opinionway

— POUR —

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Mesure de notoriété et de maturité en matière de cybersécurité auprès des TPE-PME

2025

Rapport d'étude | 25/07/25

Image de kipargeter sur freepik

opinionway

Crédits : dev-asangbam

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

La participation à l'enquête a été ouverte à toutes les entreprises sollicitées par les partenaires de Cybermalveillance.gouv.fr, sans cadrage spécifique de l'échantillon a priori. 38 entreprises de plus de 250 salariés répondantes ont répondu et ont été intégrées à la tranche des 100 à 250 salariés.

Les évolutions calculées au regard de l'échantillon d'entreprises répondantes l'an dernier ne sont pas faites sur un échantillon d'entreprises similaires.
Seule la structure des échantillons en termes de taille et de macro-secteurs est comparable.

Un protocole identique aux précédentes mesures …

Echantillon de **588 entreprises de moins de 250 salariés** en France métropolitaine et dans les départements et régions d'Outre-Mer (DROM).

Un redressement a été opéré a posteriori pour disposer d'un échantillon représentatif des entreprises françaises de moins de 250 salariés en termes de taille de moins et plus de 10 salariés et de secteurs d'activité (5 secteurs).

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

Questionnaire

Les interviews ont été réalisées **du 02 juin au 7 juillet 2025**.
Les TPE/PME ont été sollicitées via une diffusion du lien vers l'enquête sur les Réseaux Sociaux et par le biais de différentes organisations partenaires telles que l'U2P, le MEDEF et le CPME .

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 : 1,9 à 4,4 points au plus pour un échantillon de 500 répondants.

Redressement de l'échantillon

Un redressement sur le secteur d'activité et la taille des entreprises a été opéré a posteriori pour disposer d'un échantillon représentatif des entreprises françaises de moins de 250 salariés en termes de macro-secteurs d'activité et de taille.

	% Brut		% Redressé	
Secteur d'activité	*Effectif*	*%*	*Effectif*	*%*
Base	*588*		*588*	
Agriculture / Industrie / BTP	127	22%	173	29%
Commerce / HCR	68	11%	123	21%
Services aux entreprises	185	31%	176	30%
Administration / Santé / Enseignement	69	12%	59	10%
Services aux particuliers	139	24%	56	10%

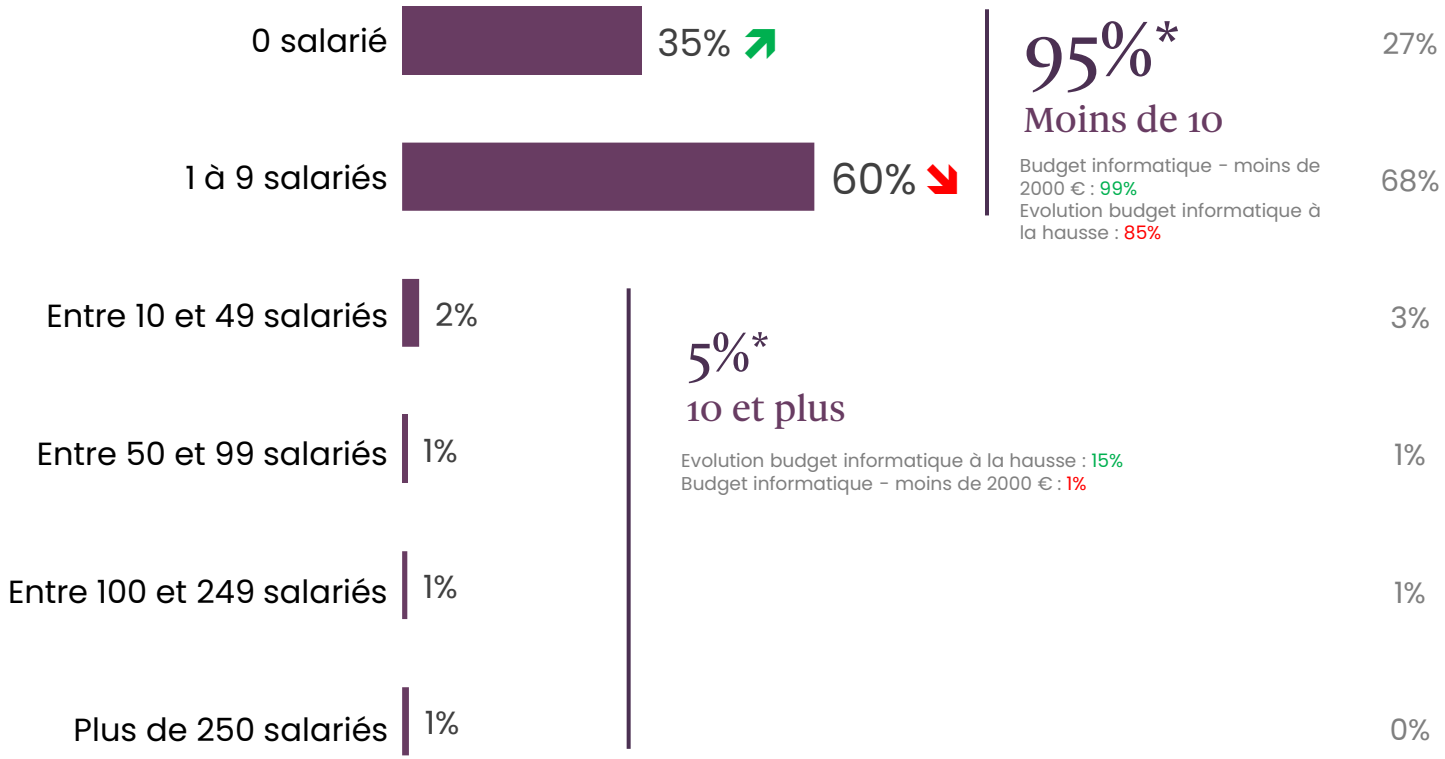
	% Brut		% Redressé	
Taille d'entreprise	*Effectif*	*%*	*Effectif*	*%*
Base	*588*		*588*	
Moins de 10 salariés	377	64%	559	95%
10 salariés et plus	211	36%	29	5%

Source INSEE 2024 - Entreprises privées de 0 à 250 salariés

Des entreprises de moins de 10 salariés, qui représentent la majorité du tissu économique français

Q2. Combien de salariés permanents compte l'entreprise ?

Base : Total répondants (588)



* Structure redressée a posteriori

: Résultat statistiquement supérieurs ou inférieurs à la vague 2024

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

Les résultats

opinionway

01

État des lieux en matière de gestion informatique

Une gestion de la sécurité informatique conditionnée par la taille de l’entreprise...

Au sein des TPE-PME, la gestion informatique reste assurée directement par le chef d'entreprise. En effet, 8 répondants sur 10 déclarent que ce dernier endosse également le rôle de responsable informatique.

Q4. Enfin, quelle est la fonction de la personne en charge de l'informatique au sein de l'entreprise ?
Base : Total répondants (588)

