opinionway

— POUR —

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Cybermalveillance.gouv.fr
Assistance et prévention en cybersécurité

État des lieux de la prise de conscience de la sécurité informatique au sein des collectivités françaises de moins de 25000 habitants

Vague 2026

Rapport d'étude | novembre 2026



Image de kjpargeter sur freepik

Contexte et Objectifs



Les cybermenaces constituent un enjeu croissant pour les collectivités territoriales, dont le fonctionnement repose sur des outils numériques et la gestion de données parfois sensibles. La continuité des services publics et la protection des informations des administrés sont ainsi directement concernées.

Dans le cadre de ses missions d'assistance aux victimes, de prévention et d'observation de la menace numérique, **Cybermalveillance.gouv.fr reconduit en 2026 son baromètre auprès des élus et agents des collectivités de moins de 25 000 habitants**, après deux premières vagues réalisées en 2023 et 2024.

Cette nouvelle vague intervient dans un contexte particulier : celui du renouvellement des équipes municipales à la suite des élections de mars 2026. Réalisée quelques mois après le scrutin, elle permet d'apprécier les perceptions et les besoins des collectivités en début de mandat, tout en poursuivant l'observation des évolutions depuis 2024.

L'étude poursuit quatre objectifs :

- *Évaluer les moyens et l'organisation informatiques des collectivités.*
- *Mesurer la perception des cyberrisques, du niveau de protection et de la préparation aux incidents.*
- *Identifier les freins à la sécurisation et les besoins prioritaires d'accompagnement.*
- *Comprendre les pratiques d'information et de recours aux différents interlocuteurs de la cybersécurité, dont Cybermalveillance.gouv.fr.*

Cette troisième vague apporte ainsi un nouvel éclairage sur la manière dont les collectivités appréhendent les enjeux de cybersécurité et sur les leviers permettant de renforcer leur protection.



La méthodologie

La méthodologie

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

Un protocole identique aux précédentes mesures …

Une enquête ouverte auprès des élus et agents des collectivités de moins de 25 000 habitants

Echantillon de **2830 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).

Un redressement a posteriori sur la taille des communes a été appliqué afin de restituer la structure des communes françaises de moins de 25 000 habitants selon ce critère et de faciliter la comparaison avec les vagues précédentes.

L'étude a été menée par questionnaire auto-administré en ligne sur système CAWI (Computer Assisted Web Interview)

Questionnaire

Les interviews ont été réalisées **du 24 août au 29 septembre 2026**

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…) et via une base « écosystème collectivités » constituée par Cybermalveillance.fr.

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 tests de significativité à 95% et donc des marges d'incertitude : 0,8 à 1,8 points au plus pour un échantillon de 2830 répondants.

Redressement de l’échantillon

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



Photo de Maria Orlova sur Pexels

	% Brut		*% Redressé*	
Taille de communes	*Effectif*	*%*	*Effectif*	*%*
Base	*2830*		*2830*	
Moins de 300 habitants	801	28%	1075	38%
Entre 300 et 999 habitants	989	35%	962	34%
Entre 1000 et 4999 habitants	755	27%	623	22%
Entre 5000 et 9999 habitants	157	6%	113	4%
Entre 10 000 et 25 000 habitants	128	4%	57	2%

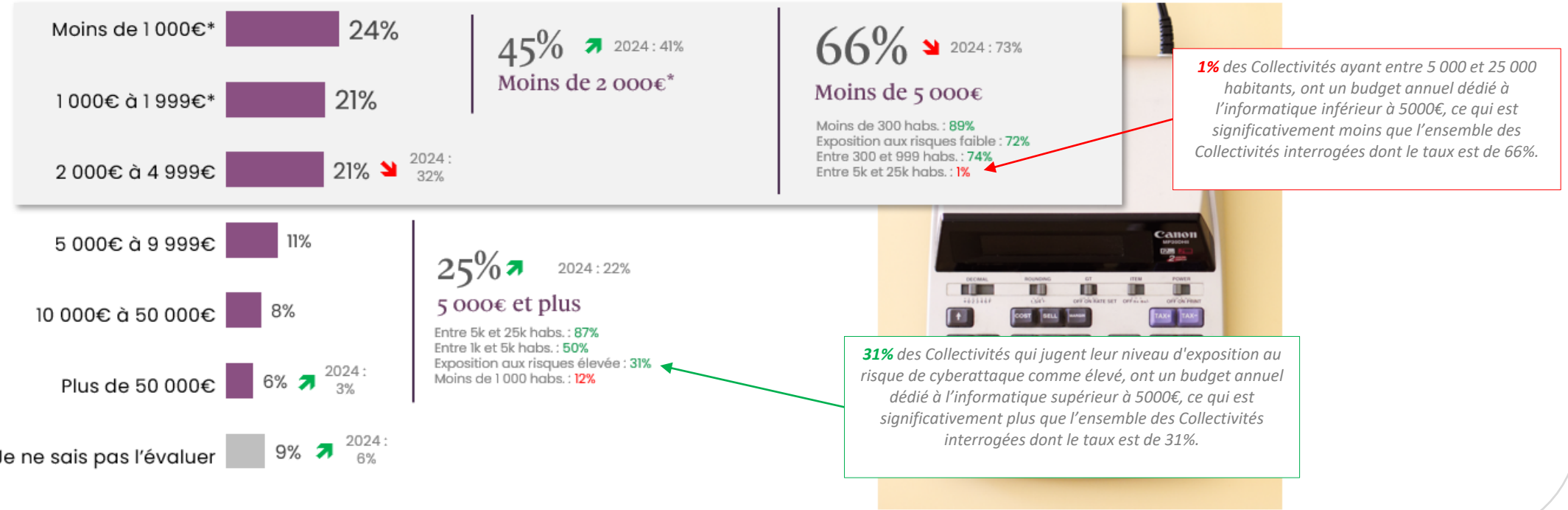
Source : Insee, Recensement de la population 2023 – populations municipales de référence en vigueur au 1er janvier 2026. Calculs sur les communes de moins de 25 000 habitants, France métropolitaine et quatre DROM (hors Mayotte).

Aide à la lecture des résultats

- **Les écarts significatifs, au seuil de 95% de confiance, seront indiqués de la manière suivante par rapport à la population totale de référence (Ensemble des élus/agents communaux) :**

  X% : résultats significativement supérieurs à l'échantillon total à 95%
  Y% : résultats significativement inférieurs à l'échantillon total à 95%

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 (2830)



***1%** des Collectivités ayant entre 5 000 et 25 000 habitants, ont un budget annuel dédié à l'informatique inférieur à 5000€, ce qui est significativement moins que l'ensemble des Collectivités interrogées dont le taux est de 66%.*

***31%** des Collectivités qui jugent leur niveau d'exposition au risque de cyberattaque comme élevé, ont un budget annuel dédié à l'informatique supérieur à 5000€, ce qui est significativement plus que l'ensemble des Collectivités interrogées dont le taux est de 31%.*



Image de vwalakte sur Magnific

Profil des collectivités interrogées et contexte municipal

Un tissu de petites communes, des répondants aux profils variés et un nouveau cycle municipal

Majoritairement composées de communes de moins de 1 000 habitants, les collectivités reflètent des réalités organisationnelles très différentes selon leur taille.

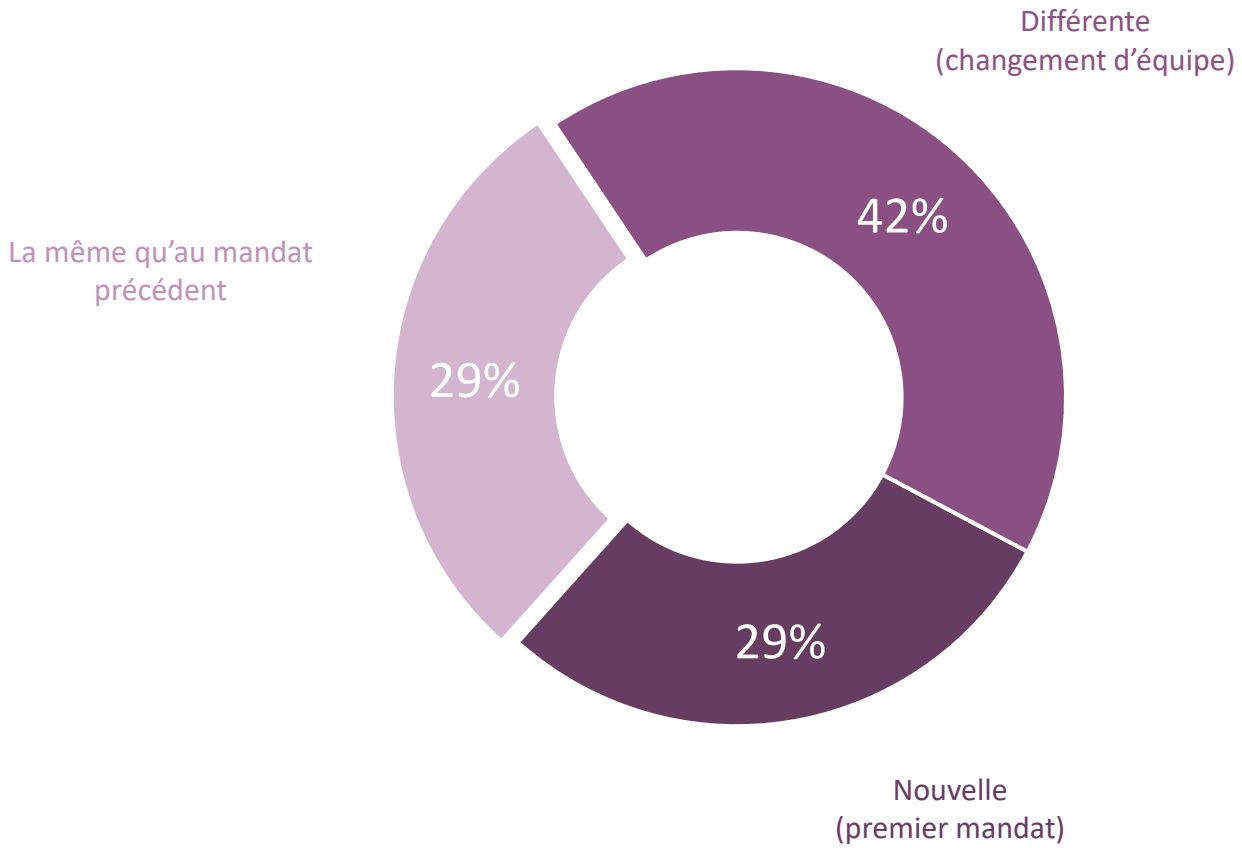
Cette vague 2026 s'inscrit également dans un contexte de renouvellement des équipes municipales, susceptible d'influencer la connaissance des dispositifs existants, l'appréciation des risques et les priorités de sécurisation.

Un contexte essentiel pour éclairer la lecture des résultats et leurs évolutions depuis 2024.

La troisième vague du baromètre intervient dans un contexte de renouvellement municipal important : 71% des répondants déclarent une équipe municipale nouvelle ou différente de celle du mandat précédent. Plus précisément, 29% évoquent une équipe nouvellement élue pour un premier mandat, 42% une équipe différente et 29% une équipe reconduite.

Q22 : Depuis les dernières élections municipales, l'équipe municipale de votre collectivité est :

Base : Total répondants (2830) – *Nouvelle question*



71%

Changement d'équipe municipale

Adjoint au maire : 38% / Maire : 38%
Secrétaire de mairie : 19%

Ce contexte constitue un élément de lecture important de la vague 2026. L'arrivée de nouveaux élus ou le renouvellement des équipes peut s'accompagner d'une réévaluation des priorités, mais également d'une connaissance encore incomplète des budgets et des dispositifs informatiques déjà en place.
Les évolutions constatées depuis 2024 doivent donc être appréciées en tenant compte de ce contexte et du profil des répondants, sans pouvoir être directement attribuées au renouvellement municipal.

Le profil des répondants reflète ainsi étroitement l'organisation des collectivités : dans les plus petites communes, ce sont avant tout les élus et les secrétaires de mairie qui répondent, alors que les collectivités plus importantes mobilisent davantage leurs fonctions administratives et informatiques.

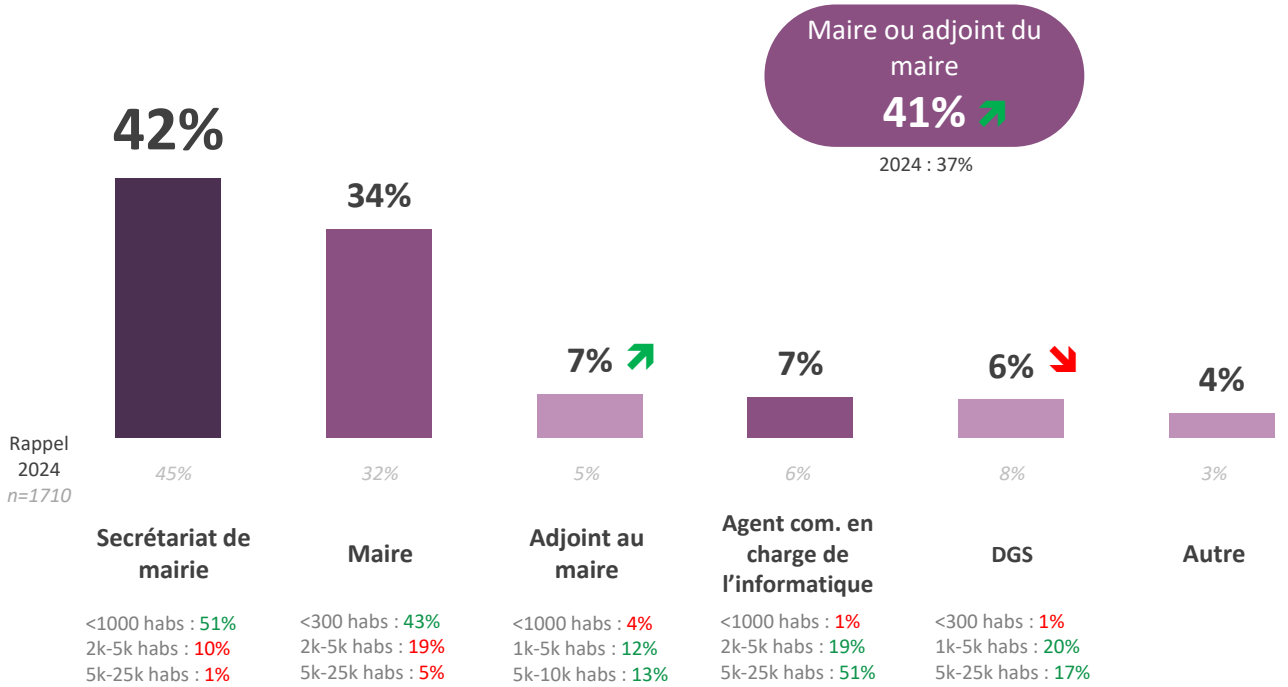
Q21. Quelle est votre fonction ?

Base : Total répondants (2830)


Photo de Efrem Efre sur Pexels: https://www.pexels.com/fr-fr/photo/38970310/

Fonction du répondant

Les maires et leurs adjoints ont davantage répondu lors de cette nouvelle mesure 2026…

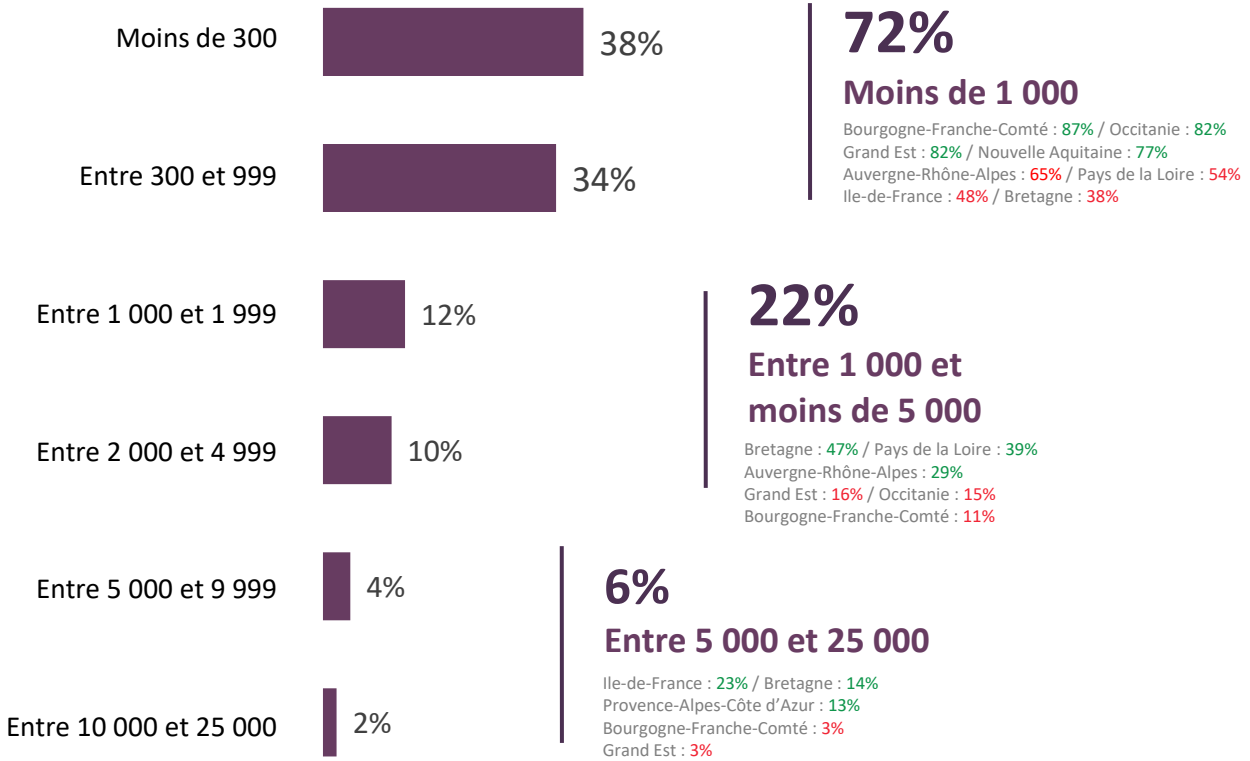


Un baromètre largement structuré par les petites communes : 72% comptent moins de 1 000 habitants, 94% moins de 5 000. Les communes de 5 000 à 25 000 habitants ne représentant, quant à elles, que 6% de l'échantillon...

