tout la production

Q7. Quel a été l'impact des cyber-attaques sur votre business ?

Base : ont constaté une attaque et une cause d'incidents de sécurité (206) / Plusieurs réponses possibles

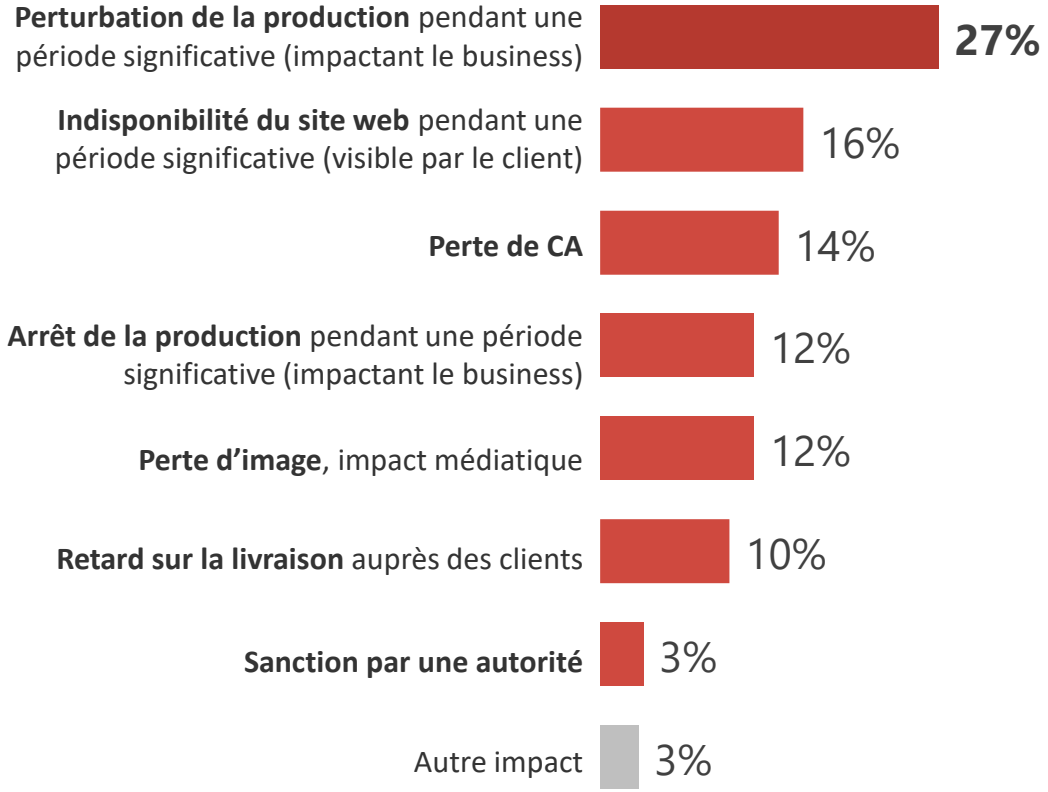
Rappel Vague 5 : 57%



Impacts sur le business

Rappel Vague 5 :43%

Aucun impact sur le business



A

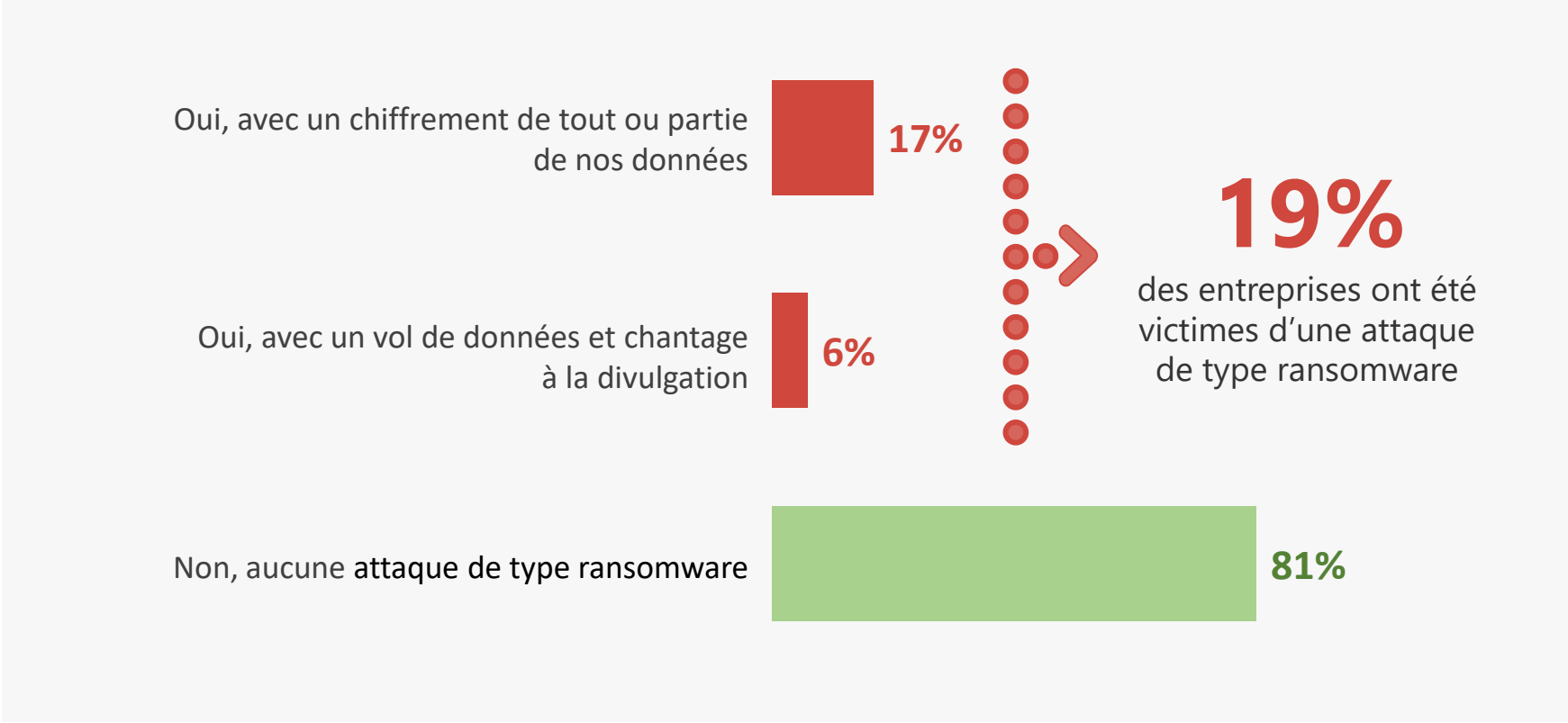
Zoom sur le ransomware

1 entreprise sur 5 déclare avoir été victime d'une attaque de type ransomware

L'année 2020 a été marquée par le renforcement de la menace par ransomware. Outre la vague d'attaques réussies dans certains cas, les attaquants ont exercé un chantage à la divulgation de données.

Q10. Avez-vous été victime d'une attaque de type ransomware ?

Base : ensemble (228)



Les grandes entreprises sont les plus touchées par ce type d'attaque

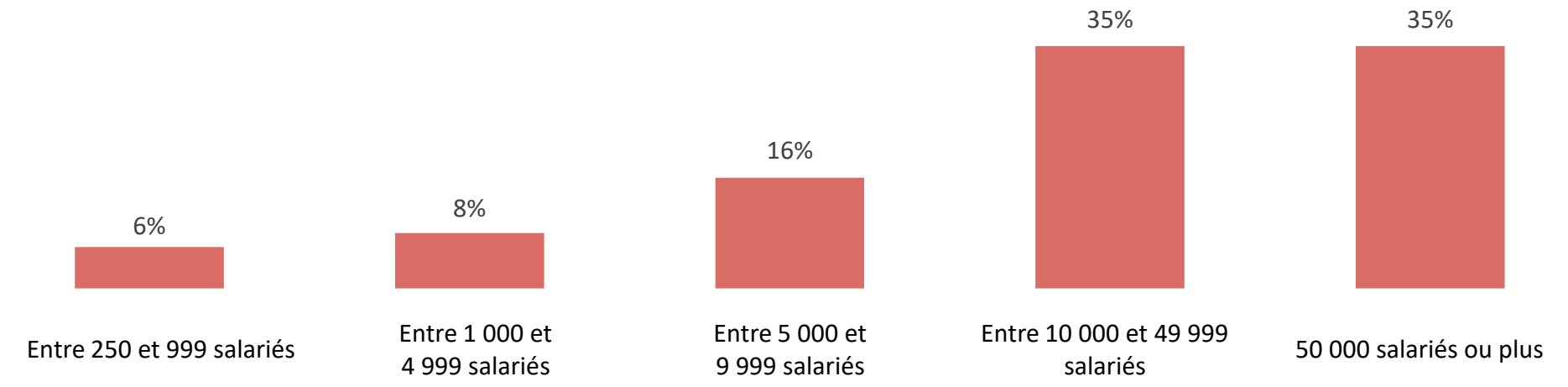
L'année 2020 a été marquée par le renforcement de la menace par ransomware. Outre la vague d'attaques réussies dans certains cas, les attaquants ont exercé un chantage à la divulgation de données.

Q10. Avez-vous été victime d'une attaque de type ransomware ?