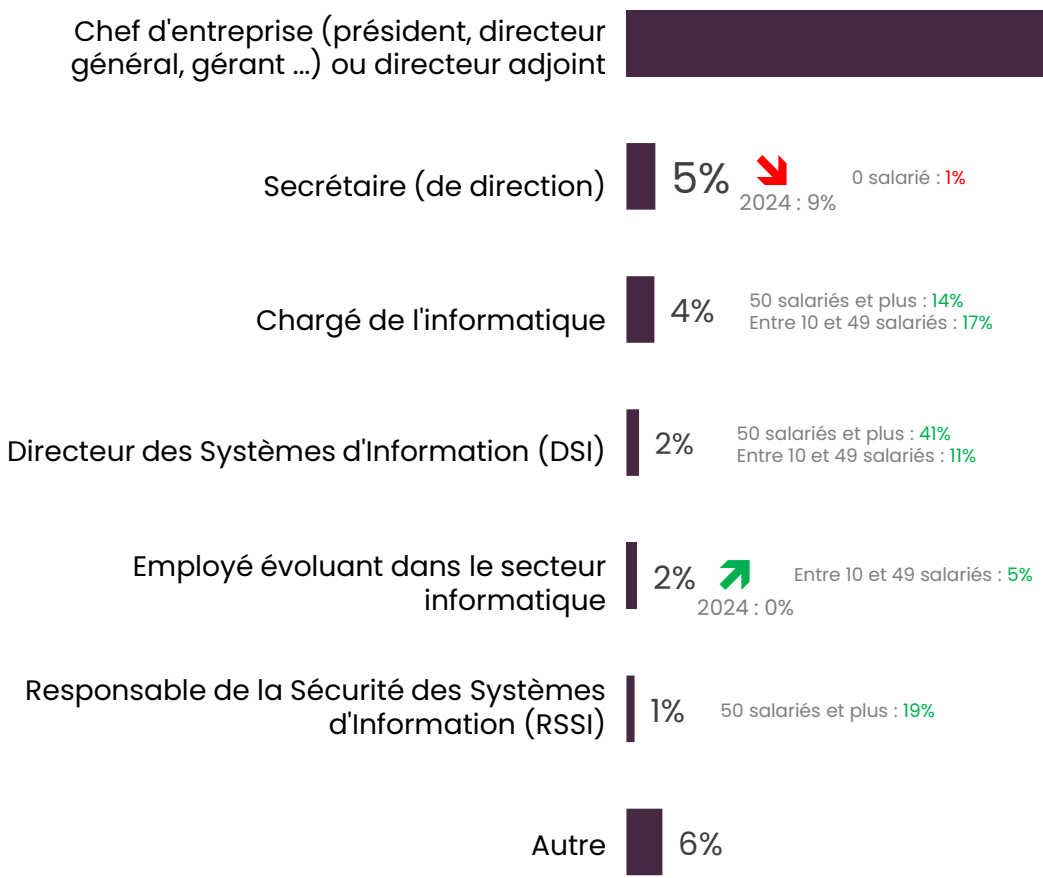
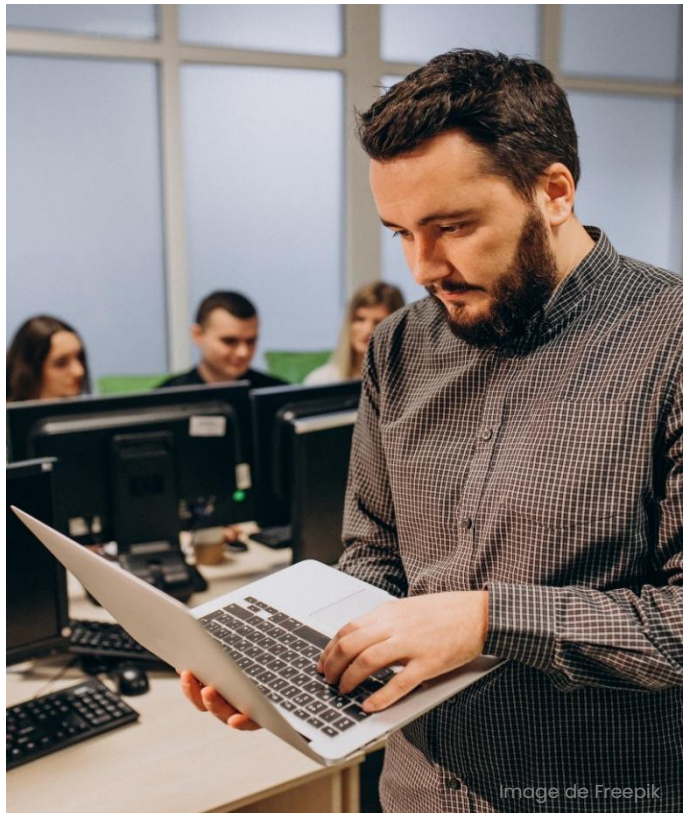
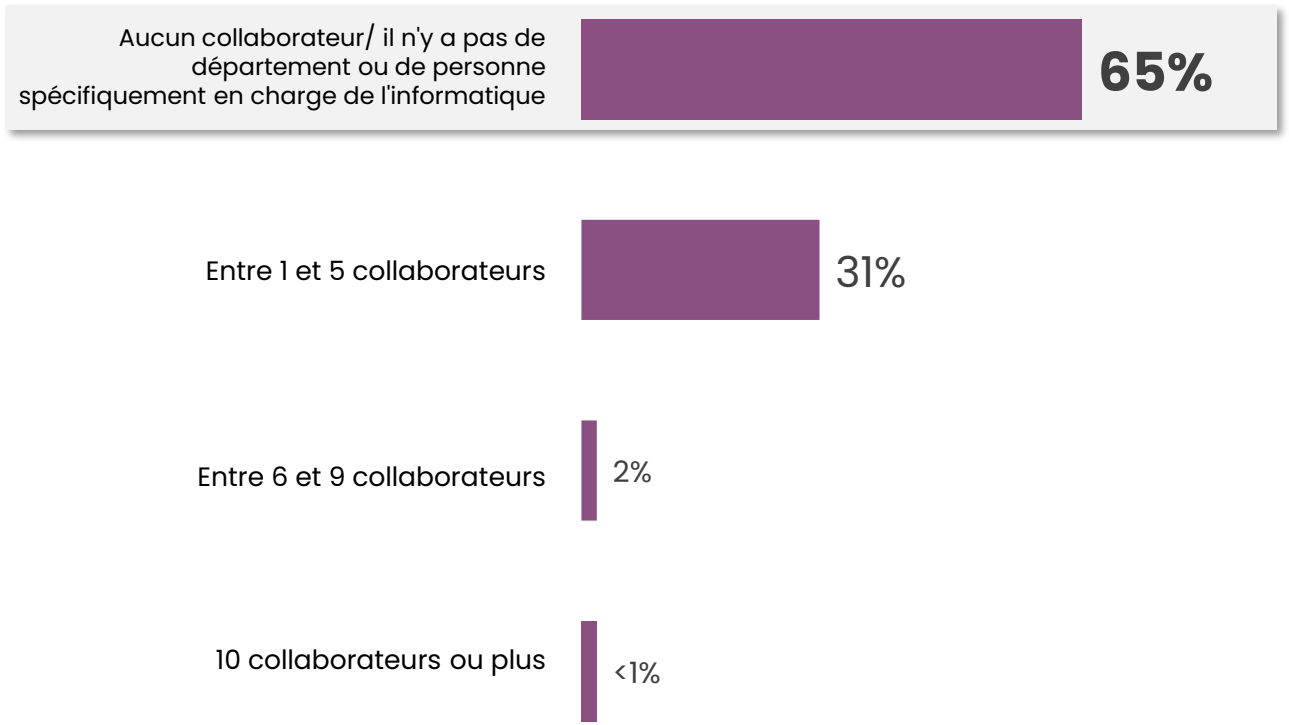



Image de Freepik

Des entreprises qui sont peu nombreuses à disposer de personnel dédié à l'informatique. En effet, 2 tiers des répondants précisent que leur entreprise ne compte pas de personnel spécifiquement dédié à cette tâche.

Q5. Combien de personnes travaillent dans l'équipe en charge de l'informatique ?
Base : Entreprise comptant au moins un salarié permanent (383)



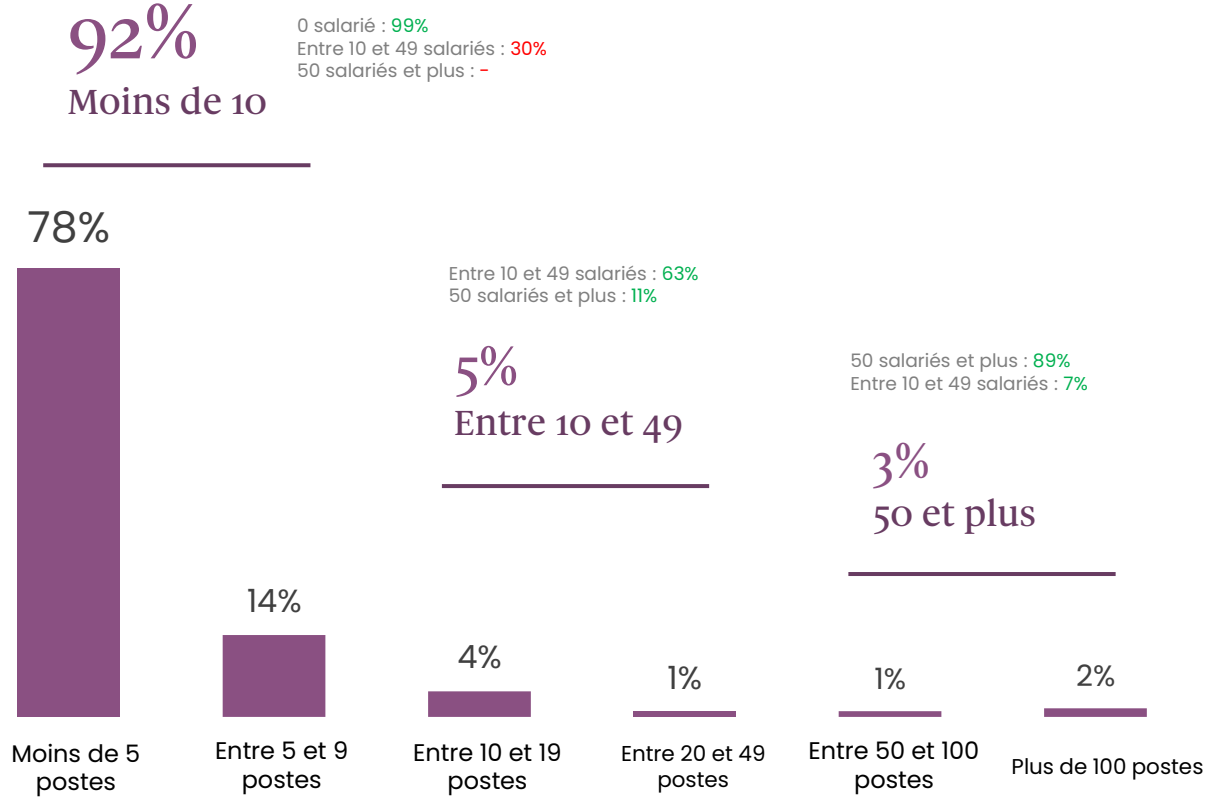


x% / x% : Résultat statistiquement supérieur ou inférieur au total

Cela se traduit également par un nombre limité de postes informatiques, fixes ou portables : près de 8 entreprises sur 10 disposent de moins de 5 postes, et 9 sur 10 en ont moins de 10…

Q6. Combien de postes informatiques (ordinateurs portables ou fixes) y a-t-il au sein de votre entreprise ?