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

Base : Total répondants (2830)





72%
Moins de 1 000
Bourgogne-Franche-Comté : 87% / Occitanie : 82%
Grand Est : 82% / Nouvelle Aquitaine : 77%
Auvergne-Rhône-Alpes : 65% / Pays de la Loire : 54%
Ile-de-France : 48% / Bretagne : 38%

22%
Entre 1 000 et moins de 5 000
Bretagne : 47% / Pays de la Loire : 39%
Auvergne-Rhône-Alpes : 29%
Grand Est : 16% / Occitanie : 15%
Bourgogne-Franche-Comté : 11%

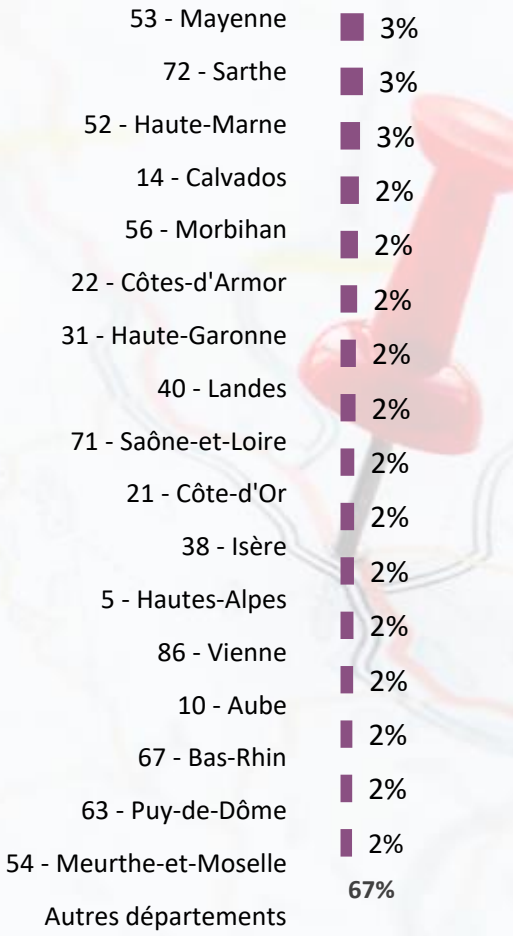
6%
Entre 5 000 et 25 000
Ile-de-France : 23% / Bretagne : 14%
Provence-Alpes-Côte d'Azur : 13%
Bourgogne-Franche-Comté : 3%
Grand Est : 3%

Structure redressée a posteriori (cf. page 5)

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

Une couverture territoriale étendue

Départements les plus représentés dans l'échantillon

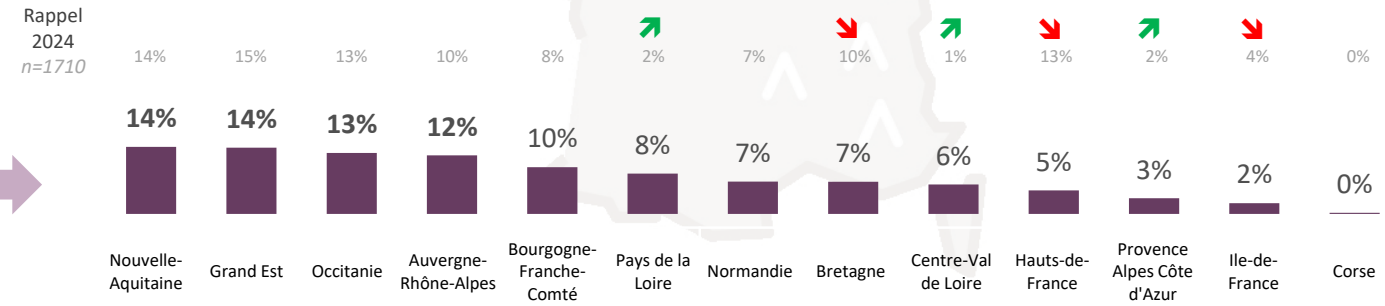


Seuls les départements supérieurs ou égaux à 1% sont présentés

France métropolitaine **100%**

DROM **<1%**

Régions représentées dans l'échantillon



Base : Total répondants (2830)

: Résultat statistiquement supérieurs ou inférieurs à la vague 2024

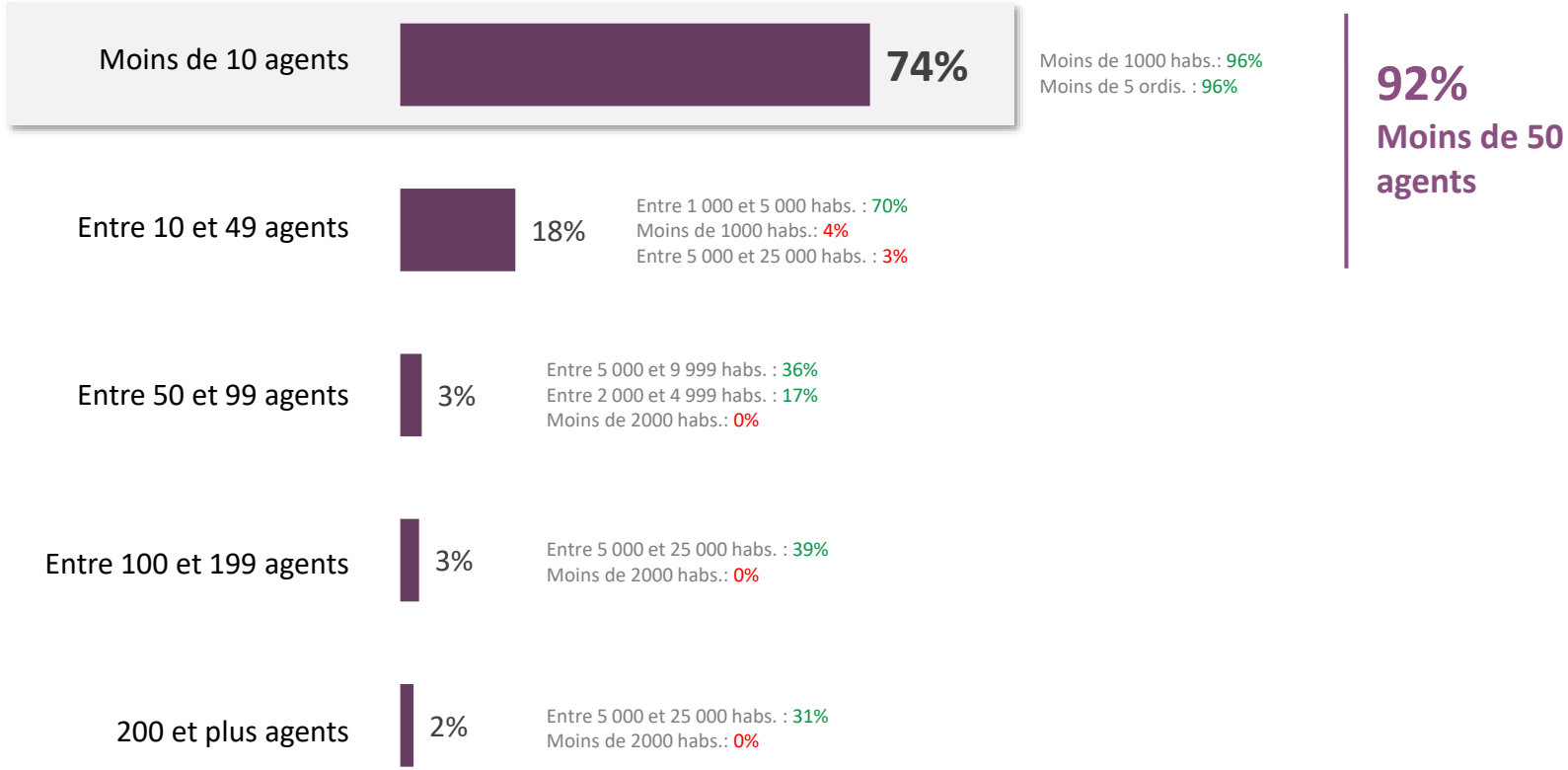
x% / x% : Résultat statistiquement supérieur ou inférieur au total

Des collectivités aux effectifs réduits : près des trois quarts comptent moins de 10 agents, en particulier les communes 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 (2830)


Image de Freepik



92%
Moins de 50 agents



Les résultats

opinionway

01

Perception de la sécurité informatique et réaction face aux cyberrisques



Cette année, les collectivités se montrent plus critiques quant à leur niveau de protection : si près de la moitié le jugent bon, **plus d'un tiers l'estiment faible**, une proportion en hausse par rapport à 2024. Le sentiment d'être bien protégé est plus marqué parmi celles qui se considèrent préparées en cas d'attaque. À l'inverse, les plus petites communes, disposant de moyens plus limités, se perçoivent davantage en difficulté.

q11. Comment évaluez-vous le niveau de protection de votre collectivité en matière de sécurité informatique ?

Base : Total répondants (2830)

52%

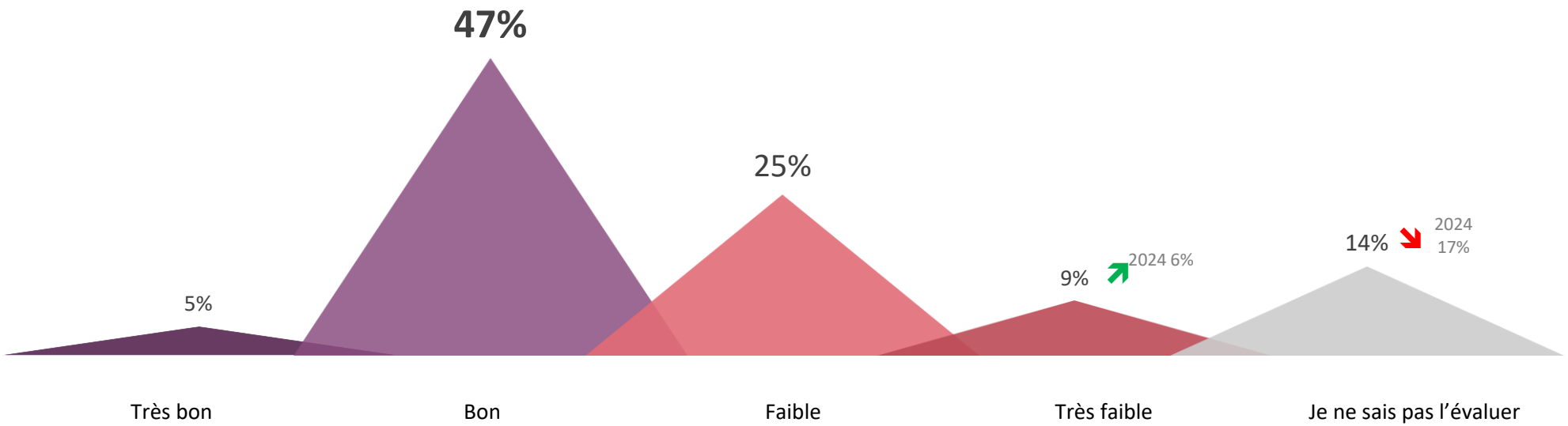
Bon niveau de protection

Préparé en cas d'attaque : 92%
DGS : 62% / Entre 5k et 25k habs. : 70%
Agent communal en charge de l'info. : 73%
Exposition aux risques faible : 60%
Moins de 300 habs. : 46%

34% ↗ 2024 : 30%

Faible niveau de protection

Pas préparé en cas d'attaque : 50%
Exposition aux risques élevée : 42%
Moins de 300 habs. : 39%



Cette perception varie nettement selon la taille : le sentiment d'être bien protégé augmente avec celle-ci, alors que **les communes de moins de 1 000 habitants portent un regard plus critique qu'en 2024,** avec davantage de jugements de protection faible (+5 points) et moins de « ne sait pas ».

q11. Comment évaluez-vous le niveau de protection de votre collectivité en matière de sécurité informatique ?
Base : Total répondants (2830)

		Nombre d'habitants dans la collectivité					
	TOTAL	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	*2830* *2024*	*1075* *2024*	*962* *2024*	*2038* *2024*	*623*	*113*	*57* *2024*
ST Bon	52%	46%	51%	49%	57%	67%	77%
Très bon	5%	4%	5%	5%	4%	6%	7%
Bon	47%	42%	46%	44%	53%	61%	70%
ST Faible	34% ↗ *30%*	39% ↗ *34%*	33% ↗ *26%*	36% ↗ *31%*	31%	26%	16%
Faible	25%	28%	24%	26%	26%	20%	12% ↘ *30%*
Très faible	9% ↗ *5%*	11% ↗ *8%*	9% ↗ *4%*	10% ↗ *7%*	5%	6%	4%
Je ne sais pas l'évaluer	14% ↘ *17%*	15% ↘ *19%*	16% ↘ *20%*	15% ↘ *19%*	12%	7%	7%

Dans le même temps, **l'exposition aux risques est partagée avec plus de 4 répondants sur 10 qui jugent leur collectivité faiblement exposée, et une proportion proche de celles qui la jugent fortement exposée, en hausse par rapport à 2024 (+4 points)**. Cette perception de forte exposition est plus répandue dans les collectivités de plus grande taille, chez les agents chargés de l'informatique et les communes déjà victimes d'une attaque…

Q10. Selon vous, le niveau d'exposition aux risques de cyberattaques de votre collectivité est :
Base : Total répondants (2830)

44%

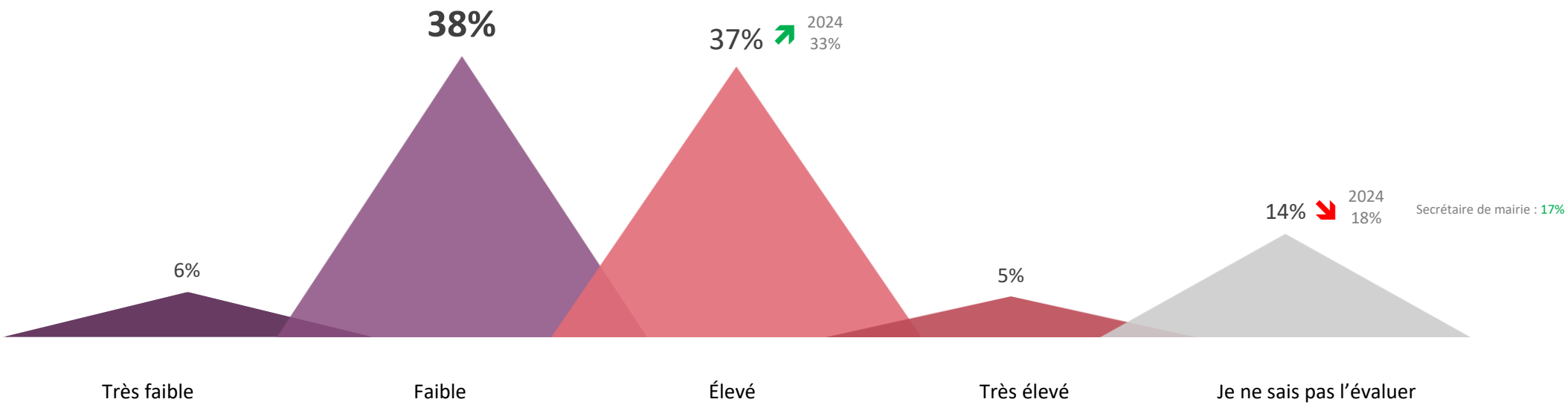
Faible exposition

Préparé en cas d'attaque : 60%
Protection perçue comme élevée : 51%
N'a pas été victime d'une attaque : 49%
Moins de 300 habs. : 52%
Entre 5k et 25k habs. : 28%

42% ↗ 2024 : 38%

Forte exposition

Victime d'au moins une attaque : 62%
Protection perçue comme faible : 51%
Pas préparé en cas d'attaque : 50%
Agent communal en charge de l'info. : 60%
DGS : 51% / Secrétaire de mairie : 38%
Entre 5k et 25k habs. : 66%
Moins de 300 habs. : 35%



