

CHIFFRES CLÉS



44% +6pts

s'estiment


faiblement exposées
aux risques

et **47%** pour les - de 1 000 hab



53% +6pts

déclarent bénéficier d'un
bon niveau de
protection

14% 
se sentent
bien préparés

et pourtant

3ÈME ÉDITION DU BAROMÈTRE DE LA MATURITÉ CYBER DES COLLECTIVITÉS :

la frontière s'accroît entre les petites collectivités
et celles de plus de 1 000 habitants



1 / 10

déclare avoir
déjà été victime
d'une ou plusieurs cyberattaques

au cours des 12 derniers mois

Principales conséquences

Interruption
d'activité
et de services

37%



Destruction
ou vol de
données

24%

mais

45%

n'en connaissent pas
la cause



77% 

indiquent dépenser
moins de 2 000 €
pour leur cybersécurité

et **87%** des - de 1 000 hab

Principaux freins : le manque...

de
connaissances

47%

de
budget

36%

de
compétences

36%



62%

appellent à une
sensibilisation accrue
des élus et agents



**RETROUVEZ L'INTÉGRALITÉ
DES CHIFFRES CLÉS DU 3ÈME BAROMÈTRE
DE LA MATURITÉ CYBER DES COLLECTIVITÉS
DE MOINS DE 25 000 HABITANTS**



GIP ACYMA

www.cybermalveillance.gouv.fr

Suivez-nous sur :      

“*opinionway*”

Pour :



3ème étude du baromètre de la maturité Cyber des Collectivités françaises

Vague 2024

25 octobre 2024 | Rapport



ESOMAR²⁴
Corporate

Image de kjpargeter sur freepik



Méthodologie et Profils des répondants



“ La méthodologie de l'enquête



Interrogation d'un échantillon de **1710 élus de collectivités/ agents communaux en charge de l'informatique et de la sécurité des communes de moins de 25 000 habitants** en France métropolitaine et dans les départements et régions d'Outre-Mer (DROM).



L'échantillon a été interrogé par **questionnaire auto-administré en ligne sur système CAWI** (Computer Assisted Web Interview).

Les élus et agents communaux ont été sollicités via une diffusion du lien vers l'enquête par les membres "collectivités" de Cybermalveillance.fr (AVICCA, COTER NUMERIQUE, AMF, APVF, DECLIC, ANCT, REGIONS PAYS DE LA LOIRE, REGIONS DE FRANCE ...) et via une base "écosystème collectivités" constituée par Cybermalveillance.fr.



Les interviews ont été réalisées **du 26 août au 4 octobre 2024.**



Questionnaire

Un redressement sur la taille des communes a été opéré a posteriori pour disposer d'un échantillon parfaitement représentatif des collectivités françaises de moins de 25 000 habitants en termes de taille.



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



Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 1,0 à 2,4 points au plus pour un échantillon de 1710 répondants



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

« Sondage OpinionWay pour Cybermalveillance.gouv.fr »
et aucune reprise de l'enquête ne pourra être dissociée de cet intitulé.



Redressement de l'échantillon

Un redressement sur la taille des communes a été opéré a posteriori pour disposer d'un échantillon parfaitement représentatif des collectivités françaises de moins de 25 000 habitants en termes de taille.



	(Brut) Total		(Redressé) Total	
<i>Base</i>	<i>1710</i>	<i>100%</i>	<i>1710</i>	<i>100%</i>
Moins de 300 habitants	530	31%	650	38%
Entre 300 et 999 habitants	557	32%	581	34%
Entre 1000 et 4999 habitants	404	24%	376	22%
Entre 5000 et 9999 habitants	118	7%	68	4%
Entre 10 000 et 25 000 habitants	101	6%	34	2%



Une majorité de petites communes dont la responsabilité informatique relève directement du Maire et de son secrétariat ...

Q21. Quelle est votre fonction ?

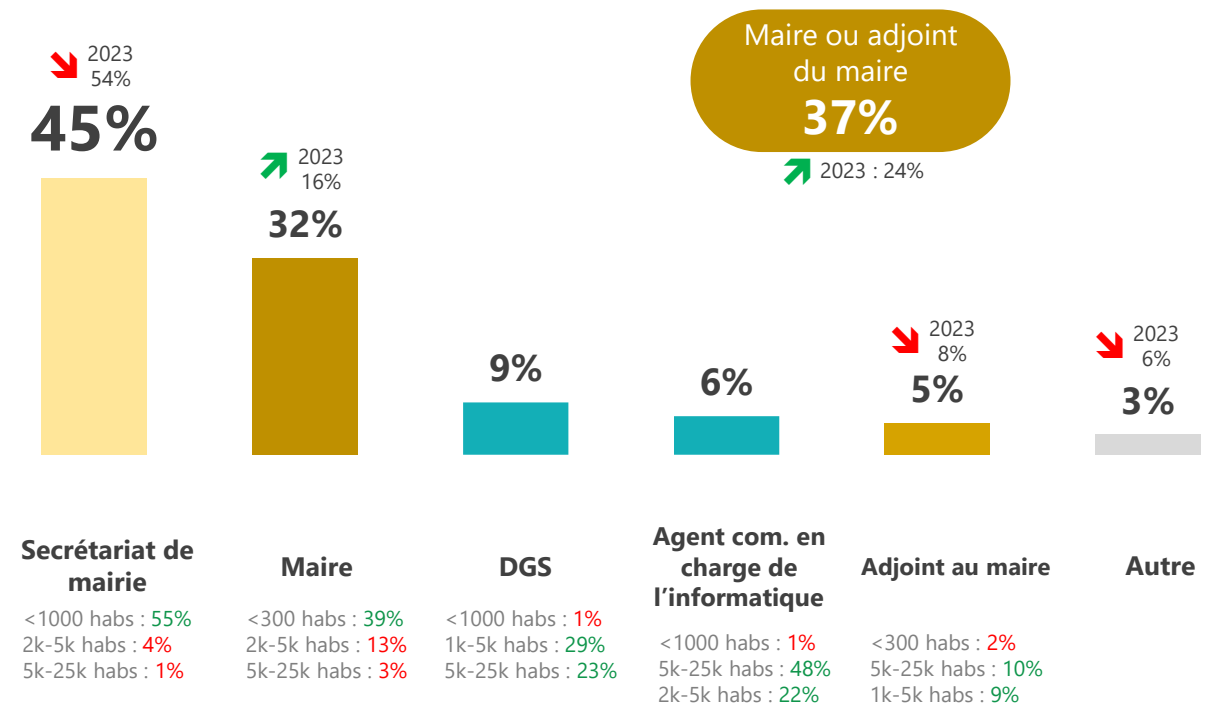
Base : Total répondants (1710)



Photo de Maria Orlova: <https://www.pexels.com/fr-fr/photo/ancien-palais-en-pierre-situe-dans-la-ville-medievale-par-temps-couvert-4917173/>

Fonction du répondant

En 2024, le Maire a davantage répondu que son secrétariat...





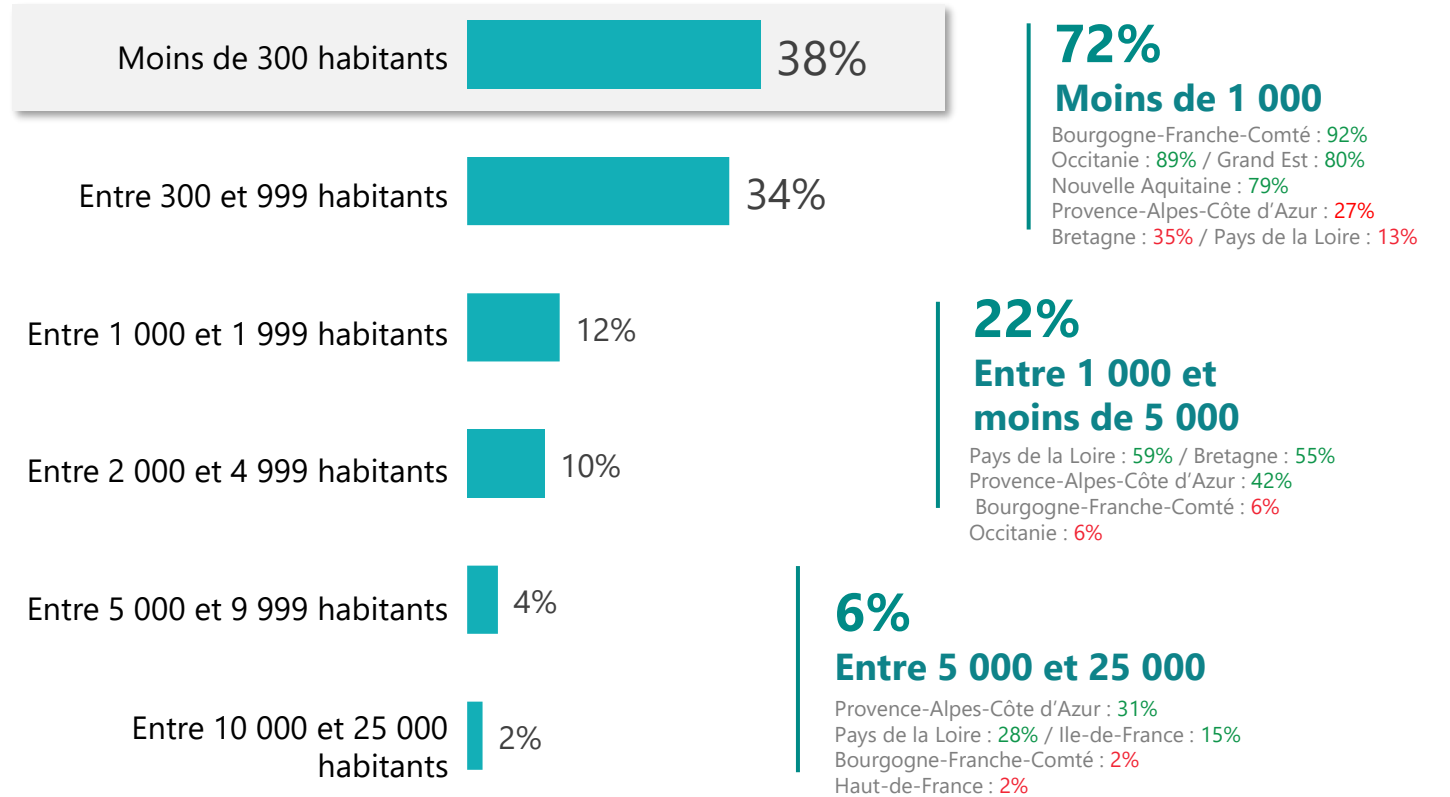
Plus de 70% des communes de France de moins de 25 000 habitants comptent moins de 1 000 habitants en France et près de 95% comptent moins de 5 000 habitants. Seules 2% ont entre 10 000 et 25 000 habitants.

Q2. Combien votre collectivité compte-t-elle d'habitants ?

Base : Total répondants (1710)



Structure redressée a posteriori (confer page 7)



x% / x% : Résultat statistiquement supérieur ou inférieur au total



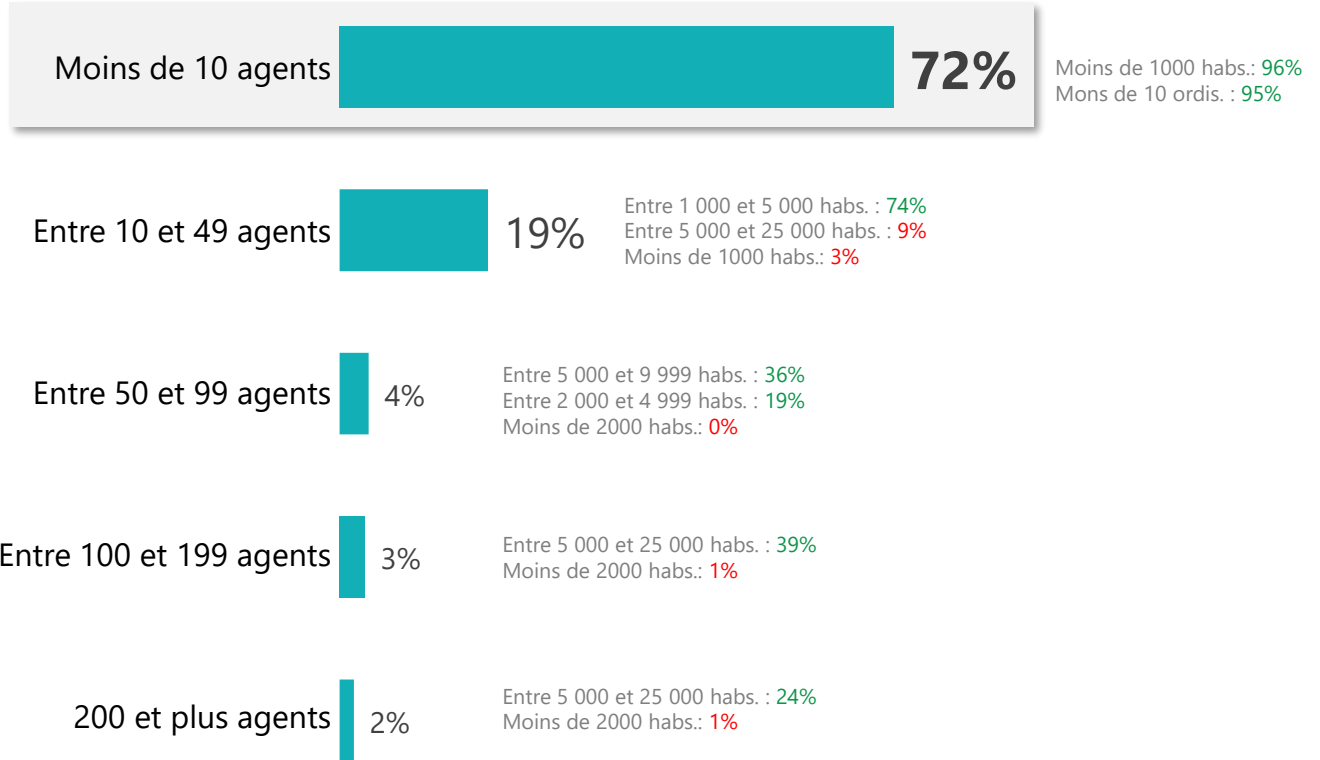
Des communes par conséquent majoritairement rurales dotées de peu d'agents communaux : près des trois quarts comptent moins de 10 agents, en particulier celles de moins de 1 000 habitants... Et 9 sur 10 en comptent moins de 50.

Q3. Combien d'agents travaillent dans votre collectivité ?

Base : Total répondants (1710)



Image de Freepik



91%
Moins de 50 agents



Les résultats





01

Des investissements qui ont peu évolué en un an notamment auprès des petites collectivités.