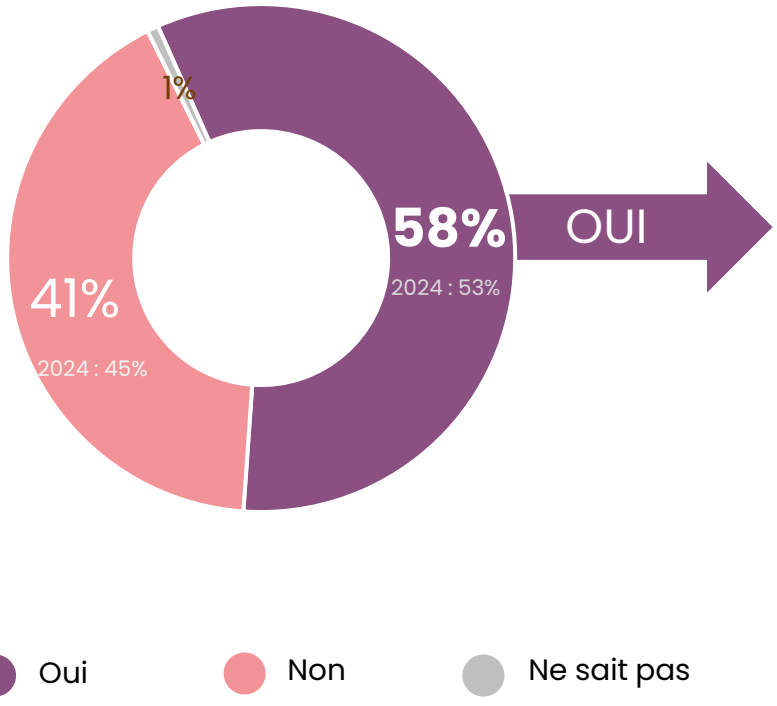
Base : Total répondants (588)

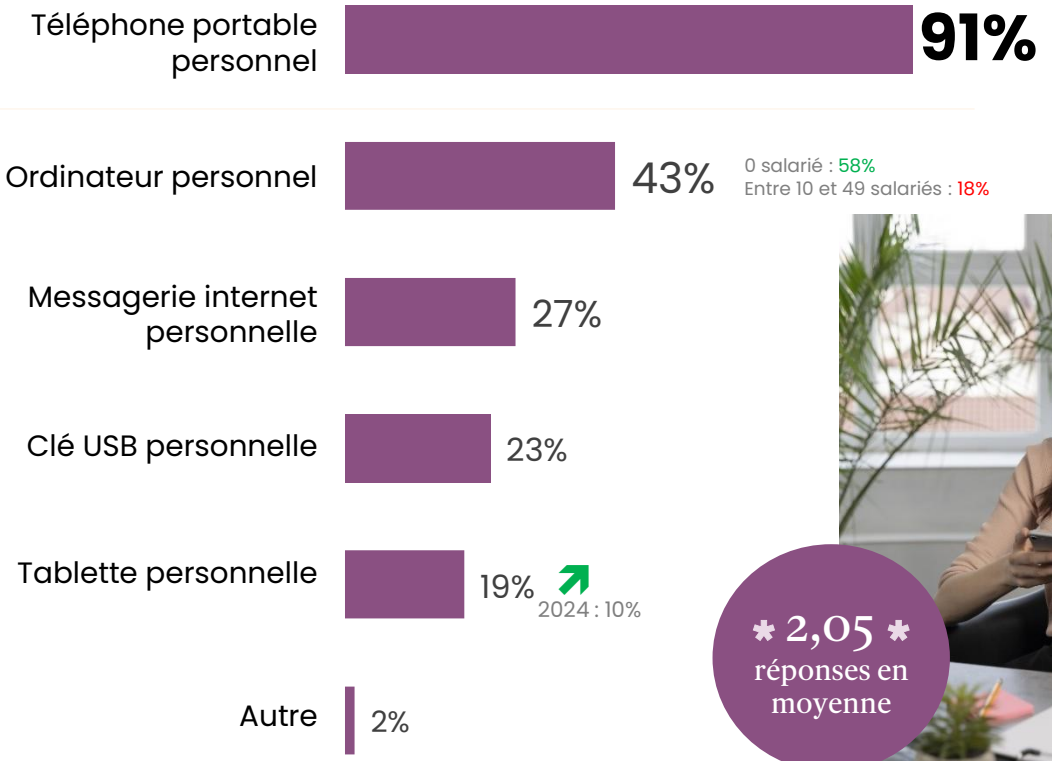


Le recours aux équipements personnels reste fréquent, avec près de 6 entreprises sur 10 déclarant en utiliser à des fins professionnelles. Le téléphone portable est de loin l'outil le plus concerné, mentionné par 9 répondants sur 10. Suivent l'ordinateur personnel, utilisé par 4 répondants sur 10, puis la messagerie internet personnelle, citée par un quart des répondants.

Q8. Des équipements personnels (non fournis par l'entreprise) tels que des téléphones portables, tablettes… sont-ils utilisés pour les activités de l'entreprise ? Base : Total répondants (588)

Q8bis. Vous avez déclaré que des équipements personnels sont utilisés pour les activités de l'entreprise. Pouvez-vous préciser lesquels ? Base : Ont déclaré que des équipements personnels étaient utilisés pour les activités de leur entreprise (339) - Plusieurs réponses possibles

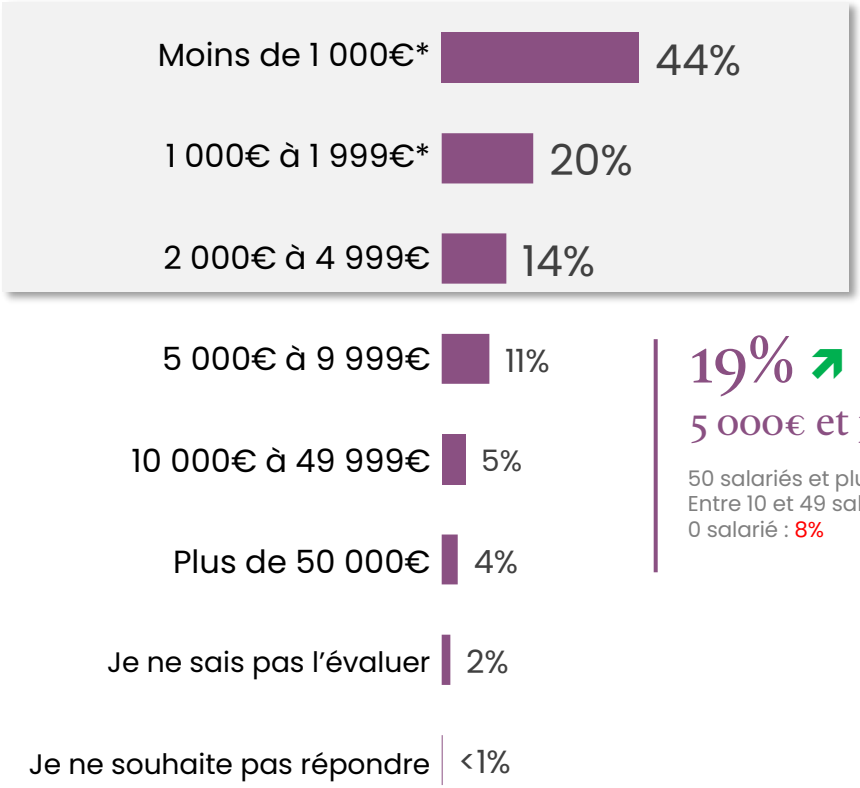




* 2,05 * réponses en moyenne

Sur 2025, les entreprises répondantes sont un peu plus nombreuses à déclarer allouer 5000 € et plus dans le budget annuel dédié à l'informatique. Malgré tout, la grande majorité d'entre elles déclarent toujours allouer moins de 5000€: près de 8 entreprises sur 10 sont concernées, particulièrement celles sans salarié. La part consacrée à la sécurité informatique, reste inférieure à 2000€ pour 77% d'entre elles, sans intention de recruter en cybersécurité à l'avenir.