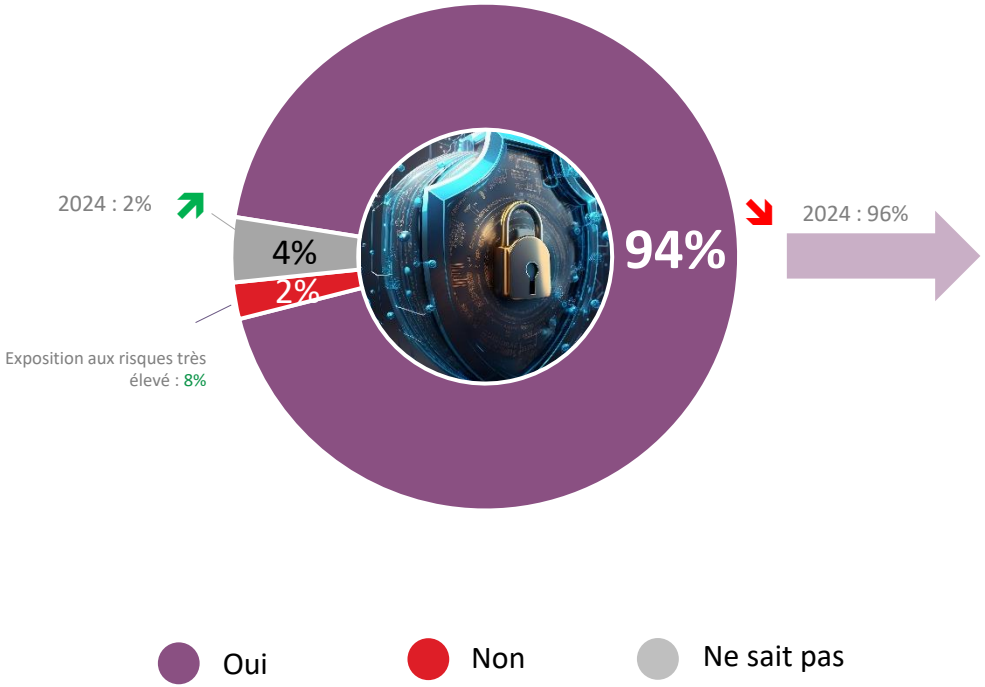
En effet, les plus grandes se jugent à la fois mieux protégées mais également plus exposées. Les communes de moins de 1 000 habitants se perçoivent certes moins exposées, mais elles sont plus nombreuses qu'en 2024 à se juger fortement exposées, et à estimer leur protection faible. Une évolution, qui conjuguée à une perception plus critique de leur protection, pourrait traduire une sensibilité accrue aux risques numériques.

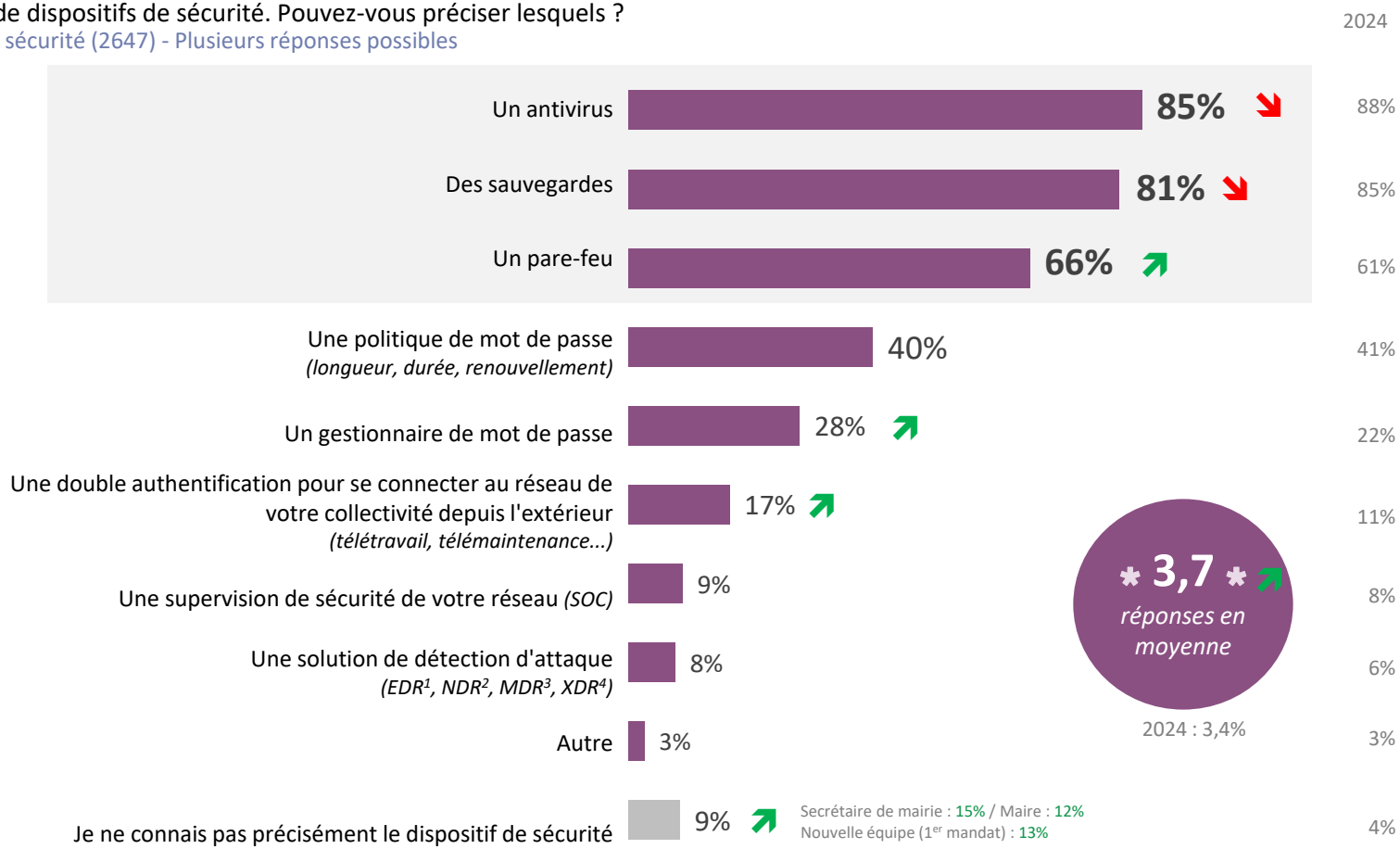
Q10. Selon vous, le niveau d'exposition aux risques de cyberattaques de votre collectivité est :
Base : Total répondants (2830)

		Nombre d'habitants dans la collectivité					
	TOTAL	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	*2830* *2024*	*1075* *2024*	*962* *2024*	*2038* *2024*	*623*	*113*	*57*
ST Faible	44%	52%	43%	47%	37%	30%	23%
Très faible	6%	10%	5%	7%	3%	4%	1%
Faible	38%	42%	38%	40%	34%	26%	22%
ST Élevé	42% ↗ *38%*	35%	41% ↗ *31%*	38% ↗ *33%*	49%	65%	69%
Élevé	37% ↗ *33%*	30%	35% ↗ *28%*	33% ↗ *29%*	43%	59%	62%
Très élevé	5%	5%	6% ↗ *3%*	5%	6%	6%	7%
Je ne sais pas	14% ↘ *18%*	13% ↘ *18%*	16% ↘ *23%*	15% ↘ *20%*	14%	5%	8%

En parallèle, la quasi-totalité des collectivités se déclarent équipées de dispositifs de sécurité, une part en retrait par rapport à 2024 sans doute due à une moins bonne connaissance du répondant sur les dispositifs en place (*hausse du taux de NSP*). Mais **globalement, le nombre moyen de dispositifs de sécurité déclarés augmente passant de 3,4 à 3,7.** Si l'antivirus et les sauvegardes restent les solutions les plus répandues, le pare-feu, **le gestionnaire de mots de passe et la double authentification progressent.**

Q12. Votre collectivité est-elle équipée de dispositifs de sécurité (exemples : pare-feu, antivirus, sauvegarde …)
Base : Total répondants (2830)
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 (2647) - Plusieurs réponses possibles





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

Si la taille reste un facteur structurant de l'équipement, les solutions les plus avancées étant surtout présentes dans les plus grandes collectivités, qui cumulent environ 5 dispositifs ou plus à partir de 5 000 habitants, **les plus petites progressent : les communes de moins de 1 000 habitants déclarent en moyenne 3,5 dispositifs (3,1 en 2024), et sont plus nombreuses à disposer d'un pare-feu, d'un gestionnaire de mots de passe ou d'une double authentification pour les connexions à distance.**

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 (2647) - Plusieurs réponses possibles

		Nombre d'habitants dans la collectivité					
	TOTAL	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	*2647* *2024*	*988* *2024*	*905* *2024*	*1893* *2024*	*593* *2024*	*107*	*54* *2024*
Un antivirus	85% ↘ *88%*	86%	84% ↘ *89%*	85% ↘ *88%*	82% ↘ *87%*	90%	86%
Des sauvegardes	81% ↘ *85%*	79%	82% ↘ *86%*	80% ↘ *83%*	81% ↘ *90%*	93%	89%
Un pare-feu	66% ↗ *61%*	60% ↗ *53%*	64% ↗ *55%*	62% ↗ *54%*	73%	91%	89%
Une politique de mot de passe	40%	41%	35%	38%	39%	65%	80%
Un gestionnaire de mot de passe	28% ↗ *22%*	27% ↗ *21%*	28% ↗ *20%*	27% ↗ *20%*	27% ↗ *21%*	42%	46%
Une double authentification pour se connecter au réseau de votre collectivité depuis l'extérieur	17% ↗ *11%*	16% ↗ *6%*	14% ↗ *8%*	15% ↗ *7%*	19%	25%	34%
Une supervision de sécurité de votre réseau	9%	4%	7%	5%	14%	31%	42%
Une solution de détection d'attaque	8%	2%	4%	3%	11%	40%	61%
Autre	3%	3%	3%	3%	2%	4%	5%
Je ne connais pas précisément le dispositif de sécurité	9% ↗ *4%*	6% ↗ *3%*	9% ↗ *3%*	8% ↗ *3%*	11% ↗ *6%*	5%	9%
Nombre moyen de dispositif de sécurité	3,7 ↗ *3,4*	3,4 ↗ *3,0*	3,5	3,5 ↗ *3,1*	3,9	5,1	5,8 ↗ *5,3*

Côté usages**, la messagerie au nom de domaine de la collectivité progresse : 52% l'utilisent (+9 points), notamment les communes de plus de 1 000 habitants,** et elle passe devant la messagerie grand public (48%), qui reste présente surtout dans les plus petites communes. Ces pratiques illustrent des niveaux de structuration numérique très différents selon les moyens disponibles.

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 (2830)

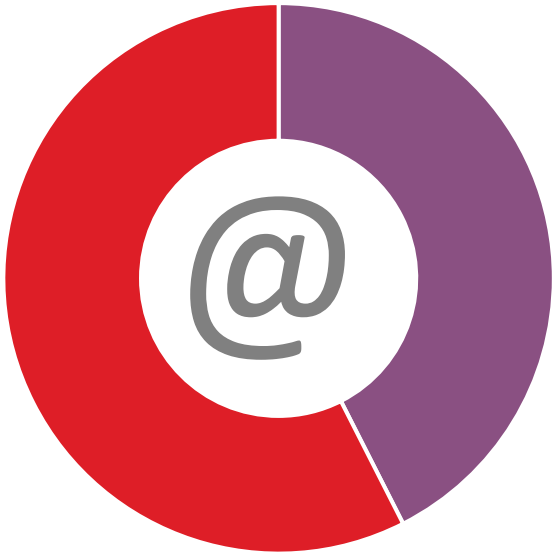
2024 : 57%

48%

Externe

(ex : Gmail, Orange, Yahoo, Hotmail…)

Moins de 300 habs. : 72%



52%

2024 : 43%

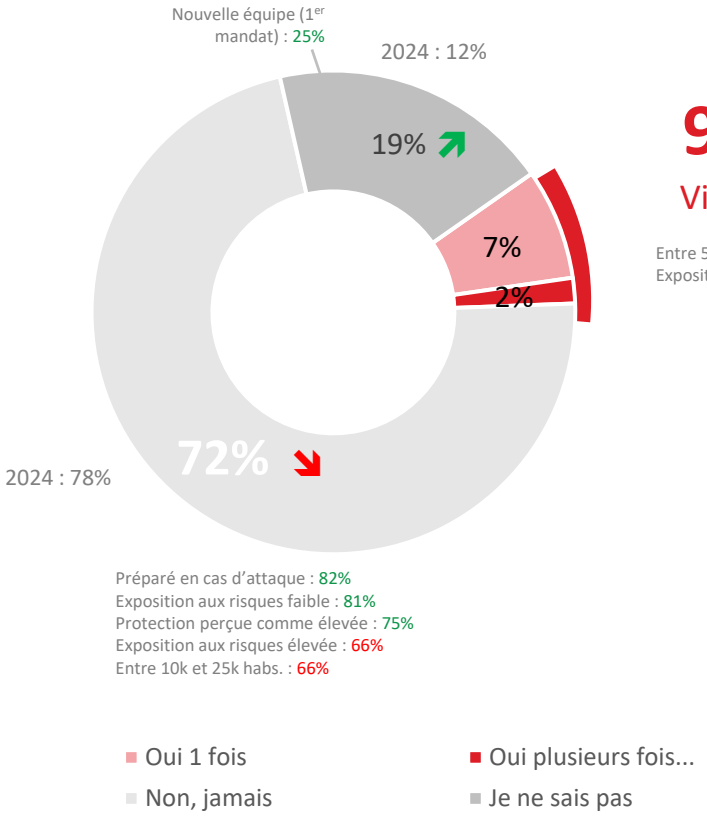
Interne

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. : 82%

Côté incidents, près **d'1 collectivité sur 10 déclare avoir été victime d'un incident de sécurité informatique au cours des douze derniers mois, avec davantage de « ne sait pas » qu'en 2024**. Parmi les victimes, **près de deux tiers identifient désormais au moins une cause**, une part en hausse, l'hameçonnage arrivant en tête, devant les failles non corrigées. Plus d'un tiers ne sait toutefois pas expliquer l'origine de l'incident.

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 (2830)

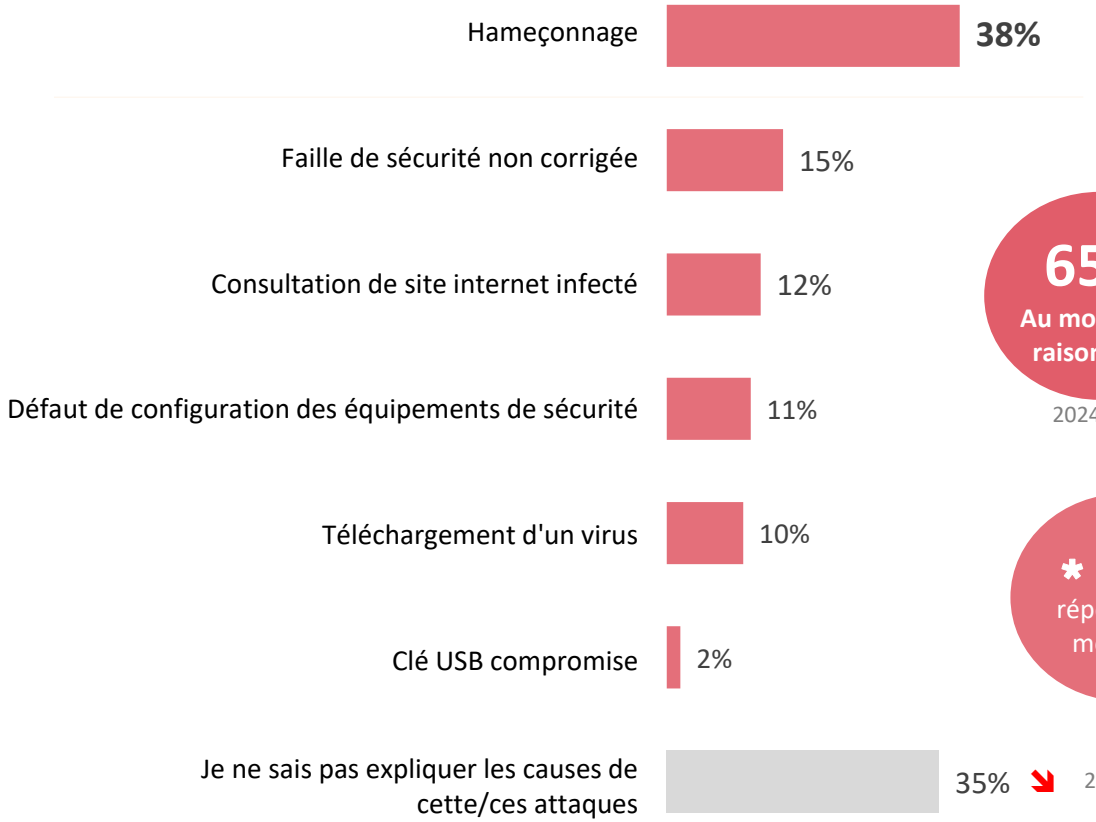


9%

Victimes de cyberattaque

Entre 5k et 25k habs. : 18%
Exposition aux risques élevée : 13%

Q16bis. A votre avis, à quoi ces attaques étaient-elles liées ? Base : Collectivités victimes d'un ou plusieurs incident(s) de sécurité informatique (259) - Plusieurs réponses possibles