Base : ensemble (228)

19% des entreprises ont été victimes d'une attaque de type ransomware

% d'entreprise victime de ransomware selon la taille d'entreprise

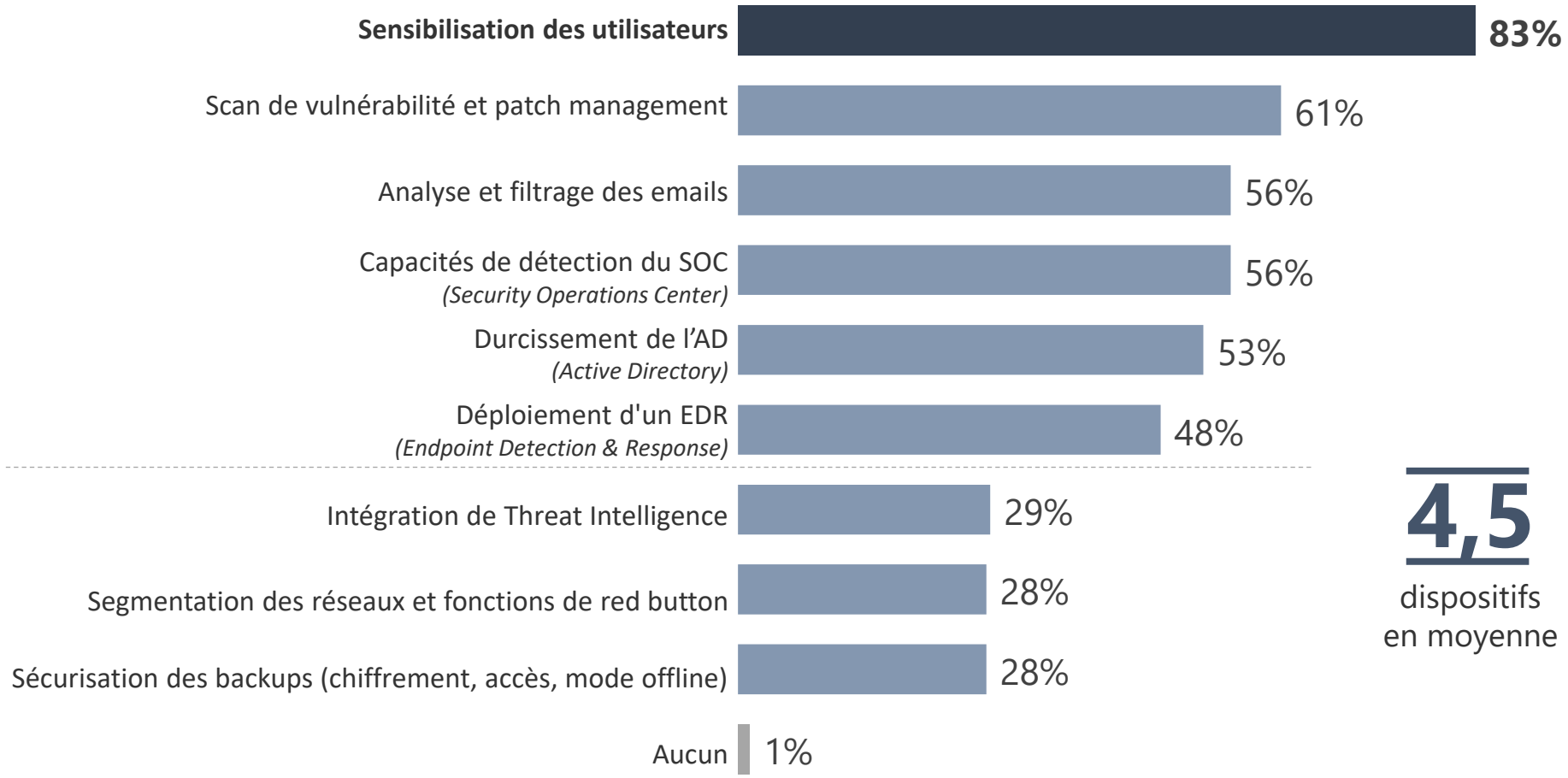


Total ETI : 7%

Total Grandes Entreprises : 30%

Pour faire face à cette menace, la sensibilisation des salariés est le premier dispositif à renforcer

Q11. Face à cette vague de cyber-attaque dominée par le ransomware, quels dispositifs avez-vous renforcés ?
Base : ensemble (228)



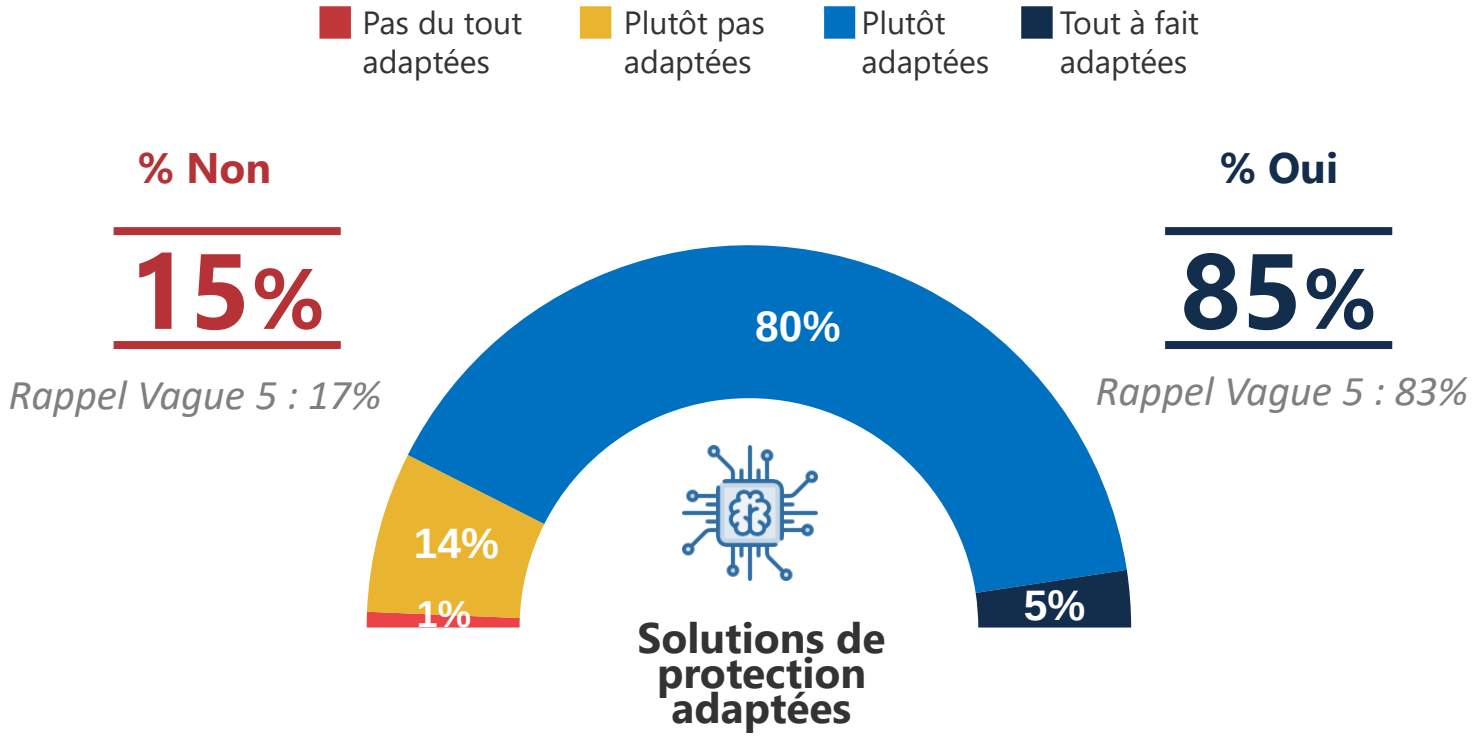
02

…et qui ne peuvent que progresser sur leur capacité à répondre aux attaques

La majorité des entreprises considère les solutions de protection du marché comme adaptées (mais la majorité ne les trouve que « plutôt » adaptées)

Q25. Pensez-vous que les solutions de protection disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptées à votre entreprise ?

Base : ensemble (228 répondants)



Des entreprises qui considèrent majoritairement disposer de moyens de prévention, mais toutes ne se disent pas forcément préparées en termes de moyens de détection face aux attaques

Q14. Selon vous, votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur en termes de…?

Base : ensemble (228 répondants)

