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

Baromètre de la cyber-sécurité des entreprises

Vague 5 – Janvier 2020

Contact presse :
AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 - vloquet@alx-communication.com

OpinionWay, 15 place de la République, 75003 Paris

Sommaire

CESIN

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.

MÉTHODOLOGIE

Méthodologie

Méthodologie

Étude quantitative réalisée par OpinionWay auprès de **253 membres du CESIN**, à partir du fichier des membres du CESIN (634 contacts).

Mode d'interrogation

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

Dates de terrain

Du **2 décembre 2019** au **7 janvier 2020**.

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 (1/3)

Les enseignements à retenir

1. Des entreprises qui se protègent de plus en plus….

Seulement 39% des entreprises se disent être suffisamment préparées en cas de cyber-attaques de grande ampleur, mais **elles se protègent mieux** avec environ 12 solutions mises en place. L'ensemble de **ces solutions sont jugées adaptées** aux besoins des entreprises (83%).

Quatre entreprises sur dix choisissent par ailleurs de faire appel à des solutions innovantes ou proposées par des start-up. Celles qui n'y ont pas recours mettent toutefois en avant le manque de maturité de ces solutions.

Les entreprises, conscientes des risques, sont **91% à mettre en place un programme de cyber-résilience** ou à envisager de le faire, **soit 12 points de plus** que l'année dernière. Elles sont également **plus nombreuses à avoir souscrit une cyber-assurance** (60% contre 50% en janvier 2019)

2. … et donc moins impactées par les cyber-attaques

Le taux d'entreprises déclarant des cyber-attaques est en baisse cette année : 65% en ont connu au moins une contre 80% l'année dernière. Les cyber-attaques **ont malgré tout un impact sur le business** similaire à l'année dernière (57%), provoquant principalement des perturbations sur la production.

Les grands types d'attaques subies par les entreprises : **l'attaque par phishing (79%), et l'arnaque au président (47%)**. L'usurpation d'identité (35%) et l'infection par un malware (34%) sont les conséquences directes de ces cyber-attaques.

Le cyber-risque le plus répandu est **la négligence ou l'erreur de manipulation ou de configuration d'un salarié (43%).**

Messages clés (2/3)

Les enseignements à retenir

3. IA et Cloud : des risques potentiels

89% des entreprises utilisent le cloud pour stocker une partie de leurs données, **55% le font avec le cloud public**. Cet outil de stockage pose cependant des risques, les plus forts étant **la non-maîtrise de la chaîne de sous-traitance de l'hébergeur (50%), la difficulté de mener des audits (46%), et la non-maîtrise de l'utilisation du cloud par les salariés (46%)**. Pour pallier ce manque de sécurité, **91% des entreprises estiment que des outils et/ou dispositifs spécifiques doivent être mis en place ce qui interroge sur la pertinence des outils de sécurité proposés par les acteurs du cloud.**

Une minorité d'entreprises utilise des solutions qui présentent de la technologie IA, le frein étant le **faible niveau de confiance (47%)** envers cette approche.

4. Des salariés qui gagneraient à être mieux mobilisés

D'après les RSSI, les usages numériques réalisés par les salariés présentent des risques **(shadow IT : 98%).** Les salariés sont pourtant **sensibilisés aux cyber-risques (74%)** mais manquent visiblement d'implication. D'après les RSSI, ils sont seulement la moitié à respecter les recommandations. Pour tenter de mobiliser les salariés plus durablement, **77% des entreprises ont mis en place des procédures pour tester l'application des recommandations par les salariés.**

5. En termes d'approche, le Zero Trust fait une entrée timide dans l'agenda du RSSI

Une majorité de RSSI reste circonspects face à l'approche Zero Trust en dépit de son battage médiatique. Seulement 16 % d'entre eux ont véritablement travaillé sur le modèle tandis qu'un petit tiers y réfléchit.

CESIN

Messages clés (3/3)

Bilan

Des entreprises qui se disent peu confiantes au final, en étant bien conscientes des efforts qui restent à fournir

Près d'une entreprise sur deux se dit inquiète quant à sa capacité à faire face aux cyber-risques.

Parmi les enjeux de demain pour cyber-sécuriser les entreprises, ceux concernant le **budget** mais surtout **l'humain** sont une nouvelle fois à privilégier.

- **La gouvernance** est le premier enjeu de demain (70%, soit **10 points de plus** que l'année dernière), vient ensuite **la formation et la sensibilisation des utilisateurs** (57%). Les ressources humaines sont une demande des entreprises : la moitié veut **augmenter ses effectifs de cybersécurité, mais** 9 sur 10 se heurtent toutefois **à une pénurie de profil SSI**, en particulier sur les métiers de pilotage, d'organisation et de gestion des risques.
- **L'augmentation du budget** (50%) est un autre enjeu majeur. La part du budget IT consacré à la sécurité augmente dans les entreprises, et devrait continuer d'augmenter puisque 62% d'entre-elles indiquent **vouloir allouer plus de ressources à la cybersécurité** et 83% souhaitent **acquérir de nouvelles solutions techniques.**

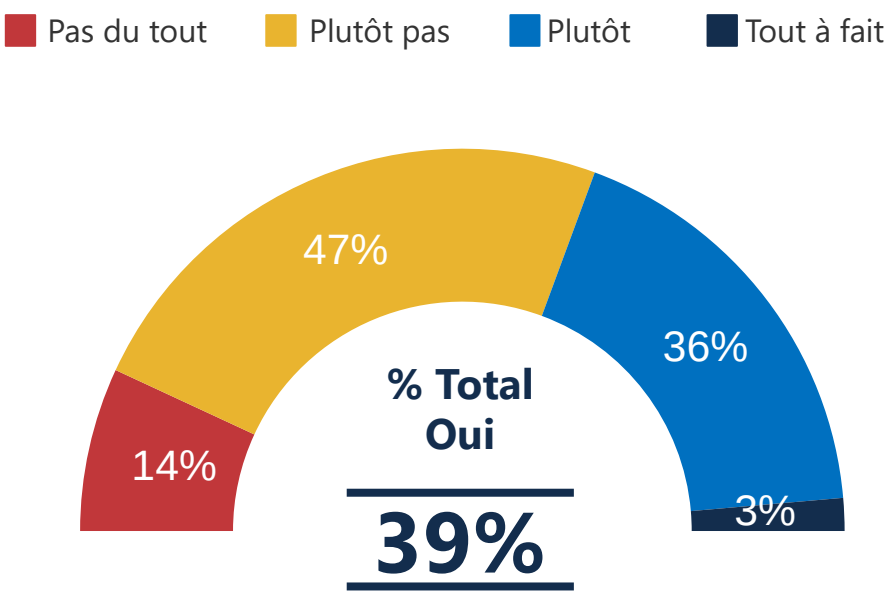
CESIN

RÉSULTATS

1. DES ENTREPRISES QUI SE PROTÈGENT DE PLUS EN PLUS

Seules 4 entreprises sur 10 se disent préparées en cas de cyber-attaque de grande ampleur

Q38. Selon vous, votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur ?
Base : ensemble (253)