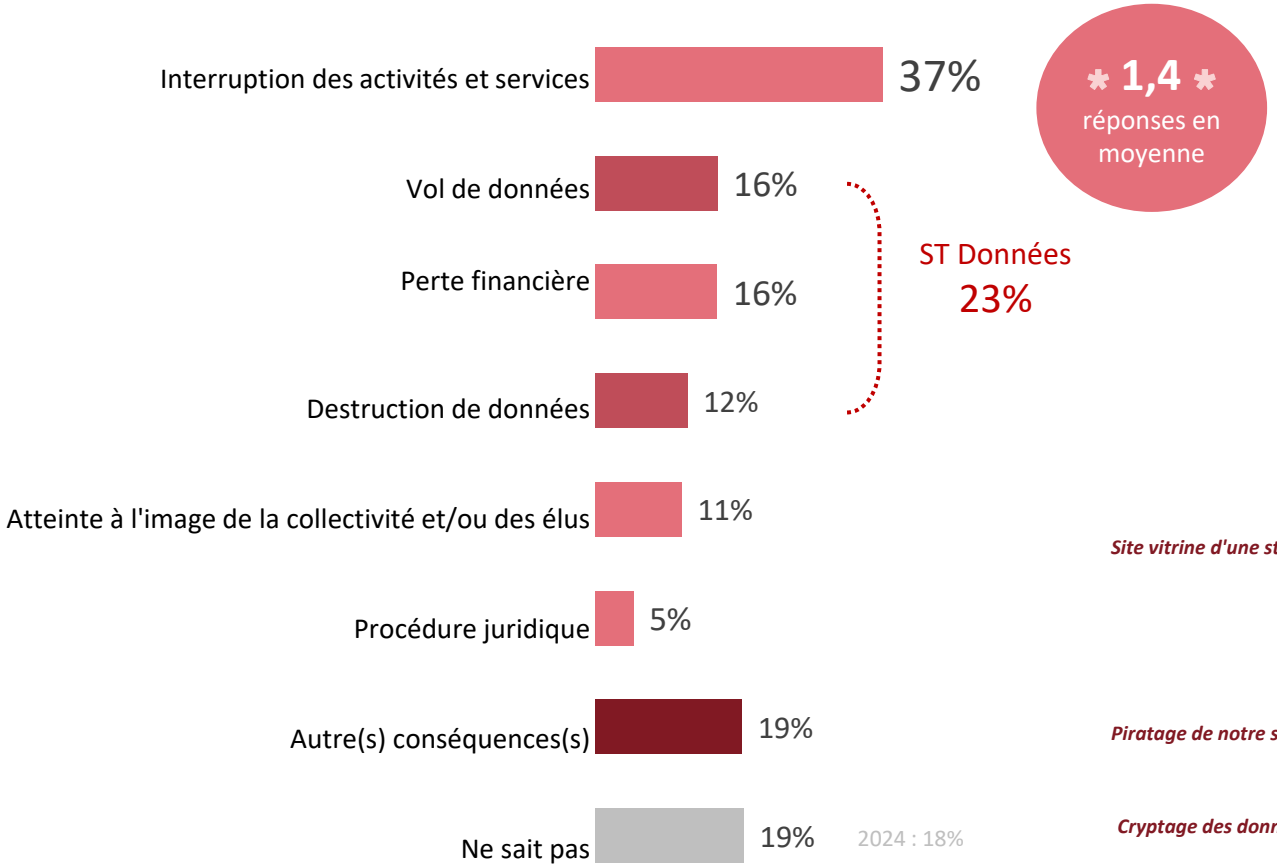


Pour les collectivités ayant subi un incident, ces attaques se traduisent d'abord par une perturbation du fonctionnement de la collectivité : p**lus d'un tiers des victimes citent une interruption de leur activité et de leurs services.** Les atteintes aux données (vol ou destruction) concernent près d'1 victime sur 4, et 1 sur 6 déclare une perte financière. **Près d'1 victime sur 5 ne sait pas évaluer les conséquences**. Ces résultats rappellent que le risque cyber ne relève pas uniquement de l'informatique : il peut affecter directement la continuité du service public

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

Base : Collectivités victimes d'un ou plusieurs incident(s) de sécurité informatique (259) - Plusieurs réponses possibles





Perte de temps pour régler le problème.

Site vitrine d'une structure annexe défiguré. Communication dégradée pour cette structure.

Coupure du site internet.

Envoi de mails frauduleux en masse.

Boite mail piratée, interruption de services.

Piratage de notre site Internet, réinitialisation du site à -60 jours. Inactivité du site qq jours.

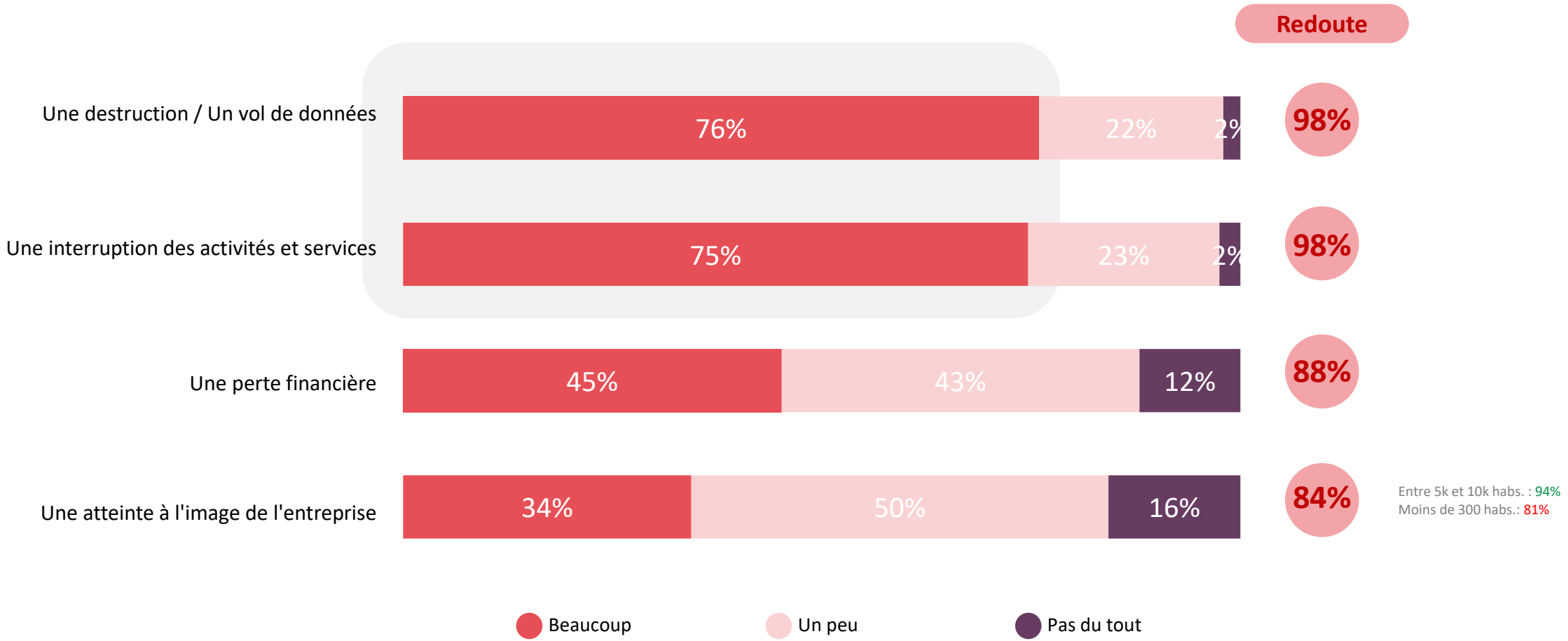
Site Internet non accessible pendant quelques jours.

Cryptage des données sur l'ancien serveur en cours de migration vers un nouveau serveur.

Quant aux craintes, elles rejoignent les conséquences subies par les victimes : **la perte ou le vol de données et l'interruption des activités sont redoutées par la quasi-totalité des répondants**, dont 3 sur 4 les craignent « beaucoup ». La perte financière et l'atteinte à l'image sont un peu moins redoutées, cette dernière surtout « un peu ». La continuité des services et la protection des données constituent ainsi deux leviers particulièrement pertinents pour sensibiliser les collectivités.

Q11b. En cas de cyberattaque, dans quelle mesure redoutez-vous ... ? *

Base : Total répondants (2830)



Une conscience du cyberrisque qui progresse, mais une préparation et sensibilisation encore insuffisante

42 %

jugent leur commune fortement exposée aux cyberrisques

Une perception en hausse de 4 points par rapport à 2024.

34 %

évaluent leur niveau de protection comme étant faible en matière de cybersécurité

Une perception en hausse de 4 points par rapport à 2024.

3,7

dispositifs de sécurité informatique en moyenne

Contre 3,4 en 2024, une évolution y compris chez les plus petites communes

65%

des victimes d'un incident citent au moins une raison de l'attaque

Une part en hausse de 10 points par rapport à 2024

L'ENSEIGNEMENT CLÉ

Un décalage persistant entre la conscience du risque et la capacité à y faire face, avec toujours la taille comme variable structurante.

Transformer la sensibilisation en actions concrètes de sécurisation, notamment dans les plus petites communes et dans un contexte de début de mandat.

02

La perception de la sécurité informatique :

Un enjeu reconnu, mais des niveaux de protection très contrastés



Pour près de deux tiers des répondants, la sécurité informatique est un sujet qui concerne tout le monde, même si cette vision collective s'est légèrement effritée par rapport à 2024. Cette vision transversale demeure majoritaire, même si les agents et les élus sont un peu plus souvent désignés comme responsables prioritaires. Très peu de répondants considèrent que la cybersécurité ne concerne pas leur collectivité

q9. Selon vous, la sécurité informatique doit impliquer en priorité...

Base : Total répondants (2830)



Si la sécurité informatique est majoritairement considérée comme une responsabilité de tous, sa place effective dans les priorités des collectivités reste contrastée : **environ un tiers lui attribue une note élevée (8 à 10)**, un autre tiers une note de 0 à 5, pour une moyenne de 6,4/10. Cet enjeu est jugé plus important dans les collectivités de plus grande taille, celles déjà victimes d'une attaque et celles qui prévoient une hausse de leur budget.

Q9b : Aujourd'hui, dans quelle mesure la cybersécurité est-elle considérée comme un enjeu important au sein de votre collectivité ?

Base : Total répondants (2830)

Nouvelle question

37%

8 à 10

Entre 5k et 25k habs. : 44% / Maire : 44%
Secrétaire de mairie : 32%

Hausse du budget prévue : 50%
Budget annuel sécurité info. <1k : 33%

Victime d'au moins une attaque : 49%

28%

6 à 7

35%

0 à 5

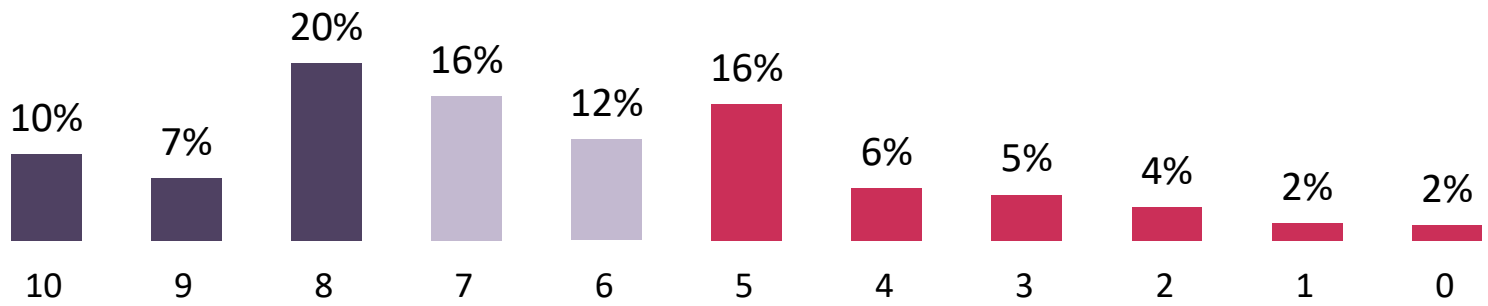
Secrétaire de mairie : 41%
Maire : 28% / Agent communal en charge de l'info : 28%
Entre 5k et 25k habs. : 23%

Budget annuel sécurité info. <1k : 40%
Budget annuel sécurité info. >5k : 29%
Hausse du budget prévue : 20%

Victime d'au moins une attaque : 28%

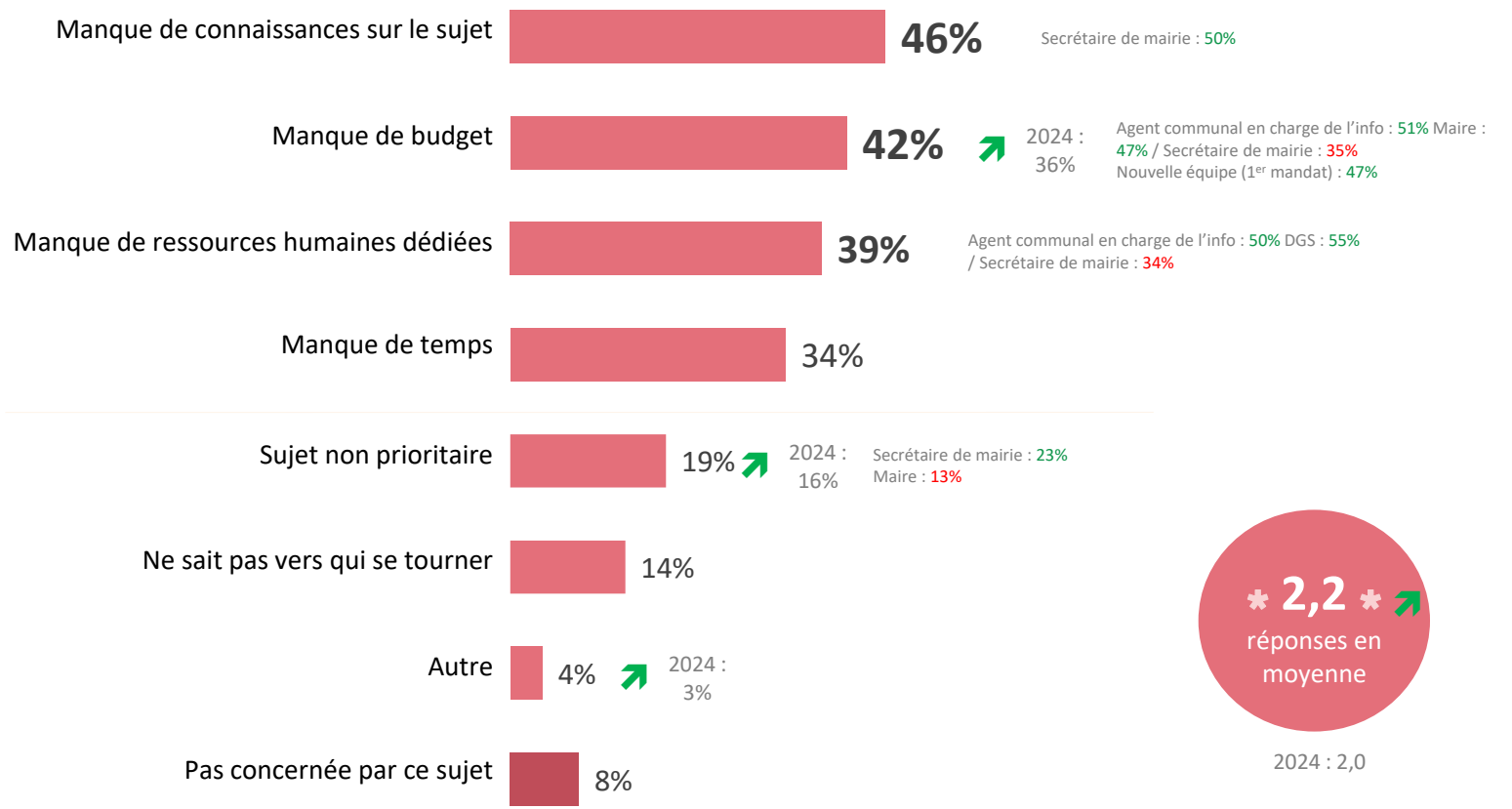
6,4 /10

Note moyenne



Sur le plan des moyens, presque toutes les collectivités citent au moins un frein à la sécurisation, et en citent en moyenne davantage qu'en 2024. **Le manque de connaissances arrive en tête, devant le manque de budget**, plus souvent cité, et le manque de ressources humaines dédiées et de temps. **Le sujet est aussi plus souvent jugé non prioritaire**, surtout auprès des secrétaires de mairie. La sécurisation des collectivités apparaît ainsi confrontée à une accumulation de contraintes, qui ne peuvent être résolues par la seule mise à disposition de solutions techniques.