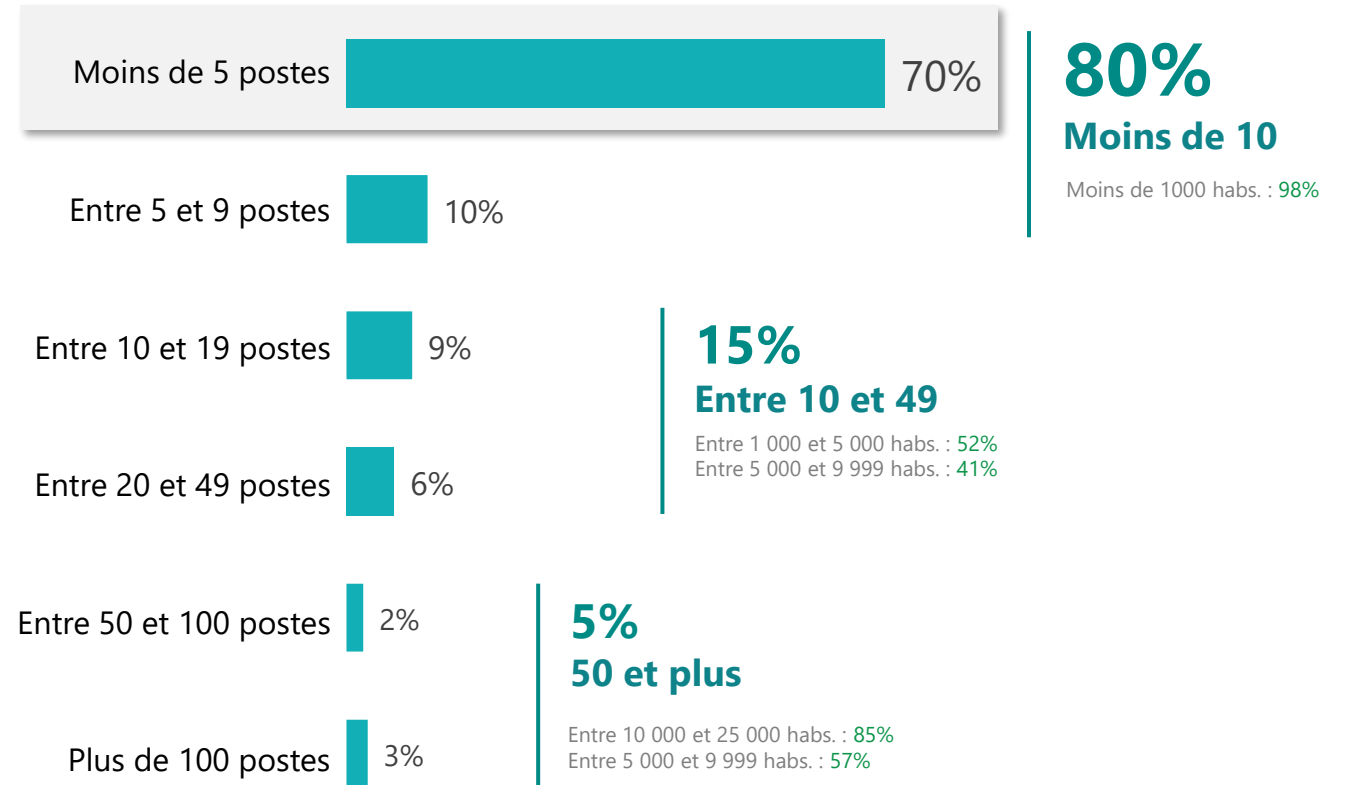
Près des trois quarts comptant moins de 10 agents, quasi tout autant (80%) sont dotées de moins de 10 postes informatiques. Un équipement logiquement corrélé à la taille des collectivités ...

Q4. Et combien de postes informatiques (ordinateurs) y a-t-il au sein de votre collectivité ?

Base : Total répondants (1710)



Image de standret sur Freepik

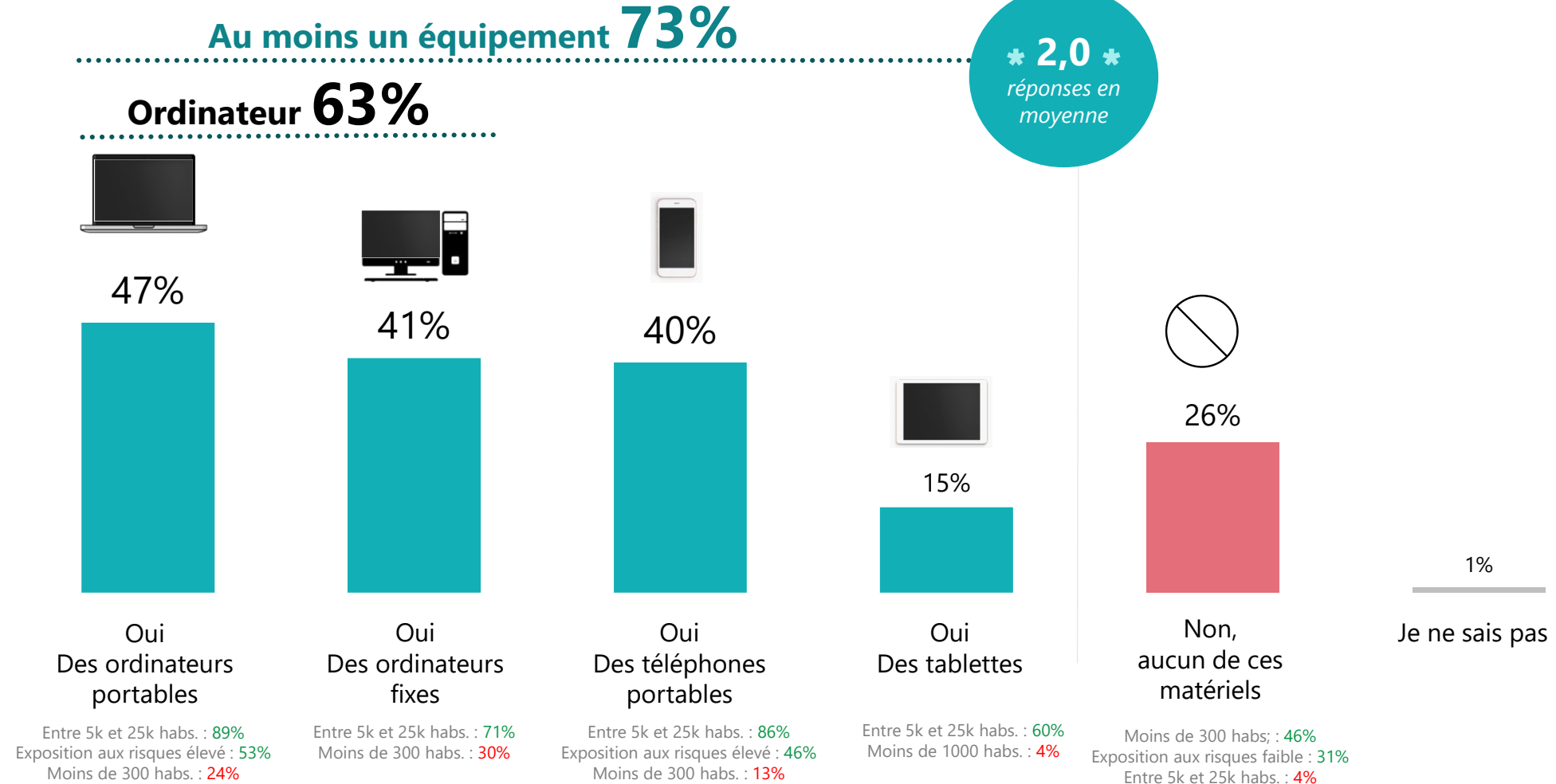




Plus précisément, 6 communes sur 10 disposent de postes informatiques, fixes ou portables. 4 sur 10 mettent aussi à disposition de leurs agents un téléphone portable notamment les plus grosses communes de plus de 5000 habitants alors qu'un peu plus d'un quart ne fournissent aucun de ce type de matériels notamment les moins de 300 hab.

Q5. Votre collectivité met-elle à disposition de certains élus et agents des équipements tels que des téléphones portables, des tablettes ou des ordinateurs ? *Base : Total répondants (1710)*

Question modifiée versus 2023

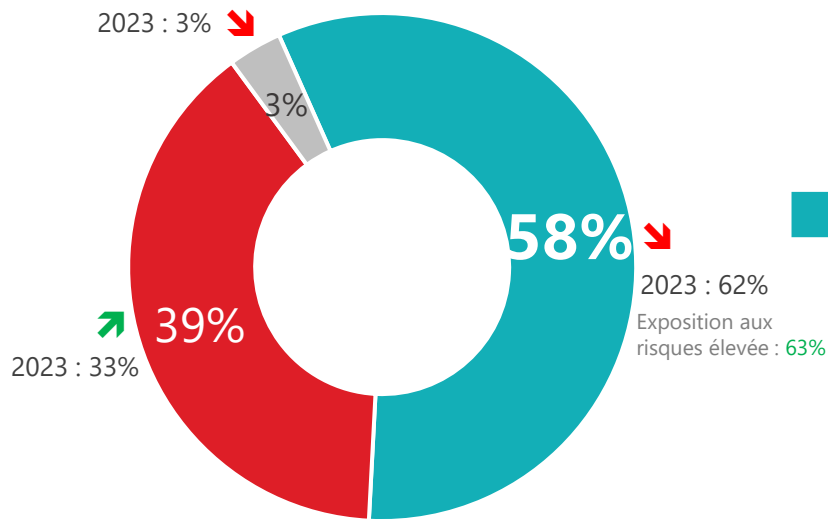




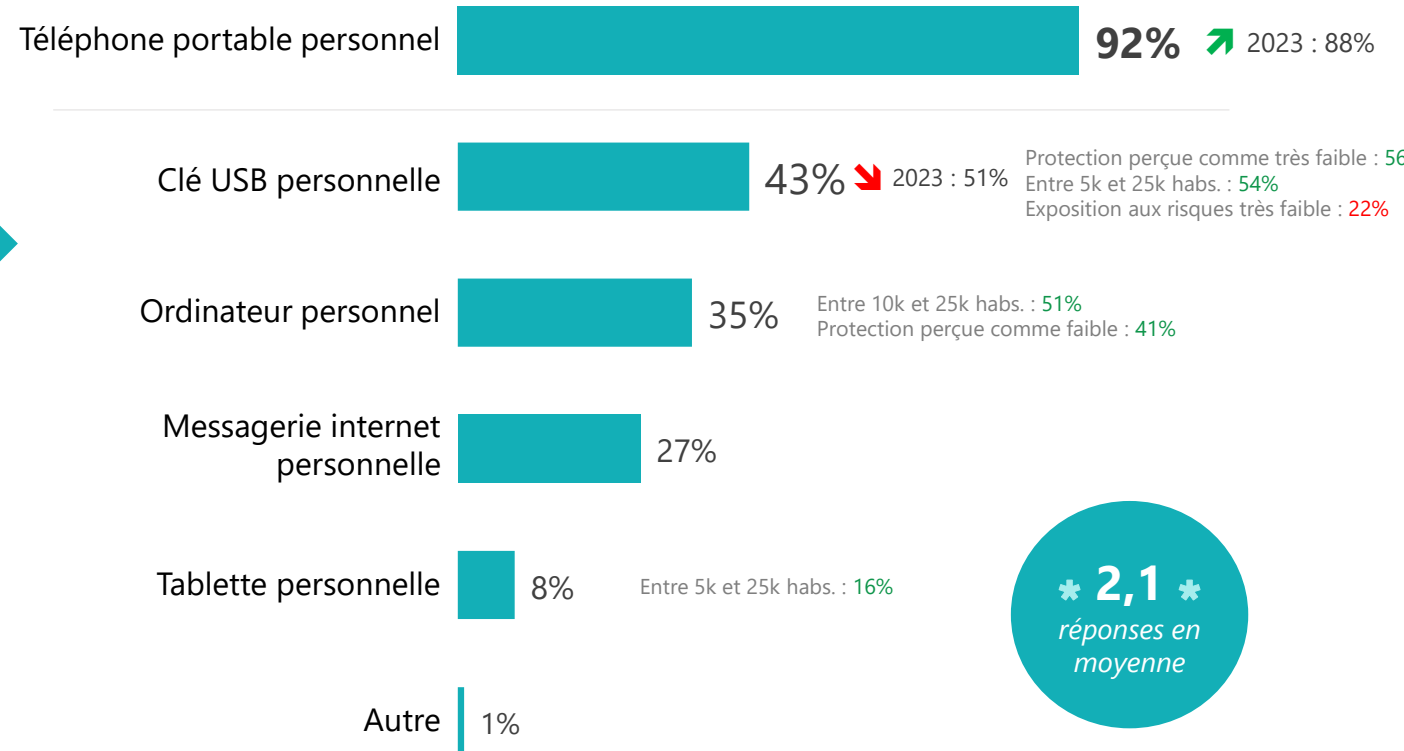
Des collectivités qui continuent en 2024 à utiliser pour une majorité d'entre elles des équipements personnels pour gérer les activités de leur commune même si cette pratique semble en légère baisse au regard des résultats obtenus l'an dernier. Le téléphone portable demeure l'équipement le plus utilisé devant la clé USB personnelle qui semble perdre du terrain cette année même si elle reste utilisée par plus de la moitié des communes de plus de 5000 hab. ou encore celles qui considèrent avoir une protection perçue comme très faible.

Q6. Des équipements personnels (non fournis par la collectivité) tels que des téléphones portables, tablettes, clés usb... sont-ils utilisés pour les activités de votre collectivité ? *Base : Total répondants (1710)*

Q6bis. Vous avez déclaré que des équipements personnels sont utilisés pour les activités de votre collectivité. Pouvez-vous préciser lesquels ? *Base : Ont déclaré que des équipements personnels étaient utilisés pour les activités de leur collectivité (983) - Plusieurs réponses possibles*



● Oui ● Non ● Ne sait pas



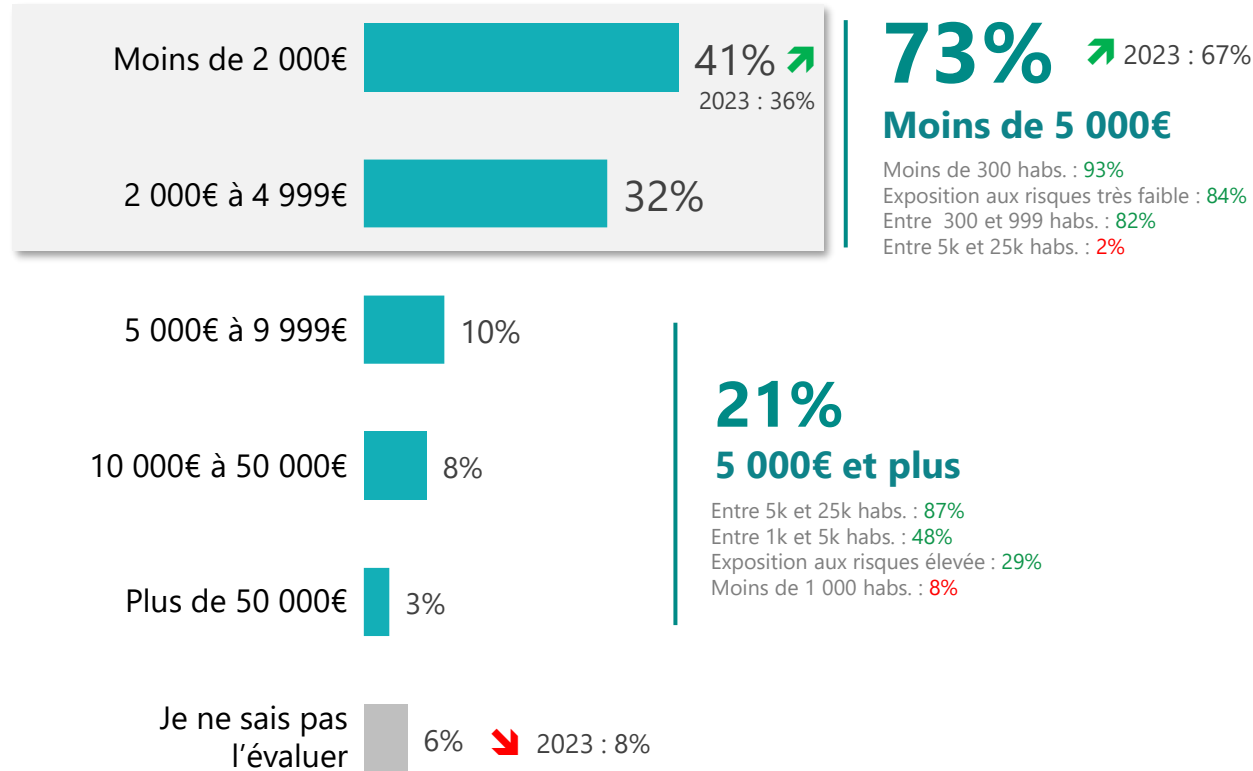
*** 2,1 ***
réponses en moyenne



Une utilisation d'équipements personnels qui s'explique notamment par une faible allocation budgétaire dédiée à l'informatique. En effet, elles sont encore nombreuses à déclarer y allouer moins de 5 000 euros par an, notamment les toutes petites communes alors que les collectivités plus grandes (+5k hab.) sont près de 9 sur 10 investir plus 5000 euros par an dans ce domaine.