Q9. Quel est le montant du budget HT annuel de l'entreprise dédié à l'informatique (il s'agit du budget d'investissement et/ou de fonctionnement incluant par exemple la maintenance, les licences logicielles, le renouvellement du parc informatique, du photocopieur, de l'imprimante etc..., hors Ressources Humaines) ?
Base : Total répondants (588)



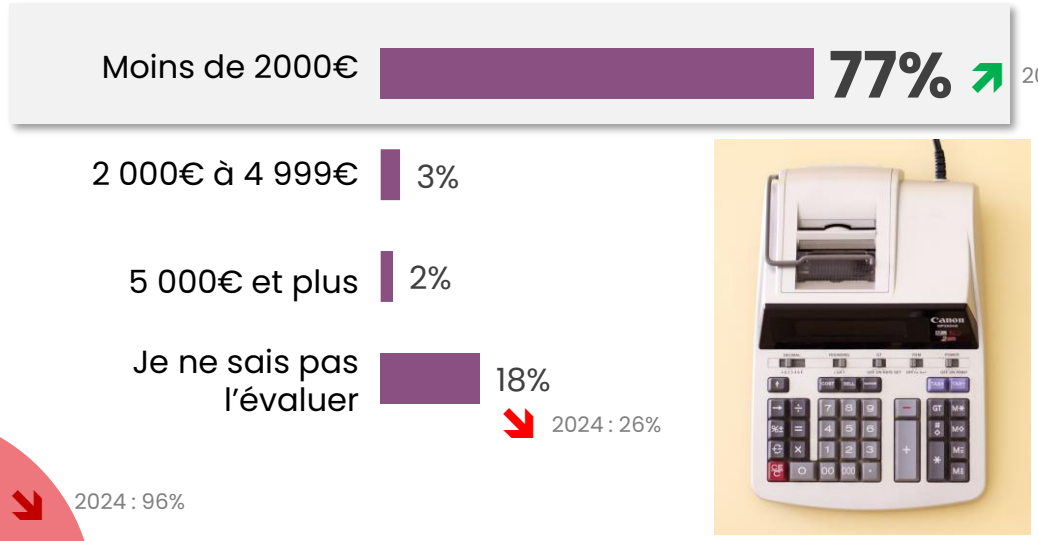
*Nouvel item ajouté

78% ↘ 2024 : 85%
Moins de 5 000€
0 salarié : 91%
Entre 10 et 49 salariés : 29%
50 salariés et plus : 1%

19% ↗ 2024 : 13%
5 000€ et plus
50 salariés et plus : 78%
Entre 10 et 49 salariés : 57%
0 salarié : 8%

92% ↘ 2024 : 96%
Ne prévoient pas de recruter des ressources humaines en cybersécurité l'an prochain
Entre 10 et 49 salariés : 80%
50 salariés et plus : 75%

Q9b. Dans ce budget, quelle est l'enveloppe consacrée à la sécurité informatique (hors Ressources Humaines) ?
Base : Ont déclaré connaitre le budget consacré à la sécurité informatique (575)



Q9e. Prévoyez-vous de recruter des ressources humaines en cybersécurité l'an prochain ? Base : Total répondants (588)

↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 x% / x% : Résultat statistiquement supérieur ou inférieur au total

Si près de 2 entreprises sur 3 prévoient de maintenir leur budget IT stable, 15 % envisagent de l'augmenter l'année prochaine, en particulier les plus grandes structures et celles qui estiment être fortement exposées aux cyberattaques. Une sur 5 … ne sait pas quelle sera l'orientation donnée pour 2026.
Parmi celles envisageant une hausse, les investissements futurs se concentreraient en priorité sur des solutions techniques et équipements de sécurité, reléguant au second plan les actions de sensibilisation…

q9c. Prévoyez-vous de faire évoluer ce budget l'an prochain ?
Base : Total répondants (588)

Comptent faire évoluer le budget lié à l'informatique…

15% ↗
A la hausse
2024 : 10%

50 salariés et plus : 49%
Entre 10 et 49 salariés : 37%
Exposition aux cyberattaques élevée : 22%
Exposition aux cyberattaques faible : 8%
Non sensibilisé à la sécurité info. : 8%

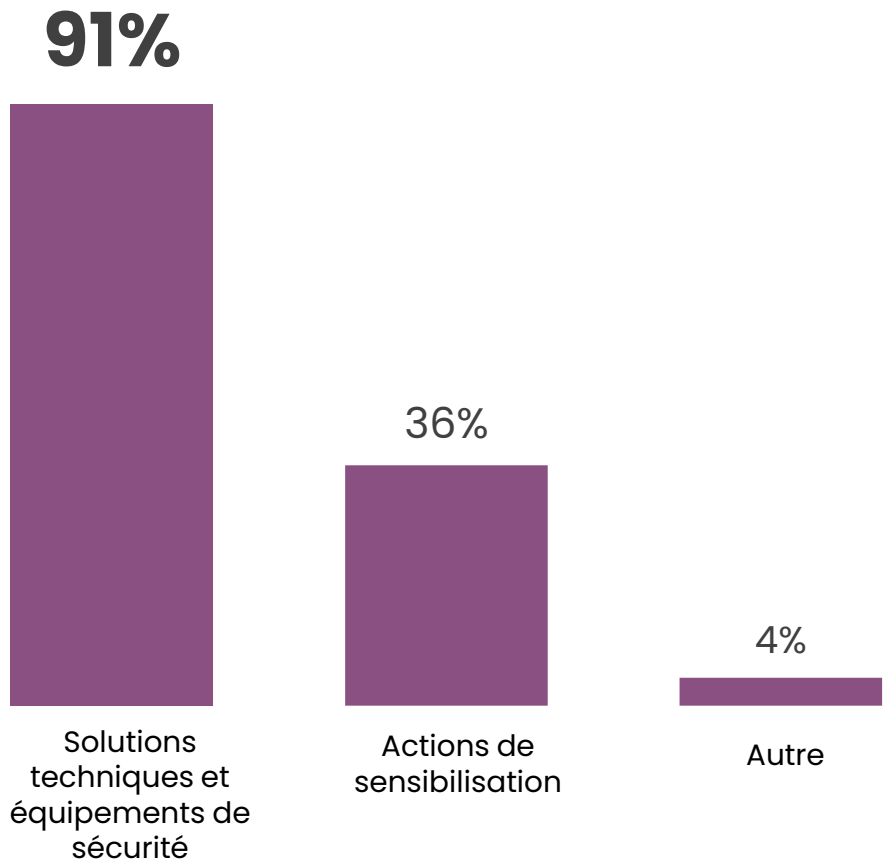
20%
Ne sait pas

1% ↘
A la baisse

64% ↘
Aucune évolution
2024 : 72%

Exposition aux cyberattaques faible : 76%
0 salariés : 73%
Entre 10 et 49 salariés : 41%
50 salariés et plus : 32%

9d. A quel poste pensez-vous allouer ce budget supplémentaire ? Base : Ont déclaré une hausse du budget consacré à la sécurité informatique l'an prochain (91)



↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 x% / x% : Résultat statistiquement supérieur ou inférieur au total

… les entreprises de 50 salariés ou plus ayant répondu au sondage cette année se montrent davantage enclines à vouloir investir également dans la sensibilisation des collaborateurs.

q9c. Prévoyez-vous de faire évoluer ce budget l'an prochain ? Base : Total répondants (588)