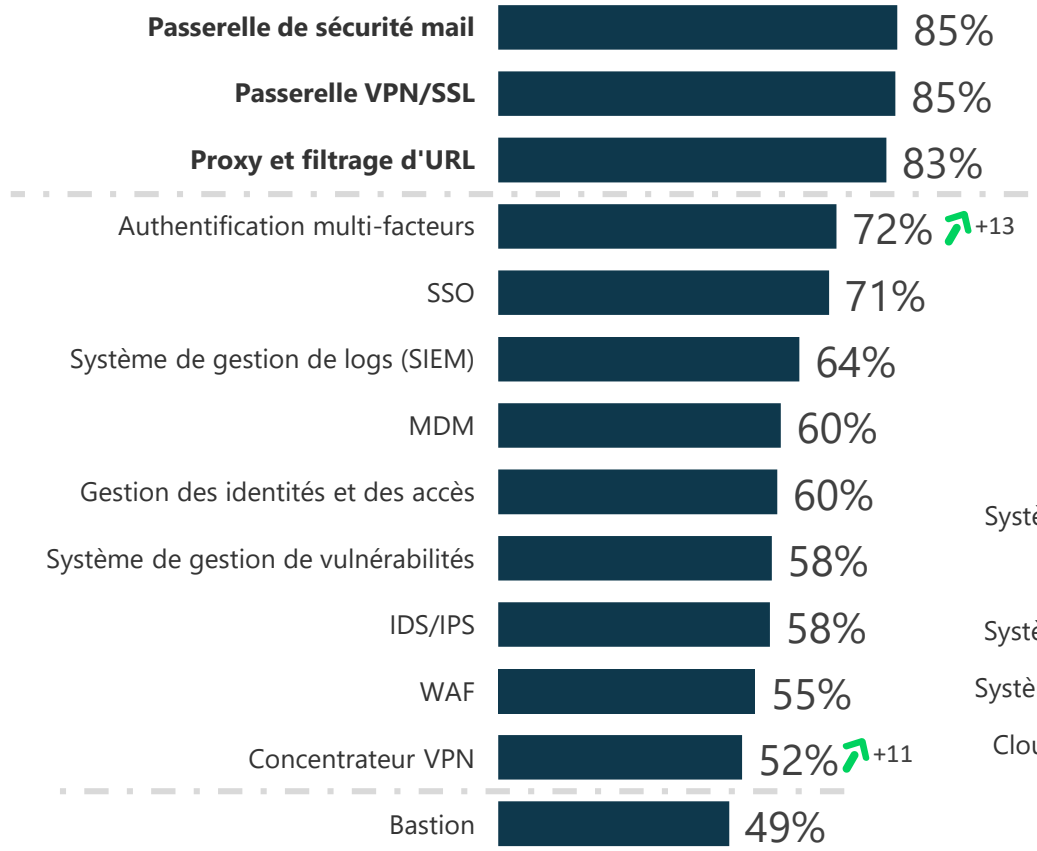


Évolution statistiquement significative vs. 01/2019

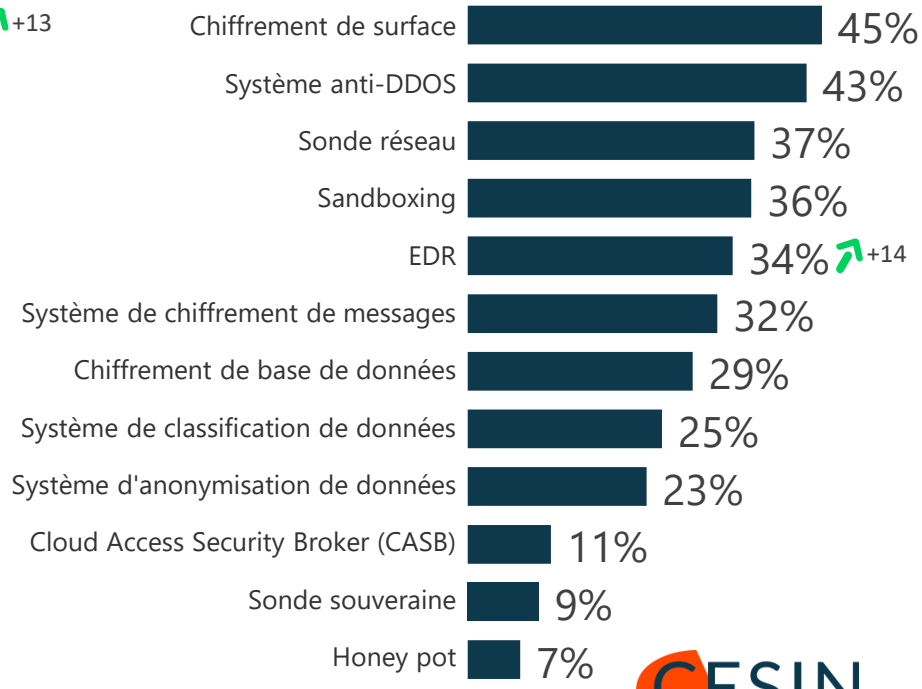
Pour cela, une douzaine de solutions sont mises en place pour prévenir les risques d'attaques,

à noter la hausse des solutions d'authentification multi-facteurs et EDR

Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ? *Base : ensemble (253 répondants) / Plusieurs réponses possibles*



11,9 solutions en moyenne



CESIN

Évolution statistiquement significative vs. 01/2019

Les offres innovantes issues de start-up séduisent 4 entreprises sur 10

Q45. En matière de cyber-sécurité, recourrez-vous à des offres innovantes issues de start-up ? *Base : ensemble (253 répondants)*
Q45b. Pour quelles raisons ne le faites-vous pas ? *Base : ne fait pas appel à des offres issues de start-up (148 répondants)*

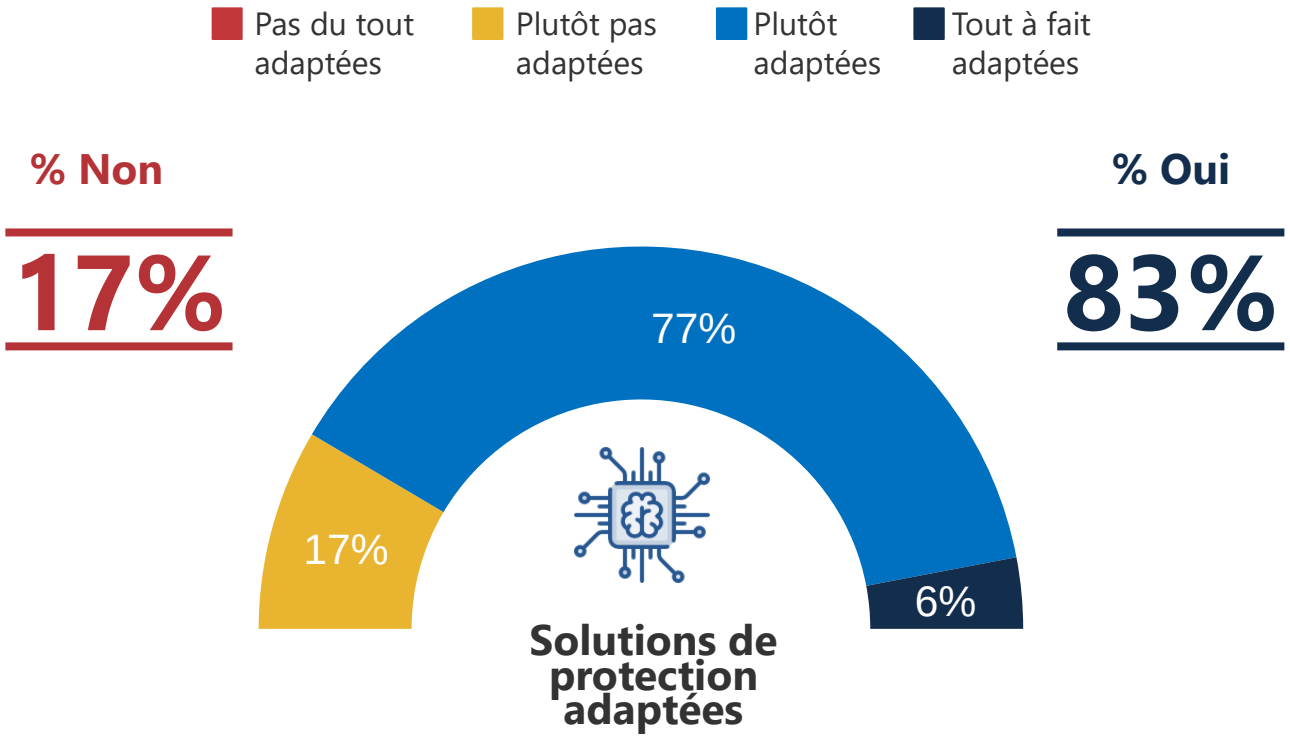
Ont recours à des offres innovantes issues de start-up

58% n'ont pas recours à ces offres

Nouvelles questions

Les entreprises sont majoritaires à considérer les solutions proposées sur le marché comme adaptées

Q29. 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 (253 répondants)*



Modalité de réponses modifiées par rapport à la vague précédente du baromètre

En parallèle des solutions de protection, le nombre d'entreprises qui ont mis ou envisagent de mettre en place un programme de cyber-résilience augmente

Q39. Votre entreprise a-t-elle mis en place un programme de cyber-résilience ?
Base : ensemble (253 répondants)

91% ↗ +12 **ont mis en place un programme de cyber-résilience ou envisagent de le faire**

19%

ont déjà un programme de cyber-résilience **en place**

36%

La mise en place du programme est **en cours**

36%

envisagent de mettre en place un programme de cyber-résilience

Pour 9%, ce n'est pas en projet.

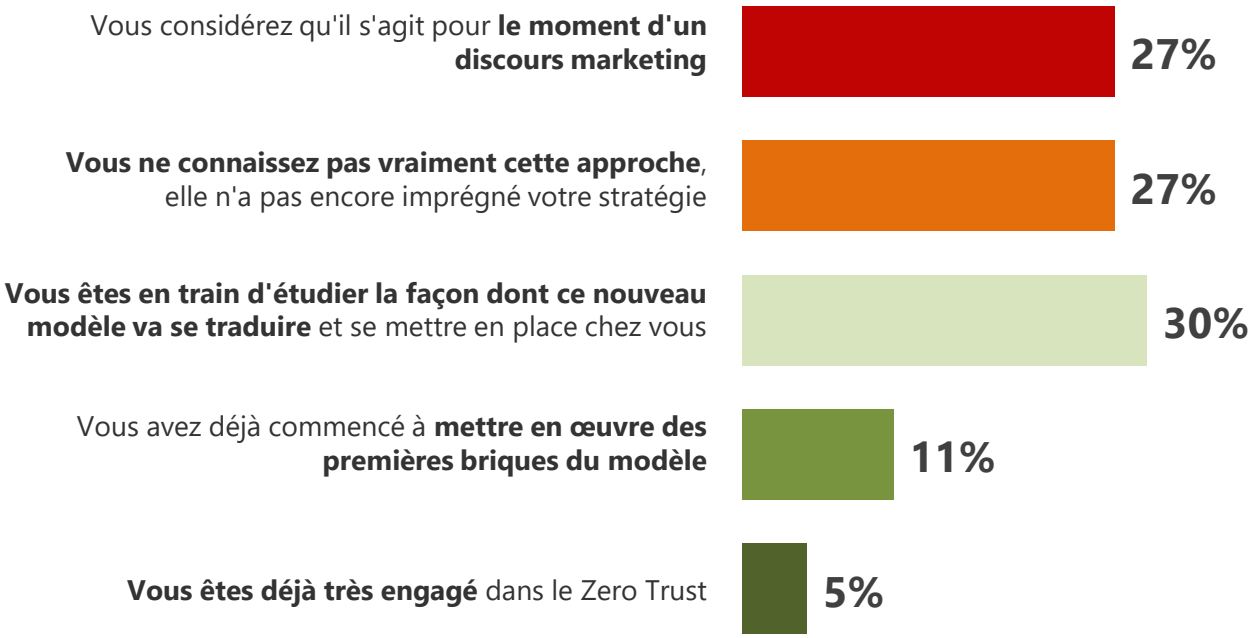
↘ -12

↗ ↘ Évolution statistiquement significative vs. 01/2019

CESIN

Une défiance non-négligeable vis-à-vis du concept Zero Trust, même si un peu plus d'une entreprise sur dix a déjà commencé à mettre en œuvre le concept

Q50. Quelle est votre opinion et votre appétence pour le concept Zero Trust?
Base : ensemble (253 répondants) / Plusieurs réponses possibles



Nouvelle question

Elles sont également plus nombreuses à avoir souscrit une cyber-assurance par rapport à l'année dernière

Q9. Par ailleurs, votre entreprise a-t-elle souscrit une cyber-assurance ?
Base : ensemble (253 répondants)