Q14. Et qu'est ce qui empêche votre collectivité d'atteindre le bon niveau de sécurité informatique qu'elle souhaite ?
Base : Total répondants (2830)



92%
Au moins un frein cité
2024 : 91%

*** 2,2 ***
réponses en moyenne
2024 : 2,0

Ces contraintes s'inscrivent dans un contexte de budgets limités : deux tiers des collectivités consacrent moins de 5 000€ par an à l'informatique, une part en recul par rapport à 2024, et **les budgets inférieurs à 2 000€ sont plus fréquents**. À l'autre extrémité, une collectivité sur quatre déclare un budget de 5 000 € et plus, en hausse, tandis que la tranche intermédiaire de 2 000 à 4 999€ se réduit nettement. Les collectivités ne sachant pas évaluer leur budget informatique sont plus nombreuses. Ces mouvements invitent à une lecture nuancée, avec des situations budgétaires qui demeurent fortement liées à la taille des communes.

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 (2830)



45% 2024 : 41%
Moins de 2 000€*

66% 2024 : 73%
Moins de 5 000€
Moins de 300 habs. : 89%
Exposition aux risques faible : 72%
Entre 300 et 999 habs. : 74%
Entre 5k et 25k habs. : 1%

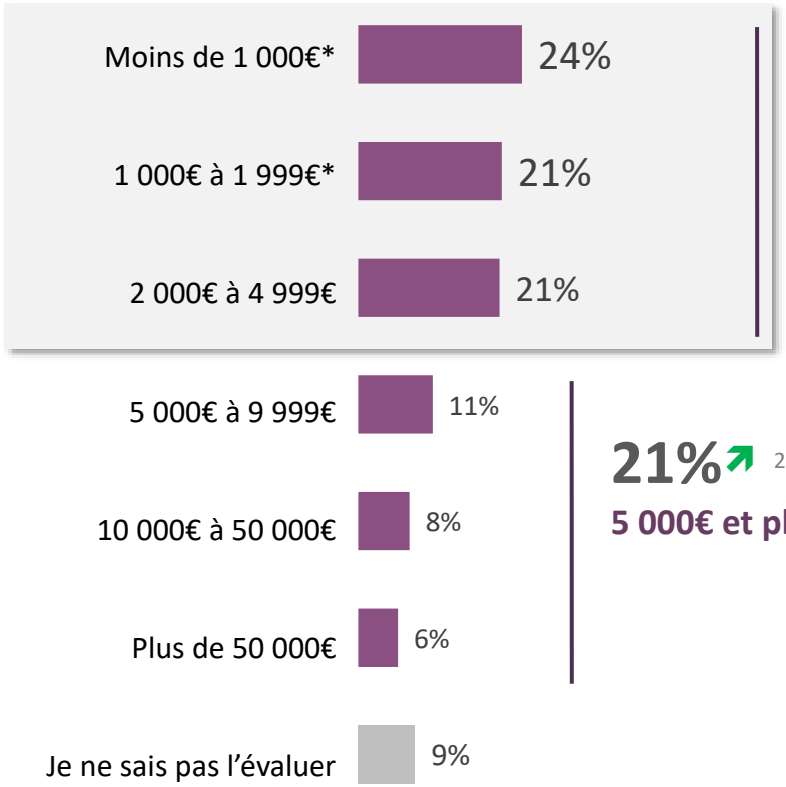
25% 2024 : 22%
5 000€ et plus
Entre 5k et 25k habs. : 87%
Entre 1k et 5k habs. : 50%
Exposition aux risques élevée : 31% Moins de 1 000 habs. : 12%



**Modification : moins de 2000 en 2024 vs Moins de 1000 et 1000 à 1999€ cette mesure ci*

En miroir, les montants consacrés à la cybersécurité restent très limités : 77% des collectivités qui connaissent **leur budget informatique y consacrent moins de 2 000€, dont 71% moins de 1 000 €, surtout parmi les plus petites communes** et celles qui se jugent peu exposées aux cyberrisques. Cette faiblesse des moyens dédiés constitue une contrainte pour le déploiement et le maintien de dispositifs de protection.

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 (2830)

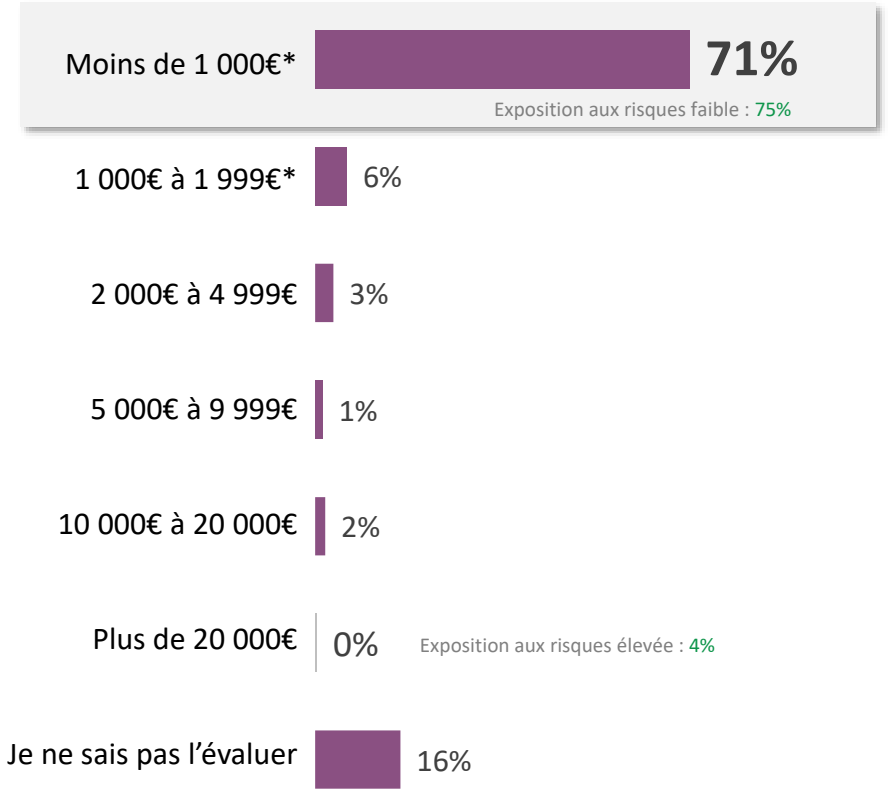


66% ↘ 2024 : 73%
Moins de 5 000€

21% ↗ 2024 : 21%
5 000€ et plus



Q7bis. Quelle est la part de ce budget consacré à la sécurité informatique ?
Base : Ont déclaré connaître le budget consacré à l'informatique (2590)

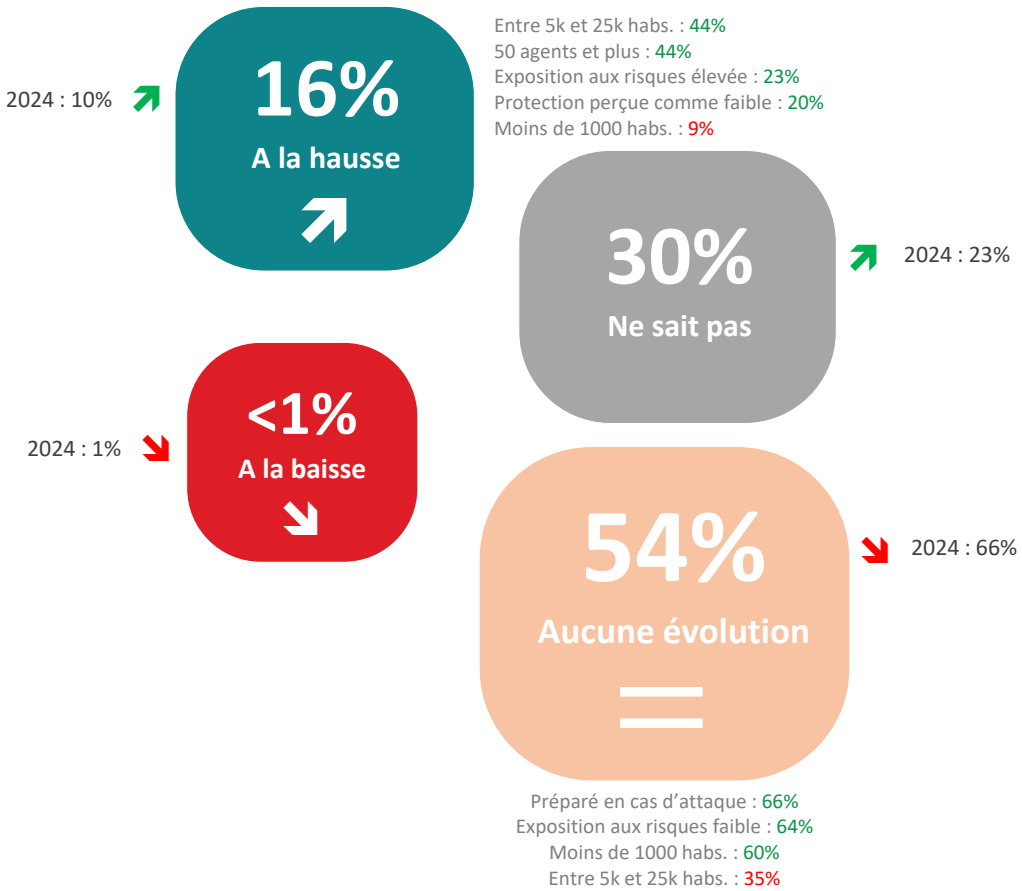


77%
Moins de 2 000€
2024 : 77%

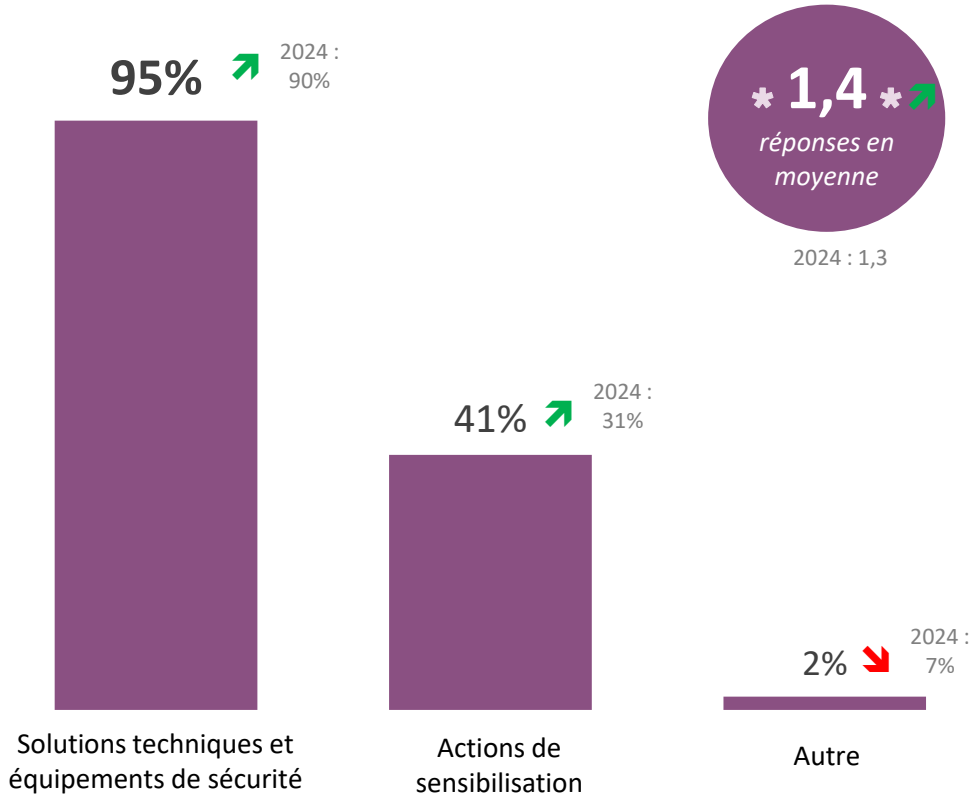
Des signaux qui paraissent encourageants : si plus d'une collectivité sur deux ne prévoit aucune évolution de son budget, **16% envisagent une hausse pour leur cybersécurité**, surtout les plus grandes communes et celles qui se considèrent peu protégées. Cette augmentation irait en priorité aux solutions techniques et équipements de sécurité, et plus souvent qu'en 2024 aux actions de sensibilisation. L'incertitude reste toutefois importante : 3 répondants sur 10 ne savent pas se prononcer sur l'évolution du budget.

Q7ter. Prévoyez-vous de faire évoluer ce budget de cybersécurité l'an prochain ? Base : Ont déclaré connaître le budget consacré à l'informatique (2590)

Comptent faire évoluer le budget lié à la sécurité informatique…



Q7c. A quel poste pensez-vous allouer ce budget ? Base : Ont déclaré une hausse du budget consacré à la sécurité informatique l'an prochain (406)



Des budgets fortement corrélés à la taille de la collectivité : plus la collectivité est grande, plus le budget de sécurité informatique est élevé. Les plus petites communes restent concentrées sur les montants les plus faibles. Les perspectives d'évolution suivent le même gradient : la hausse du budget est davantage envisagée dans les communes de plus de 5 000 habitants, alors que les plus petites déclarent plus souvent ne prévoir aucune évolution ou ne pas savoir.

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 : Ont déclaré connaître le budget consacré à l'informatique (2590)

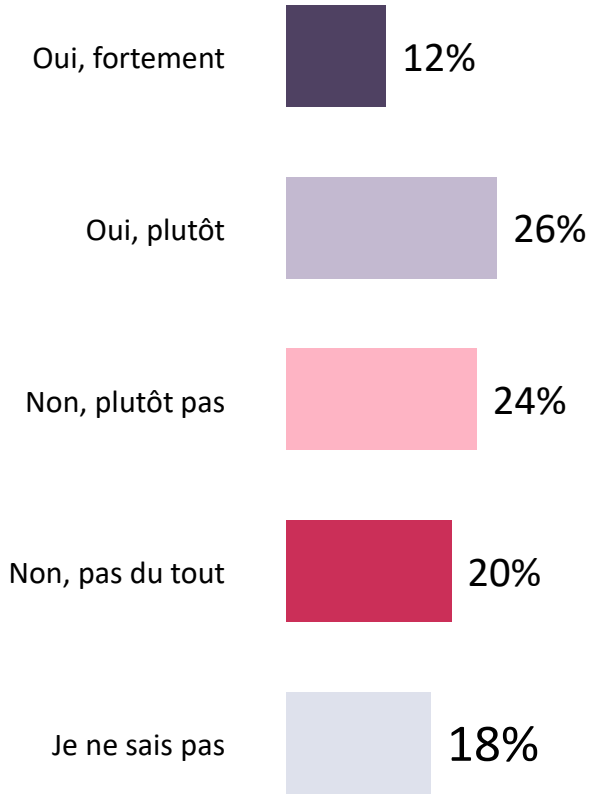
		Nombre d'habitants dans la collectivité					
	TOTAL	Moins de 300	Entre 300 et 999	ST Moins de 1000	Entre 1 000 et 4 999	Entre 5 000 et 9 999	Entre 10 000 et 25 000
Base	*2590* *2024*	*1027* *2024*	*883* *2024*	*1910* *2024*	*530* *2024*	*99* *2024*	*50* *2024*
Moins de 1000€*	71%	86%	75%	81%	49%	16%	9%
1 000€ à 1 999€*	6%	1%	6%	3%	14%	11%	5%
ST Moins de 2000	77%	87%	81%	84%	63%	27% ↗ *14%*	14%
2 000€ à 4 999€	3% ↘ *7%*	0% ↘ *1%*	2% ↘ *4%*	1% ↘ *2%*	9% ↘ *18%*	22%	9%
5 000€ à 9 999€	1% ↘ *1%*	-	0% ↘ *1%*	0% ↘ *0%*	3%	16%	12%
10 000€ à 20 000€	2%	0%	0%	0%	1%	20%	37% ↗ *13%*
Plus de 20 000€	0%	-	-	-	0%	1%	12% ↘ *36%*
Je ne sais pas l'évaluer	16% ↗ *11%*	12% ↗ *8%*	17% ↗ *12%*	14% ↗ *10%*	24% ↗ *16%*	14%	16%
Oui, à la hausse	16% ↗ *10%*	9% ↗ *4%*	13% ↗ *6%*	11% ↗ *5%*	24%	46% ↗ *29%*	40%
Oui, à la baisse	0% ↘ *<1%*	- ↘ *1%*	0% ↘ *1%*	0% ↘ *1%*	0%	2%	-
Non, aucune évolution du budget prévu	54% ↘ *66%*	63% ↘ *74%*	56% ↘ *68%*	60% ↘ *71%*	41% ↘ *55%*	34% ↘ *48%*	39%
Je ne sais pas	30% ↗ *23%*	28% ↗ *21%*	31% ↗ *25%*	29% ↗ *23%*	35% ↗ *24%*	18%	21%

Toutefois, la recrudescence des cyberattaques ne semble pas constituer un facteur déterminant dans les décisions budgétaires des collectivités : 44% indiquent qu'elle n'a pas pesé dans leurs arbitrages, contre 38% qui déclarent qu'elle a eu une influence. À noter que 18% ne savent pas se prononcer sur cette question. Cette influence est toutefois plus fréquemment mentionnée par les collectivités de grande taille, celles ayant déjà subi un incident cyber et, plus particulièrement, celles qui envisagent d'augmenter leur budget consacré à la sécurité informatique.

q7d. Selon vous, la recrudescence des violations de données et des cyberattaques a-t-elle influencé les décisions de votre collectivité en matière de budget de cybersécurité ?