69%

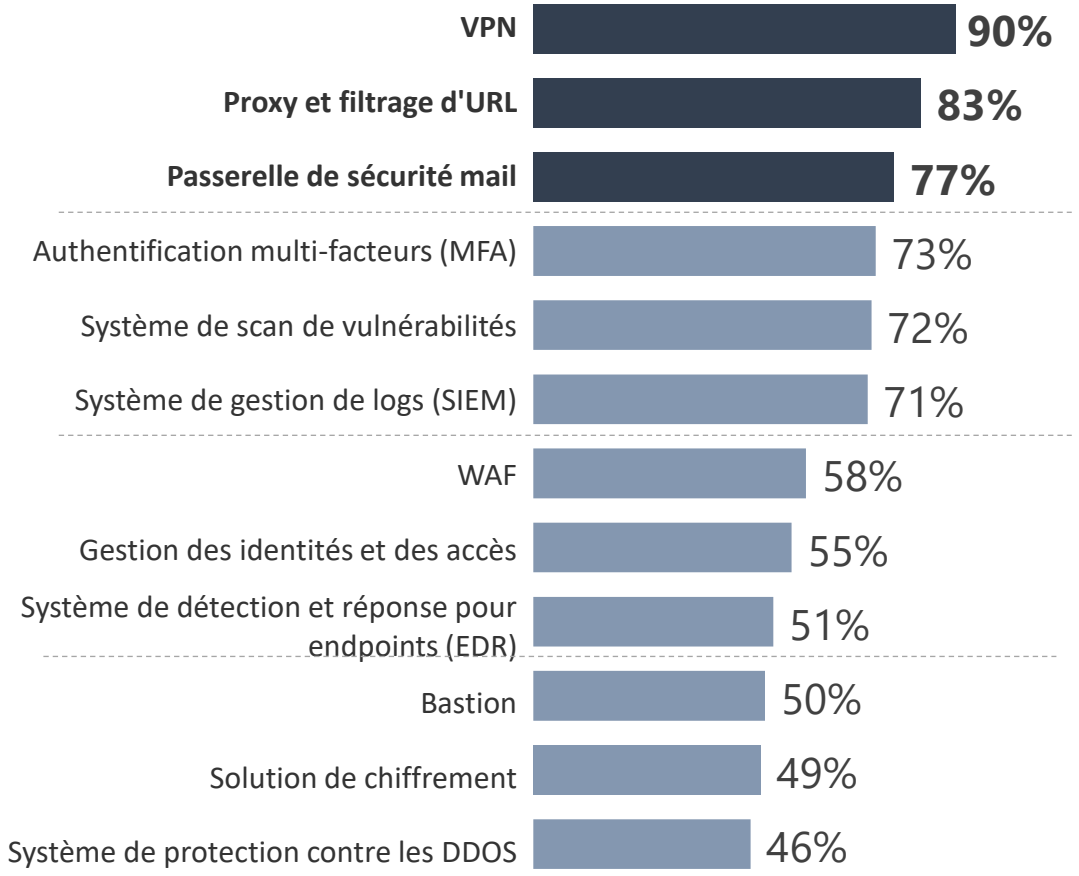
Moyens de prévention

59%

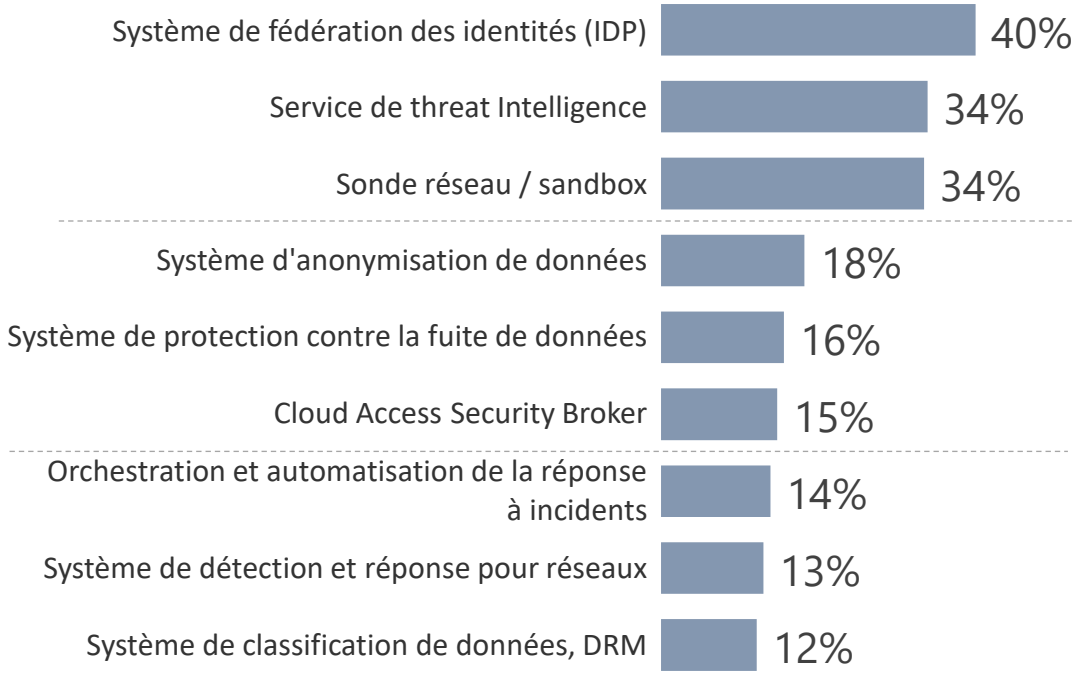
Moyens de détection

Une dizaine de solutions mises en place en moyenne par les entreprises, le recours au télétravail contribue à l'utilisation massive du VPN et de l'authentification multi-facteurs

Q12. D'une manière plus générale, parmi les solutions de protection suivantes, quelles sont celles qui sont en place dans votre entreprise, en plus des antivirus et pare-feu ? *Base : ensemble (228) / Plusieurs réponses possibles*



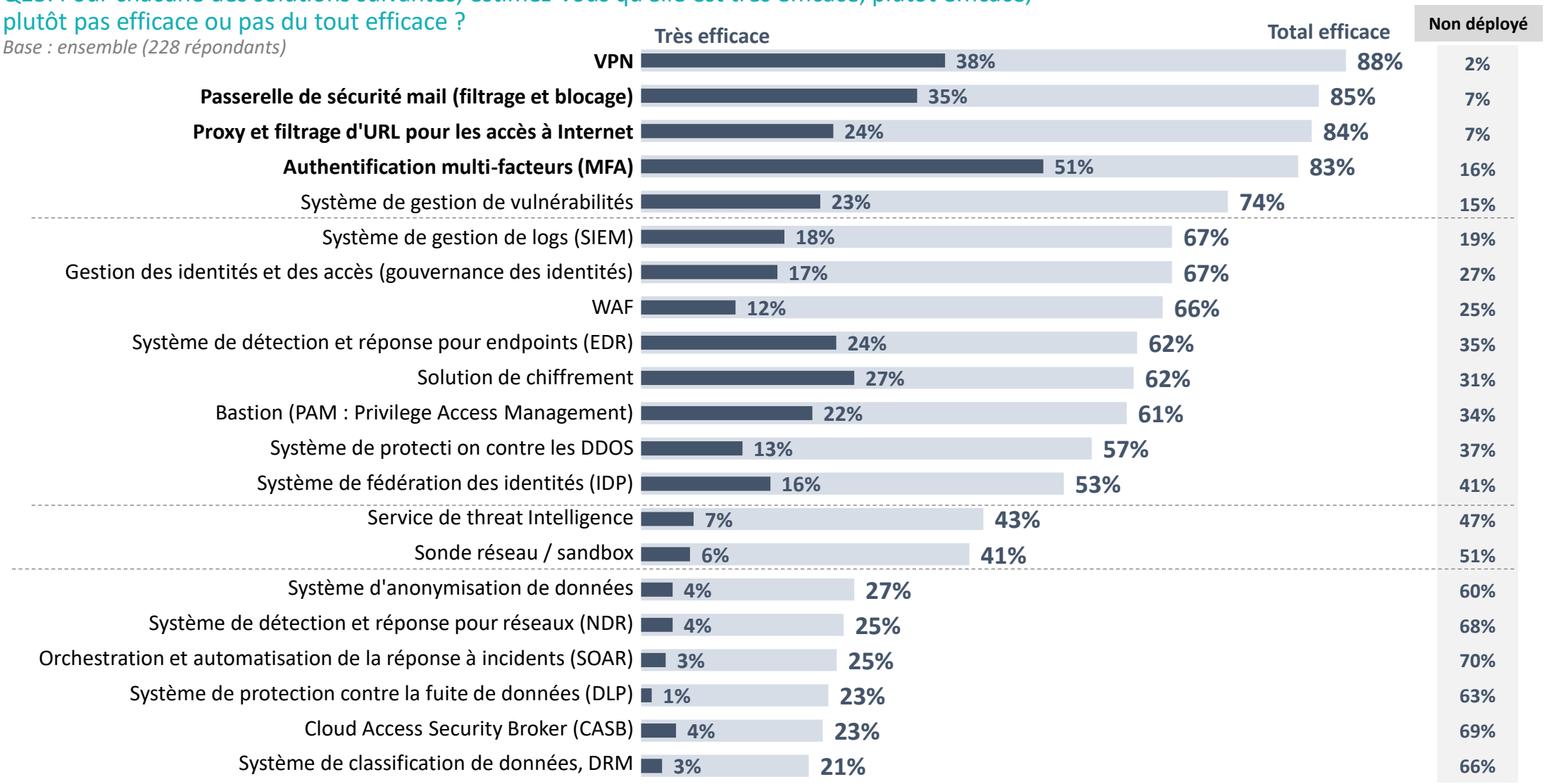
9,7 solutions en moyenne



Les premières solutions sont jugées comme les plus efficaces, à noter que l'authentification multi-facteurs est jugée très efficace par la moitié des entreprises

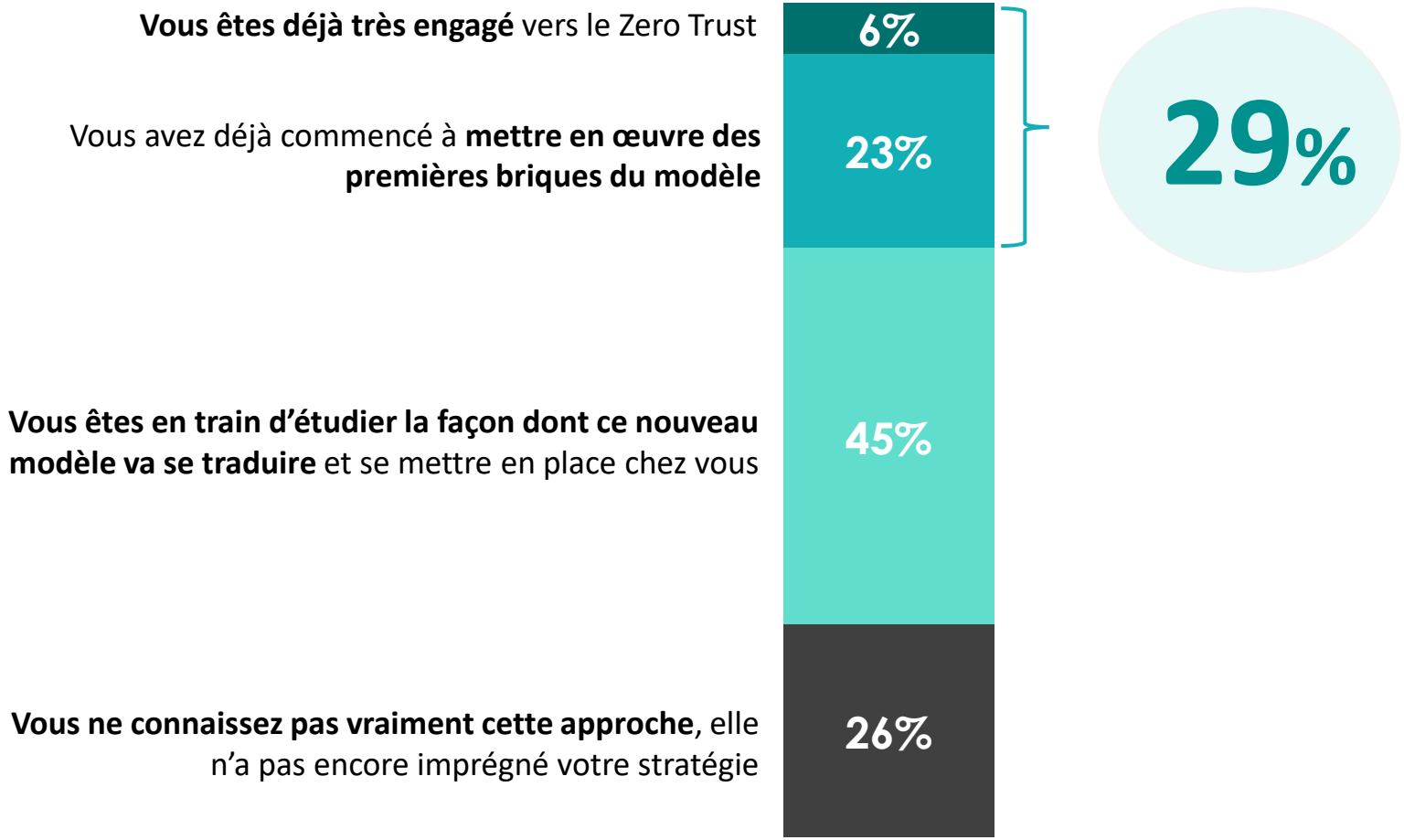
Q13. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ?