60% ↗ +10

ont souscrit une cyber-assurance

13%

souscription **en cours**

11% ↘ -7

envisagent de souscrire à plus long terme

↗↘ Évolution statistiquement significative vs. 01/2019

2. DES ENTREPRISES IMPACTÉES MOINS FORTEMENT PAR DES CYBER-ATTAQUES

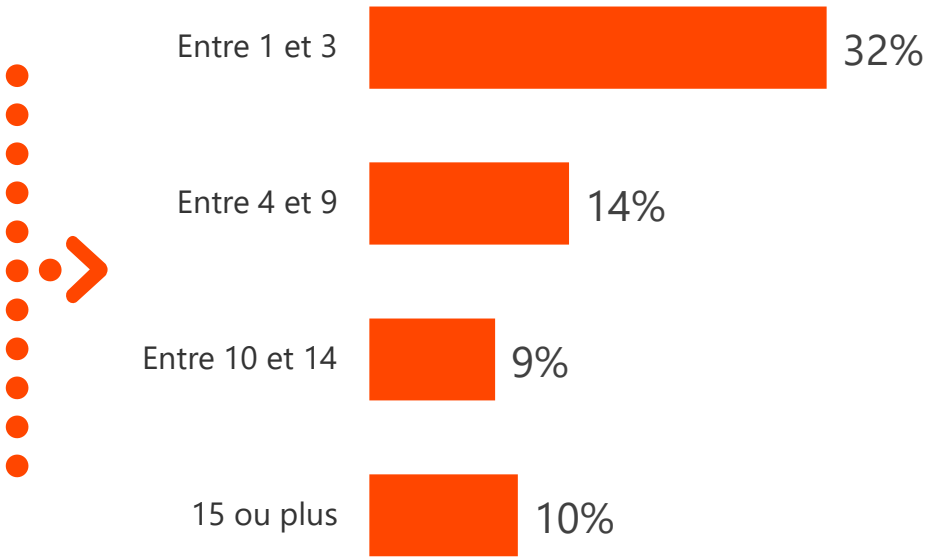
2 entreprises sur 3 déclarent avoir constaté au moins une cyber-attaque

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (253 répondants)

Définition donnée pour cette vague 5 : *« La cyber-attaque 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 entrainant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise. »*

65%

des entreprises ont constaté au moins une cyber-attaque



Rappel vague 4 : 80%
(mais la définition donnée cette année n'était pas précisée)

Le nombre de cyber-attaques par entreprise ne diminue pas

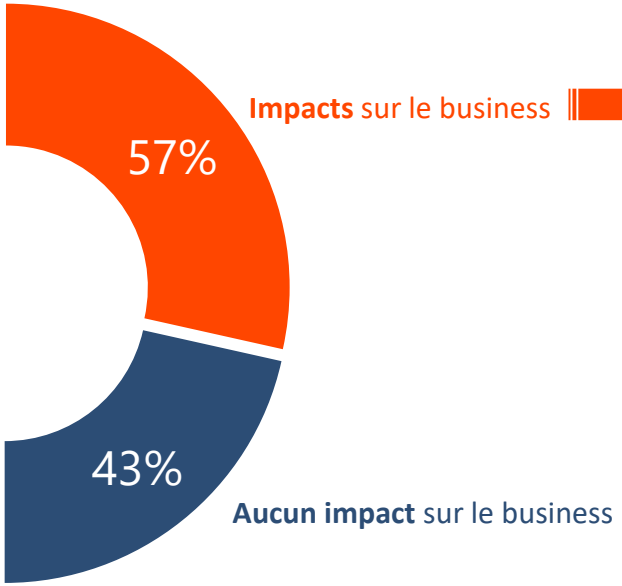
Q5BIS. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ?
Base : ensemble (253 répondants)

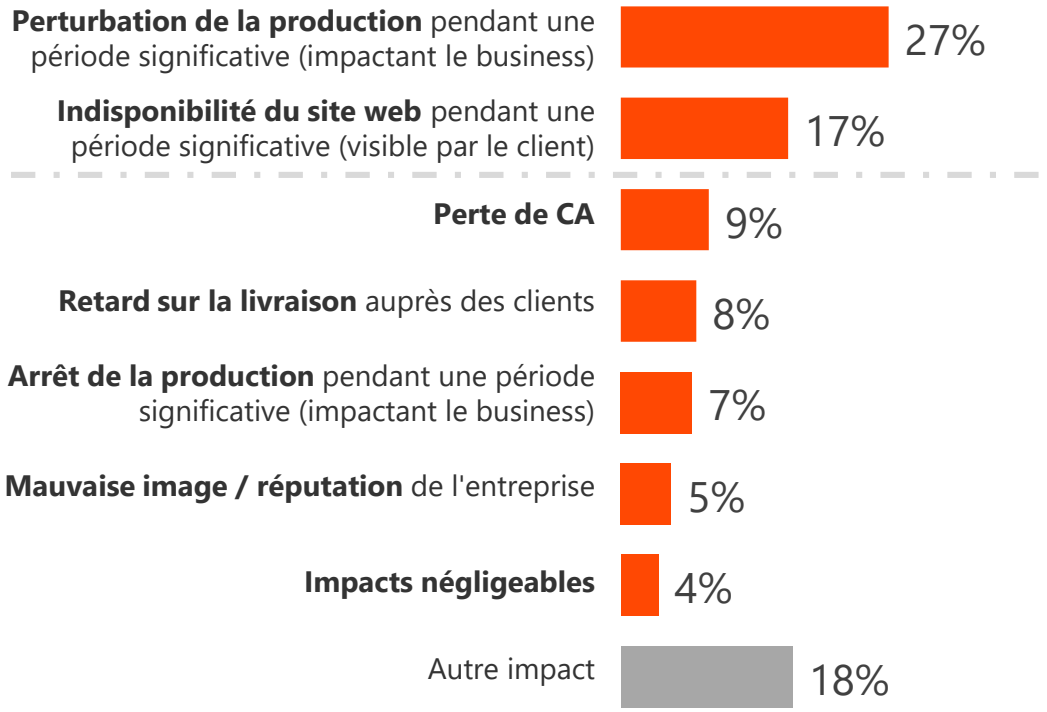
En un an, le nombre d'attaques…

Évolution statistiquement significative vs. 01/2019

Les cyber-attaques impactent en premier lieu la production

Q30. Quel a été l'impact des cyber-attaques sur votre business ?
Base : ont constaté une attaque et une cause d'incidents de sécurité (234 répondants) / Plusieurs réponses possibles



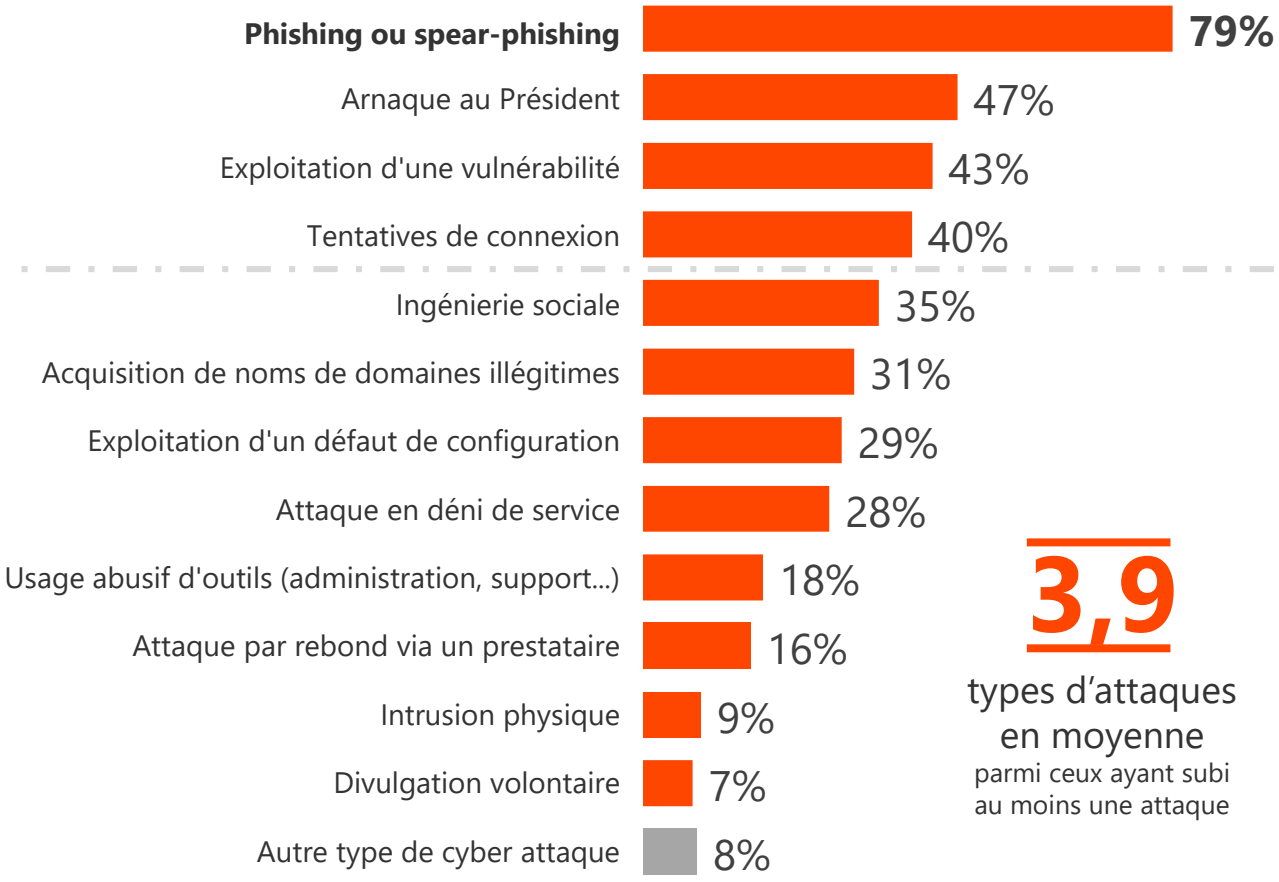


Évolution statistiquement significative vs. 01/2019

Le phishing reste en tête des vecteurs d'attaques constatées suivi par l'arnaque au président

Q6C. Parmi les vecteurs d'attaques suivants, lesquels ont impactés votre entreprise au cours des 12 derniers mois ?