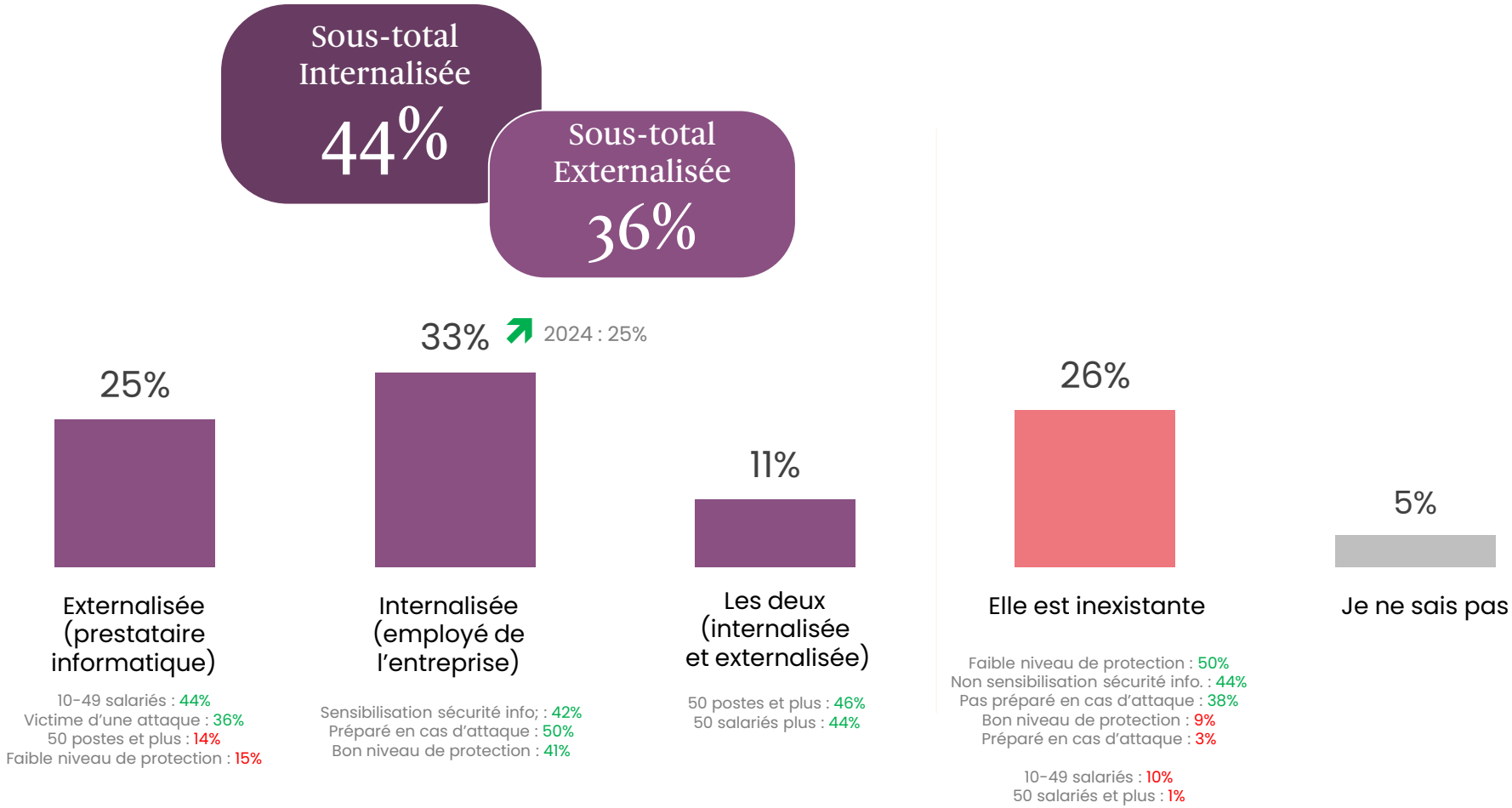
		Tailles des entreprises				Secteur d'activité				
	TOTAL	0 salarié	1 à 9 salariés	Entre 10 et 49 salariés	50 salariés et plus	Agriculture / Industrie / BTP	Commerce / HCR	Services aux entreprises	Administration / Santé / Enseignement	Services aux particuliers
Base (non pondéré)	*588*	*152*	*225*	*103*	*108*	*127*	*68*	*185*	*69*	*139*
Oui, à la hausse	15%	9%	17%	**37%**	**49%**	12%	10%	22%	14%	19%
Oui, à la baisse	1%	2%	1%	0%	3%	4%	0%	-	-	0%
Non, aucune évolution de budget prévu	64%	73%	60%	**41%**	**32%**	65%	65%	64%	59%	62%
Je ne sais pas	20%	16%	22%	22%	16%	19%	25%	14%	27%	19%

9d. A quel poste pensez-vous allouer ce budget supplémentaire ? Base : Ont déclaré une hausse du budget consacré à la sécurité informatique l'an prochain (91)

Base (non pondéré)	*147*	*15**	*44*	*38*	*50*	*33**	*8**	*60*	*16**	*30**
Solutions techniques et équipements de sécurité	91%	97%	89%	91%	93%	87%	98%	92%	100%	79%
Actions de sensibilisation	36%	-	42%	45%	**69%**	47%	22%	41%	12%	34%
Autre	4%	3%	3%	**13%**	8%	1%	2%	6%	-	10%

La gestion de la sécurité informatique se partage entre internalisation et externalisation, avec une part plus notable de l'approche interne pour l'échantillon d'entreprises répondantes cette année. Cependant, plus d'un quart des entreprises déclarent encore une gestion inexistante. Une absence de gouvernance qui touche bien moins les plus grosses structures et celles qui se déclarent préparées en cas d'attaque.

q10. La gestion de la sécurité informatique de l'entreprise est-elle ?
Base : Total répondants (588)

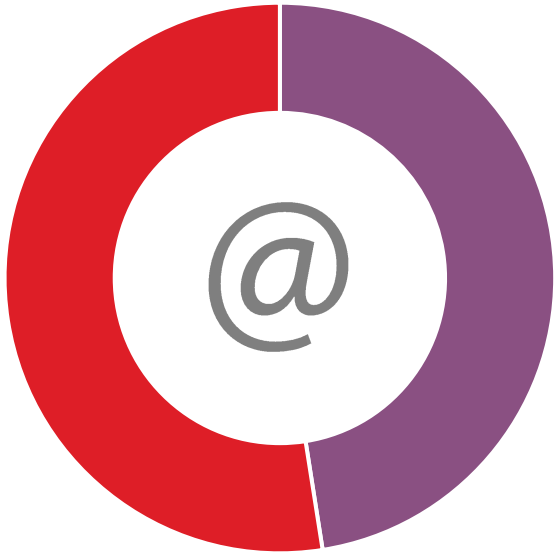


À l'instar de la gestion sécuritaire informatique, la messagerie professionnelle témoigne à nouveau d'une utilisation partagée entre externe et interne, avec une adoption de la messagerie interne plus forte auprès des plus grandes entreprises.

q14. Pour communiquer avec vos collègues, clients prestataires ou administrations (fiscales, sociales, etc.), utilisez-vous un service de messagerie de type :
Base : Total répondants (588)

52%
Externe
(ex : Gmail, Orange, Yahoo, Hotmail...)

2024 : 57%



48%
Interne
avec un nom de domaine au nom de l'entreprise (ex:xx.xx@monentreprise.fr)