Base : Total répondants (2830)

Nouvelle question



38%
ST Oui

Agent communal en charge de l'info. : 63%
DGS : 59% / Adjoint au maire : 47%
Secrétaire de mairie : 28%

Entre 5k et 25k habs. : 65%
Moins de 1000 habs. : 33%

Budget annuel sécurité info. >5k : 76%
Budget annuel sécurité info. <1k : 35%

Victime d'au moins une attaque : 51%

Hausse du budget prévue : 85%
Aucune évolution du budget prévue : 31%

44%
ST Non

Maire : 48% / DGS : 28%
Agent communal en charge de l'info. : 24%

Moins de 1000 habs. : 49%
Entre 5k et 25k habs. : 23%

Budget annuel sécurité info. <2k : 47%
Budget annuel sécurité info. >5k : 17%

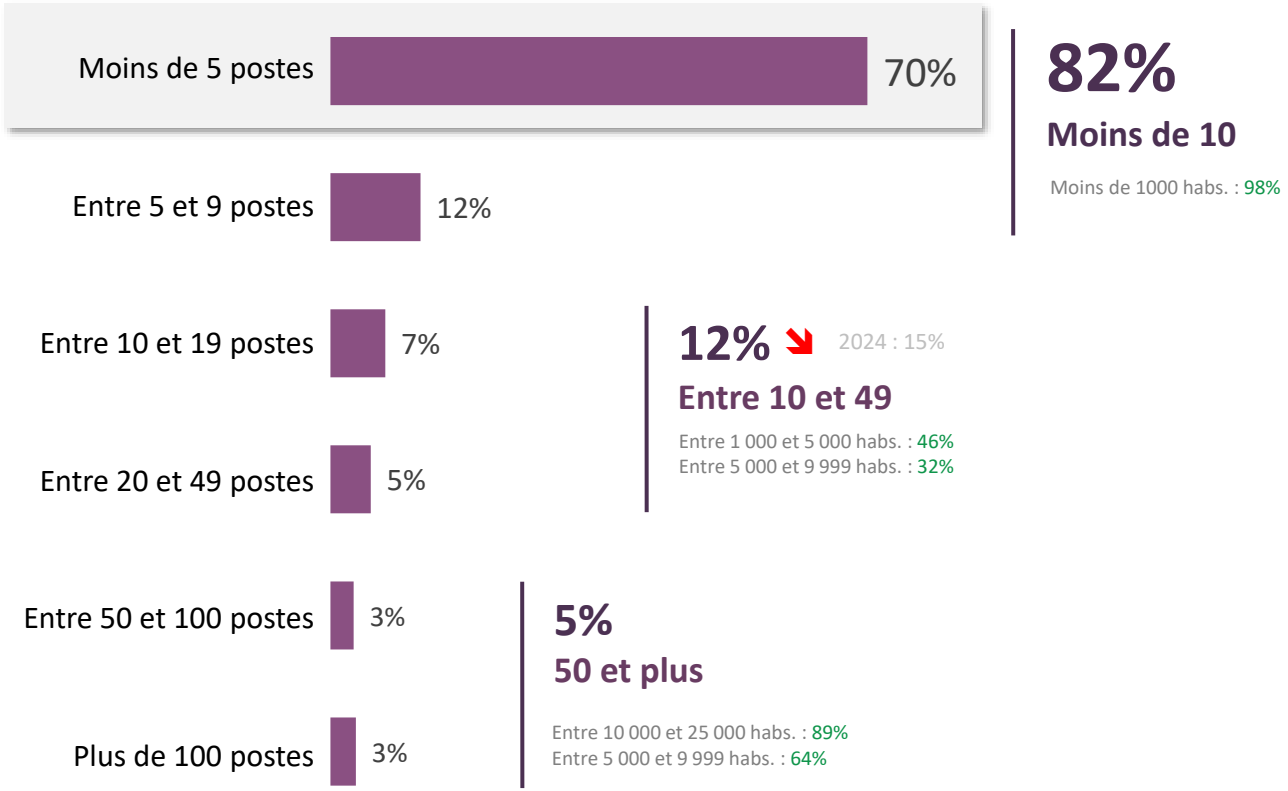
Victime d'au moins une attaque : 36%

Aucune évolution du budget prévue : 57% Hausse du budget prévue : 12%

À l'image de leurs moyens humains et des moyens contraints, les collectivités disposent majoritairement de parcs informatiques de petite taille. En effet un peu plus de 8 sur 10 disposent de moins de 10 postes informatiques, une proportion qui atteint la quasi-totalité des communes de moins de 1 000 habitants. À l'inverse, les collectivités de plus grande taille disposent de parcs nettement plus importants, à l'image de leurs effectifs et de leurs besoins.

Q4. Et combien de postes informatiques (ordinateurs) y a-t-il au sein de votre collectivité ?
Base : Total répondants (2830)


Image de standret sur Freepik



Plus précisément, **près de deux tiers des communes mettent à disposition de leurs élus ou agents des postes informatiques, fixes ou portables.** Quatre sur dix leur fournissent un téléphone portable, notamment les communes de plus de 5 000 habitants. À l'inverse, plus d'un quart ne mettent à disposition aucun de ces équipements, une situation plus fréquente dans les plus petites communes…

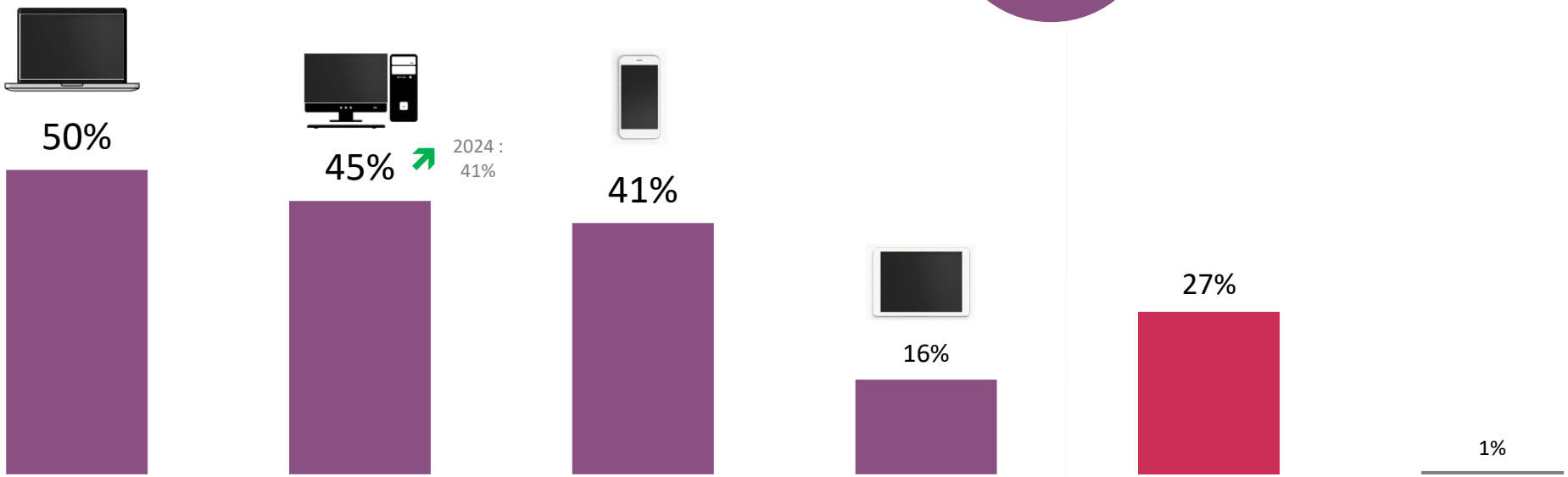
Q5. Votre collectivité met-elle à disposition de certains élus et agents des équipements tels que des téléphones portables, des tablettes ou des ordinateurs ?

Base : Total répondants (2830)

Au moins un équipement 73%

Ordinateur 65%

*** 2,1 ***
réponses en moyenne



Entre 5k et 25k habs. : 86%
Moins de 300 habs. : 26%

Entre 5k et 25k habs. : 70%
Moins de 300 habs. : 34%

Entre 5k et 25k habs. : 85%
Moins de 300 habs. : 15%

Entre 5k et 25k habs. : 67%
Moins de 1000 habs. : 6%

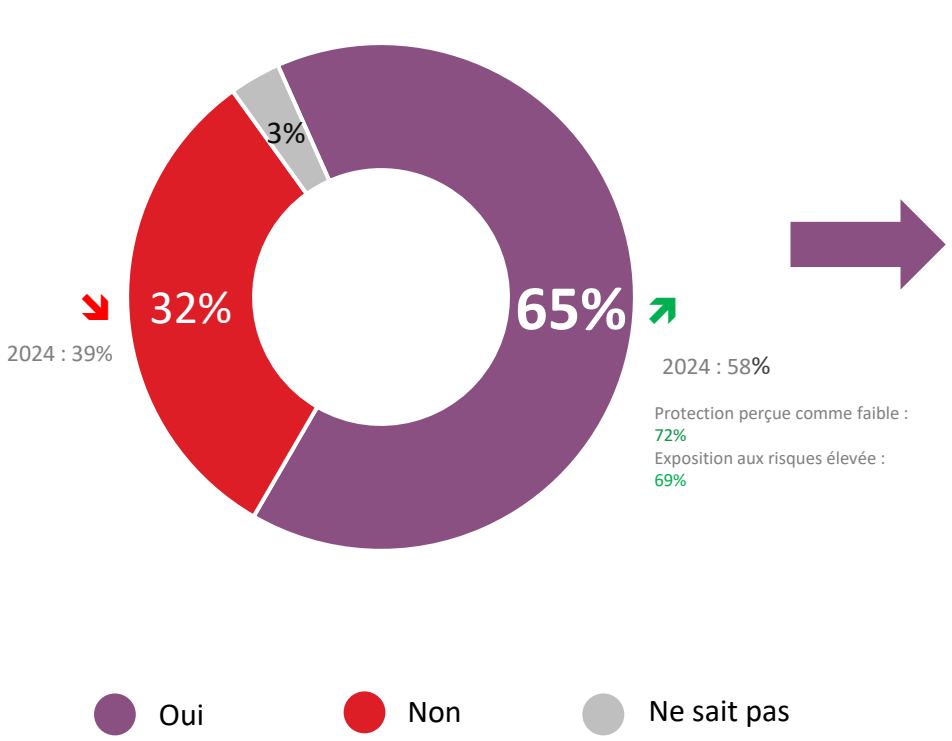
Moins de 300 habs. : 45%
Entre 5k et 25k habs. : 4%

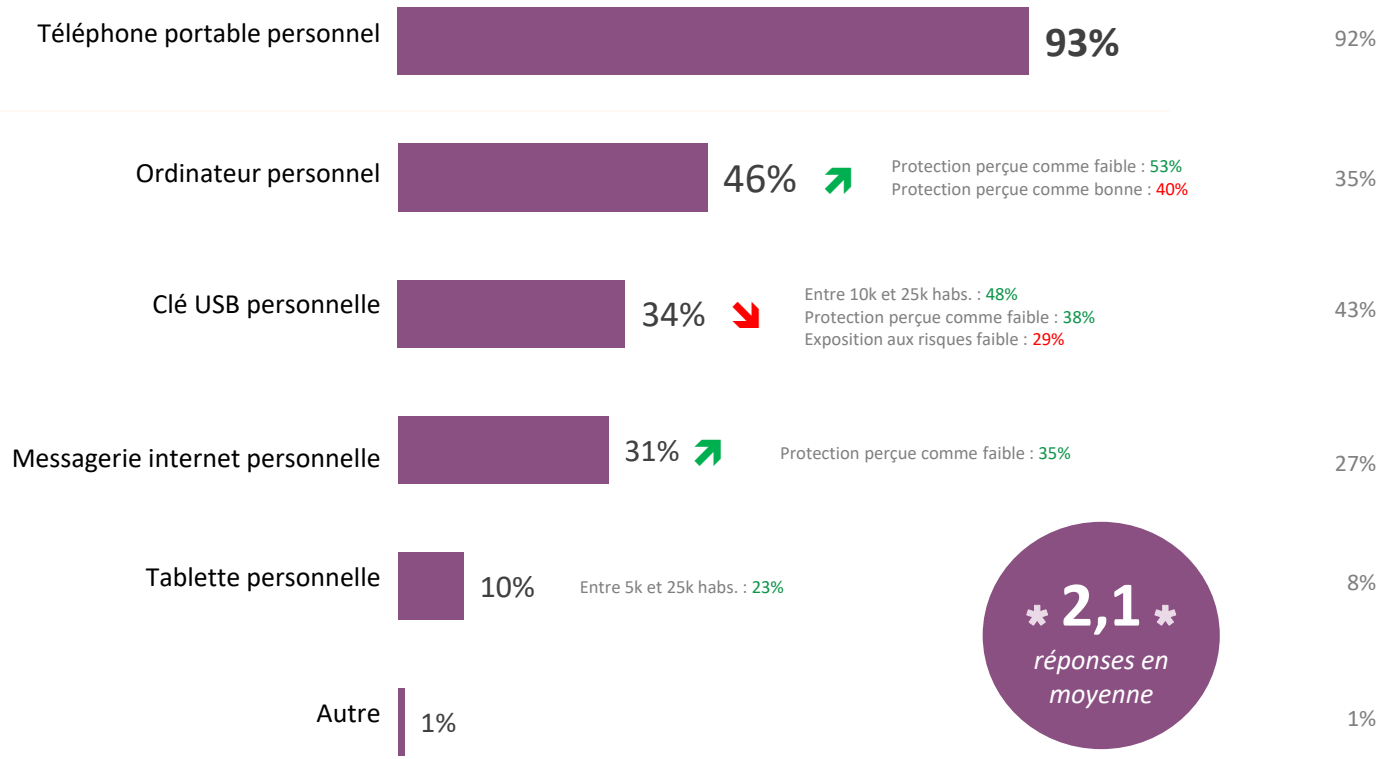
Ainsi, le recours aux équipements personnels pour des usages professionnels concerne désormais près de deux répondants sur trois, contre 58% en 2024. Le téléphone portable personnel reste de loin le support le plus fréquent, tandis que l'ordinateur et la messagerie personnels sont davantage cités. Cette pratique souligne l'importance des usages mixtes, particulièrement dans les petites collectivités, et pose la question de la séparation des environnements professionnels et privés.

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 (2830)

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 (1840) - Plusieurs réponses possibles

Résultats 2024

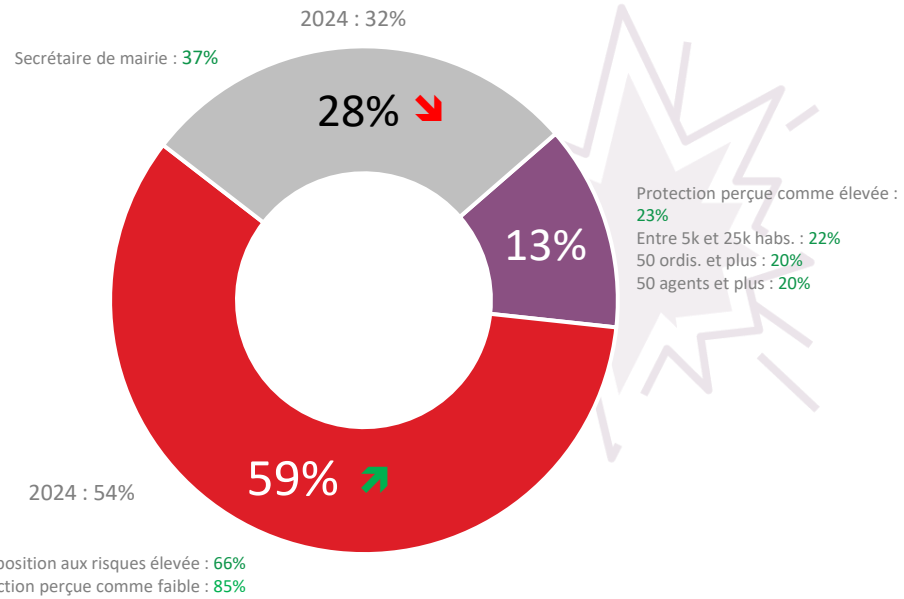




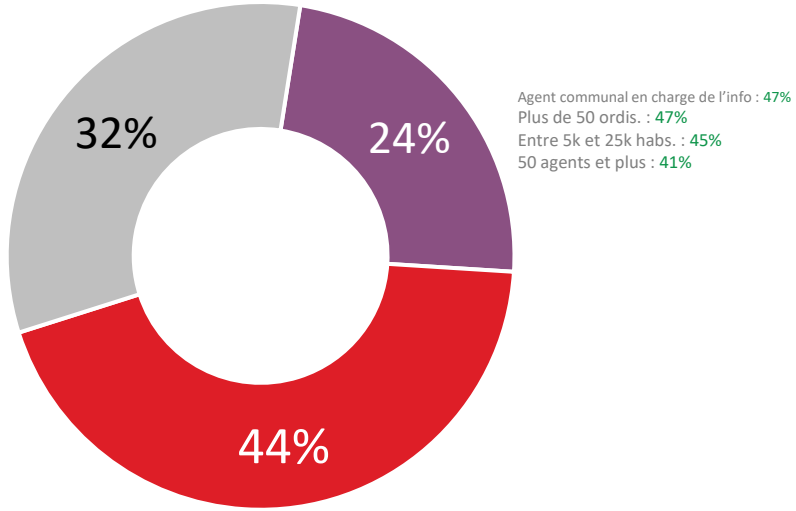
Le décalage entre la perception du risque et la capacité à y faire face apparaît particulièrement marqué : **environ 1 collectivité sur 10 se juge suffisamment préparée,** tandis que près de 6 sur 10 estiment ne pas l'être, une part en hausse par rapport à 2024. Parmi celles qui se disent préparées, **seule 1 sur 4 déclare disposer d'une procédure de réaction,** ce qui souligne le faible niveau de formalisation des dispositifs de réponse…

Q15. A votre connaissance, votre collectivité est-elle suffisamment préparée en cas d'attaque ? Base : Total répondants (2830)
Q15bis. Disposez-vous d'une procédure de réaction (PRA*/PCA**) en cas d'attaque informatique ? Base : Déclare être suffisamment préparé en cas d'attaque (371)

Préparées en cas d'attaque



Disposent d'une procédure de réaction



Note: il s'agit d'une préparation déclarée, et non d'un audit technique.