Base : ont constaté une attaque (163 répondants) / Plusieurs réponses possibles



3,9

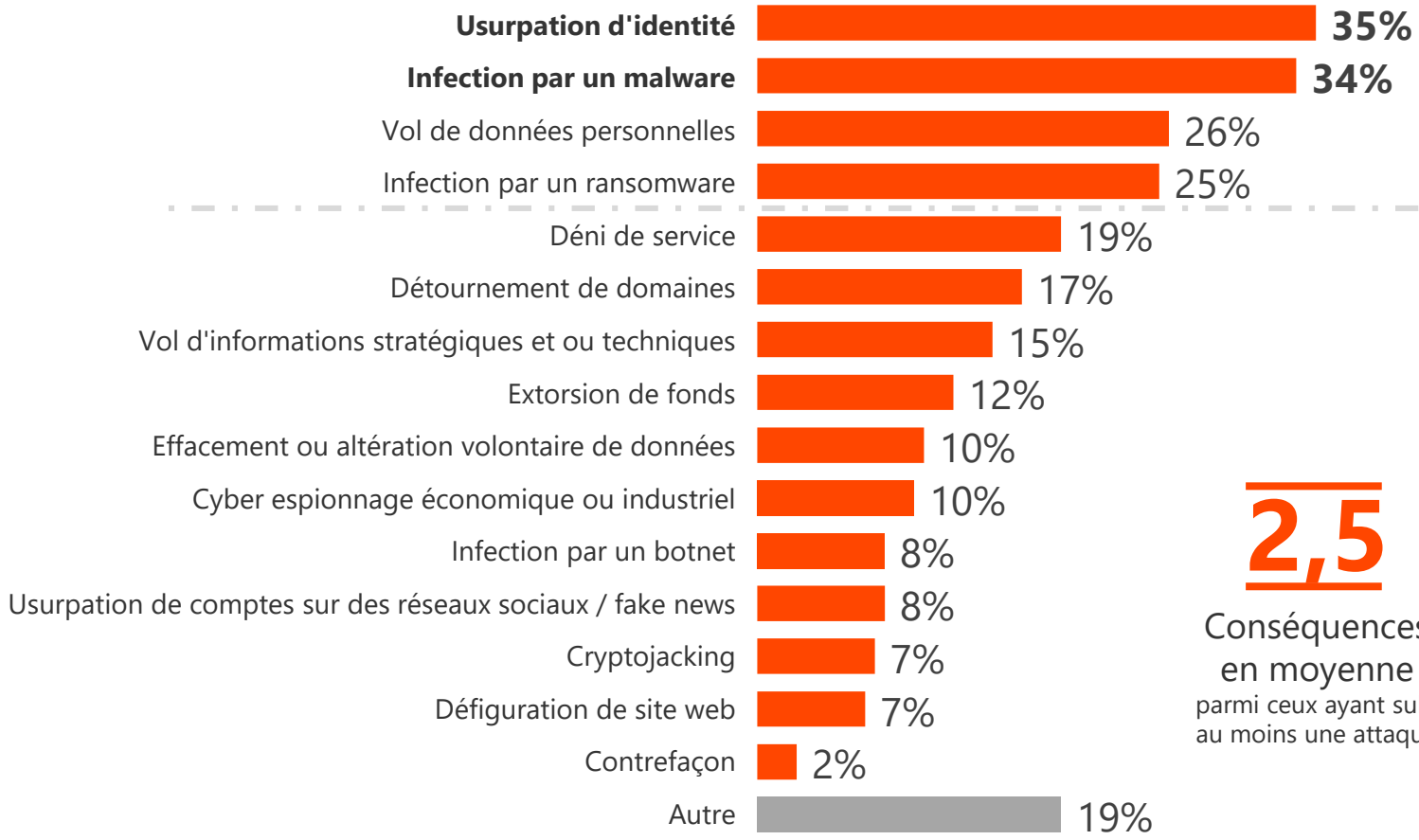
types d'attaques en moyenne

parmi ceux ayant subi au moins une attaque

Nouvelle question

L'usurpation d'identité et l'infection par malware sont les conséquences les plus fréquentes

Q6D. Et quelles ont été les conséquences de cette / ces attaques ?
Base : ont constaté une attaque (163 répondants) / Plusieurs réponses possibles



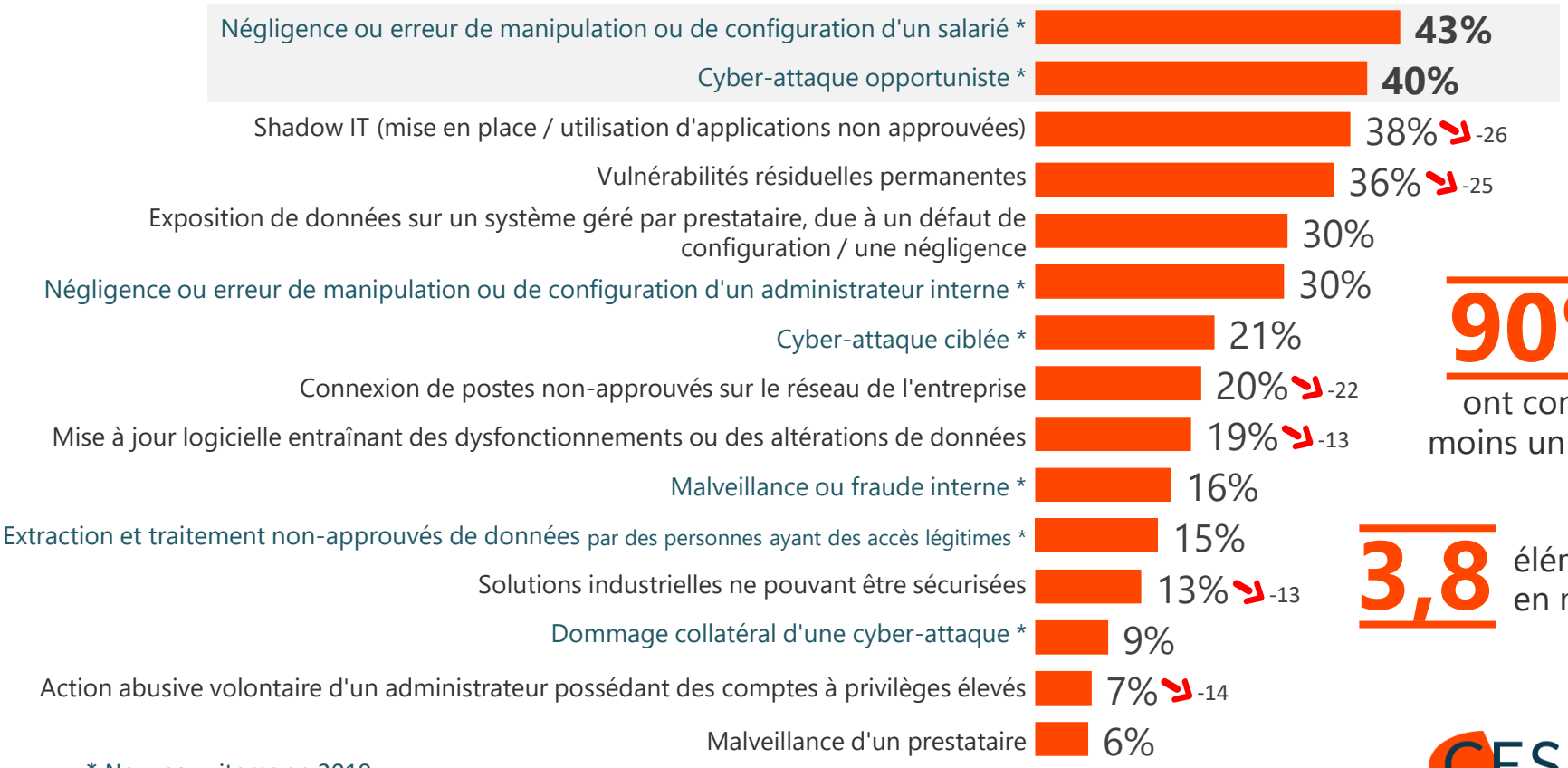
2,5

Conséquences en moyenne
parmi ceux ayant subi au moins une attaque

Nouvelle question

En lien avec la cyber-sécurité, la négligence des salariés est relevée par près de la moitié des entreprises

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 ? *Base : ensemble (253 répondants) / Plusieurs réponses possibles*