Q7. Quel est le montant du budget annuel de la collectivité dédié à l'informatique (compris dans le budget d'investissement et/ou de fonctionnement incluant par exemple la maintenance informatique, l'entretien du photocopieur, de l'imprimante etc.) ?

Base : Total répondants (1710)

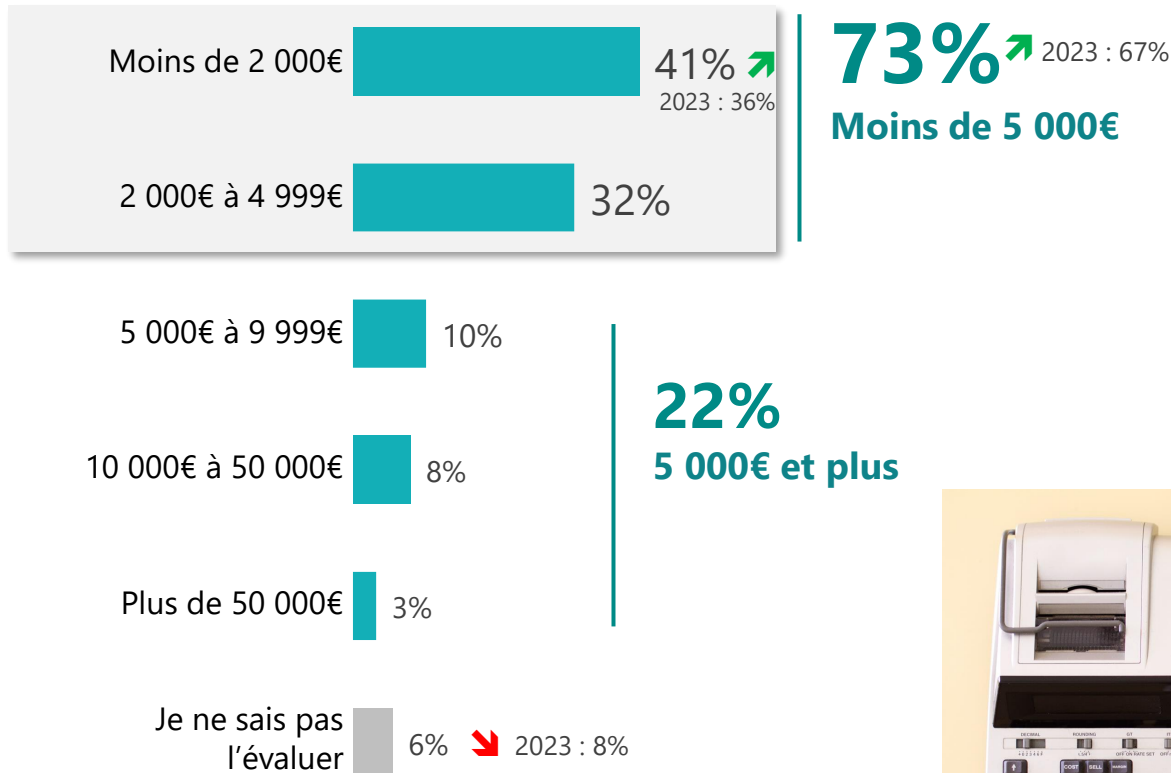




Quant à la part allouée à la sécurité informatique, elle reste inférieure à 2 000 euros par an pour plus des trois quarts des collectivités. Un résultat qui reste stable sur un an. Un niveau d'allocation qui est surtout caractéristiques des communes qui se considèrent comme peu exposées aux risques.

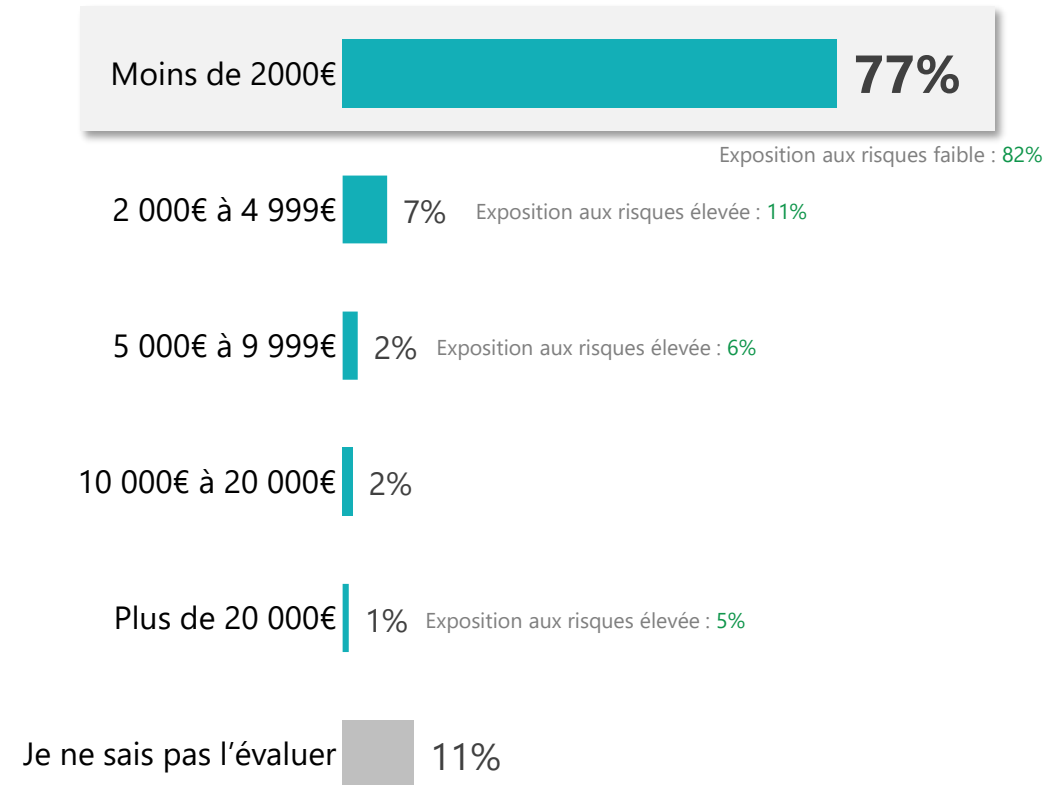
Q7. Quel est le montant du budget annuel de la collectivité dédié à l'informatique (compris dans le budget d'investissement et/ou de fonctionnement incluant par exemple la maintenance informatique, l'entretien du photocopieur, de l'imprimante etc.) ?

Base : Total répondants (1710)



Q7bis. Quelle est la part de ce budget consacré à la sécurité informatique ?

Base : Ont déclaré connaître le budget consacré à l'informatique (1613)

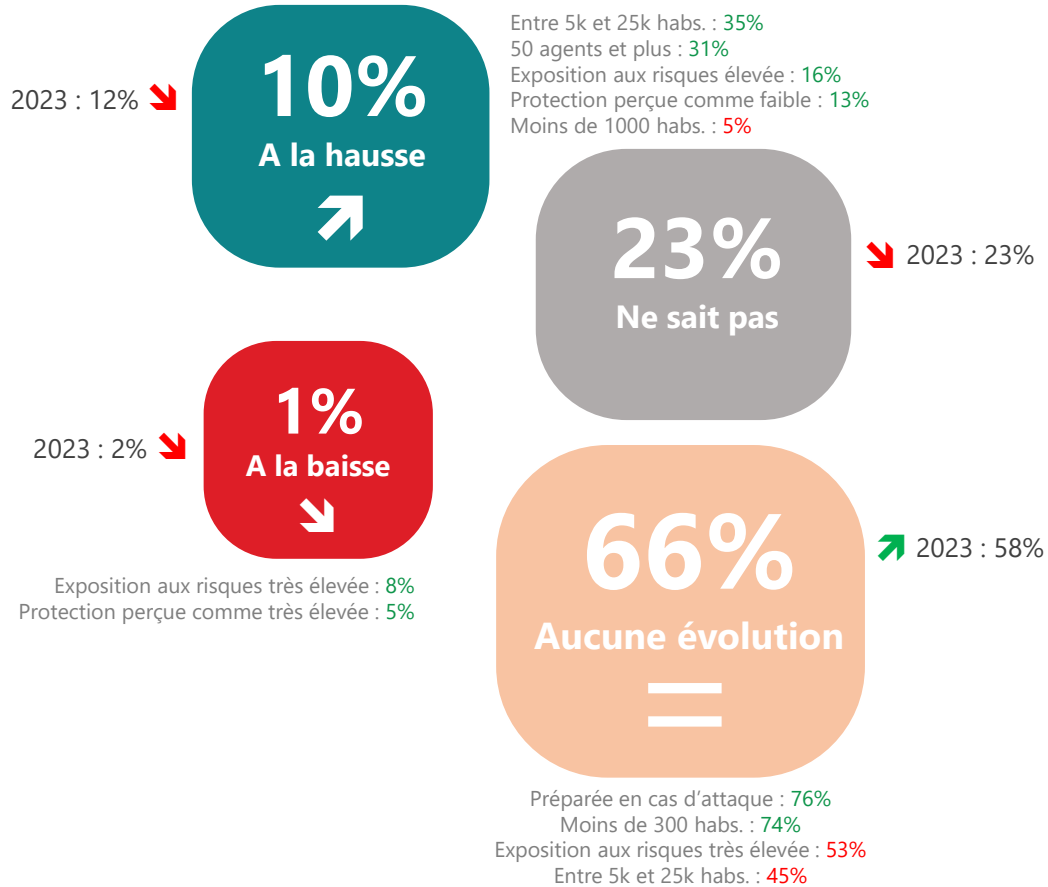




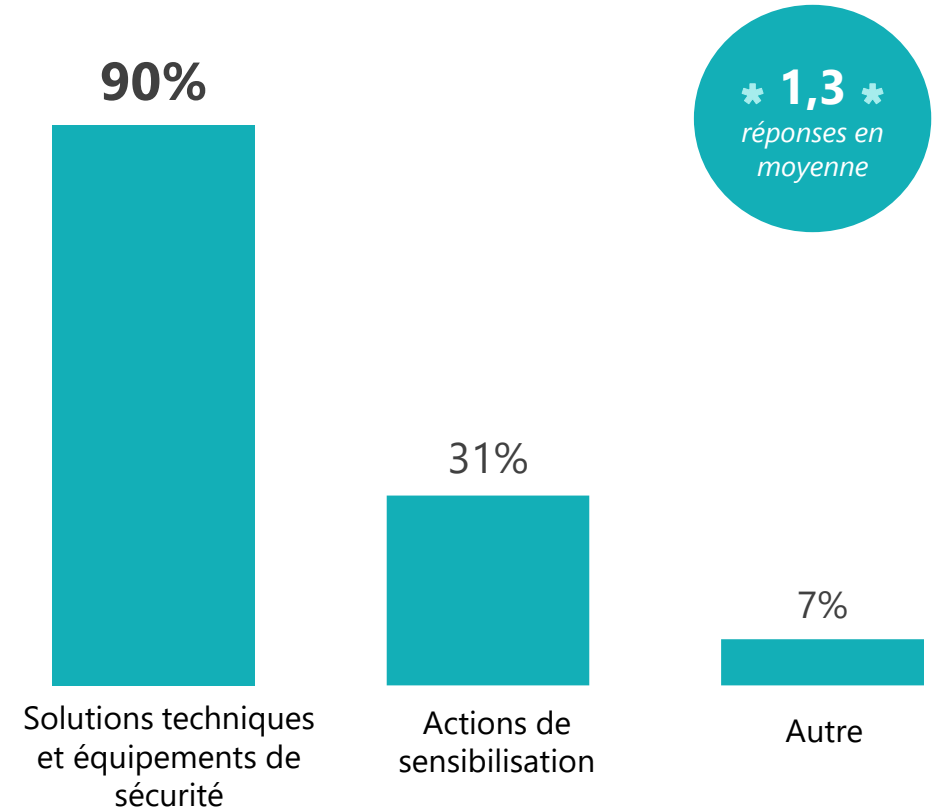
Et si deux tiers des collectivités n'envisagent pas de modifier ce budget l'an prochain notamment celles qui considèrent avoir déjà investi et être cette année préparées en cas d'attaque, 1 collectivité sur 10 envisage une augmentation, en particulier les plus grandes communes et dans une moindre mesure celles qui considèrent avoir une protection déficiente.

Q7ter. Prévoyez-vous de faire évoluer ce budget l'an prochain ?
Base : Ont déclaré connaître le budget consacré à l'informatique (1613)

Comptent faire évoluer le budget...



Q7d. A quel poste pensez-vous allouer ce budget ? *Base : Ont déclaré une hausse du budget consacré à la sécurité informatique l'an prochain (158)*





Une propension à augmenter le budget annuel consacré à la sécurité informatique qui est surtout caractéristique des plus grandes collectivités ...

Q7bis. Quelle est la part de ce budget consacré à la sécurité informatique ?

Q7ter. Prévoyez-vous de faire évoluer ce budget l'an prochain ?