2024 : 43%

Préparé en cas d'attaque : 71%
Informatique externalisée : 60%

50 salariés et plus : 89%
10-49 salariés : 74%
0 salarié : 36%

Service aux entreprises : 64%

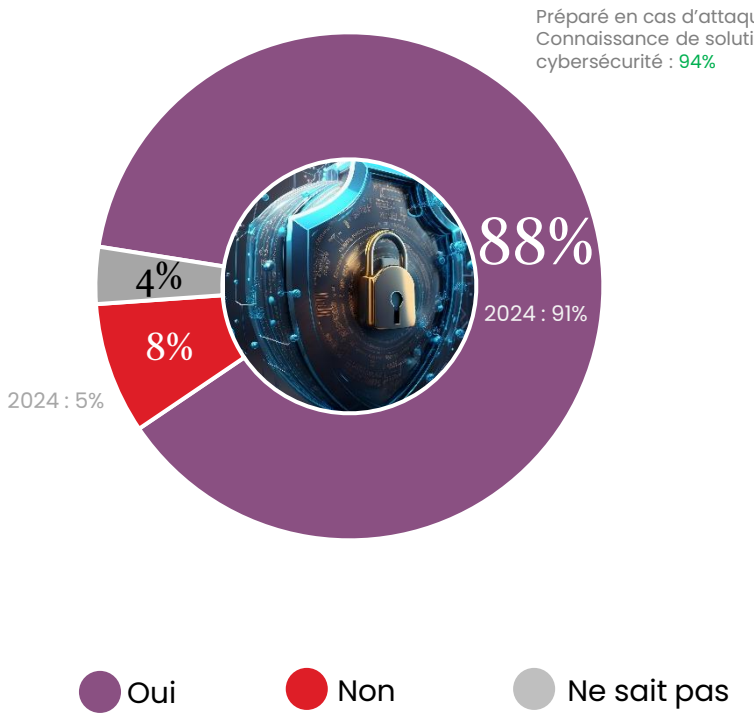
02

État des lieux en matière de sécurité informatique

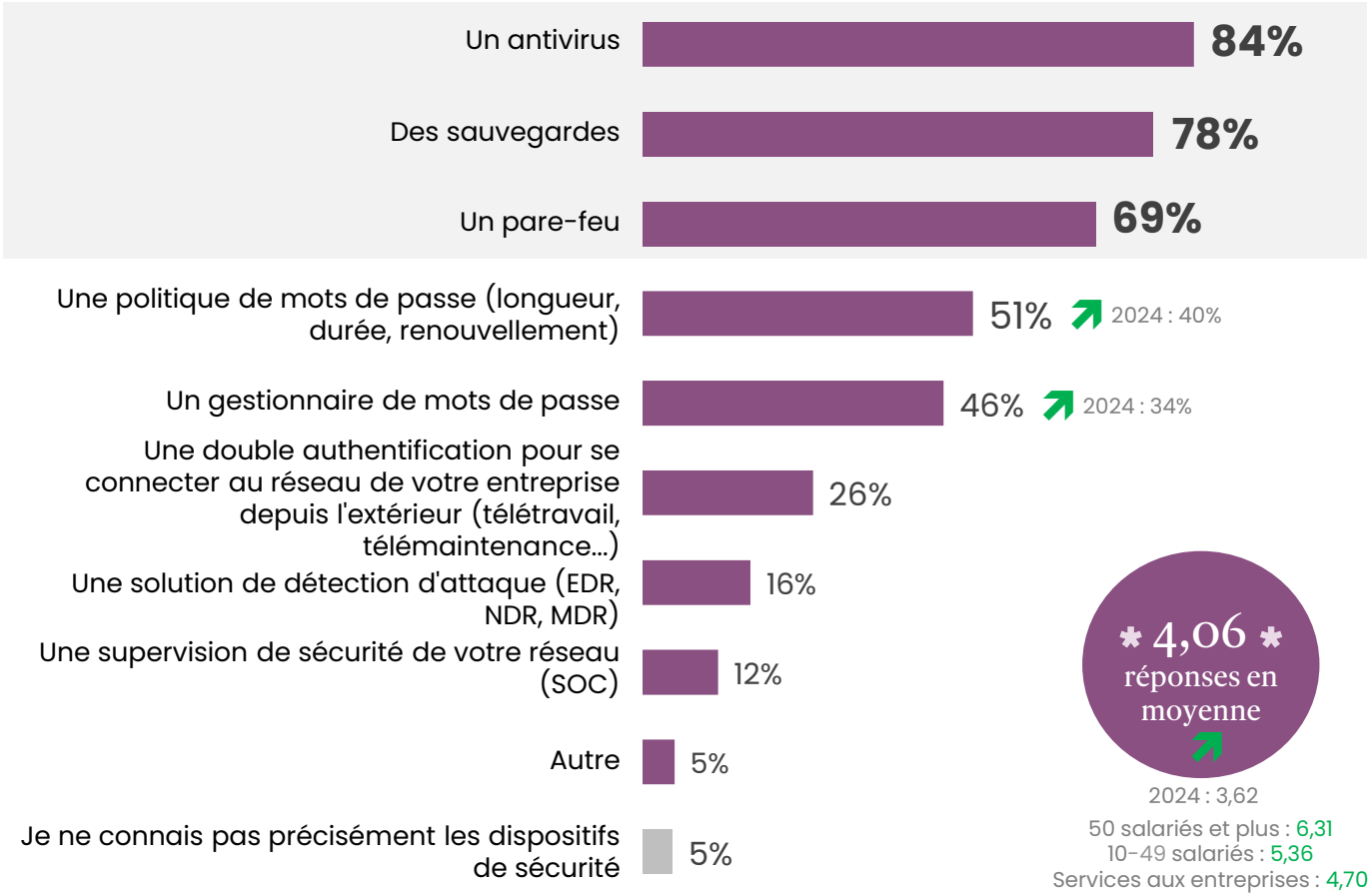
Un niveau de protection bien plus fort auprès des plus grandes entreprises interrogées cette année

Près de 9 entreprises sur 10 déclarent disposer d'au moins un dispositif de sécurité. Les solutions les plus couramment utilisées restent les antivirus, les sauvegardes et les pares-feux. Un niveau de protection en termes de dispositifs qui s'avère corrélé à la taille des structures, les grandes entreprises employant davantage de dispositifs en moyenne.

q13. Votre entreprise est-elle équipée de dispositifs de cybersécurité ? (exemples : pare-feu, antivirus, sauvegardes, politique de mots de passe ...)
Base : Total répondants (588)



q13b. Vous avez déclaré que votre entreprise était équipée de dispositifs de sécurité. Pouvez-vous préciser lesquels ? Plusieurs réponses possibles
Base : Ont déclaré que leur entreprise était équipée de dispositifs de sécurité (518)



* 4,06 * réponses en moyenne

2024 : 3,62
50 salariés et plus : 6,31
10-49 salariés : 5,36
Services aux entreprises : 4,70

↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 x% / x% : Résultat statistiquement supérieur ou inférieur au total

Un niveau de protection en termes de dispositifs qui reste effectivement étroitement lié à la taille de l'entreprise.

q13. Votre entreprise est-elle équipée de dispositifs de cybersécurité ? (exemples : pare-feu, antivirus, sauvegardes, politique de mots de passe …)
Base : Total répondants (588)

		Tailles des entreprises				Secteur d'activité				
	TOTAL	0 salarié	1 à 9 salariés	Entre 10 et 49 salariés	50 salariés et plus	Agriculture / Industrie / BTP	Commerce / HCR	Services aux entreprises	Administration / Santé / Enseignement	Services aux particuliers
Base (non pondéré)	*588*	*152*	*225*	*103*	*108*	*127*	*68*	*185*	*69*	*139*
OUI	88%	**95%**	84%	92%	**96%**	89%	83%	91%	86%	91%
NON	8%	3%	11%	5%	**1%**	8%	11%	7%	9%	3%
Ne sait pas	4%	2%	5%	3%	3%	3%	6%	2%	5%	6%

q13b. Vous avez déclaré que votre entreprise était équipée de dispositifs de sécurité. Pouvez-vous préciser lesquels ?
Base : Ont déclaré que leur entreprise était équipée de dispositifs de sécurité (518) - Plusieurs réponses possibles

Base (non pondéré)	*588*	*152*	*225*	*103*	*108*	*114*	*57*	*173*	*62*	*128*
Un antivirus	84%	82%	86%	82%	87%	90%	82%	80%	91%	82%
Des sauvegardes	78%	77%	78%	**91%**	**93%**	73%	70%	86%	80%	85%
Un pare-feu	69%	67%	69%	**84%**	**94%**	68%	77%	67%	69%	66%
Une politique de mots de passe (longueur, durée, renouvellement)	51% ↗	57%	44%	59%	**83%**	39%	54%	57%	53%	55%
Un gestionnaire de mots de passe	46% ↗	49%	43%	56%	**67%**	40%	35%	**58%**	47%	48%
Une double authentification pour se connecter au réseau de votre entreprise depuis l'extérieur	26%	22%	26%	**46%**	**68%**	19%	16%	**43%**	**11%**	30%
Une solution de détection d'attaque (EDR, NDR, MDR)	16%	11%	16%	**39%**	**65%**	16%	12%	25%	**2%**	16%
Une supervision de sécurité de votre réseau (SOC)	12%	**5%**	13%	**37%**	**50%**	11%	3%	**19%**	5%	13%
Autre	5%	7%	3%	5%	**14%**	7%	5%	4%	3%	3%
Je ne connais pas précisément les dispositifs de sécurité	5%	5%	4%	7%	2%	3%	5%	7%	3%	3%

↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 **x%** / **x%** : Résultat statistiquement supérieur ou inférieur au total

En termes de niveau de protection perçue, les entreprises ayant répondu cette année sont près de 6 sur 10 à déclarer avoir un bon niveau, notamment les plus grosses structures et celles qui évoluent dans le secteur des services aux entreprises, davantage contraintes et sensibilisées aux enjeux de sécurité pour répondre aux besoins de leurs clients BtoB…

q12. Comment évaluez-vous le niveau de protection de votre entreprise en matière de sécurité informatique ?

Base : Total répondants (588)

10-49 salariés : 78%
50 salariés et plus : 75%
Services aux entreprises : 69%
Exposition aux risques faible : 68%

58% ↗ 2024 : 39%

Bon niveau de protection

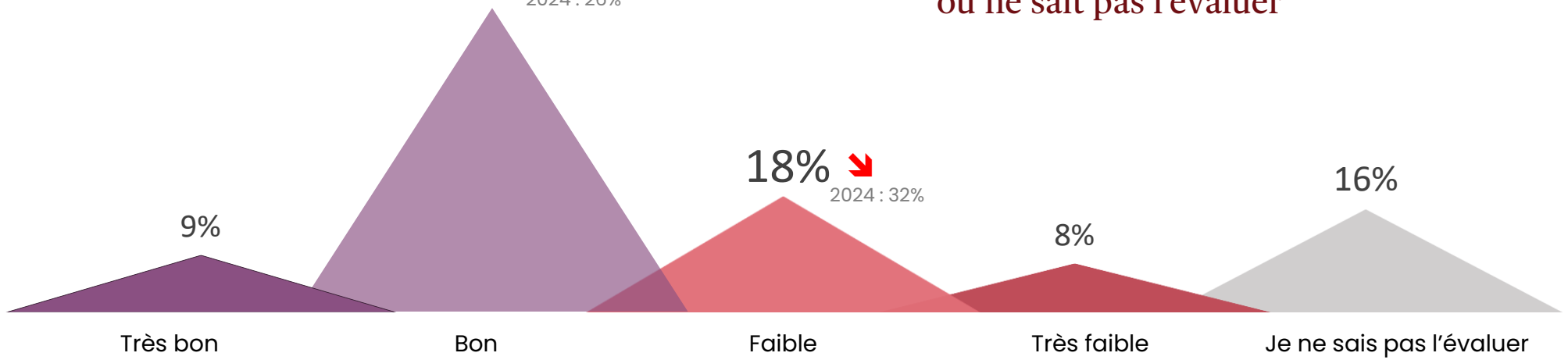
26% ↘ 2024 : 42%

Faible niveau de protection

Non connaissance des solutions de cybersécurité : 36%

42% ↘ 2024 : 61%

Faible niveau de protection ou ne sait pas l'évaluer



↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 x% / x% : Résultat statistiquement supérieur ou inférieur au total