90% ont connu au moins un élément

3,8 éléments en moyenne

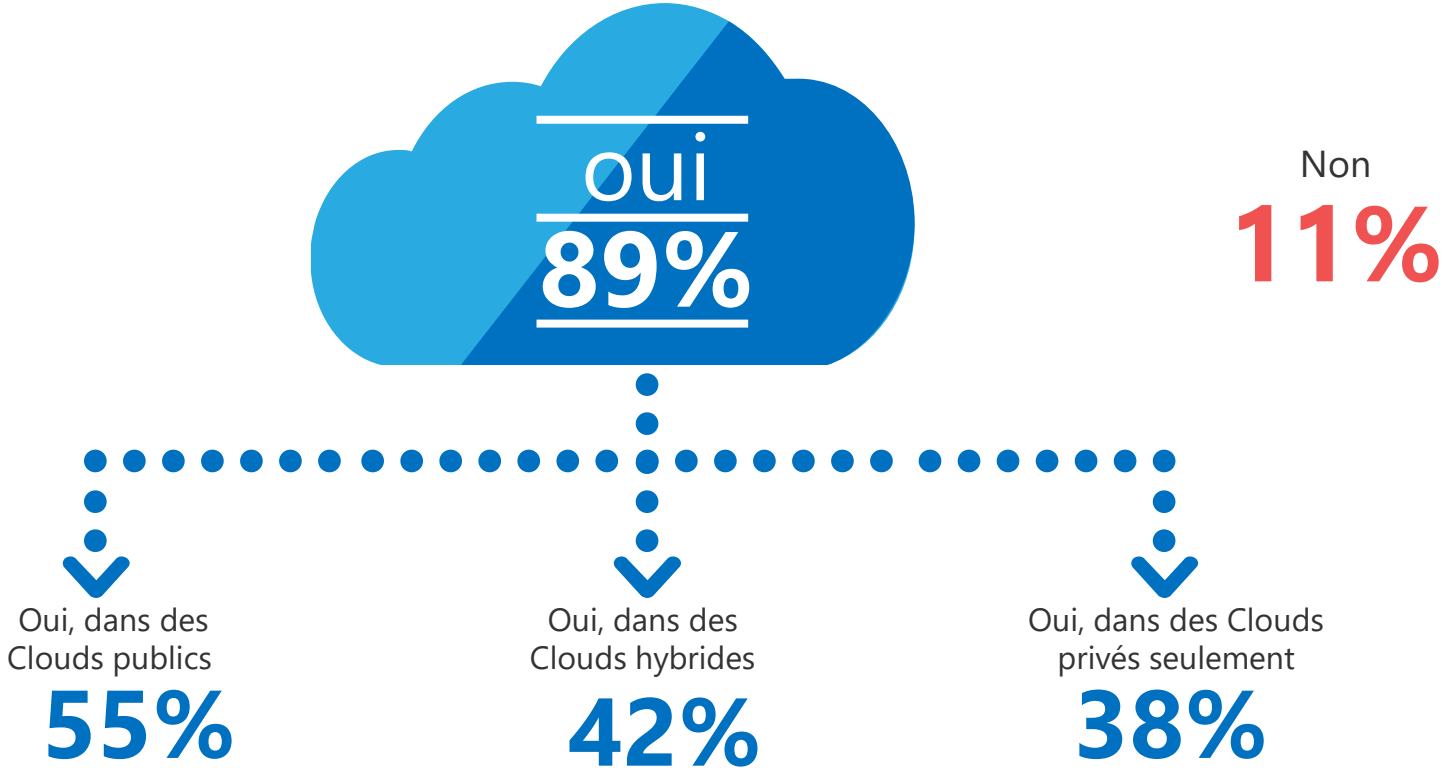
* Nouveaux items en 2019

Évolution statistiquement significative vs. 01/2019

3. CLOUD : DES RISQUES TOUJOURS PRÉGNANTS

La grande majorité des entreprises stockent leurs données dans le Cloud

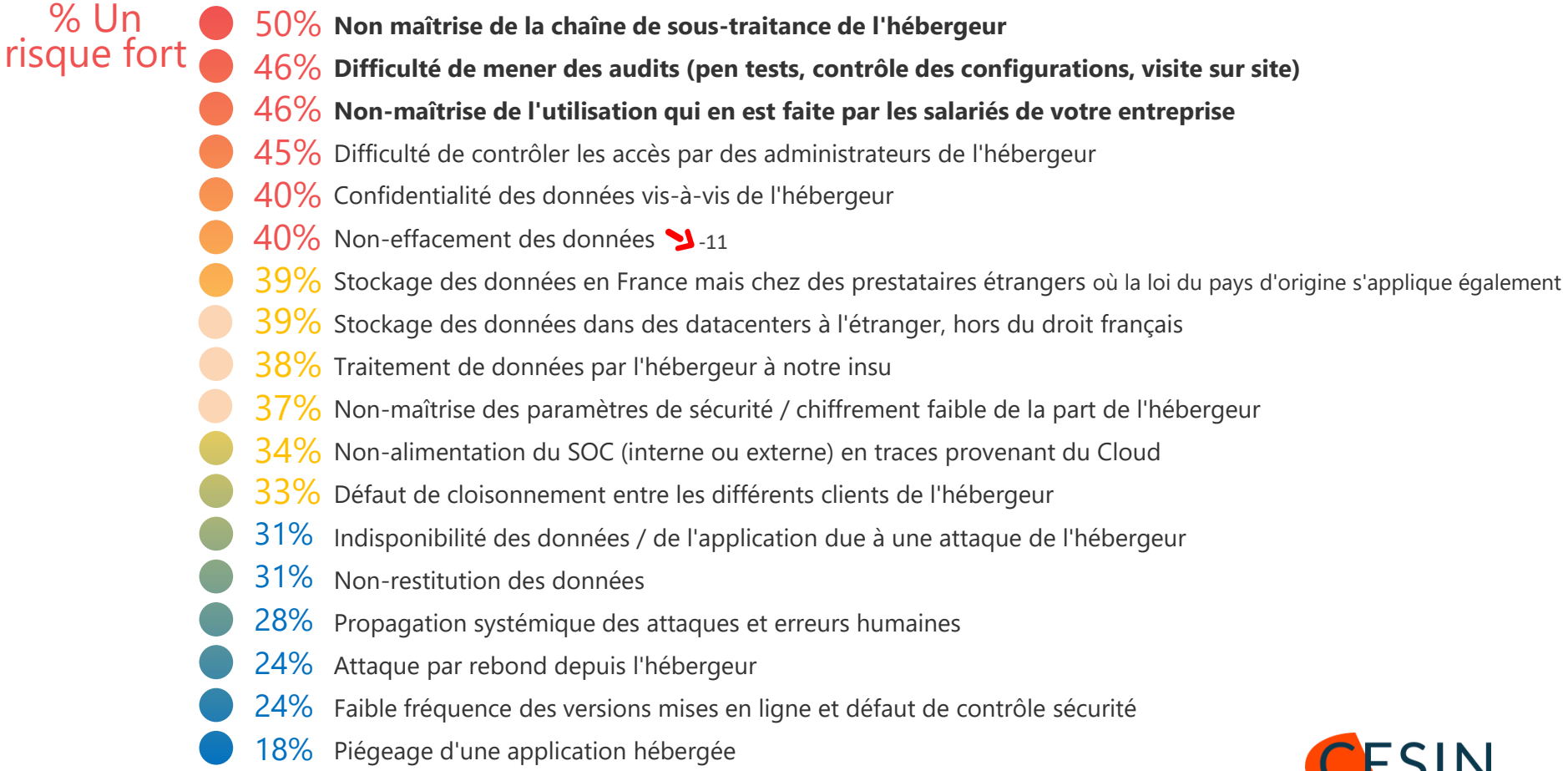
Q20. Certaines des données de votre entreprise sont-elles stockées dans un Cloud ?
Base : ensemble (253 répondants), plusieurs réponses possibles



Évolution statistiquement significative vs. 01/2019

Le Cloud présente cependant des risques majoritairement liés à un manque de maîtrise

Q22. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ? *Base : ensemble (253 répondants)*

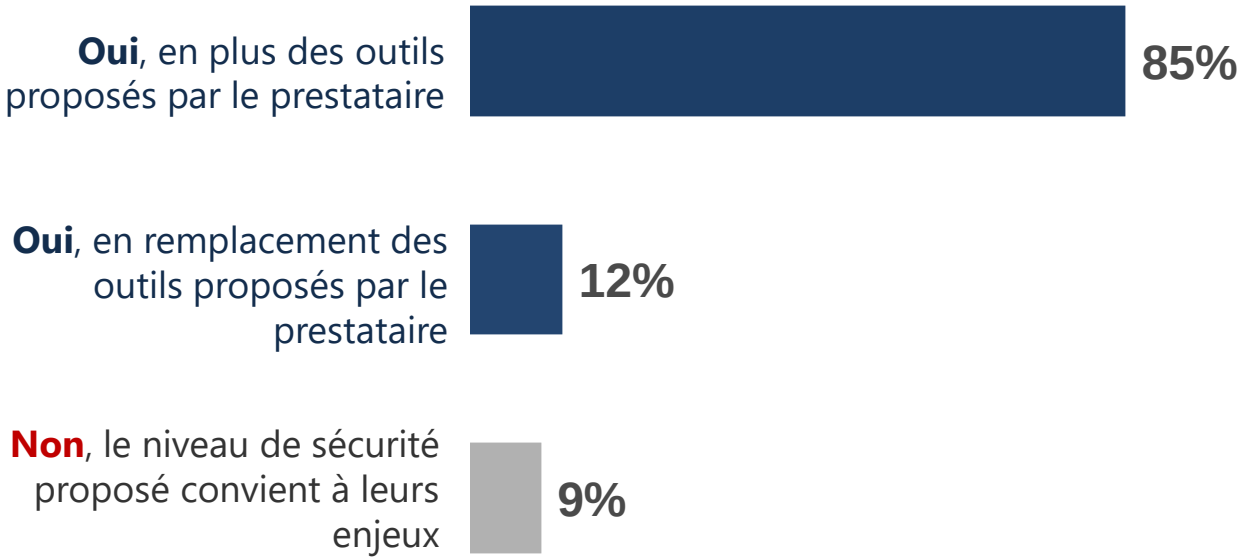


Évolution statistiquement significative vs. 01/2019

Pour 9 entreprises sur 10, les outils actuellement mis en place par les offreurs de services Cloud pour sécuriser les données stockées ne suffisent pas

Q23. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble (253 répondants)

… 91% estiment que la sécurisation des données stockées dans le Cloud requiert des outils ou dispositifs spécifiques



Évolution statistiquement significative vs. 01/2019

La présence d'IA dans les solutions de protection est relativement marginale dans les critères de choix…

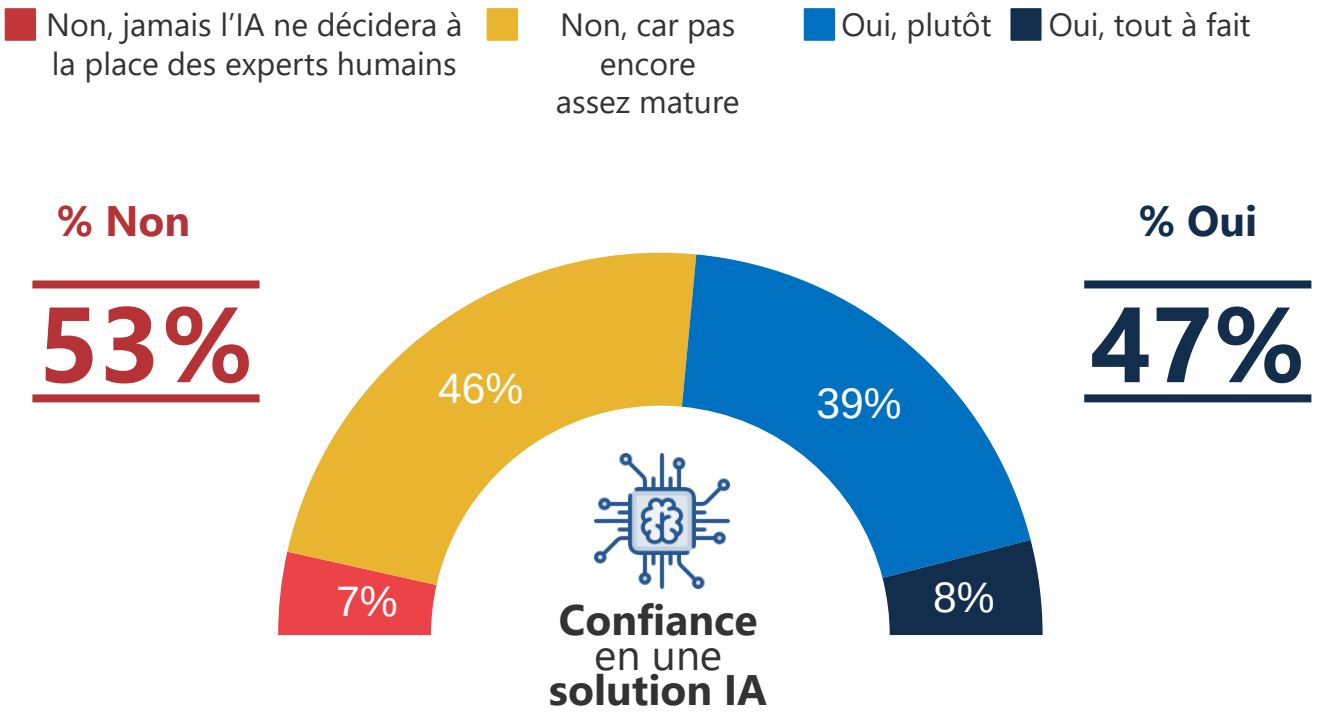
Q40. Parlons maintenant du rôle potentiel de l'IA dans la sécurité informatique. Dans votre entreprise, la présence d'IA est-elle un critère déterminant dans le choix de vos solutions ? *Base : ensemble (253 répondants)*