Base : ensemble (228 répondants)



3 entreprises sur 10 ont déjà mis en œuvre le concept Zero Trust, et la moitié étudie le modèle

Q28. Quelle est votre opinion et votre appétence pour le concept Zero Trust ?
Base : ensemble (228 répondants)



Moins de la moitié des entreprises se disent préparées à gérer une cyber-attaque

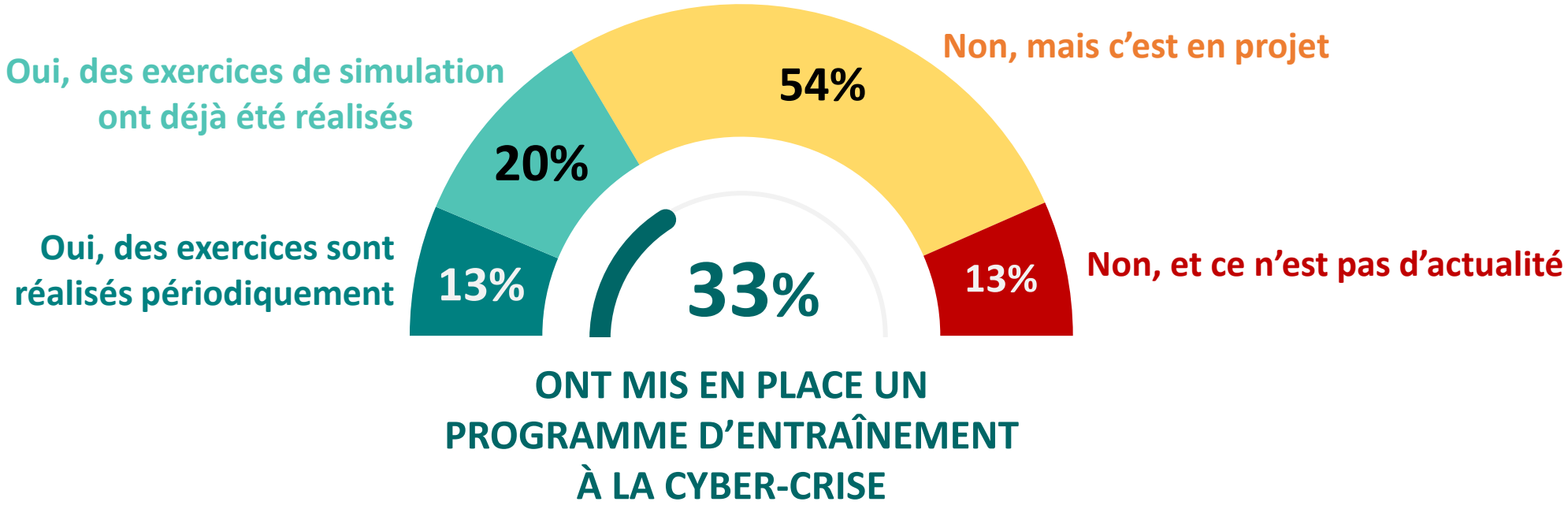
Q14. Selon vous, votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur en termes de…?
Base : ensemble (228 répondants)

46%

Réponse à l'attaque

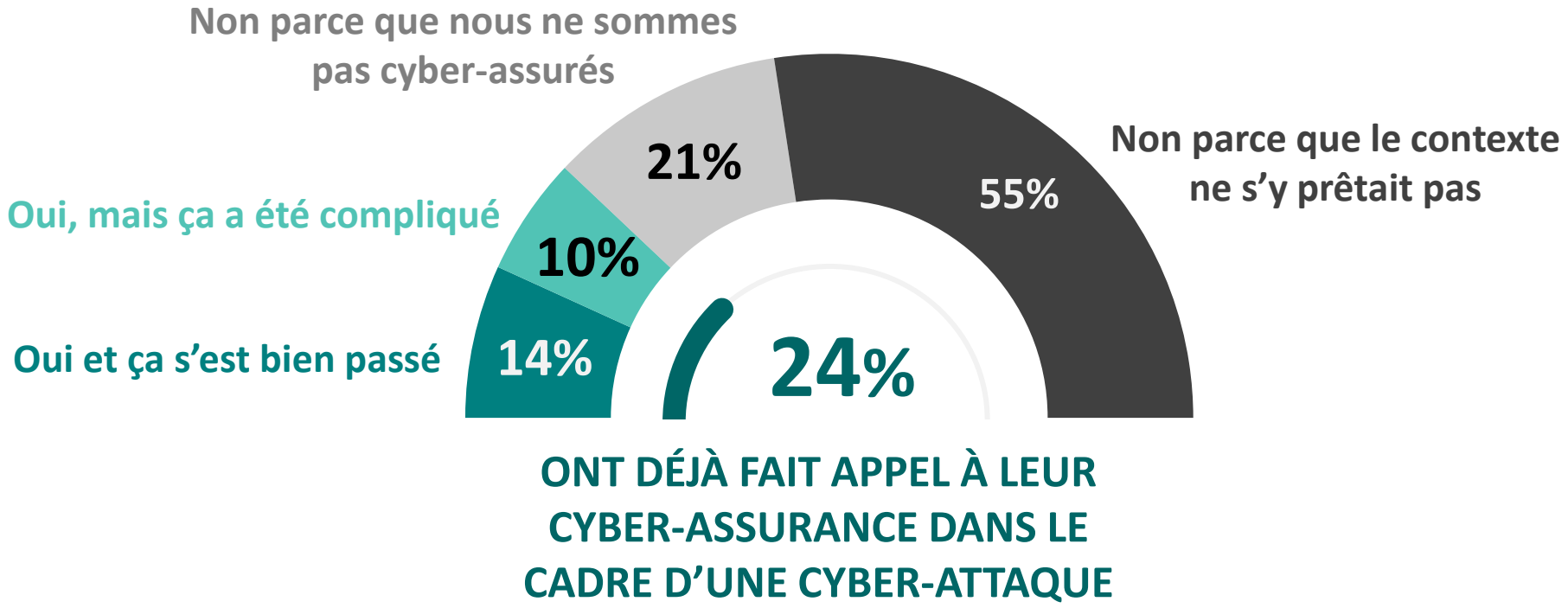
1 tiers des entreprises a mis en place un programme d'entraînement au cyber-risque et plus de la moitié compte le faire

Q15. Votre entreprise a-t-elle mis en place un programme d'entraînement à la cyber-crise ?
Base : ensemble (228 répondants)



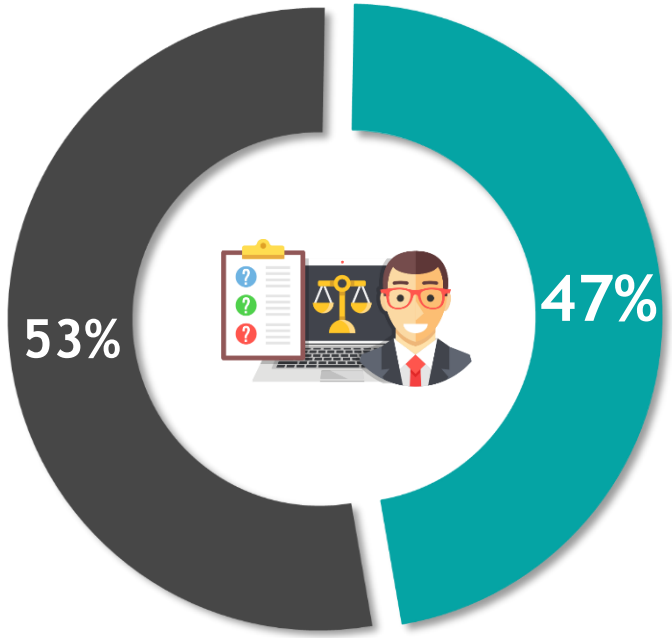
¼ des entreprises a déjà utilisé la cyber-assurance lors d'une attaque

Q16. Votre entreprise a-t-elle déjà fait appel à sa cyber-assurance dans le cadre d'une cyber-attaque ?
Base : ensemble (228 répondants)



Et la moitié de celles ayant subi une attaque ont porté plainte…

Q8. Avez-vous porté plainte à la suite de la cyber-attaque / des cyber-attaques dont votre entreprise a été victime ?
Base : ont constaté une attaque (129)

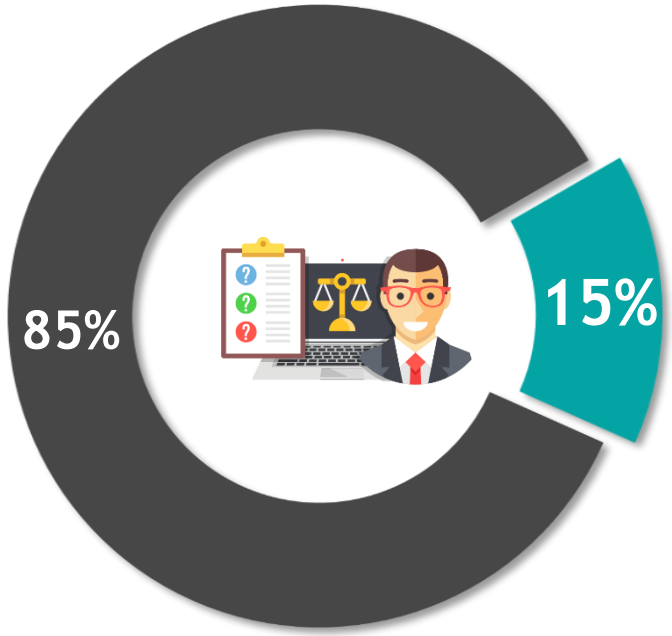


pour **toutes les attaques** : **12%**

pour **certaines attaques** : **35%**

…conduisant à l'identification des attaquants seulement une fois sur 10

Q8bis. Suite à votre ou vos plainte(s), l'enquête a-t-elle permis d'identifier et/ou d'interpeller le ou les attaquant(s) ?
Base : ont porté plainte (61)