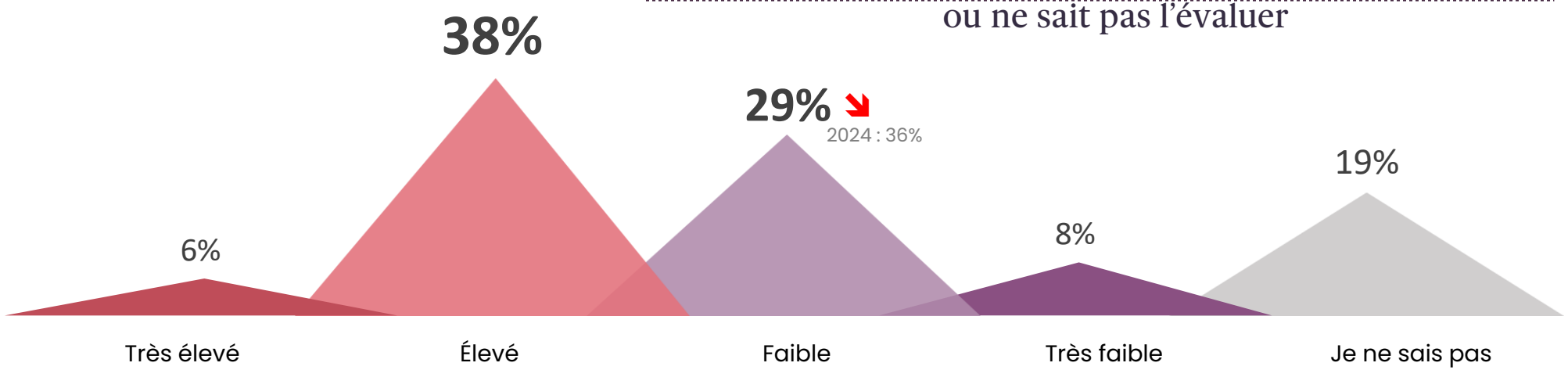
Si les entreprises se sentent globalement mieux protégées, la perception d'exposition reste élevée : 44 % d'entre elles se considèrent fortement exposées aux cyberattaques - un sentiment particulièrement marqué chez les plus grandes structures et celles ayant déjà été victimes d'un incident. À l'inverse, plus d'un tiers des répondants ne se sentent pas particulièrement menacés, notamment ceux estimant bénéficier d'un très bon niveau de protection. A noter que près d'1 sur 5 ne sait toujours pas évaluer son niveau de risque face aux cybermenaces.

q15. Et selon vous, le niveau d'exposition aux risques de cyberattaques de votre entreprise est :
Base : Total répondants (588)

44%
Forte exposition
2024 : 38%
50 salariés et plus : 67%
Victime d'une attaque : 62%

37%
Faible exposition
2024 : 41%
Très bon niveau de protection : 57%
50 salariés et plus : 22%

57%
Faible exposition ou ne sait pas l'évaluer
2024 : 63%



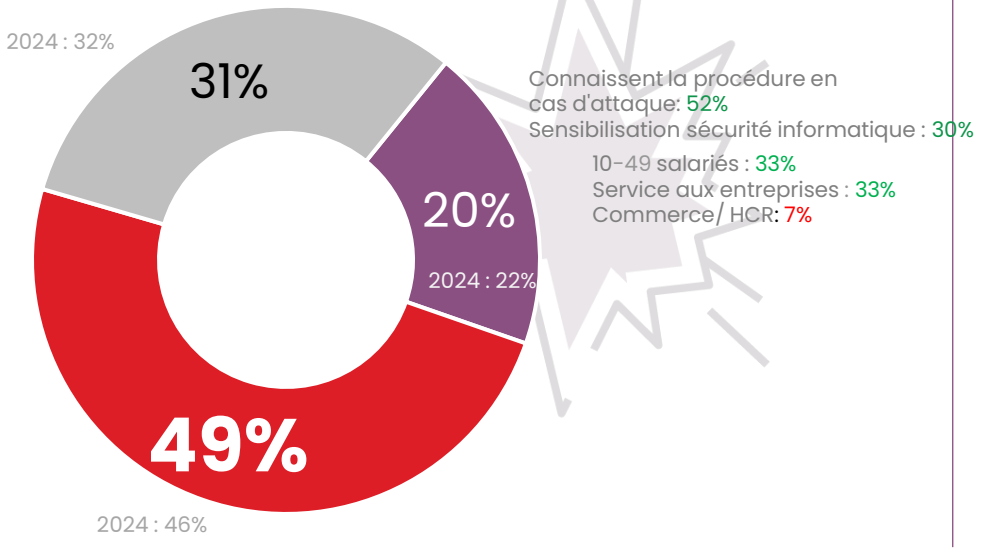
: Résultat statistiquement supérieurs ou inférieurs à la vague 2024

Un sentiment d'exposition qui peut être justifié par un manque de préparation, surtout dans un contexte de menaces en constante évolution. Ainsi, près de la moitié des entreprises reconnaissent ne pas être suffisamment préparées en cas de cyberattaque, et près des deux tiers déclarent ne pas disposer de procédure de réaction en cas d'incident.

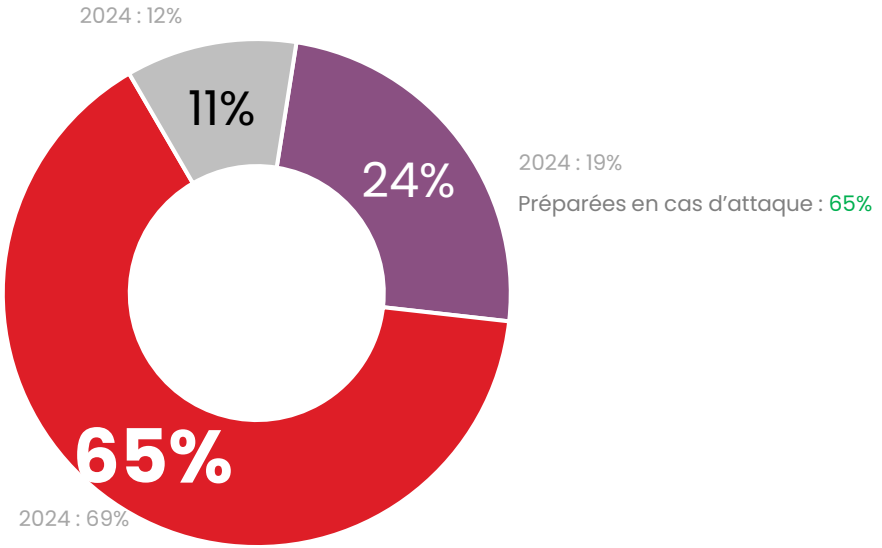
q18. A votre connaissance, votre entreprise est-elle suffisamment préparée en cas d'attaque informatique ?
q19. Disposez-vous d'une procédure de réaction en cas d'attaque informatique ?

Base : Total répondants (588)