Estiment que **la présence d'IA est un critère déterminant dans le choix de leurs solutions**

Question modifiée par rapport à la vague précédente du baromètre

… probablement en raison, pour le moment, d'un manque de confiance dans ces solutions

Q41. Seriez-vous prêt(e) à laisser une solution IA prendre des décisions en matière de sécurité pour ce qui concerne la détection et/ou la remédiation ? *Base : ensemble (253 répondants)*

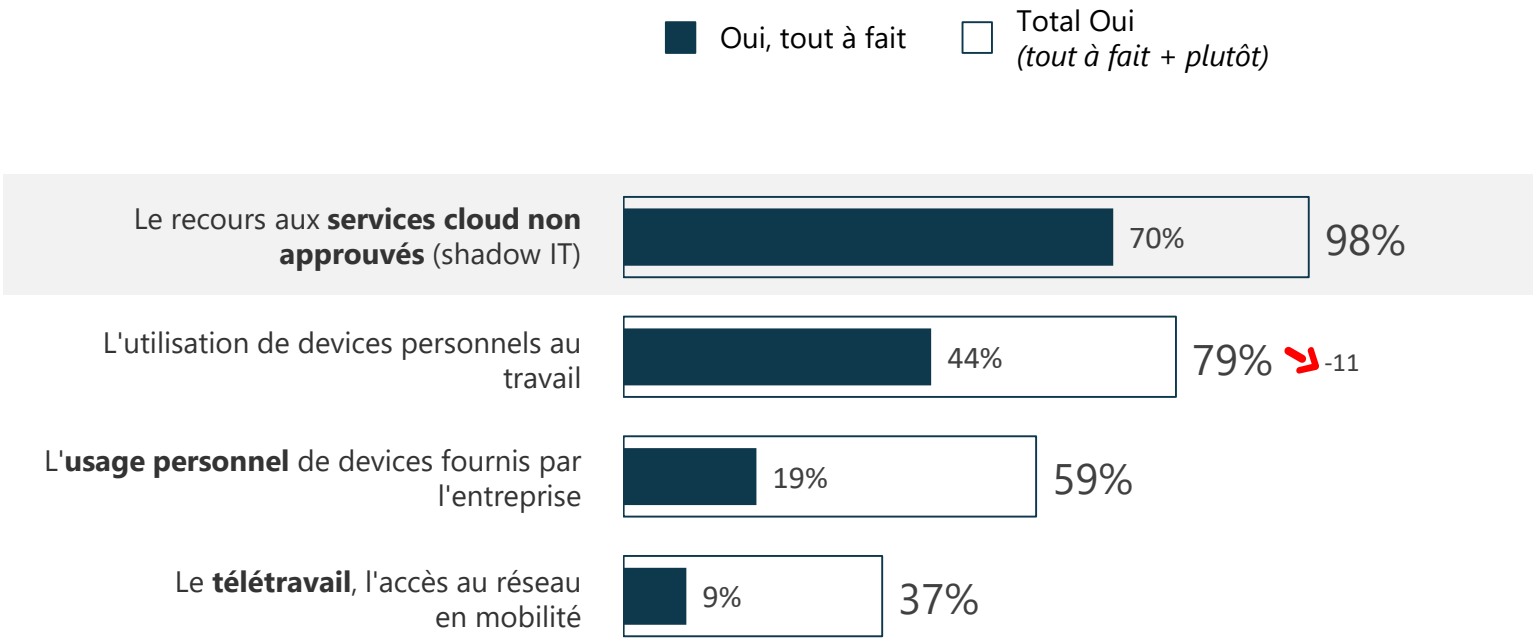


Évolution statistiquement significative vs. 01/2019

4. DES SALARIÉS TOUJOURS DIFFICILEMENT MOBILISABLES

D'après les RSSI, le shadow IT reste le plus grand cyber-risque de l'usage des salariés

Q24. À vos yeux, les usages suivants du numérique par les salariés représentent-ils un risque pour la cyber-sécurité des entreprises ? *Base : ensemble (253 répondants)*



Évolution statistiquement significative vs. 01/2019

Des salariés qui, malgré une bonne sensibilisation aux cyber-risques, pourraient davantage s'impliquer

Q15. En ce qui concerne la cyber-sécurité, pensez-vous que les salariés de votre entreprise… ?
Base : ensemble (253 répondants)

74%
pensent que les salariés **sont sensibilisés** aux cyber-risques

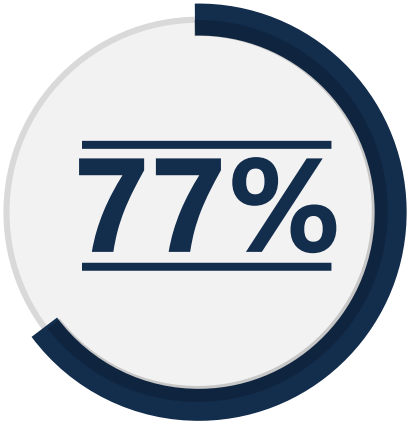
55%
pensent que les salariés **respectent les recommandations**

16%
pensent que les salariés **prennent des précautions au-delà des recommandations** données

Évolution statistiquement significative vs. 01/2019

Pour palier ce manque d'implication, de plus en plus d'entreprises mettent en place des vérifications

Q15BIS. Avez-vous mis en place des procédures pour tester l'application des recommandations par les salariés dans des situations concrètes, comme des audits, campagnes de faux phishing, contrôles internes, etc. ?
Base : ensemble (253 répondants)



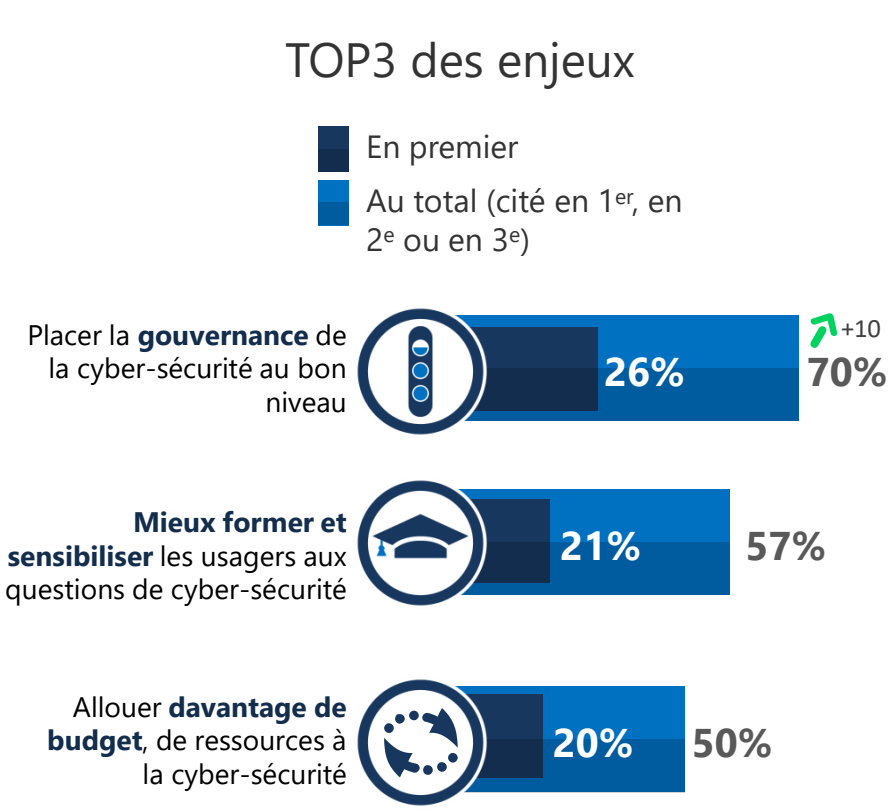
ont **mis en place des procédures pour tester** l'application des recommandations par les salariés