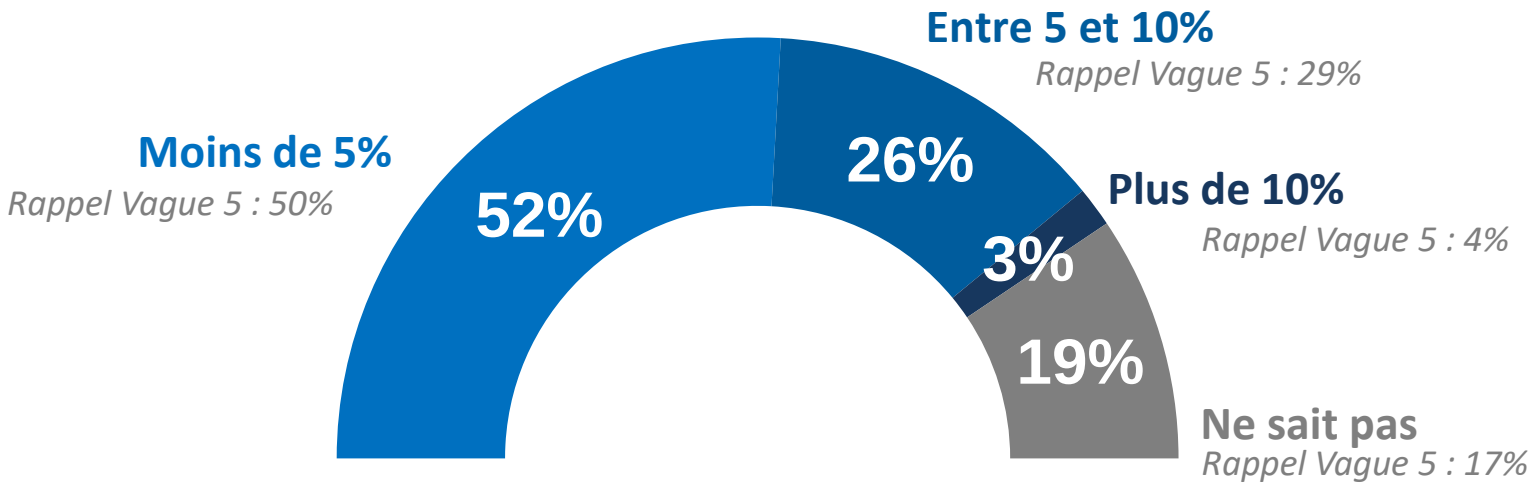
Oui, l'enquête a permis une identification

pour **toutes les plaintes**: **3%**

pour **certaines plaintes** : **12%**

La part du budget IT consacrée à la sécurité reste similaire à l'année dernière

Q18. Dans votre entreprise, quelle part du budget IT est consacrée à la sécurité ?
Base : ensemble (228 répondants)

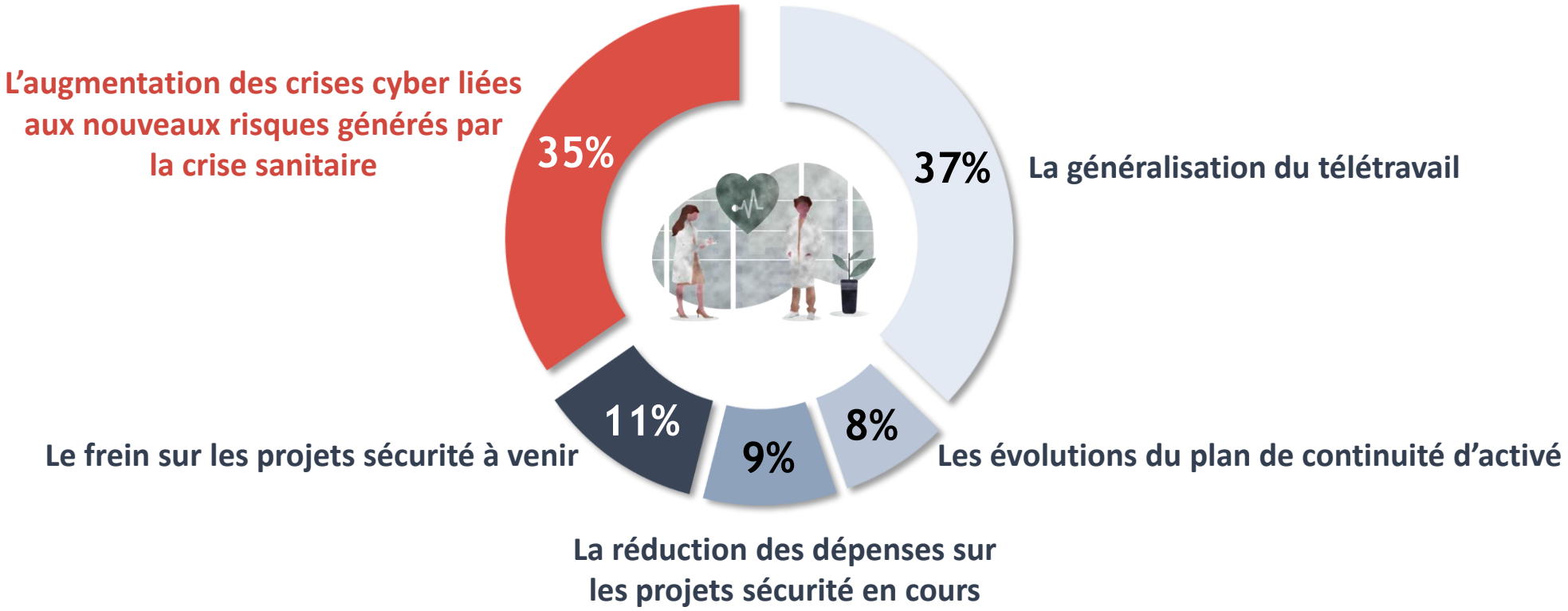


03

La crise sanitaire apporte de nouveaux risques

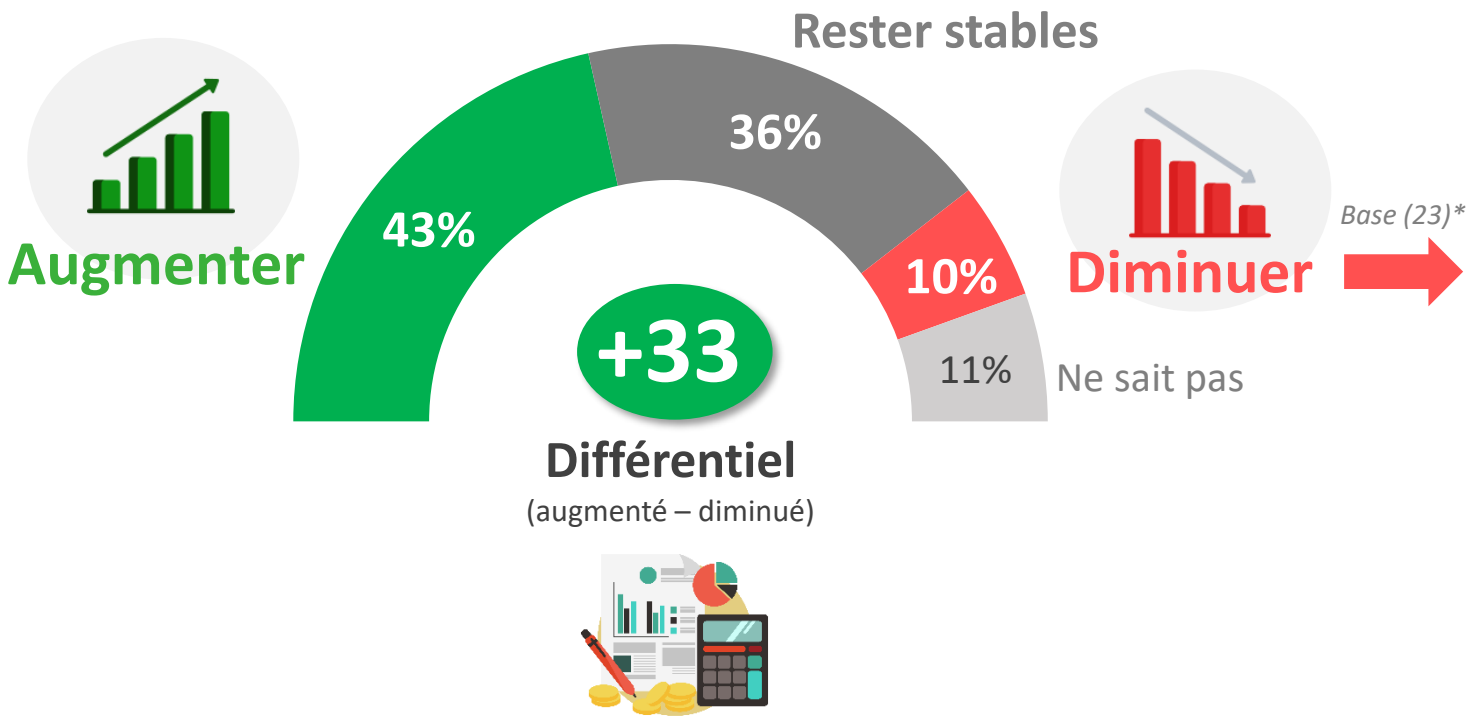
Le télétravail et l'augmentation des crises cyber sont les changements les plus impactants pour les entreprises pendant la crise sanitaire

Q1. Avec la crise sanitaire en cours, quel phénomène impacte le plus l'activité de cybersécurité de votre entreprise ?
Base : ensemble (228)



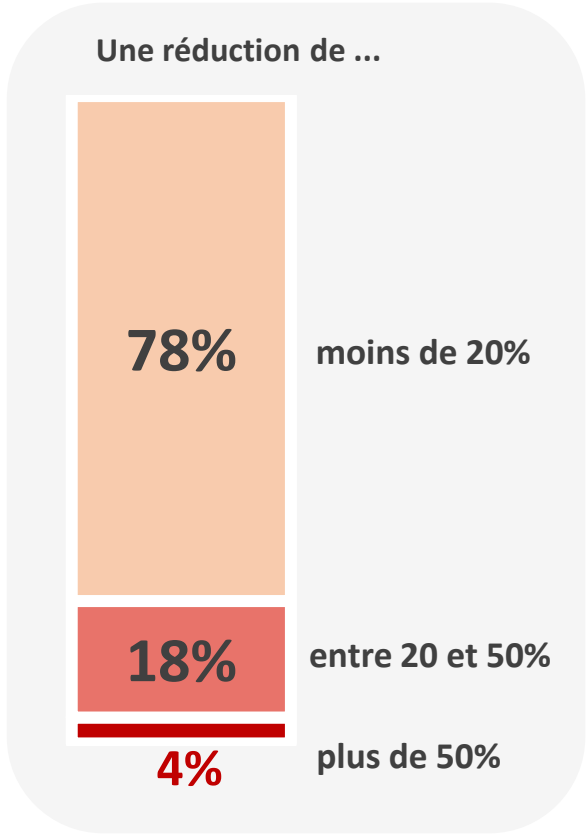
Poussant 2 entreprises sur 5 à augmenter les budgets cybersécurité pour 2021

Q2. En 2021, les budgets cybersécurité de votre entreprise vont-ils… ?
Base : ensemble (228)



Q2bis. De combien devraient diminuer les budgets cybersécurité en 2021 ?