Base : Collectivités qui connaissent le budget consacré à l'informatique (1613)

	TOTAL	Nombre d'habitants dans la collectivité					
		Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	1613	635	554	1189	332	60	31
Moins de 2000€	77%	91%	83%	87%	58%	14%	9%
2 000€ à 4 999€	7%	1%	4%	2%	18%	29%	18%
5 000€ à 9 999€	2%	0%	1%	1%	5%	20%	15%
10 000€ à 20 000€	2%	-	0%	0%	3%	18%	13%
Plus de 20 000€	1%	0%	-	0%	-	5%	36%
Je ne sais pas l'évaluer	11%	8% 2023 4%	12% 2023 17%	10%	16%	14%	9%
Oui, à la hausse	10% 2023 12%	4%	6%	5% 2023 7%	20%	29%	48%
Oui, à la baisse	1% 2023 2%	1%	1%	1%	1% 2023 3%	1%	2%
Non, aucune évolution du budget prévu	66% 2023 58%	74%	68% 2023 58%	71% 2023 65%	55% 2023 41%	48%	38%
Je ne sais pas	23% 2023 28%	21%	25% 2023 32%	23%	24% 2023 34%	22%	12%

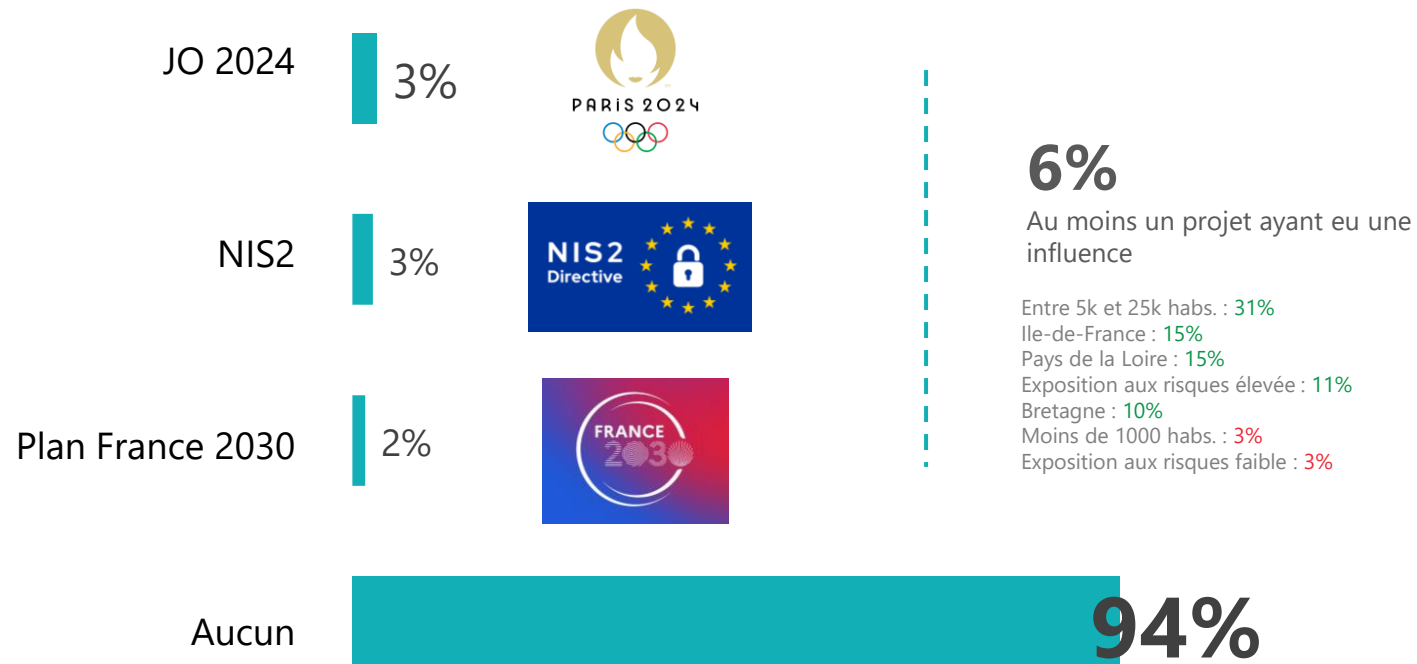


Un résultat stable qui n'a pas été influencé par la survenue de certains événements spécifiques cette année. En effet, peu de communes déclarent avoir renforcé leur politique cyber du fait des JO , de NIS2 ou encore du plan France 2030...

Q15c. Est-ce que l'un ou plusieurs de ces évènements/projets a ou ont eu une influence sur le renforcement de votre politique cyber ?

Base : Total répondants (1710)

Nouvelle question ajoutée en 2024.

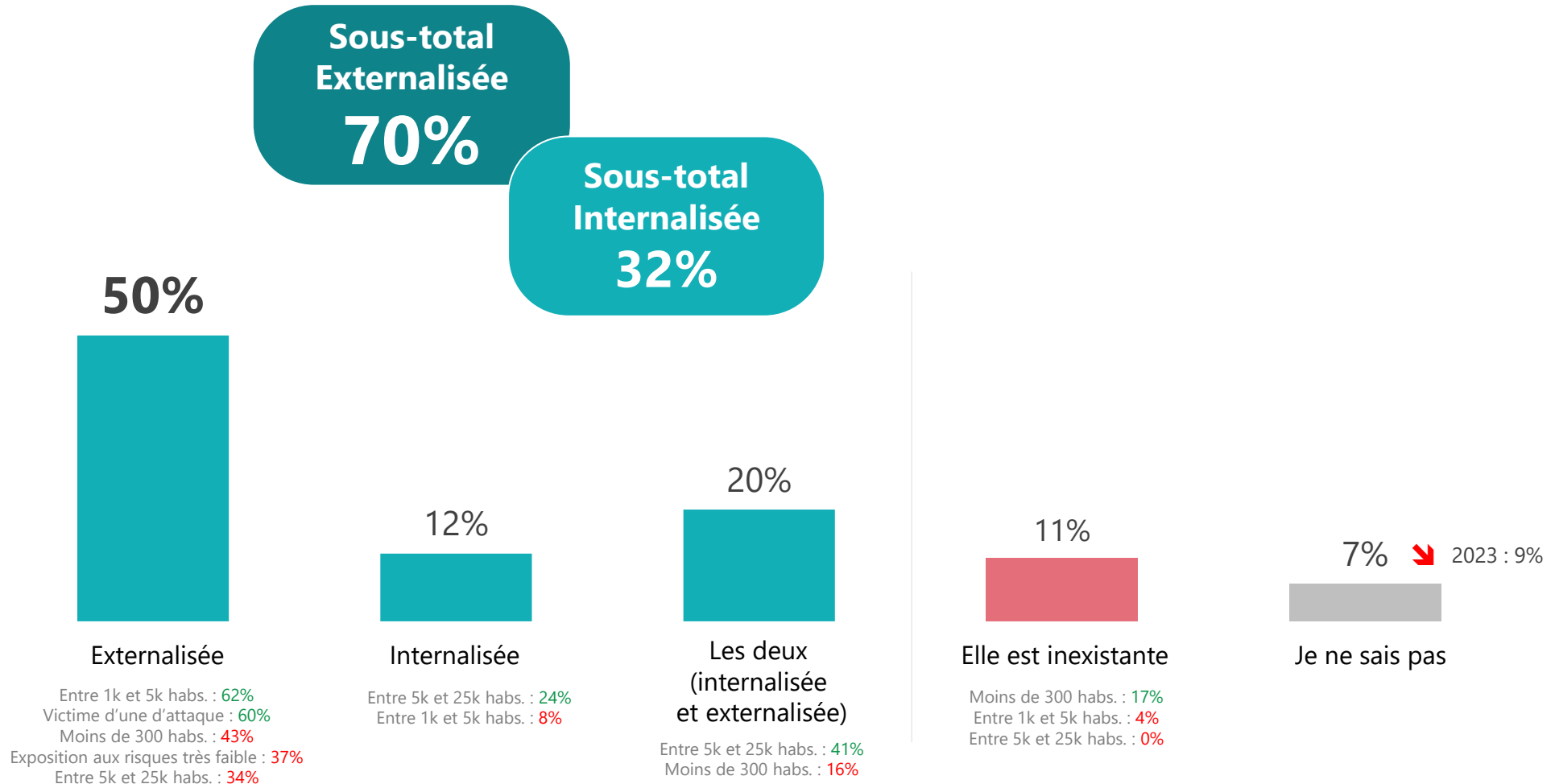




Une gestion de la sécurité informatique qui demeure surtout externalisée, avec la moitié l'externalisant en intégralité.

Q8. La gestion de la sécurité informatique de la collectivité est-elle ?

Base : Total répondants (1710)





Plus d'une collectivité sur 2 communique avec une messagerie externe. Une hausse sans doute due à une meilleure connaissance du répondant sur le fonctionnement avec davantage de maires participant cette année. Une utilisation qui reste toujours très corrélée à la taille des communes. Si celles de moins de 1 000 habitants optent plutôt pour une messagerie externe pour près de 6 sur 10, les collectivités de 5 000 habitants et plus sont plus de 9 sur 10 à privilégier davantage les adresses de messageries internes. Des scores très stables à l'an 2023

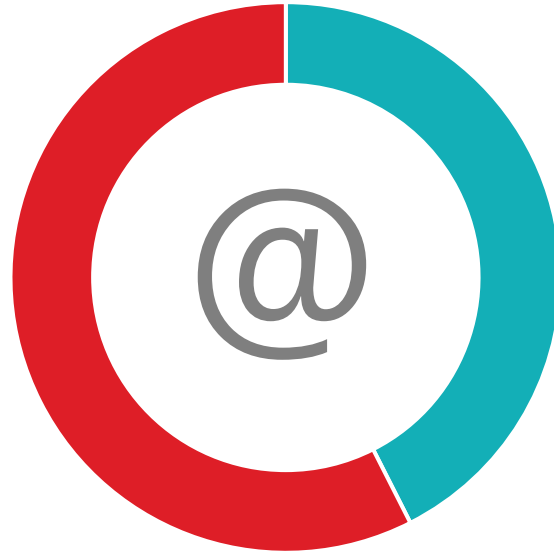
Q13. Pour communiquer avec vos administrés et les acteurs économiques et associatifs de votre territoire, utilisez-vous un service de messagerie de type :

Base : Total répondants (1710)

2023 : 51% ↗ **57%**

Externe (ex : Gmail, Orange, Yahoo, Hotmail...)

Moins de 300 habs. : 80%
Entre 300 et 999 habs. : 62%



43% ↘ 2023 : 49%

Interne avec un nom de domaine au nom de votre collectivité (ex : xx.xx@ville-de-xx.fr)

Entre 5k et 25k habs. : 94%
Entre 1k et 5k habs. : 75%



02

Des pratiques d'investissements révélatrices d'une constance dans l'appréhension des enjeux de sécurité informatique qui opposent petites et grandes collectivités

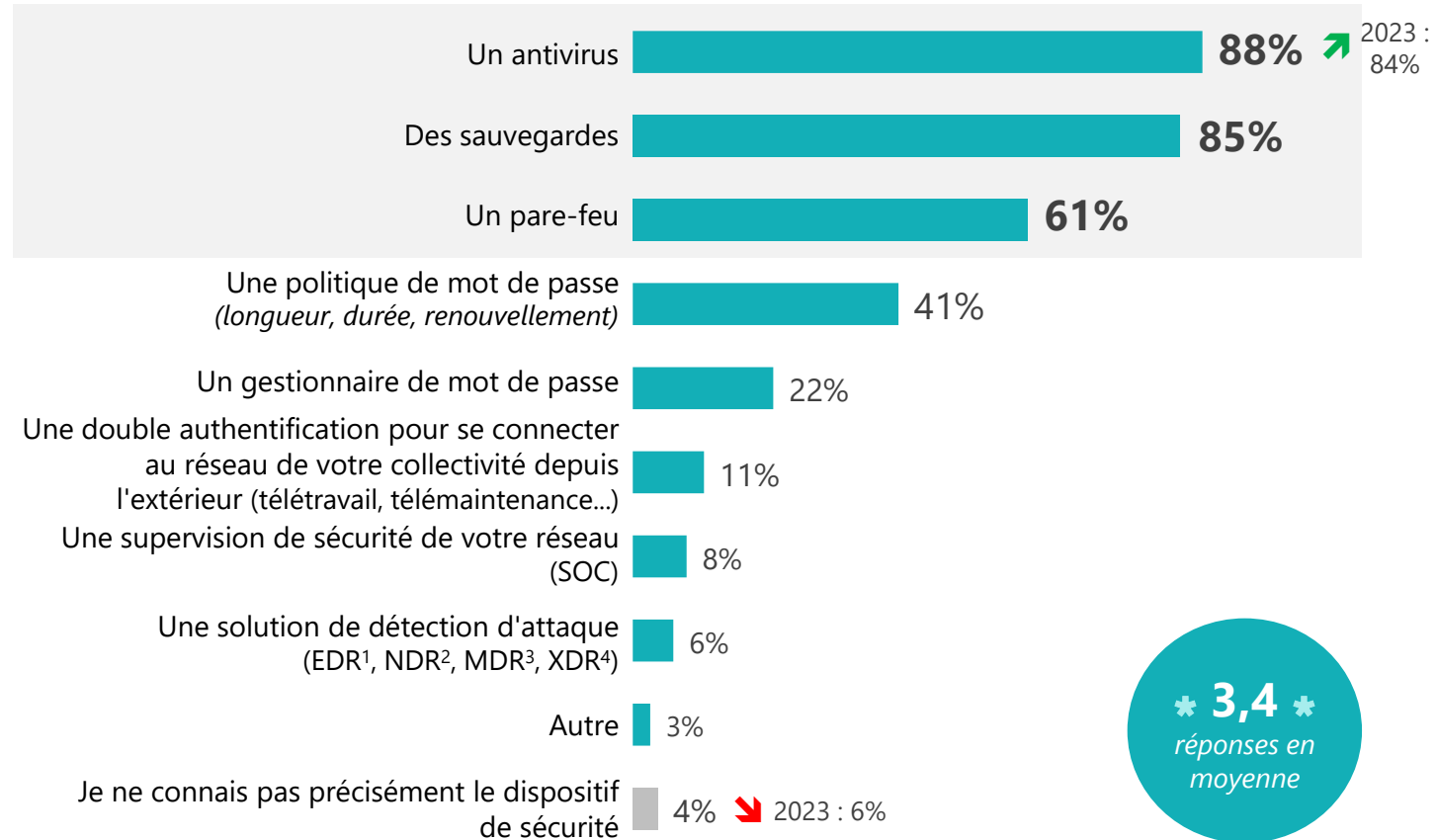
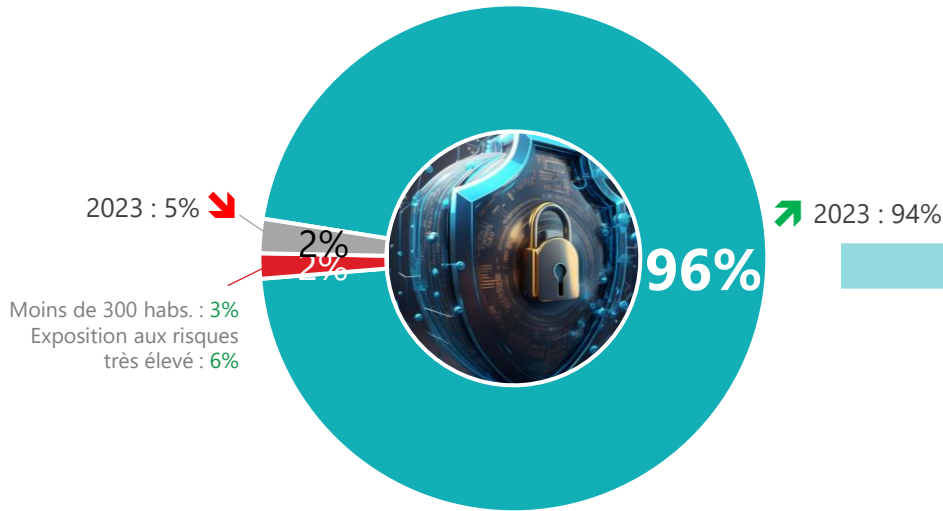


Des communes qui sont un peu plus nombreuses à déclarer être équipées de dispositifs de sécurité, là encore du fait d'une meilleure connaissance du répondant (baisse du taux de NSP). Les antivirus restent l'équipement le plus présent avec les sauvegardes et les pare-feux.