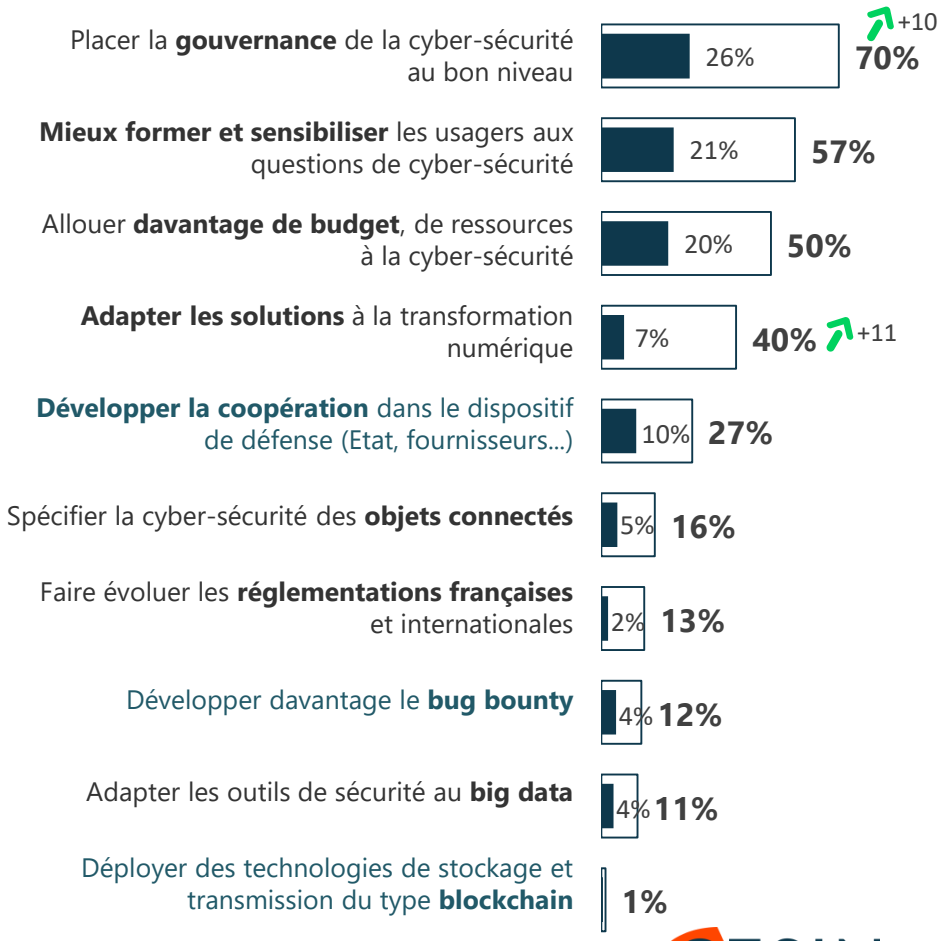
Évolution statistiquement significative vs. 01/2019

5. DES ENTREPRISES QUI SE DISENT PEU CONFIANTES

Cette année encore, les enjeux humains prennent le pas sur les enjeux techniques

Q28. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cyber-sécurité des entreprises ? *Base : ensemble (253 répondants)*



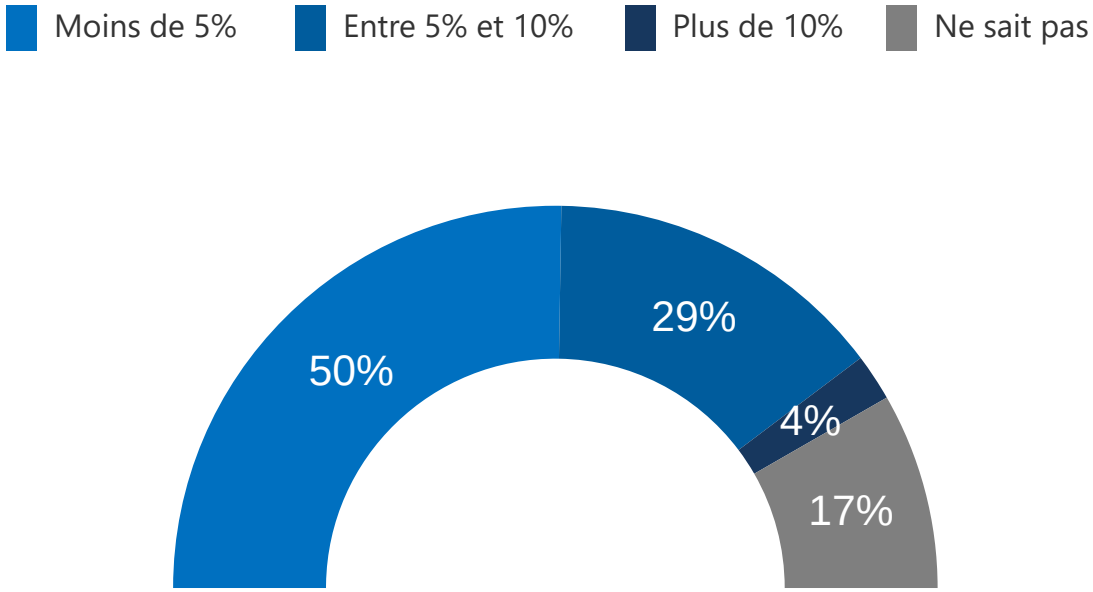


Nouveaux items en 2019

Évolution statistiquement significative vs. 01/2019

La part du Budget IT pour la sécurité augmente en tendance par rapport à l'année dernière

Q37. Dans votre entreprise, quelle part du budget IT est consacrée à la sécurité ? *Base : ensemble (253 répondants)*



Évolution statistiquement significative vs. 01/2019

Mais les entreprises souhaitent encore augmenter ce budget, avant tout pour acquérir de nouvelles solutions de sécurité

Q11BIS. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ? *Base : ensemble (253 répondants)*

d'acquérir de **nouvelles solutions techniques** destinées à la protection contre les cyber-risques

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

Évolution statistiquement significative vs. 01/2019

La moitié des entreprises souhaite également augmenter les effectifs liés à la cyber-sécurité

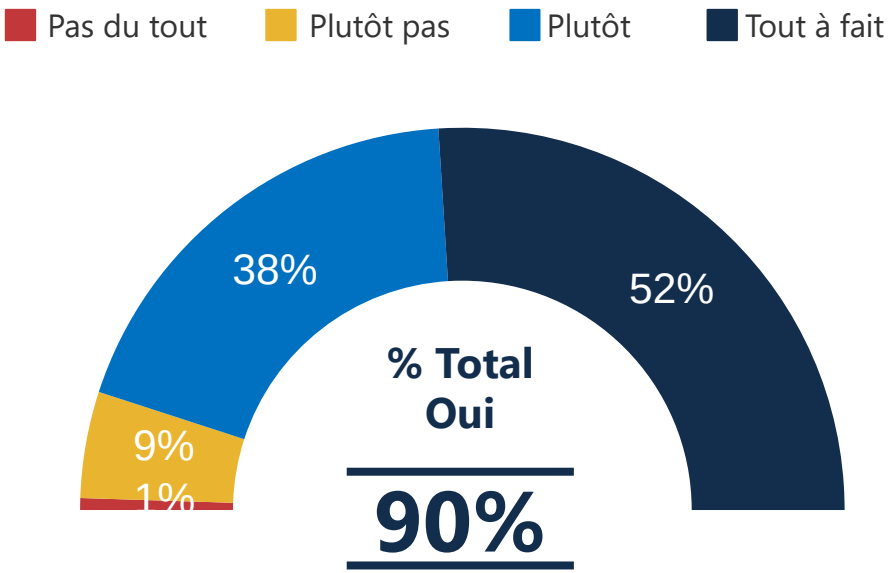
Q11BIS. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ? *Base : ensemble (253 répondants)*

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

Elles sont toutefois confrontées à une forte pénurie des profil SSI

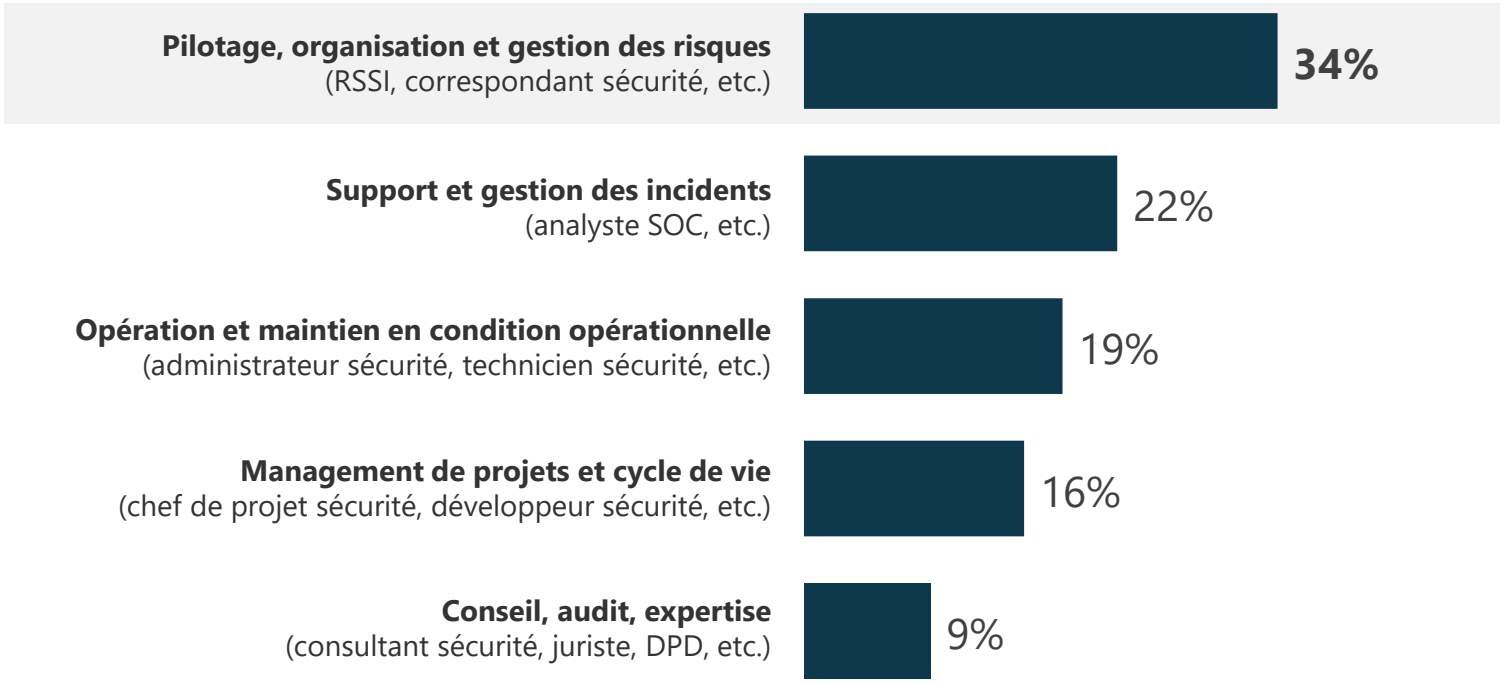
Q43. Pour finir, voici quelques questions sur le sujet du recrutement en SSI. Constatez-vous une pénurie de profils en SSI entraînant des difficultés de recrutement ? *Base : ensemble (253)*