Oui | Non | Ne sait pas

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

Si la part des collectivités préparées disposant d'une procédure de réaction reste stable à environ 1 sur 4, une tendance à la hausse se dessine dans les communes de moins de 1 000 habitants (19%, contre 14% en 2024), portée notamment par celles de 300 à 999 habitants (+11 points).

Q15. A votre connaissance, votre collectivité est-elle suffisamment préparée en cas d'attaque ? Base : Total répondants (2830)
Q15bis. Disposez-vous d'une procédure de réaction (PRA*/PCA**) en cas d'attaque informatique ? Base : Déclare être suffisamment préparé en cas d'attaque (371)

		Nombre d'habitants dans la collectivité					
	TOTAL	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
Préparées en cas d'attaque							
Base	*2830* *2024*	*1075* *2024*	*962* *2024*	*2038* *2024*	*623* *2024*	*113*	*57*
Oui	13%	10%	13%	12%	16%	24%	18%
Non	59% ↗ *54%*	60%	56% ↗ *50%*	58% ↗ *54%*	59% ↗ *52%*	61%	66%
Je ne sais pas	28% ↘ *32%*	30%	31% ↘ *37%*	30% ↘ *34%*	25% ↘ *31%*	15%	16%
Disposent d'une procédure de réaction							
Base	*371*	*111*	*124*	*235*	*98*	*27*	*10*
Oui	24% *22%*	14% *14%*	24% *13%*	19% *14%*	25% *28%*	37%	65%
Non	44% *50%*	51% *52%*	44% *56%*	47% *53%*	41% *48%*	39%	17%
Je ne sais pas	32% *28%*	35% *34%*	32% *31%*	34% *33%*	34% *24%*	24%	18%

Des communes qui ne font pas toutes de la cybersécurité un enjeu de premier plan

Des choix qui se retrouvent à travers des budgets contraints et encore modestes, en dépit de la recrudescence des attaques.

Un fonctionnement encore peu structuré dans les plus petites communes. Des parcs informatiques limités et des équipements personnels largement utilisés à titre professionnel caractérisent une partie importante des collectivités.

Des freins qui se cumulent. Connaissances, budget et ressources humaines constituent trois obstacles majeurs à la sécurisation des collectivités, avec des enjeux différents selon leur taille.

Une préparation très insuffisante. 59% des collectivités ne se jugent pas suffisamment préparées en cas d'attaque. Même parmi celles qui se disent préparées, les procédures de réaction restent peu déclarées.

➡ Les démarches de sécurisation doivent être adaptées à des collectivités dont les moyens, les compétences et les modalités d'organisation sont très hétérogènes.

03

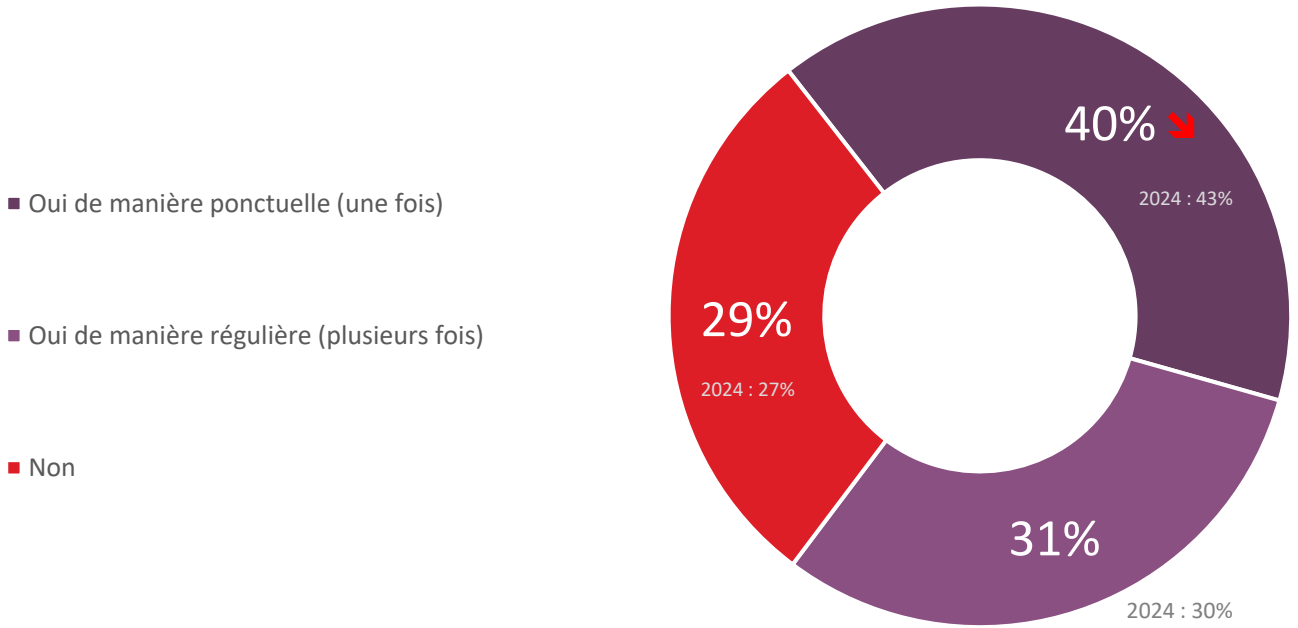
Besoin prioritaire de sensibilisation



Dans un contexte de moyens limités, la sensibilisation est la première réponse apportée : 7 répondants sur 10 déclarent en avoir bénéficié au cours des douze derniers mois, un niveau stable par rapport à 2024.
La sensibilisation reste toutefois plus souvent ponctuelle que régulière, et la part de sensibilisation ponctuelle est en recul. Les collectivités les plus importantes et celles qui se jugent bien préparées déclarent plus fréquemment en avoir bénéficié. L'enjeu est désormais d'inscrire ces actions dans la durée, au-delà de contacts isolés...

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 (2830)



71% 2024 : 73%

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

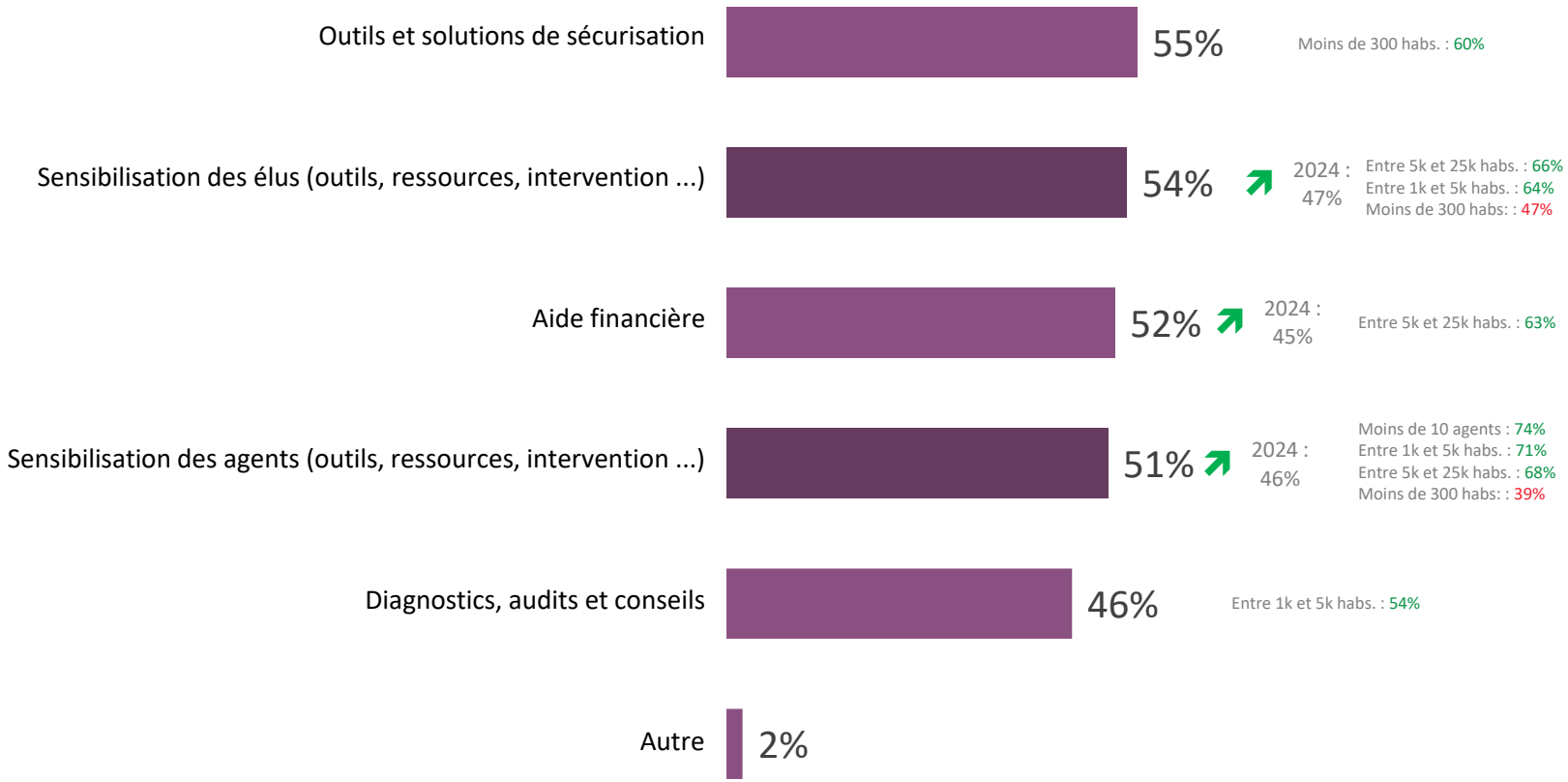
Préparé en cas d'attaque : 90%
Protection perçue comme élevée : 78%
Protection perçue comme faible : 64%
Exposition aux risques très faible : 54%

Entre 5k et 25k d'habs. : 83%
50 agents et plus : 80%
50 ordis et plus : 80%

... d'autant que les besoins exprimés sont variés et plus nombreux qu'en 2024. Les outils et solutions de sécurisation restent prioritaires, **mais les besoins de sensibilisation des élus et des agents et d'aide financière progressent**. Les communes de moins de 300 habitants expriment **avant tout un besoin d'outils de sécurisation**. Les attentes varient selon la taille, ce qui confirme la nécessité de combiner solutions opérationnelles, accompagnement pédagogique et soutien aux collectivités les moins dotées.

q18. Quels seraient vos besoins prioritaires en matière de sécurité informatique ?

Base : Total répondants (2830)



67% Sensibilisation des agents ou élus

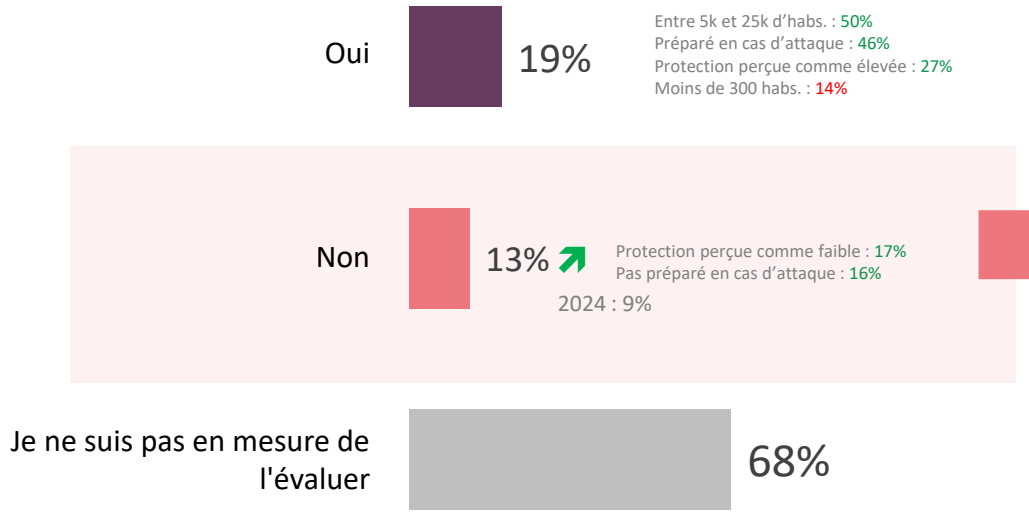
2024 : 62%

*** 2,6 *** *réponses en moyenne*

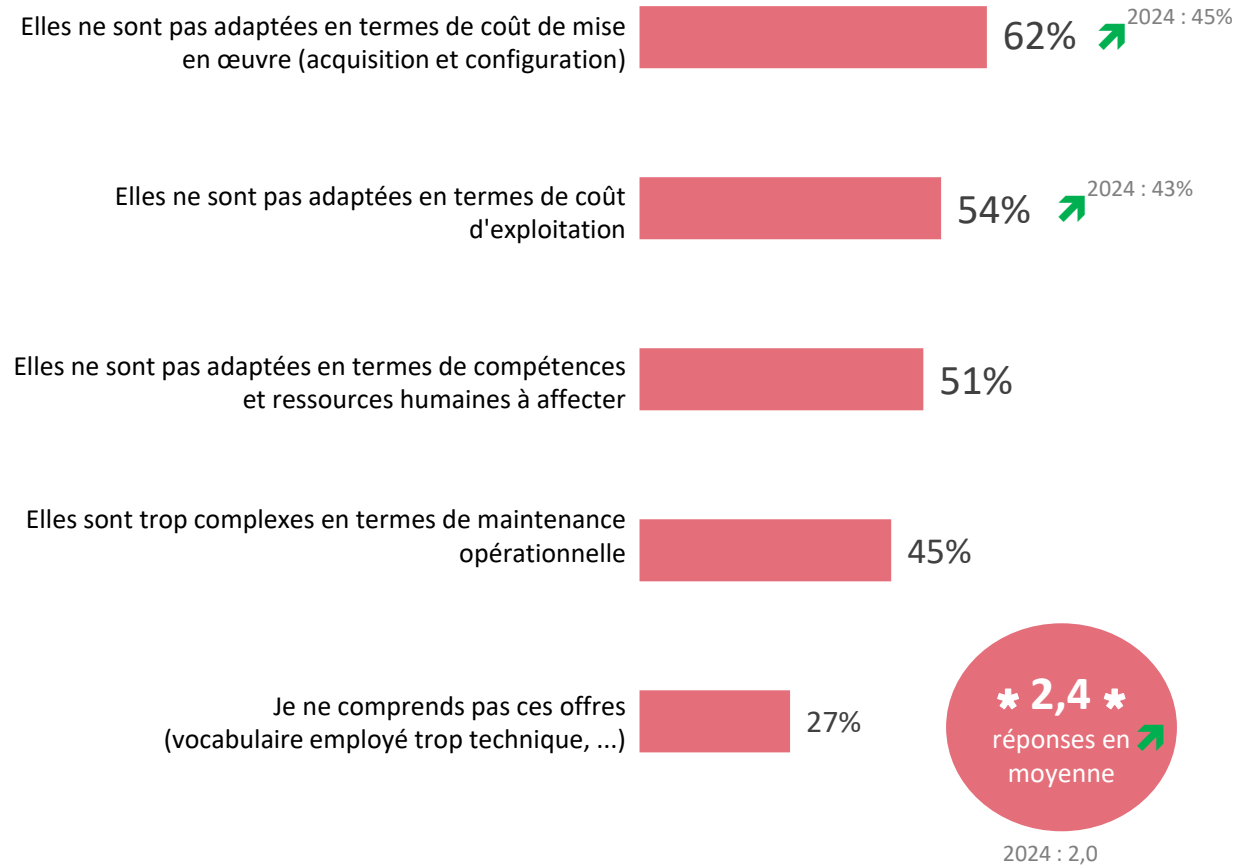
2024 : 2,4

Mais face à cette diversité de besoins, **près de 7 collectivités sur 10 ne se sentent pas en mesure d'évaluer si les solutions de cybersécurité du marché y répondent**. Parmi celles qui se prononcent, les avis favorables restent plus fréquents, mais les avis défavorables progressent. Parmi ces dernières, les coûts de mise en œuvre et d'exploitation sont plus souvent mis en cause qu'en 2024. Ce résultat révèle un besoin important d'aide à la décision et d'orientation vers les solutions adaptées.