Q12. Votre collectivité est-elle équipée de dispositifs de sécurité (exemples : pare-feu, antivirus, sauvegarde ...) Base : Total répondants (1710)

Q12bis. Vous avez déclaré que votre collectivité était équipée de dispositifs de sécurité.

Pouvez-vous préciser lesquels ? Base : Ont déclaré que leur collectivité était équipée de dispositifs de sécurité (1645) - Plusieurs réponses possibles



*** 3,4 ***
réponses en moyenne

Entre 5k et 25k habs. : 5,1
Moins de 300 habs. : 3,1

● Oui ● Non ● Ne sait pas

1 EDR : Endpoint Detection Response / 2 NDR : Network Detection Response / 3 MDR : Managed Detection Response / 4 XDR : Extended Detection Response

x% / x% : Résultat statistiquement supérieur ou inférieur au total

↑ : Significativement supérieur à la vague précédente
↓ : Significativement inférieur à la vague précédente



Un taux d'équipement qui augmente en fonction de la taille de la collectivité.

Q12bis. Vous avez déclaré que votre collectivité était équipée de dispositifs de sécurité.

Pouvez-vous préciser lesquels ? Base : Ont déclaré que leur collectivité était équipée de dispositifs de sécurité (1645) - Plusieurs réponses possibles

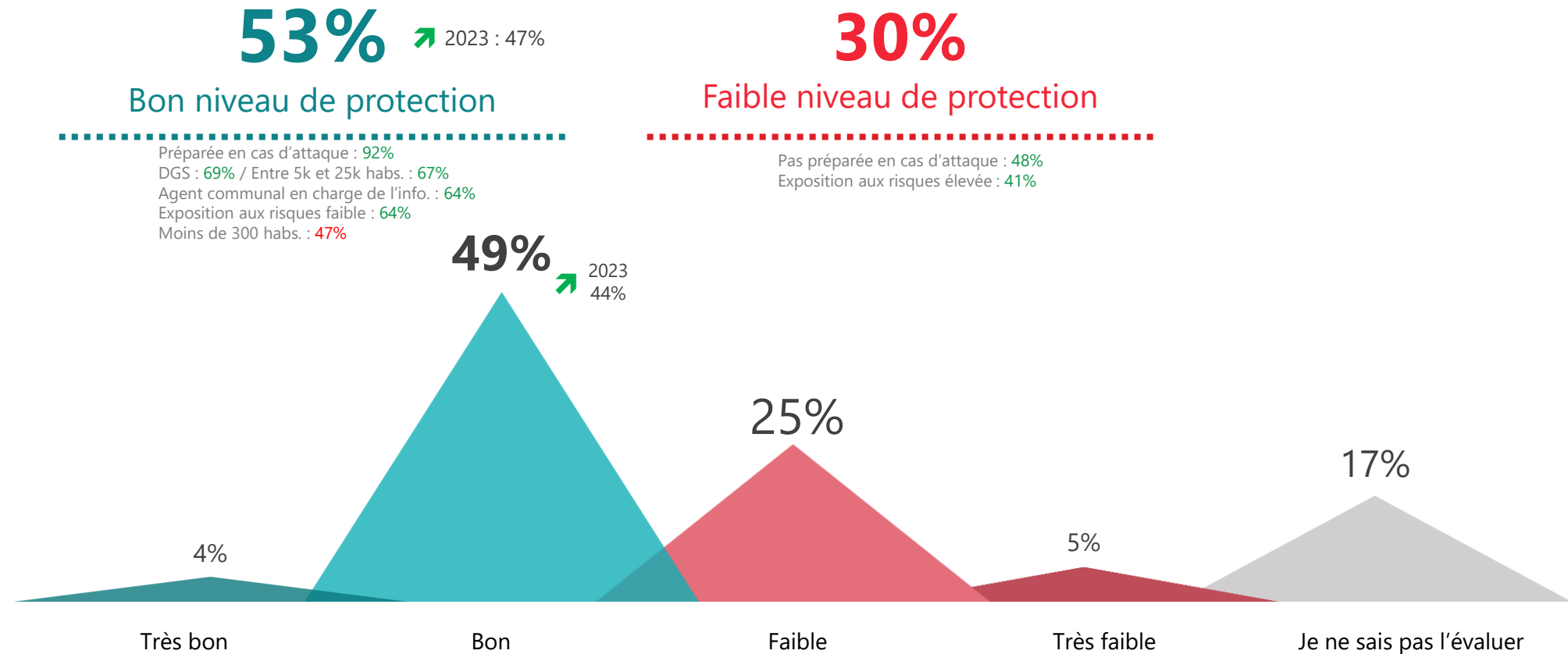
	TOTAL	Nombre d'habitants dans la collectivité					
		Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	1645	614	565	1179	366	68	33
Un antivirus	88% 2023 84%	88% 2023 81%	89%	88% 2023 83%	87%	88%	91%
Des sauvegardes	85%	80%	86%	83%	90%	84% 2023 96%	93%
Un pare-feu	61%	53%	55%	54%	78%	87%	89%
Une politique de mot de passe	41%	38%	40%	39%	42%	59%	76%
Un gestionnaire de mot de passe	22%	21%	20%	20%	21%	38%	47%
Une double authentification pour se connecter au réseau de votre collectivité depuis l'extérieur	11%	6%	8%	7%	18%	32%	38%
Une supervision de sécurité de votre réseau	8%	3%	6%	5%	14%	34%	29%
Une solution de détection d'attaque	6%	2%	4%	3%	9%	31%	45%
Autre	3%	2% 2023 5%	2%	2%	4%	2%	7%
Je ne connais pas précisément le dispositif de sécurité	4% 2023 6%	3% 2023 6%	3%	3% 2023 6%	6%	8%	3%
Nombre moyen de dispositif de sécurité	3,4	3,0	3,2	3,1	3,8	4,9	5,3



Des élus et agents qui sont plus de la moitié à considérer disposer d'un bon niveau de protection notamment les plus grandes collectivités (> de 5k hab.) ou celles considérant être préparées désormais en cas d'attaque. Un jugement qui s'avère en hausse par rapport à la vague précédente (+6pts). Néanmoins, 3 élus sur 10 estiment ne pas se sentir suffisamment protégés, en particulier ceux exposés à un risque élevé de cyberattaque et ceux qui jugent ne pas être assez préparés en cas d'incident.

Q11. Comment évaluez-vous le niveau de protection de votre collectivité en matière de sécurité informatique ?

Base : Total répondants (1710)





Une perception de la protection qui s'améliore aussi auprès des plus petites collectivités ...

Q11. Comment évaluez-vous le niveau de protection de votre collectivité en matière de sécurité informatique ?

Base : Total répondants (1710)

	TOTAL	Nombre d'habitants dans la collectivité					
		Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	1710	650	581	1231	376	68	34
ST Bon	53% 2023 47%	47% 2023 41%	54%	50%	57% 2023 49%	70%	59%
Très bon	4%	4%	4%	4%	4%	3%	2%
Bon	49% 2023 44%	43%	50%	46%	53%	67%	57%
ST Faible	30%	34%	26%	31%	32%	22%	31%
Faible	25%	26%	22%	24%	28%	19%	30%
Très faible	5%	8%	4%	7%	4%	3%	1%
Je ne sais pas l'évaluer	17%	19%	20%	19%	11% 2023 18%	8%	10%



03

Des collectivités qui sont plus nombreuses à déclarer avoir un bon niveau de protection et qui sont davantage à considérer être moins exposées notamment du fait d'une mise en place d'une protection accrue face aux attaques permettant de réduire le sentiment d'exposition,

... mais aussi du fait de petites collectivités qui se sentent plus éloignées des situations à risque et dont le diagnostic est faussé.



Un niveau de protection qui est globalement mieux perçu par les collectivités qui se traduit - par excès de confiance ou du fait de réelles actions de défense - par un sentiment d'être ainsi moins exposées (+6pts également). Ce ressenti est particulièrement marqué notamment auprès des toutes petites communes et des collectivités n'ayant jamais été victimes d'attaques ...

Q10. Selon vous, le niveau d'exposition aux risques de cyberattaques de votre collectivité est :

Base : Total répondants (1710)

44% ↗ 2023 : 38%

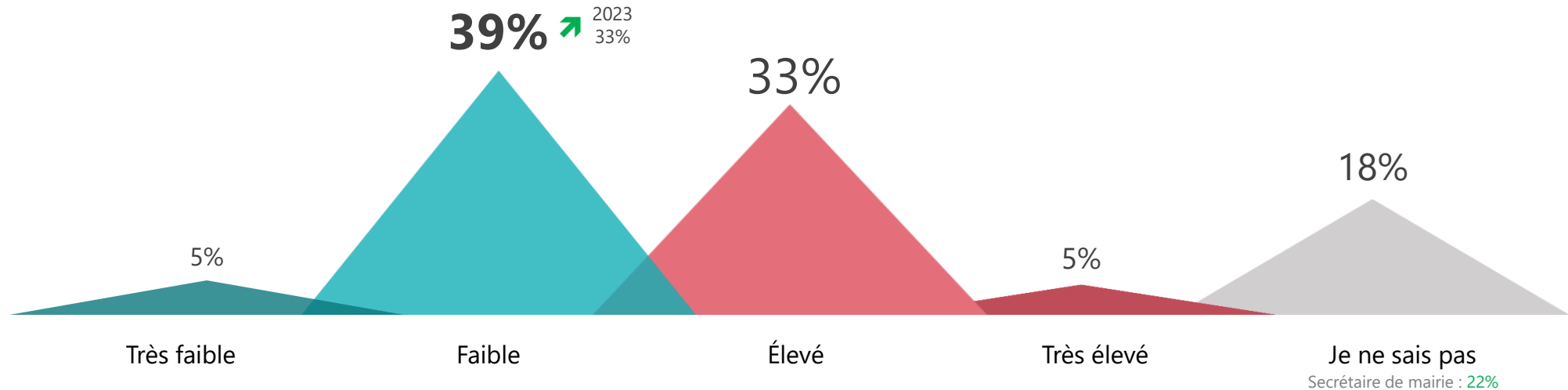
Faible exposition

- Préparée en cas d'attaque : 55%
- Protection perçue comme élevée : 53%
- N'a pas été victime d'une attaque : 48%
- Moins de 300 habs. : 49%
- Pas préparée en cas d'attaque : 39%
- Entre 5k et 25k habs. : 28%

38% ↘ 2023 : 42%

Forte exposition

- Entre 5k et 25k habs. : 63%
- Agent communal en charge de l'info. : 59%
- DGS : 50% / Victime d'une attaque : 50%
- Protection perçue comme faible : 50%
- Entre 1k et 5k habs. : 49%
- Pas préparée en cas d'attaque : 47%
- Moins de 1000 habs. : 33%
- Secrétaire de mairie : 32%





Les collectivités de moins de 1000 habitants sous-estime davantage les risques de cyberattaque malgré leur plus faible taux d'équipement.

Q10. Selon vous, le niveau d'exposition aux risques de cyberattaques de votre collectivité est :

Base : Total répondants (1710)

	TOTAL	Nombre d'habitants dans la collectivité					
		Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	1710	650	581	1231	376	68	34
ST Faible	44% 2023 38%	49% 2023 41%	46%	47% 2023 41%	36%	34%	14%
Faible	39% 2023 33%	41% 2023 34%	42% 2023 35%	41% 2023 34%	32%	33%	14%
Très faible	5%	8%	4%	6%	4%	1%	-
ST Elevé	38% 2023 42%	33%	31%	33% 2023 38%	49%	56%	80%
Très élevé	5%	4%	3%	4%	6%	7%	15%
Elevé	33%	29%	28%	29%	43%	49%	65%
Je ne sais pas	18%	18%	23%	20%	15%	10%	6%

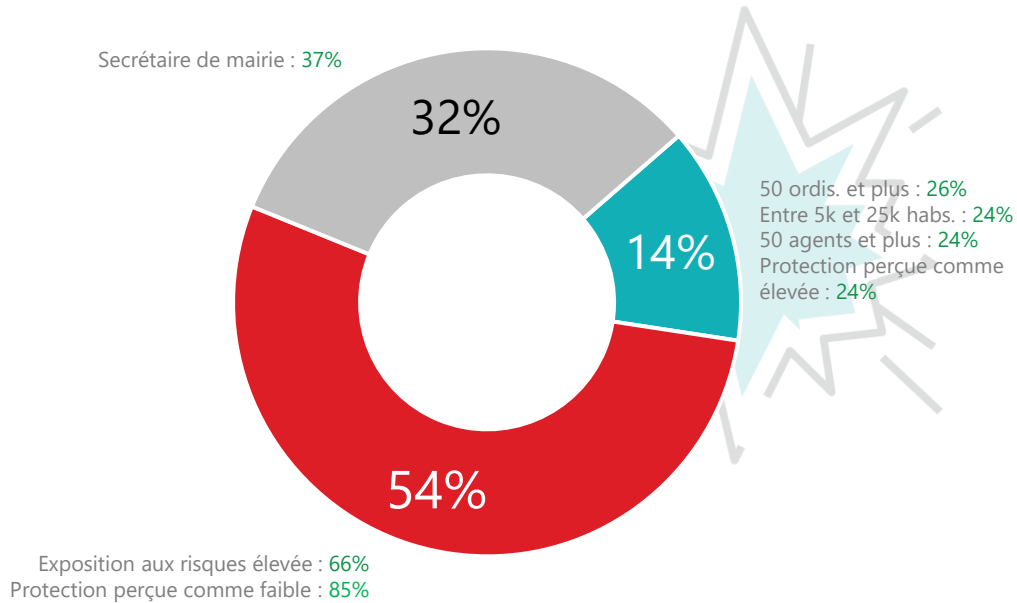


Pour autant elles sont toujours autant à considérer ne pas être suffisamment préparées en cas d'attaque. En effet, seulement 14 % estiment l'être suffisamment même si seule une sur 5 environ déclare disposer d'une procédure de réaction. Des résultats qui traduisent ainsi une hausse de la sous-estimation des cyberattaques...