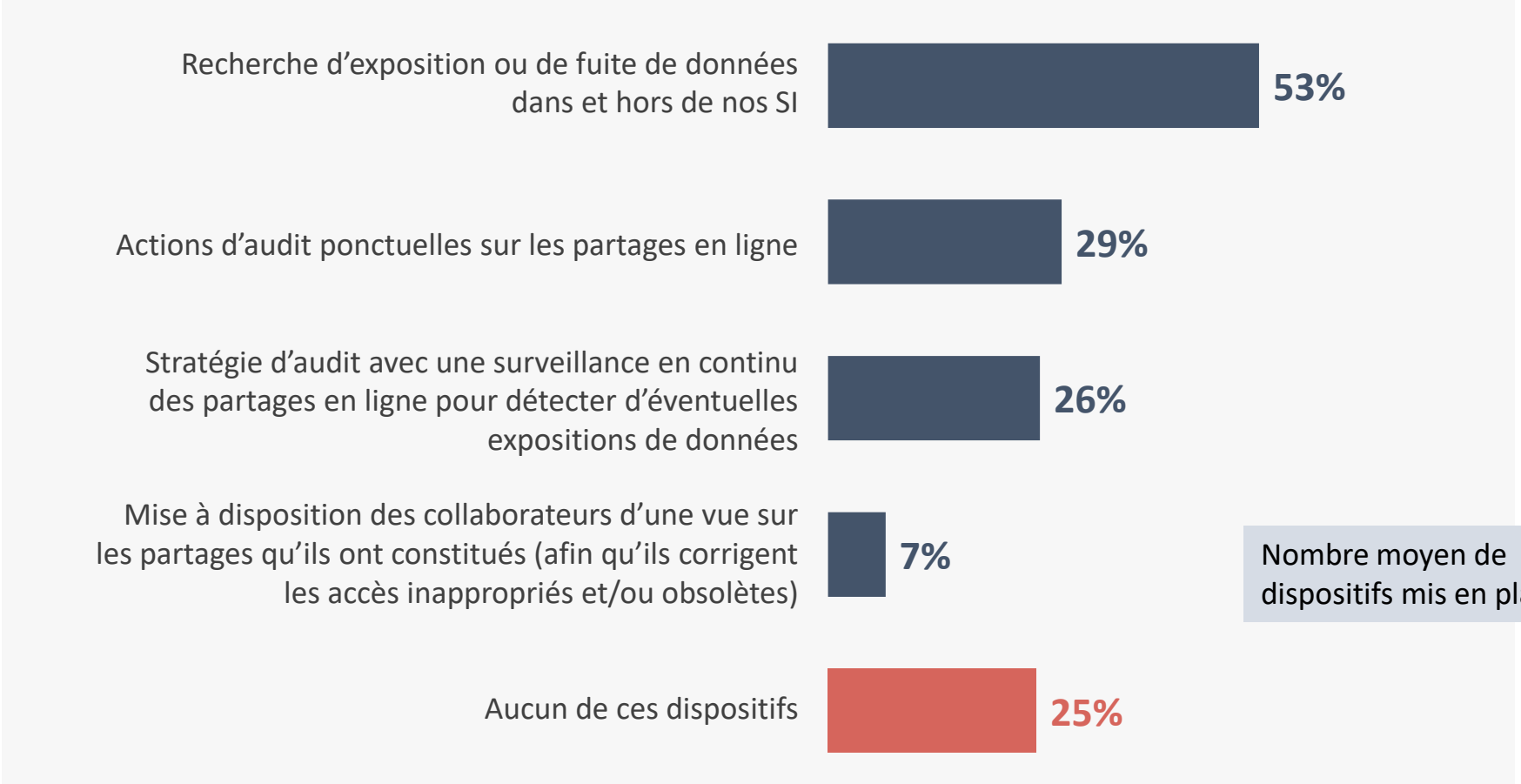
*Base (23)**



1 entreprise sur 2 a mis en place une recherche dans et hors des SI pour se prémunir de l'exposition ou de fuites de données

Q3. Votre entreprise a-t-elle mis en place les dispositifs suivants pour détecter l'exposition des données en ligne et/ou les fuites de données avérées ?

Base : ensemble (228)



04

Une sensibilisation des salariés en continu

Les ¾ des entreprises estiment que leurs salariés sont sensibilisés à la cybersécurité, mais que tous ne respectent pas les recommandations

Q19. En ce qui concerne la sensibilisation des salariés à la cybersécurité, pensez-vous qu'ils… ?

Base : ensemble (228 répondants)

77%

pensent que les salariés **sont sensibilisés** aux cyber-risques

63%

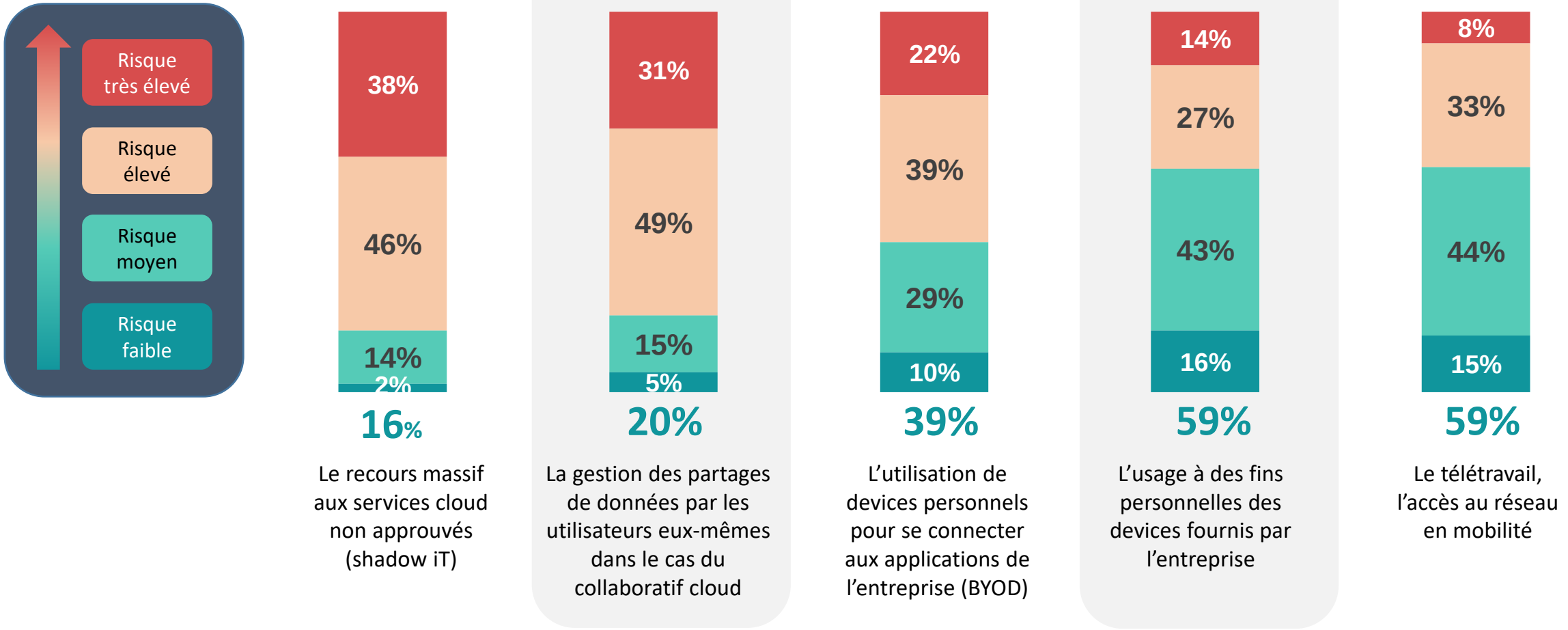
pensent que les salariés **respectent les recommandations**

16%

pensent que les salariés **prennent des précautions au-delà des recommandations** données

Les entreprises évaluent également des risques élevés dans l'usage numérique quotidien de leurs salariés, en particulier avec le Shadow IT et le Cloud

Q23. Comment évaluez-vous le niveau de risque induit par les usages suivants du numérique par les salariés ?
Base : ensemble (228 répondants)



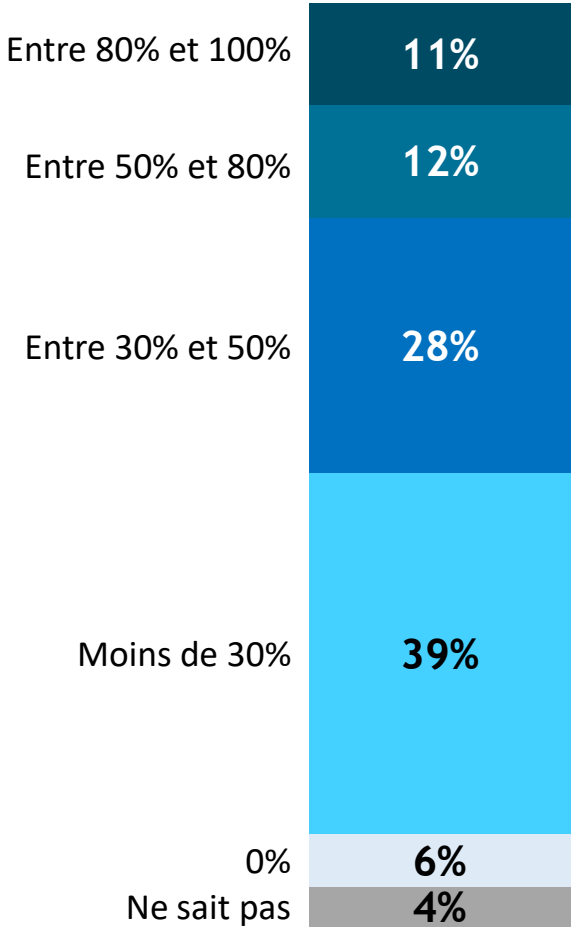
05

Le Cloud, environnement toujours à risques

La pénétration du cloud est effective chez la très grande majorité des entreprises

Q20. Quel est le degré de pénétration de votre SI dans le cloud, que ce soit en mode Iaas, Paas ou Saas ?