« Le constat d'une **pénurie de profils en SSI** entraînant des difficultés de recrutement »



Pénurie qui touche principalement les métiers liés aux risques

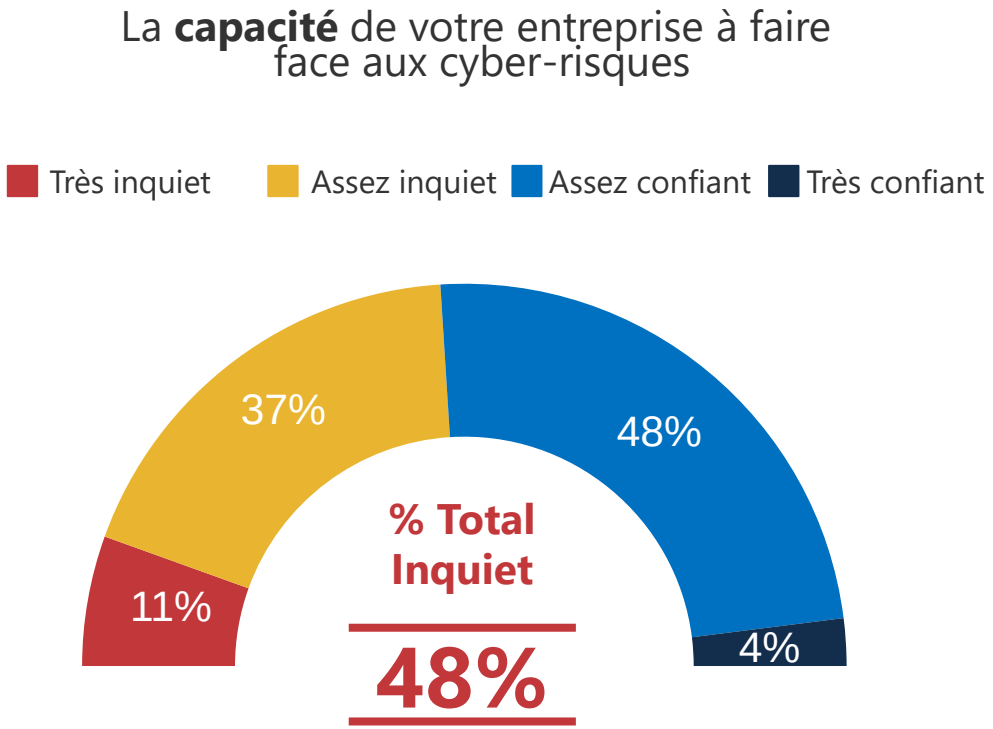
Q44. Quel est, d'après vous, le métier de la SSI le plus touché par une pénurie de profils ?
Base : ensemble (253)



Évolution statistiquement significative vs. 01/2019

Près d'une entreprise sur deux toujours inquiète sur sa capacité à faire face aux cyber-risques

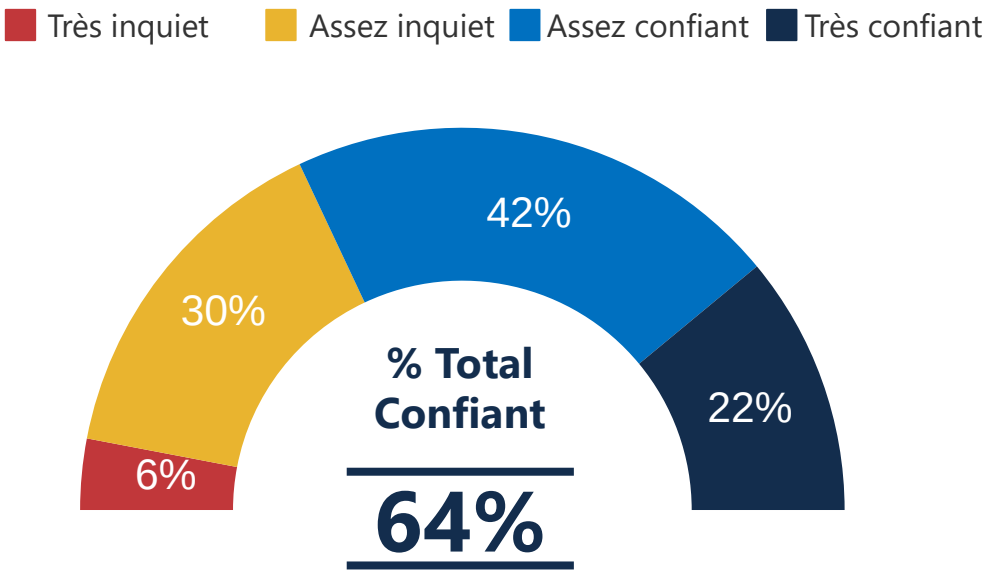
Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (253 répondants)



2/3 des entreprises prennent en compte les enjeux de la cyber-sécurité au sein du COMEX

Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (253 répondants)

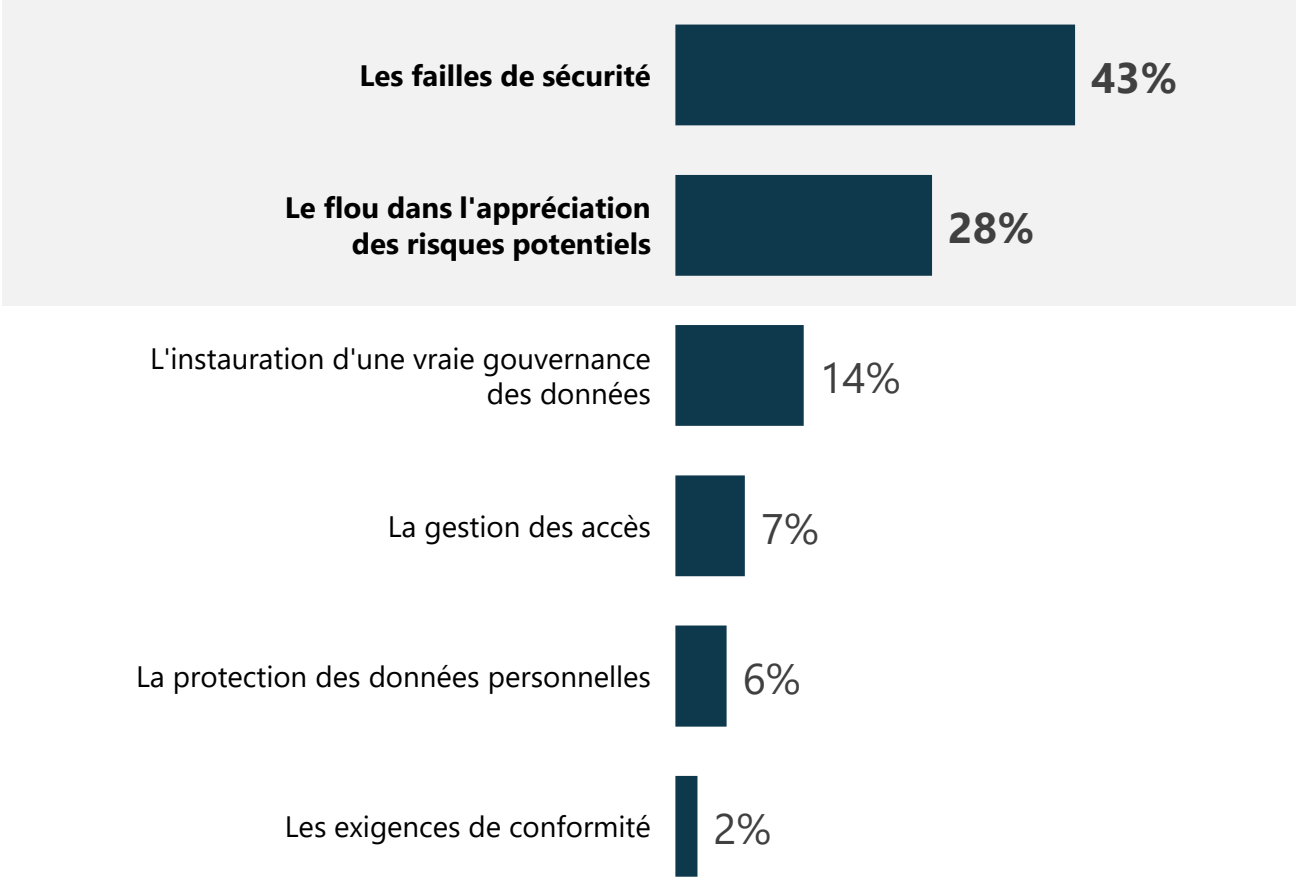
La **prise en compte des enjeux** de la cyber-sécurité au sein du COMEX votre entreprise



ANNEXES

Défi à relever pour le RSSI

Q36. D'après vous, quel est le principal défi à relever pour le RSSI en ce qui concerne l'IoT (*Internet of Things*) en entreprise ?
Base : ensemble (253)

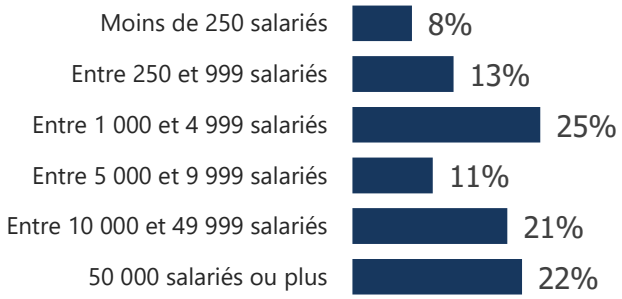


Évolution statistiquement significative vs. 01/2019

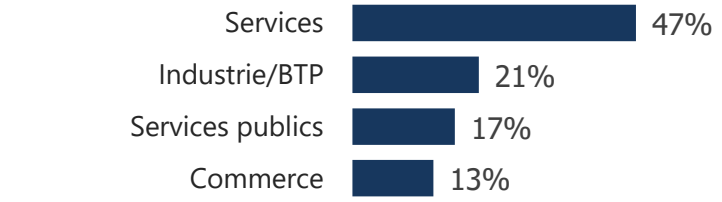
Profil des répondants

253 membres du CESIN ont participé à cette enquête

Nombre de salariés de l'entreprise :



Secteur d'activité de l'entreprise :



Évolution statistiquement significative vs. 01/2019