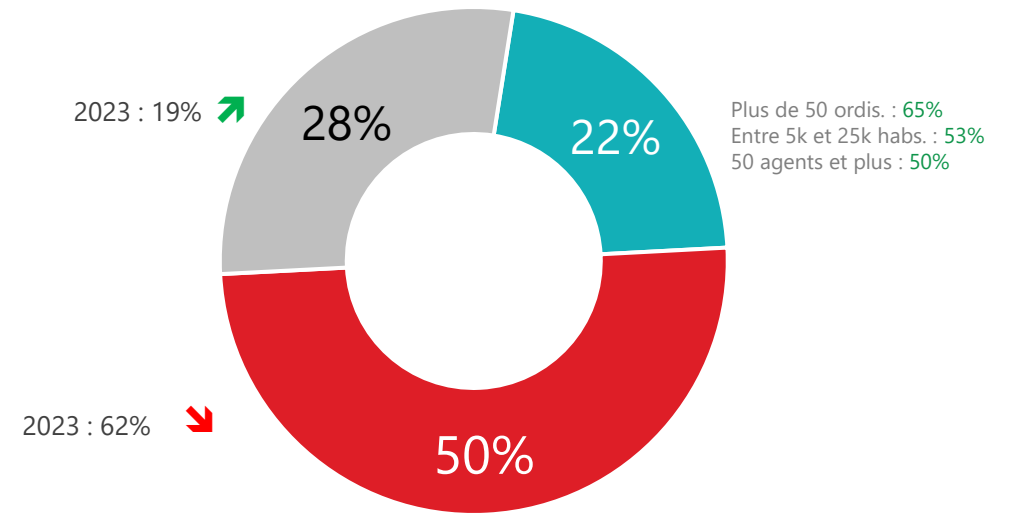
Q15. A votre connaissance, votre collectivité est-elle suffisamment préparée en cas d'attaque ? *Base : Total répondants (1710)*
 Q15bis. Disposez-vous d'une procédure de réaction (PRA*/PCA**) en cas d'attaque informatique ?

Base : Déclare être suffisamment préparé en cas d'attaque (236)

Préparées en cas d'attaque



Disposent d'une procédure de réaction



● Oui ● Non ● Ne sait pas

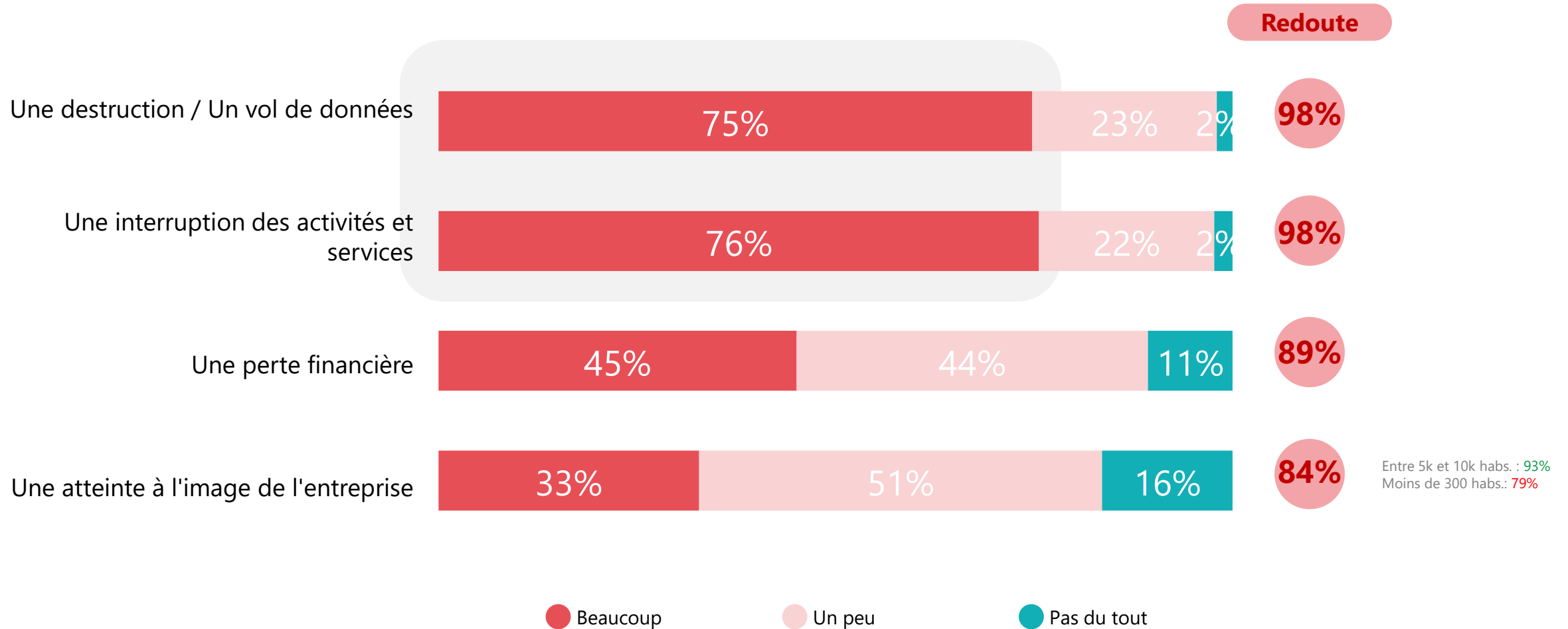
*PRA : Plan de reprise d'activité
 **PCA : Plan continuité d'activité



D'ailleurs, les collectivités redoutent le plus les interruptions d'activité et la destruction ou le vol de données

Q11b. En cas de cyberattaque, dans quelle mesure redoutez-vous ... ? * Nouvelle question ajoutée en 2024.

Base : Total répondants (1710)

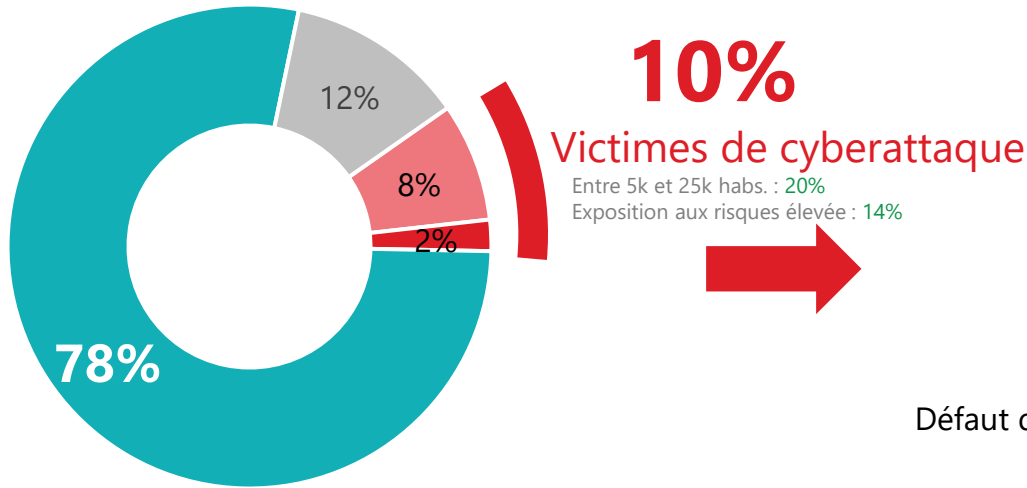




Pourtant 1 collectivité sur 10 déclare avoir été confrontée à un incident de sécurité informatique dans l'année, un score qui ne diminue donc pas. Des incidents surtout liés à de l'hameçonnage; ce dernier même si moins cité, demeure en effet de loin l'attaque la plus fréquente. Des attaques dont 45% des répondants déclarent ne pas en connaître les causes.

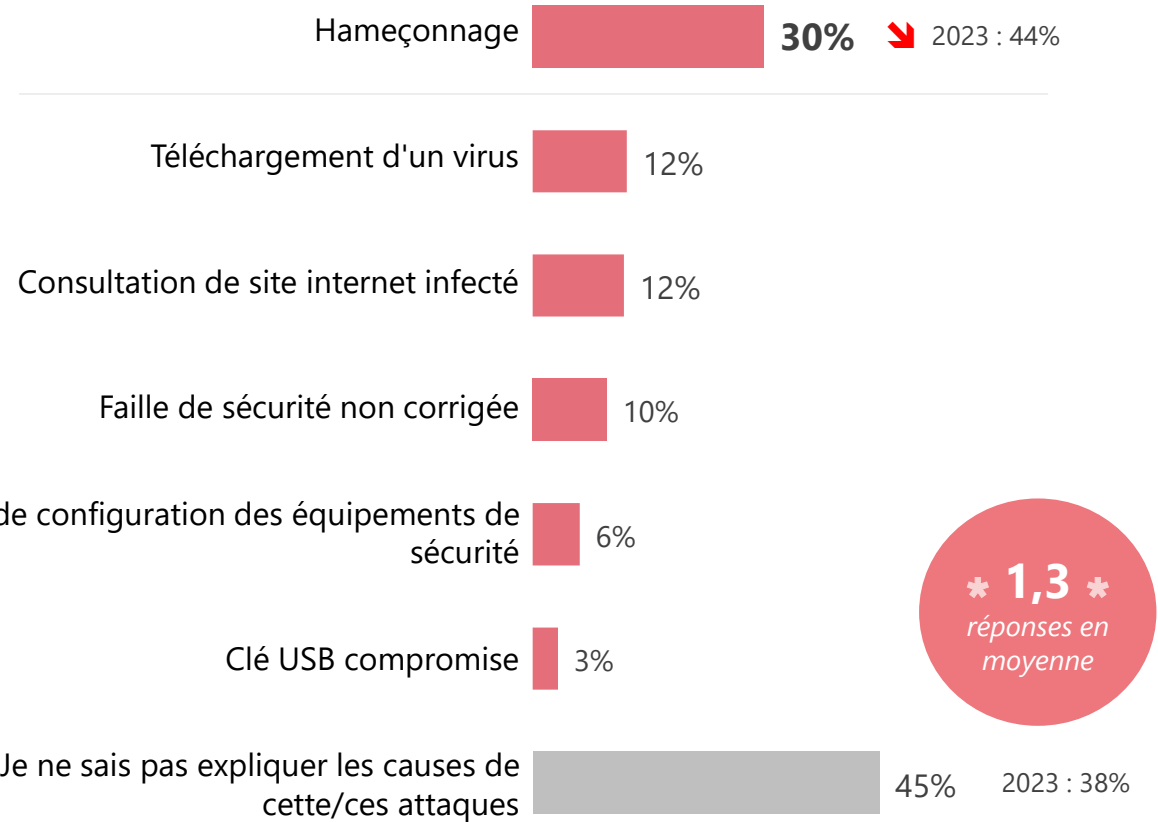
Q16. A votre connaissance, votre collectivité a-t-elle été victime d'un ou plusieurs incident(s) de sécurité informatique (rançongiciel, vol ou fuite de données, défiguration de site internet ...) autre qu'une panne au cours des 12 derniers mois ? Base : Total répondants (1710)

Q16bis. A votre avis, à quoi ces attaques étaient-elles liées ? Base : Collectivités victimes d'un ou plusieurs incident(s) de sécurité informatique (171) - Plusieurs réponses possibles



Exposition aux risques faible : 85%
Préparé en cas d'attaque : 84%
Protection perçue comme élevée : 82%
Exposition aux risques élevée : 71%
Entre 10k et 25k habs. : 69%

■ Oui 1 fois ■ Oui plusieurs fois...
■ Non, jamais ■ Je ne sais pas



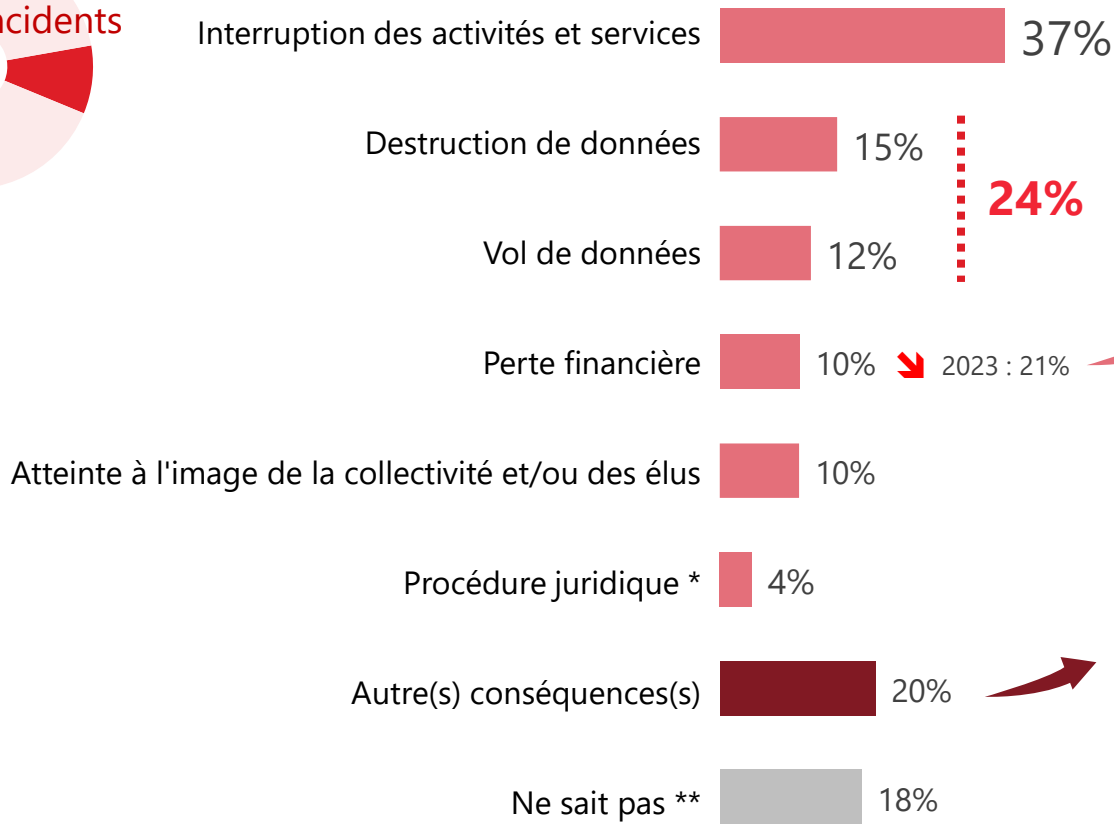
*** 1,3 ***
réponses en moyenne



Les conséquences restent avant tout des interruptions d'activité ...

Q16ter. Et quelles ont été les conséquences de cet/ces incident(s) ?