Base : ensemble (228 répondants)



La non-maîtrise et les difficultés des contrôles sont les principaux risques de l'utilisation du Cloud

Q21. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ?

Base : ensemble (228 répondants)

% Un risque fort

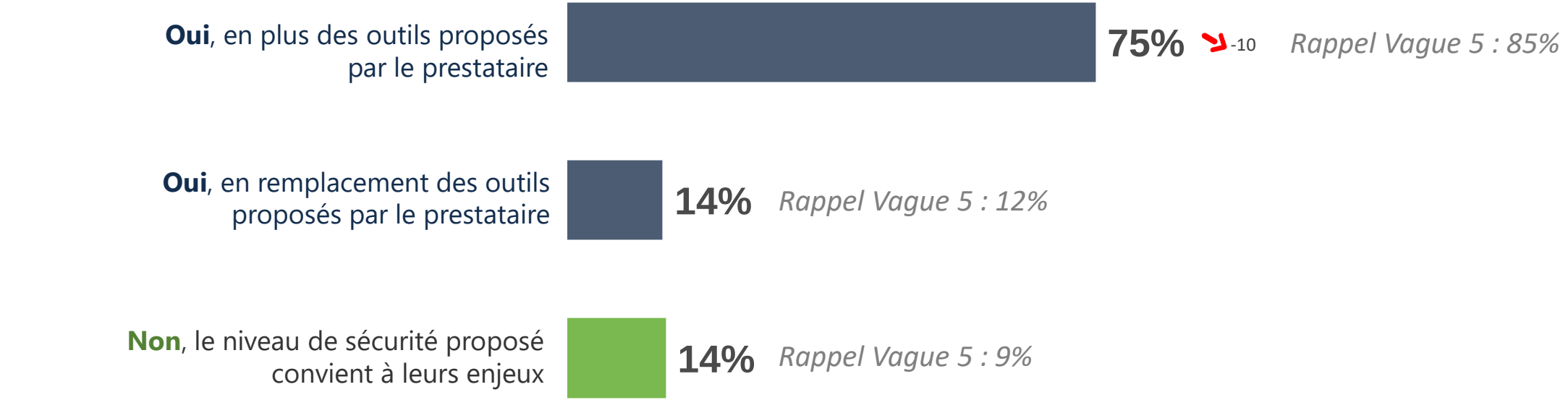
51%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
45%	**Difficulté de contrôler les accès par des administrateurs de l'hébergeur**
44%	**Non-maîtrise de l'utilisation qui en est faite par les salariés de votre entreprise**
41%	Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
38%	Stockage des données dans des datacenters à l'étranger, hors du droit français
38%	Confidentialité des données vis-à-vis de l'hébergeur
36%	Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur
33%	Forte fréquence des nouvelles versions mises en ligne avec contrôles et potentielles évolutions non contrôlées des principes de sécurité
31%	Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant du Cloud
31%	Stockage des données en France mais assuré et/ou opéré par des prestataires étrangers où la loi du pays d'origine s'applique également
28%	Propagation systémique des attaques et erreurs humaines
28%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur
28%	Défaut de cloisonnement entre les différents clients de l'hébergeur
27%	Non-effacement des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
25%	Non-effacement des données au cours de l'usage, les suppressions et purges opérées par le client n'étant pas réellement effectives
23%	Attaque par rebond depuis l'hébergeur
22%	Traitement et exploitation des données par l'hébergeur à l'insu de ses clients
20%	Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
17%	Piégeage d'une application hébergée

Pour près de 9 entreprises sur 10, la sécurisation des données du Cloud nécessite des outils spécifiques, autres que ceux fournis par les prestataires

Q22. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble (228 répondants)

... 86% estiment que la sécurisation des données stockées dans le Cloud requiert des outils ou dispositifs spécifiques

Rappel Vague 5 : 91%



Évolution statistiquement significative par rapport à la vague précédente

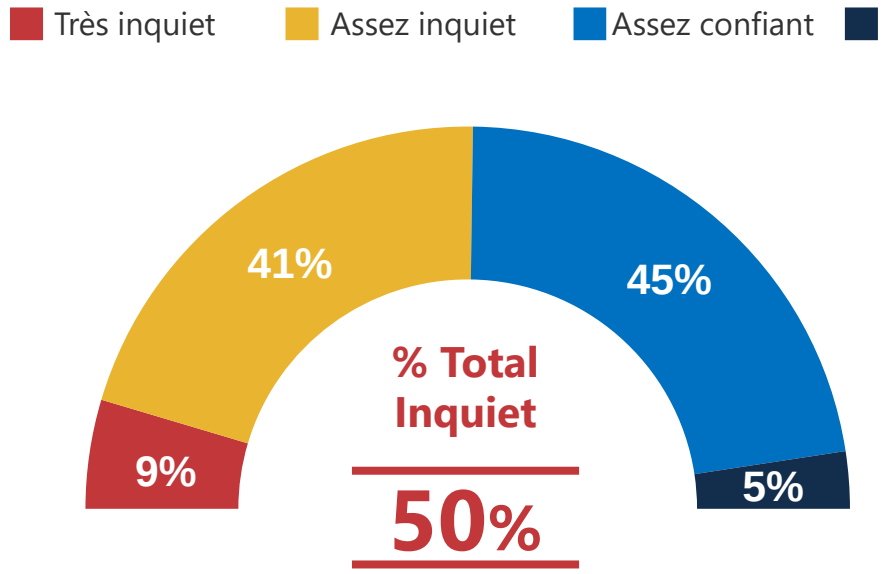
06

Des entreprises inquiètes, mais clairvoyantes sur les enjeux de demain

1 entreprise sur 2 est inquiète quant à sa capacité à faire face aux cyber-risques

Q24. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (228 répondants)

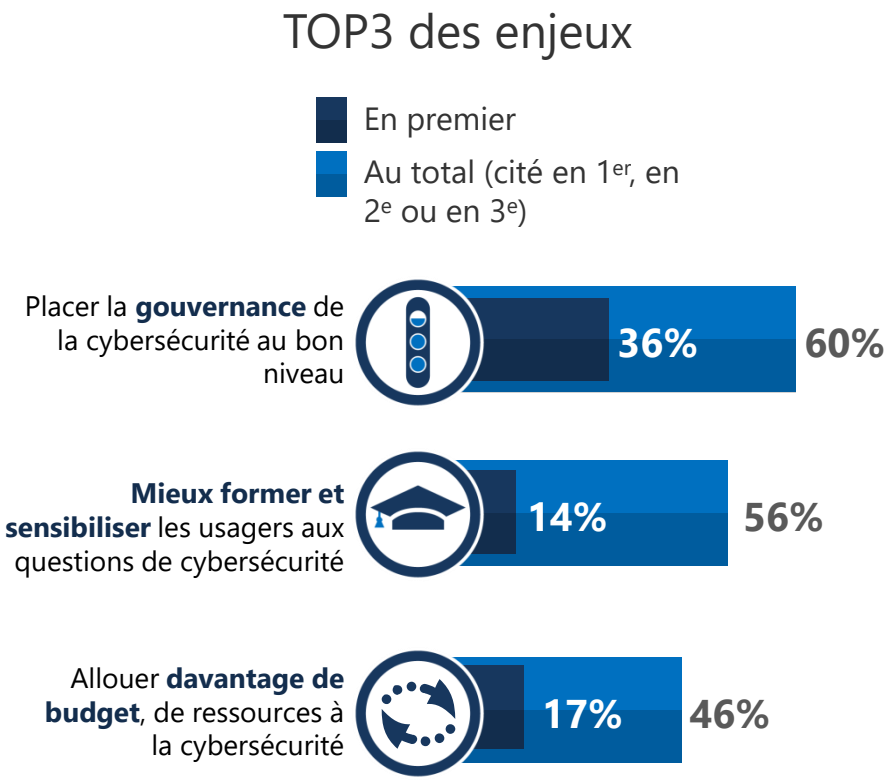
La **capacité** de votre entreprise à faire face aux cyber-risques

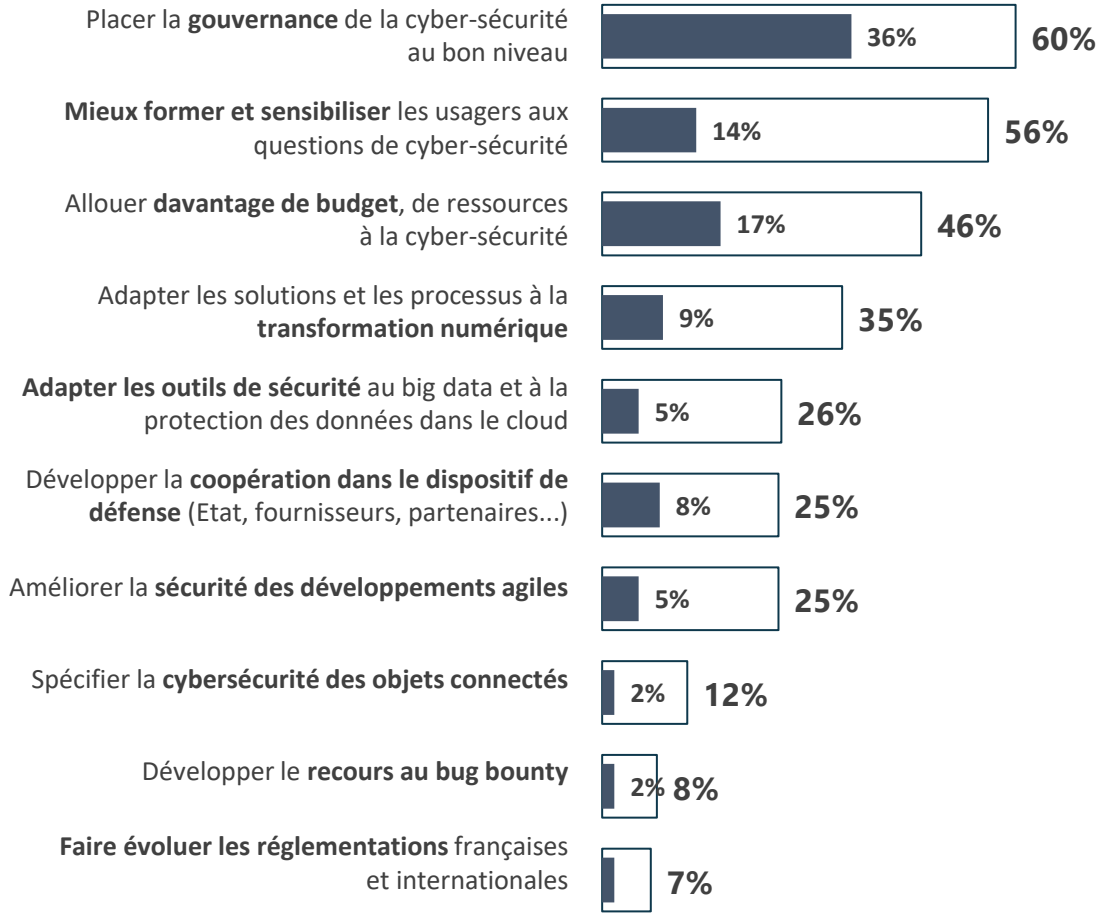


Rappel Vague 5 : 48%

Similairement aux années précédentes, l'enjeu humain est la priorité des entreprises