Q18b. Pensez-vous que les solutions de cybersécurité actuellement proposées sur le marché soient adaptées aux besoins de votre collectivité… ? Base : Total répondants (2830)



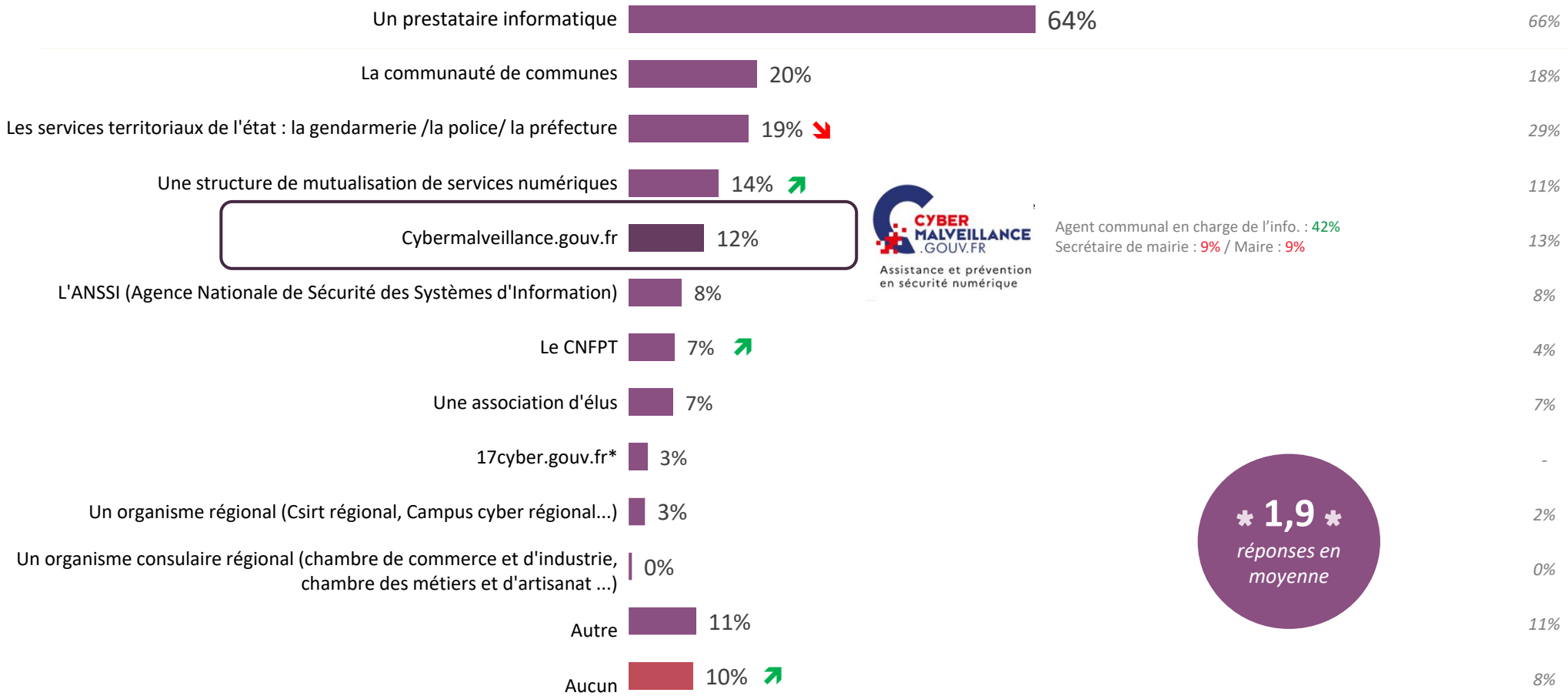
Q18c. Pourquoi indiquez-vous que ces solutions de cybersécurité proposées sur le marché ne sont pas adaptées à vos besoins … ?
Base : Ont déclaré que les solutions de cybersécurité proposées ne sont pas adaptées aux besoins de leurs collectivités (358) - Plusieurs réponses possibles



Pour s'informer ou se faire aider, **les collectivités se tournent d'abord vers un prestataire informatique, cité par près de 2 répondants sur 3, très loin devant les autres interlocuteurs**. Cybermalveillance.gouv.fr est cité par un peu plus d'1 répondant sur 10, surtout par les agents en charge de l'informatique, moins par les maires et secrétaires. Une collectivité sur dix ne se tourne vers aucun interlocuteur, une part en hausse sur les collectivités interrogées cette année. Cette situation met en évidence un double enjeu de visibilité du dispositif et de mobilisation des prestataires comme relais d'information.

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 (2830)

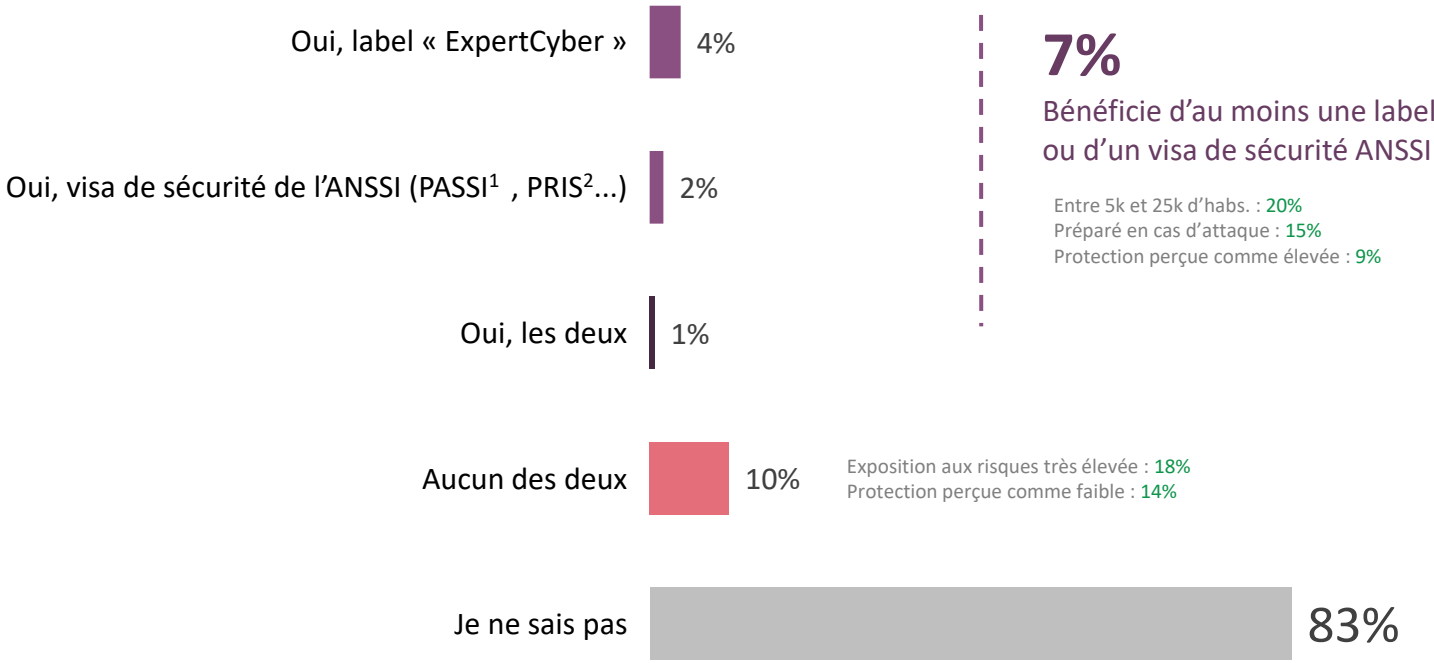


*Nouvel items

Parmi les répondants se tournant vers un prestataire ou une structure de mutualisation, **plus de 8 d'entre elles sur 10 ne savent pas si celui-ci bénéficie d'une labellisation ou d'un visa de sécurité attestant de son expertise en cybersécurité**. Seuls 7% déclarent qu'il en dispose, et 1 sur 10 qu'il n'en a aucun. Ce résultat souligne moins une absence démontrée de professionnels qualifiés qu'un manque de visibilité sur les garanties offertes, et renforce l'intérêt d'outils d'orientation simples pour les collectivités.

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 (2022)

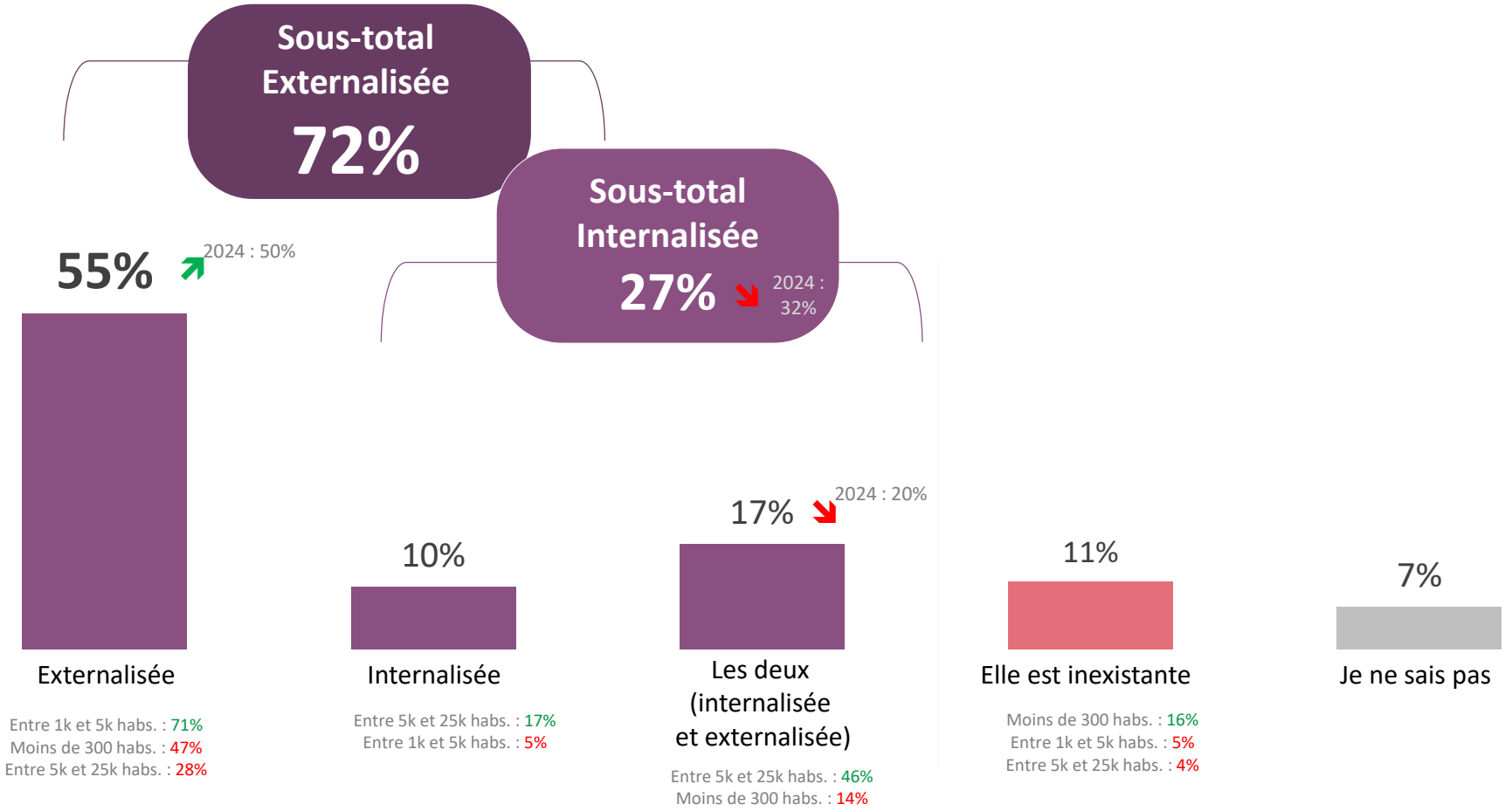


(1) PASSI : Prestataire d'audit de la sécurité des systèmes d'information
(2) PRIS : Prestataire de réponse aux incidents de sécurité

Une place centrale des prestataires, qui se couple à une gestion largement externalisée, totale ou partielle : plus de la moitié des collectivités l'externalisent entièrement, et plus de 7 sur 10 y ont recours au moins en partie. La gestion internalisée, seule ou mixte, est bien moins répandue. Les communes de plus de 5 000 habitants combinent plus souvent les deux approches, **tandis que les plus petites sont davantage dépourvues de gestion de la sécurité informatique**. Cette dépendance aux prestataires renforce l'importance de l'orientation et de la capacité des collectivités à apprécier les services qui leur sont proposés.

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

Base : Total répondants (2830)



Des communes qui ont besoin d'être guidées pour choisir, déployer et pérenniser leur protection

Une sensibilisation existante mais trop ponctuelle. Sept répondants sur dix déclarent avoir été sensibilisés au cours des douze derniers mois, mais le plus souvent de façon ponctuelle (40 % contre 31 % de façon régulière).

Une offre difficile à évaluer. Près de sept répondants sur dix ne savent pas juger si les solutions disponibles correspondent aux besoins de leur collectivité, ce qui souligne un déficit d'accompagnement à la décision.

Des prestataires centraux, mais des qualifications peu lisibles. Les collectivités se tournent d'abord vers leur prestataire informatique, sans toujours connaître son niveau de qualification en cybersécurité

Cybermalveillance.gouv.fr en sa qualité de **dispositif national d'assistance et de prévention en cybersécurité** poursuit plus que jamais son accompagnement auprès des élus, des secrétaires de mairie et des prestataires qui les accompagnent.



Synthèse générale et pistes de recommandations

La conscience du cyberrisque progresse, mais les communes restent insuffisamment préparées pour y faire face



Image de rawpixel.com sur Magnific

1. Une troisième vague dans un contexte de renouvellement municipal important
Réalisée quelques mois après les élections de mars 2026, l'enquête recueille les perceptions d'élus et d'agents dans un contexte où 71% des répondants déclarent une équipe municipale nouvelle ou différente. Ce début de mandat constitue un élément de lecture des évolutions du baromètre et une opportunité d'accompagnement des collectivités.

2. Des moyens informatiques qui demeurent fortement contraints, surtout dans les petites communes
Budgets modestes, recours fréquent aux équipements personnels, externalisation de la gestion de la sécurité : les capacités de protection restent largement déterminées par la taille de la commune. Les perspectives d'augmentation budgétaire concernent une minorité des collectivités.

3. Une sensibilité accrue aux cyberrisques, sans préparation suffisante
La proportion de collectivités se jugeant fortement exposées atteint 42% (+4 points depuis 2024). Dans le même temps, 34% estiment leur protection faible (+4 points) et 59% ne se considèrent pas suffisamment préparées en cas d'attaque. L'enjeu dépasse ainsi la seule prise de conscience et concerne la capacité concrète à prévenir et gérer les incidents.

4. Un besoin d'accompagnement qui va au-delà des solutions techniques
Le manque de connaissances arrive en tête des freins et 68% des répondants ne savent pas apprécier si les solutions de cybersécurité du marché sont adaptées à leurs besoins. Les prestataires restent les principaux interlocuteurs, tandis que leurs qualifications demeurent largement méconnues.

L'enseignement clé : passer de la sensibilisation à la mise en sécurité opérationnelle des collectivités, avec des solutions simples, lisibles et adaptées à leurs moyens.

opinionway

PARIS • BORDEAUX • VARSOVIE • CASABLANCA • ABIDJAN

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.

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.

esomar Corporate 2026

afaq ISO 20252 Étude marketing et d'opinion AFNOR CERTIFICATION

Restons *connectés* !

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

Je m'abonne

Vos contacts OpinionWay

Christine PUJOL
Directrice du département
AdVanced Methods
Tel. +33 7 76 91 19 23
cpujol@opinion-way.com

Larissa Xia
Analyste sénior
Département AdVanced Methods
lxia@opinion-way.com

AdVanced opinionway #quant #analytics #multi-sector
Enable today, shape tomorrow

Une expertise data transversale sur mesure pour éclairer vos insights