Base : Collectivités victimes d'un ou plusieurs incident(s) de sécurité informatique (171) - Plusieurs réponses possibles



*** 1,3 ***
réponses en moyenne

Baisse liée à l'ajout d'un code NSP en 2024 et notamment à une diminution tendancielle des destructions et vol de données (24% vs 34%) limitant en bout de chaîne, les pertes financières (conséquences de 2nd niveau)

“
Indisponibilité du site internet
Tentative de détournement de paiement par le biais d'un faux RIB
Accès messagerie provisoirement impossible
Piratage de boîtes mails
Interruption du travail le temps de la résolution de la contamination messagerie
Mobilisation de ressources humaines internes pour limiter les conséquences du « piratage »
Défiguration du site internet de la commune
Changement adresse mail
Phishing depuis la boîte mail piratée
 ”

**Ajout / *Modification d'items versus 2023.



04

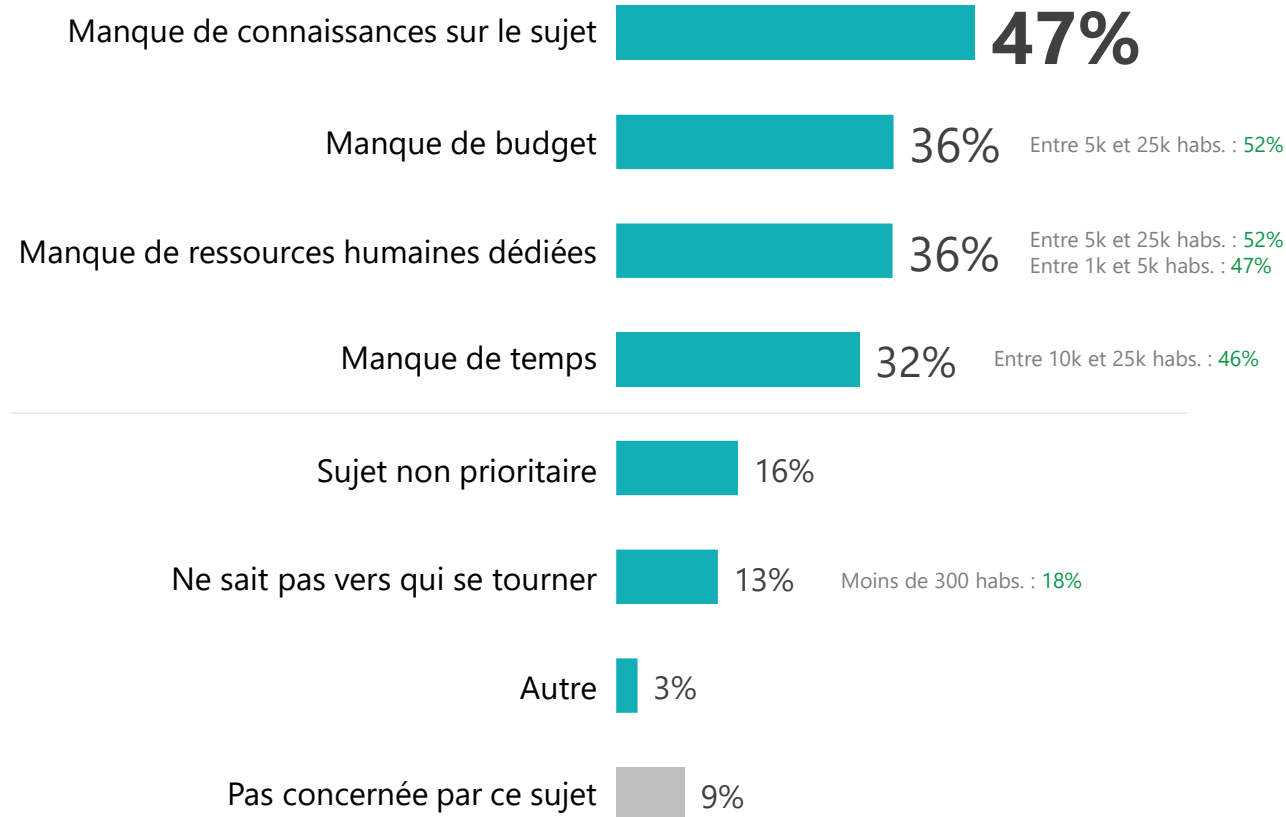
Le manque de connaissance demeure le frein principal pour être en capacité de faire le bon diagnostic quant au niveau de sécurité informatique, avant même des problématiques de budget et de temps



Les principaux freins à l'atteinte d'un bon niveau de sécurité informatique demeurent le manque de connaissances, l'insuffisance de personnel spécialisé, ainsi que des contraintes en termes de temps et de budget.

Q14. Et qu'est ce qui empêche votre collectivité d'atteindre le bon niveau de sécurité informatique qu'elle souhaite ?

Base : Total répondants (1710) - Plusieurs réponses possibles



91%
Au moins un frein cité

* **2,0** *
réponses en moyenne



Les grandes collectivités ont un besoin plus important de ressources, tant en temps homme qu'en budget, par rapport aux plus petites.

Q14. Et qu'est ce qui empêche votre collectivité d'atteindre le bon niveau de sécurité informatique qu'elle souhaite ?

Base : Total répondants (1710) - Plusieurs réponses possibles

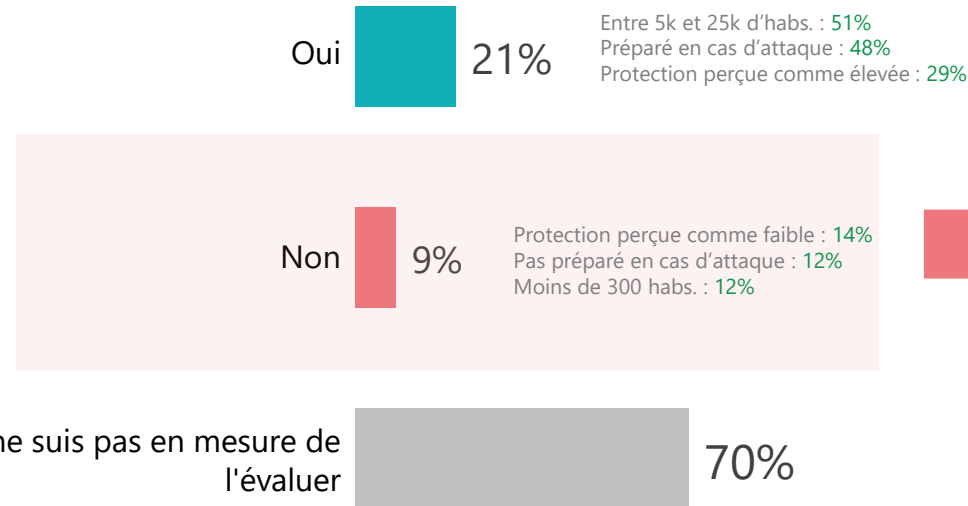
	TOTAL	Nombre d'habitants dans la collectivité					
		Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	1710	650	581	1231	376	68	34
Manque de connaissances sur le sujet	47%	47%	51%	49%	45%	24%	20%
Manque de ressources humaines dédiées	36%	37%	32%	35%	36%	49%	58%
Manque de temps	36%	29%	33%	31%	47%	51%	53%
Manque de budget	32%	29%	32%	31%	34%	29%	46%
Sujet non prioritaire	16%	17%	16%	16%	15%	14%	9%
Ne sait pas vers qui se tourner	13%	18%	13%	16%	7%	3%	6%
Autre	3%	2%	2%	2%	3%	5%	7%
Pas concernée par ce sujet	9%	7%	9%	8%	12%	14%	8%
Nombre moyen de freins	2,0	1,9	2,0	1,9	2,1	2,0	2,2



En outre, seulement 1 collectivité sur 5 considère que les solutions de cybersécurité proposées sur le marché répondent à ses besoins, tandis qu'1 sur 10 pense qu'elles ne sont pas adaptées. Parmi celles qui le pensent, le principal problème réside dans le manque d'adéquation avec leurs ressources humaines et des contraintes budgétaires.

Q18b. Pensez-vous que les solutions de cybersécurité actuellement proposées sur le marché soient adaptées aux besoins de votre collectivité... ?

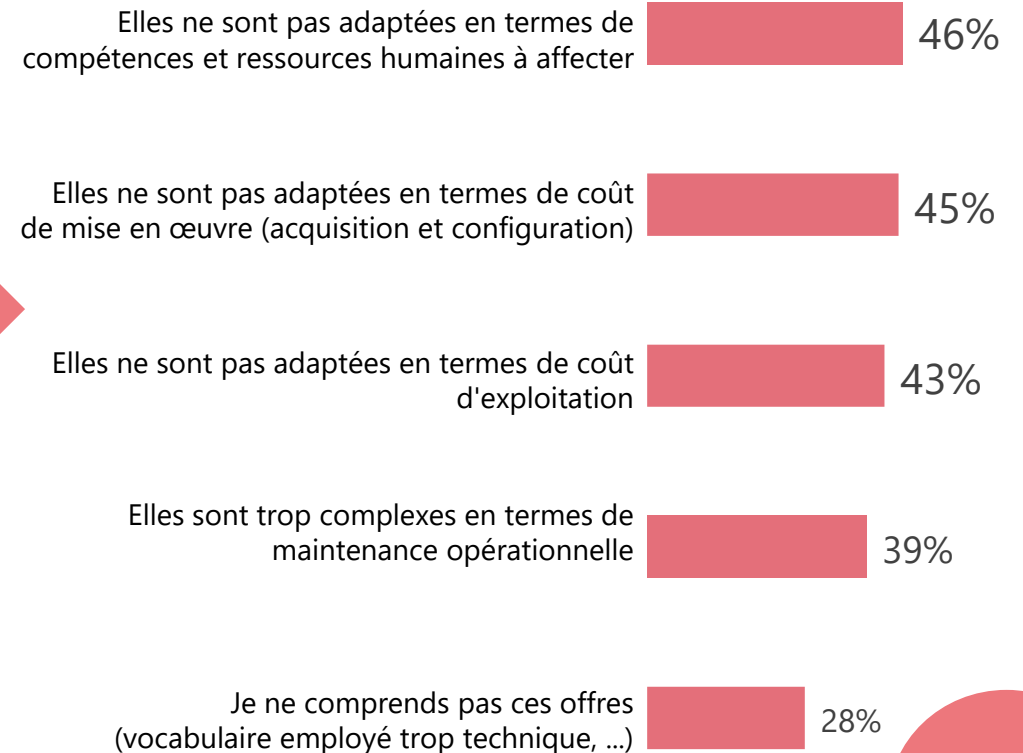
Base : Total répondants (1710)
Nouvelle question ajoutée en 2024.



Q18c. Pourquoi indiquez-vous que ces solutions de cybersécurité proposées sur le marché ne sont pas adaptées à vos besoins ... ?

Base : Ont déclaré que les solutions de cybersécurité proposées ne sont pas adaptées aux besoins de leurs collectivités (147) - Plusieurs réponses possibles

Nouvelle question ajoutée en 2024.



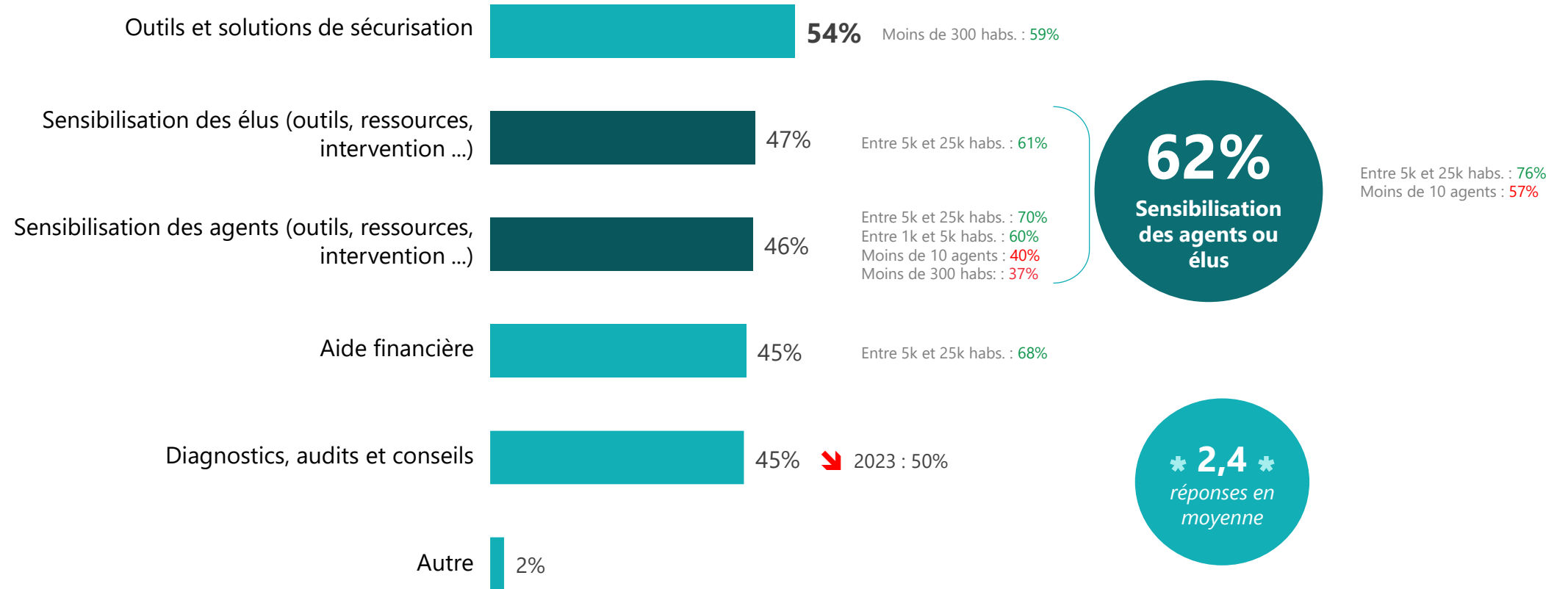
*** 2,0 ***
réponses en moyenne



Face à ces obstacles, les collectivités expriment différents besoins et notamment des besoins prioritaires en outils de sécurisation, en sensibilisation des agents et élus, et en aide financière.

Q18. Quels seraient vos besoins prioritaires en matière de sécurité informatique ?