Q27. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cybersécurité des entreprises ?
Base : ensemble (228 répondants)

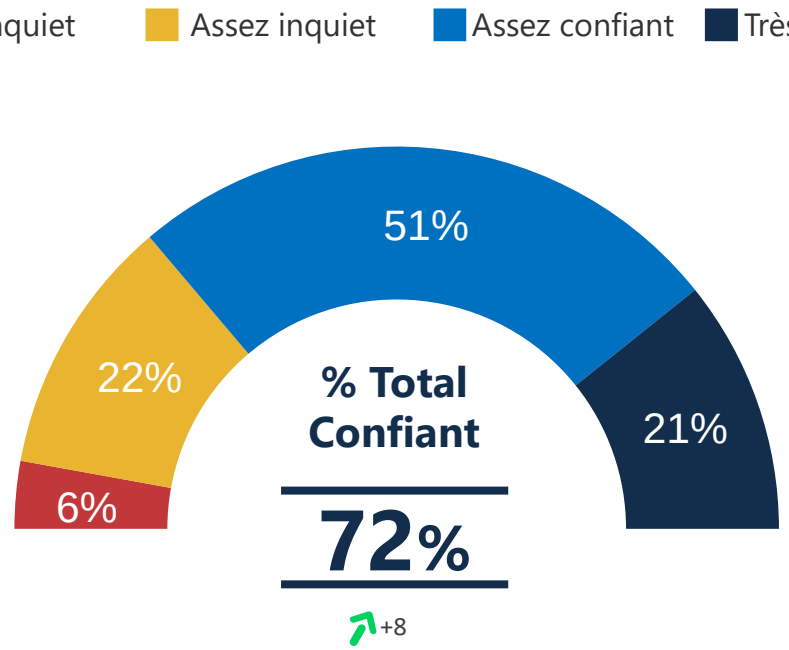




Les entreprises prennent de plus en plus conscience de l'importance de la cybersécurité dans la stratégie

Q24. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (228 répondants)

La **prise en compte des enjeux** de la cybersécurité au sein du COMEX votre entreprise



Rappel Vague 5 : 64%

Évolution statistiquement significative par rapport à la vague précédente

Ce qui explique que plus de la moitié d'entre elles comptent augmenter les budgets et les effectifs liés à la cybersécurité.

Q17. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?

Base : ensemble (228 répondants)

d'**augmenter les budgets** alloués à la protection contre les cyber-risques

Rappel Vague 5 : 62%

d'**augmenter les effectifs** alloués à la protection contre les cyber-risques

Rappel Vague 5 : 51%

Plus de 8 entreprises sur 10 souhaitent acquérir de nouvelles solutions techniques pour se prémunir des cyber-risques

Q17. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?

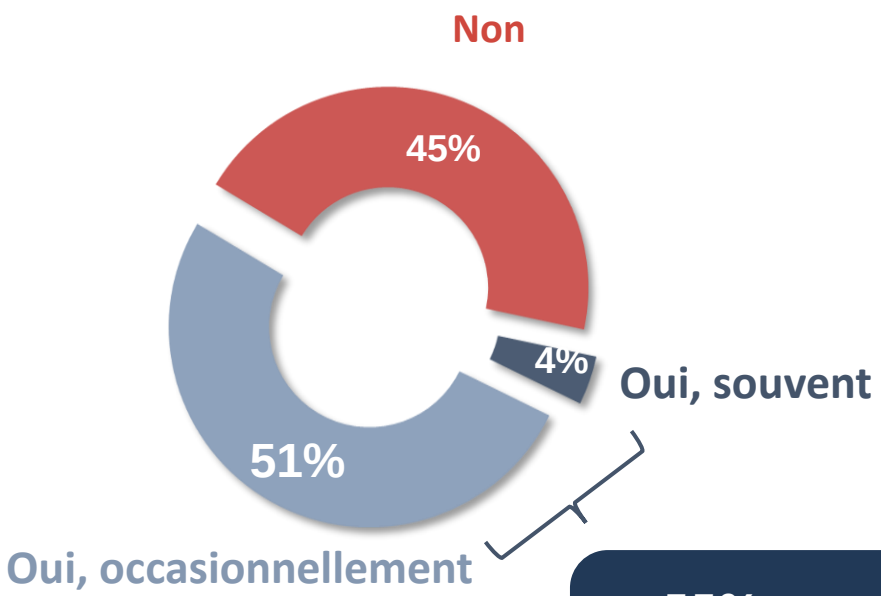
Base : ensemble (228 répondants)

d'**acquérir de nouvelles solutions techniques** destinées à la cybersécurité

Rappel Vague 5 : 83%

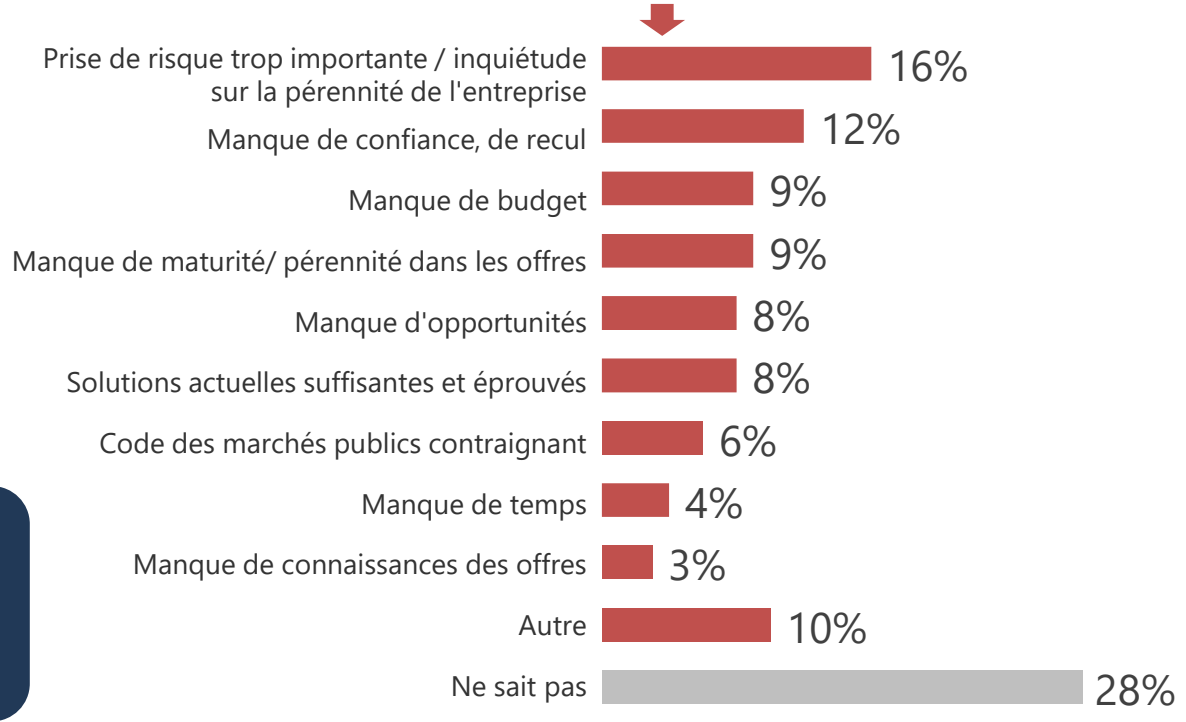
Et plus de la moitié des entreprises ont recours à des offres innovantes

Q26. En matière de cybersécurité, recourrez-vous à des offres innovantes issues de start-up ? *Base : ensemble (228)*
Q26bis. Pour quelle(s) raison(s) ne le faites-vous pas ? *Base : ne fais pas appel à des offres issues de start-up (102)*



55% ont recours à des offres innovantes issues de start-up

45% n'ont pas recours à ces offres



WE ARE DIGITAL !

Fondé en 2000 sur cette idée radicalement innovante pour l'époque, OpinionWay a été précurseur dans le renouvellement des pratiques de la profession des études marketing et d'opinion.

Forte d'une croissance continue depuis sa création, l'entreprise n'a eu de cesse de s'ouvrir vers de nouveaux horizons pour mieux adresser toutes les problématiques marketing et sociétales, en intégrant à ses méthodologies le Social Média Intelligence, l'exploitation de la smart data, les dynamiques créatives de co-construction, les approches communautaires et le storytelling.

Aujourd'hui OpinionWay poursuit sa dynamique de croissance en s'implantant géographiquement sur des zones à fort potentiel que sont l'Europe de l'Est et l'Afrique.

Rendre le monde intelligible pour agir aujourd'hui et imaginer demain

C'est la mission qui anime les collaborateurs d'OpinionWay et qui fonde la relation qu'ils tissent avec leurs clients.

Le plaisir ressenti à apporter les réponses aux questions qu'ils se posent, à réduire l'incertitude sur les décisions à prendre, à tracker les insights pertinents et à co-construire les solutions d'avenir, nourrit tous les projets sur lesquels ils interviennent.

Cet enthousiasme associé à un véritable goût pour l'innovation et la transmission expliquent que nos clients expriment une haute satisfaction après chaque collaboration - 8,9/10, et un fort taux de recommandation – 3,88/4.

Le plaisir, l'engagement et la stimulation intellectuelle sont les trois mantras de nos interventions.

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN

RESTONS CONNECTÉS !

www.opinion-way.com

Envie d'aller plus loin ?

Recevez chaque semaine nos derniers résultats d'études dans votre boite mail en vous abonnant à notre newsletter !