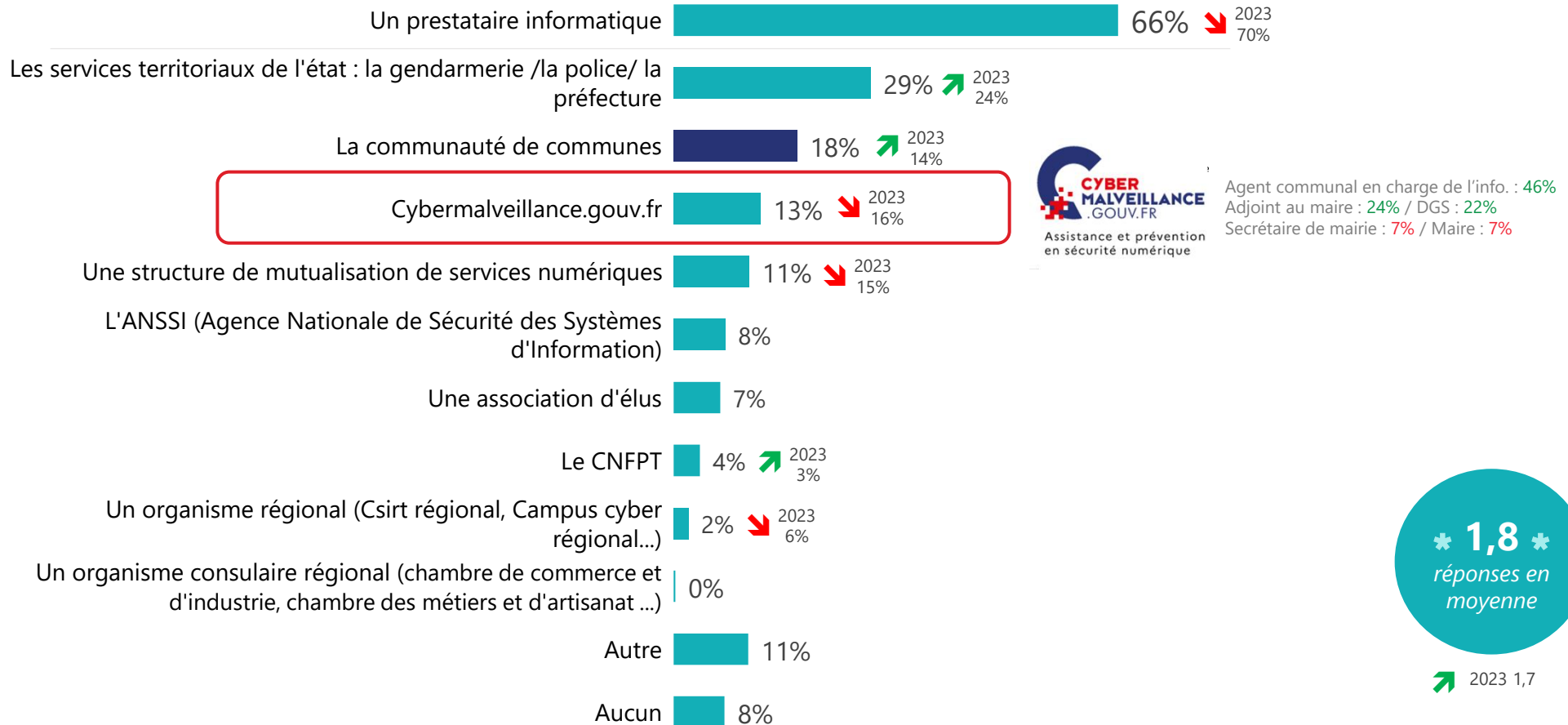
Base : Total répondants (1710) - Plusieurs réponses possibles





Une prise d'information à la sécurité qui passe notamment par le prestataire informatique qui demeure le point de contact le plus utilisé par les communes pour s'informer ou se faire aider dans un contexte où elles sont une majorité (7 sur 10) à externaliser leur gestion informatique. Des acteurs de proximité, comme les services territoriaux de l'état ou encore la communauté de communes, semblent davantage avoir été utilisés cette année.

Q19. Sur votre territoire, vers qui vous tournez-vous actuellement pour vous informer ou vous aider sur le sujet de la sécurité informatique ? Base : Total répondants (1710) - Plusieurs réponses possibles





Les collectivités de moins de 1 000 habitants se tournent moins vers Cybermalveillance.gouv.fr, contrairement à celles de 5 000 habitants qui demeurent un interlocuteur privilégié tout comme l'ANSSI

Q19. Sur votre territoire, vers qui vous tournez-vous actuellement pour vous informer ou vous aider sur le sujet de la sécurité informatique ? Base : Total répondants (1710) - Plusieurs réponses possibles

	TOTAL	Nombre d'habitants dans la collectivité					
		Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	1710	650	581	1231	376	68	34
Un prestataire informatique	66% 2023 70%	63%	66% 2023 72%	64% 2023 69%	71%	73%	59%
Les services territoriaux de l'état : la gendarmerie /la police/ la préfecture	29% 2023 24%	31% 2023 23%	29%	30% 2023 24%	28%	25%	23%
La communauté de communes	18% 2023 14%	19%	18% 2023 11%	19% 2023 13%	19%	12%	14%
Cybermalveillance.gouv.fr	13% 2023 16%	8% 2023 13%	9%	9% 2023 13%	18%	44%	46%
Une structure de mutualisation de services numériques	11% 2023 15%	10%	13%	11% 2023 15%	11% 2023 18%	9%	15%
L'ANSSI	8%	2% 2023 4%	4%	3%	12%	44%	62%
Une association d'élus	7%	7%	8% 2023 5%	8%	5%	3%	4%
Le CNFPT	4% 2023 3%	2%	4%	3%	6% 2023 3%	3%	8%
Un organisme régional (Csirt régional, Campus cyber régional...)	2% 2023 6%	1% 2023 7%	1%	1% 2023 5%	3%	11%	12%
Un organisme consulaire régional (chambre de commerce et d'industrie, chambre des métiers et d'artisanat...)	0%	-	1%	0%	0%	-	1%
Autre	11%	12%	11%	12%	10%	3%	4%
Aucun	8%	10%	8%	9%	4%	4%	5%
Nombre moyen d'acteurs cités	1,8 2023 1,7	1,7	1,8 2023 1,6	1,8 2023 1,6	1,9	2,4	2,6

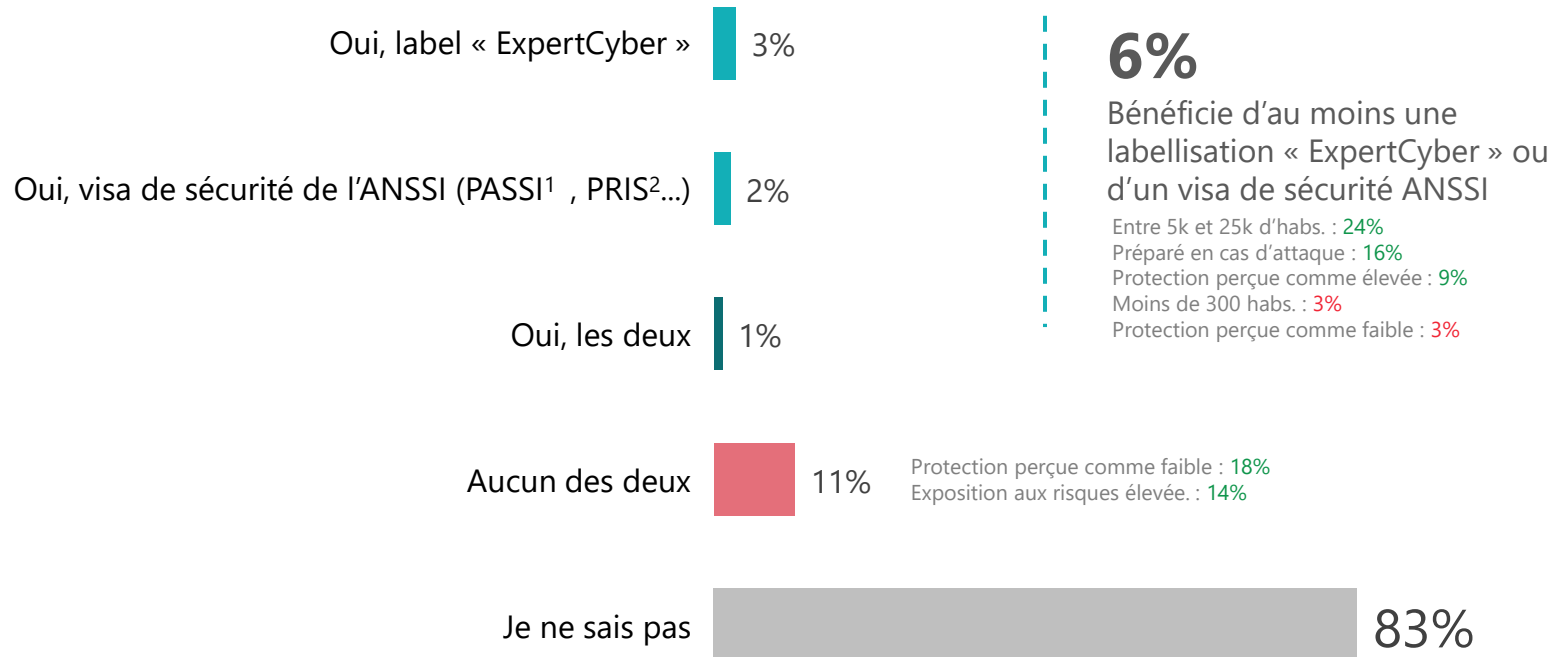


Des points de contacts tel que le prestataire informatique ou la structure de mutualisation dont plus de 8 collectivités sur 10 qui les utilisent ne peuvent en attester le niveau d'expertise en cybersécurité.

Q19b. Votre prestataire informatique ou votre structure de mutualisation bénéficie-t-il d'une labellisation « ExpertCyber » ou d'un visa de sécurité de l'ANSSI (PASSI1, PRIS2...) pour attester de son expertise en cybersécurité ?

Base : Ont déclaré se tourner vers un prestataire informatique ou une structure de mutualisation pour s'informer (1227)

Nouvelle question ajoutée en 2024.

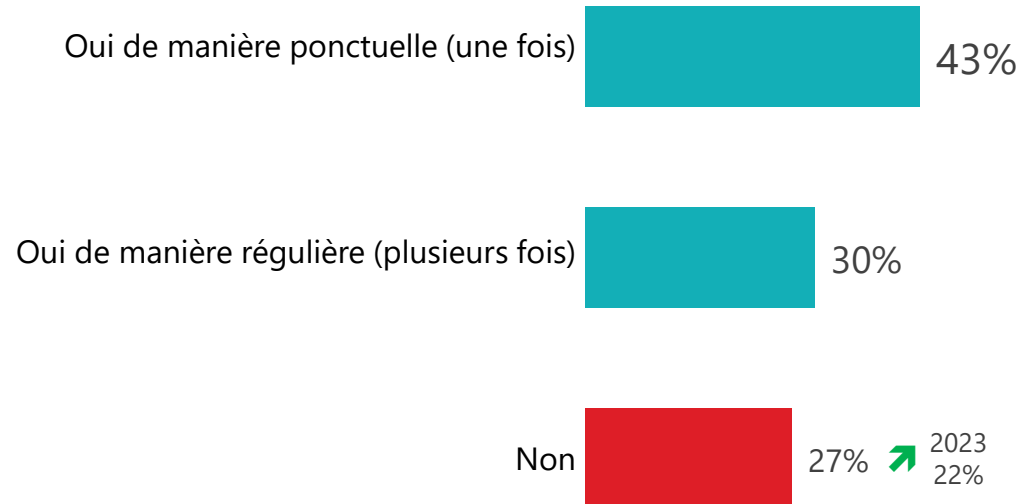




Une sensibilisation à la sécurité informatique qui a touché 7 élus sur 10 au cours des 12 derniers mois Notamment les plus grandes communes qui sont aussi celles qui perçoivent un risque d'exposition élevé

Q17. Avez-vous, en tant qu'élu(e) ou agent, été sensibilisé(e) à la sécurité informatique au cours des 12 derniers mois ?

Base : Total répondants (1710)



73%

↘ 2023 : 78%

Ont déjà été sensibilisé au moins une fois à la sécurité informatique

Préparé en cas d'attaque : 95%

50 ordis et plus : 89%

Entre 5k et 25k d'habs. : 86%

Protection perçue comme élevée : 84%

50 agents et plus : 82%

Exposition aux risques élevée : 78%

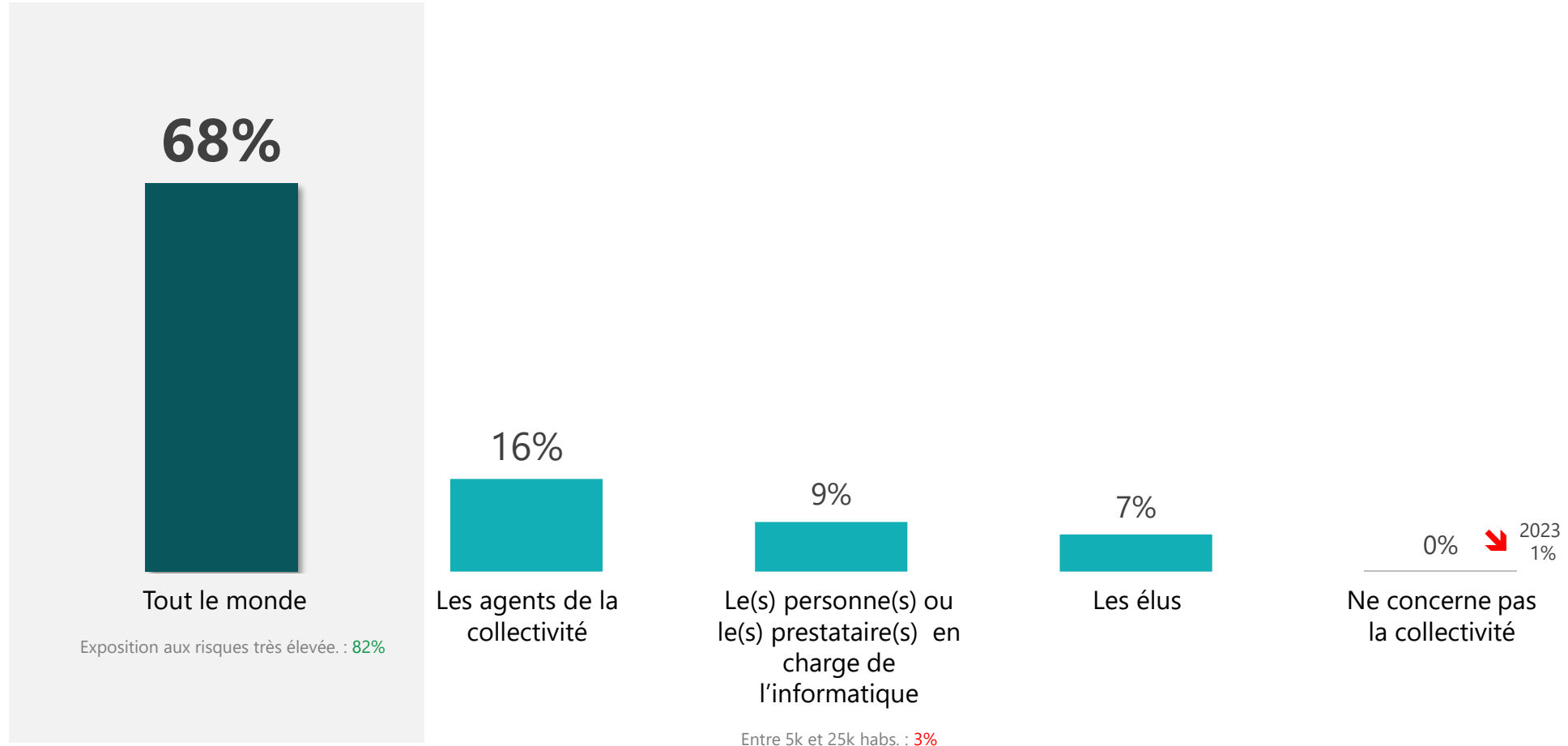
Protection perçue comme faible : 64%



Une vision quant à la sécurité informatique qui demeure stable avec près de 7 élus et agents sur 10 qui estiment que la sécurité informatique est la responsabilité de tous, qu'il s'agisse des agents de la collectivité, des prestataires informatiques ou des élus.

Q9. Selon vous, pour la collectivité, la sécurité informatique doit impliquer en priorité...

Base : Total répondants (1710)





RESTONS CONNECTÉS !

www.opinion-way.com



Envie d'aller plus loin ?

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

[newsletter !](#)

“opinionway

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN

Vos contacts

Larissa Xia

Analyste confirmée Département *AdVanced Methods*
lxia@opinion-way.com

Christine Pujol

Directrice du Département *AdVanced Methods*
Tel. +33 7 76 91 19 23
cpujol@opinion-way.com

“AdVanced #quant
#analytics
#multi-sector
“opinionway