Préparées en cas d'attaque



Disposent d'une procédure de réaction

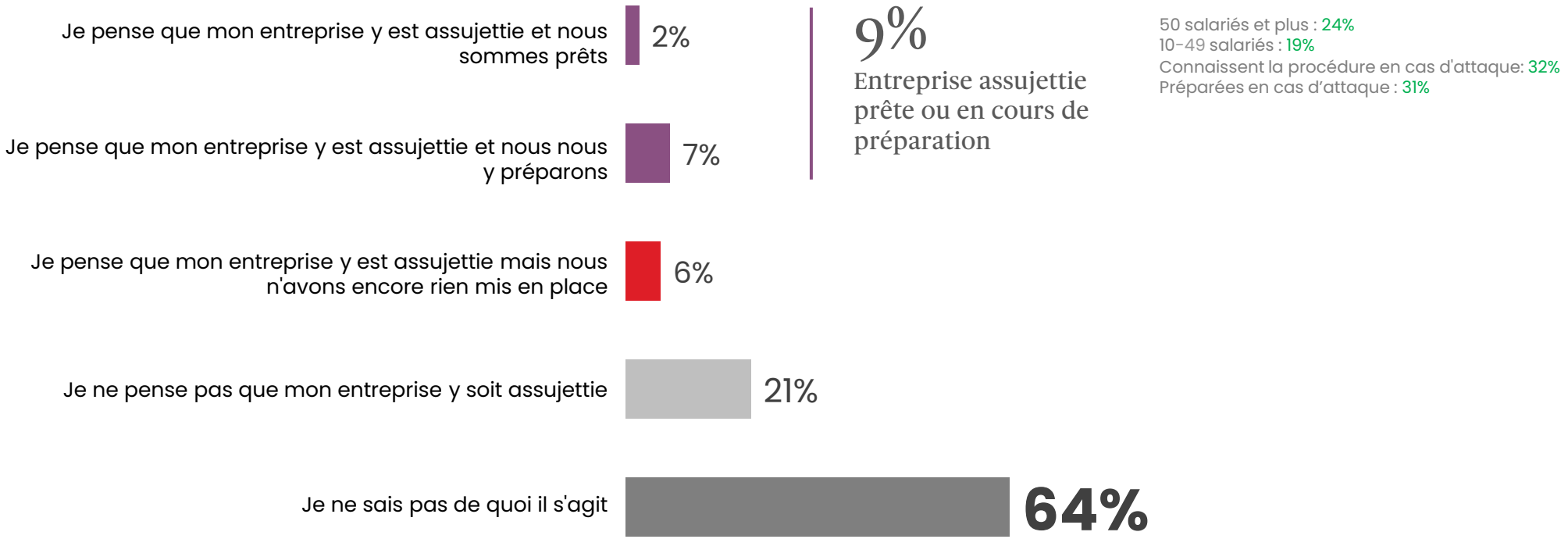


Oui | Non | Ne sait pas

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

Une préparation insuffisante qui se reflète aussi dans la méconnaissance des évolutions réglementaires : 64 % des répondants déclarent ne pas connaître la directive NIS2. Un chiffre à relativiser pour les TPE/PME qui, pour beaucoup, ne sont pas directement concernées par cette réglementation… Seules 9 % des entreprises se disent assujetties, prêtes ou en cours de préparation.

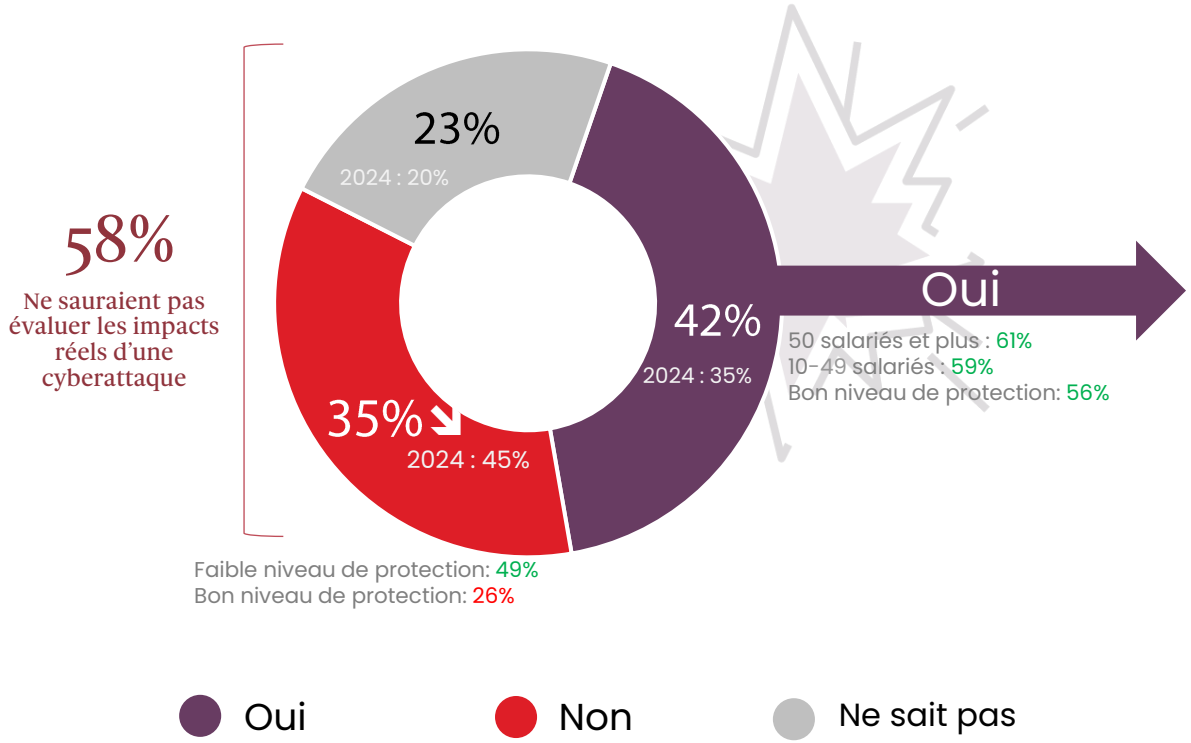
q19bis. Comment appréhendez-vous la directive NIS2 ?
Base : Total répondants (588) *Nouvelle question*



4 entreprises sur 10 se sentent capables d'évaluer les conséquences d'une cyberattaque. Celles-ci anticipent principalement une interruption ou une baisse d'activité, des atteintes aux données (perte, vol ou destruction), ainsi que des répercussions financières.

q16. Sauriez-vous évaluer les impacts (conséquences) réels d'une cyberattaque sur votre entreprise ? Base : Total répondants (588)
q16b. Quels impacts une cyberattaque pourrait avoir sur votre entreprise ? Base : Ont déclaré savoir évaluer l'impact d'une cyberattaque sur leur entreprise (247) - Question ouverte

Sait évaluer les impacts réels d'une cyberattaque

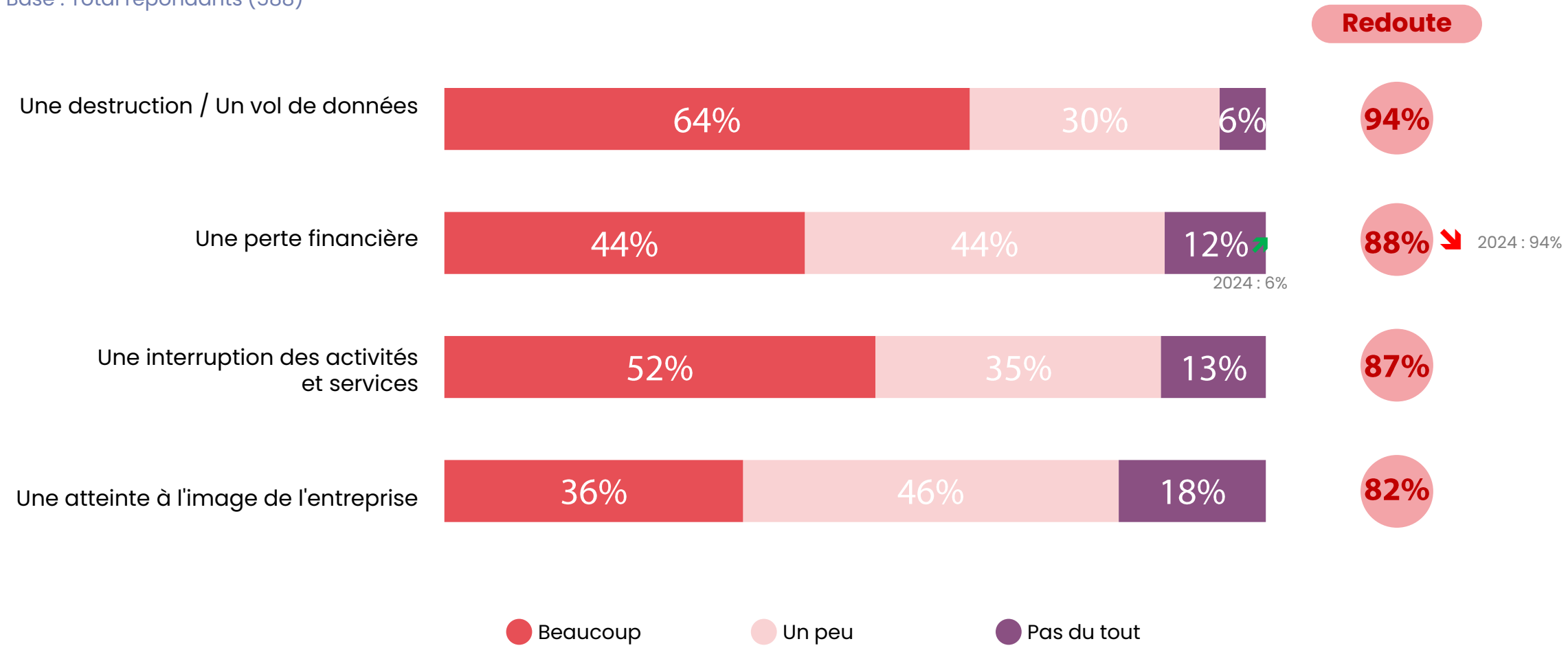


Autre impact sur l'entreprise	**65%**
Interruption ou baisse de l'activité (services, production, réseaux sociaux, etc…)	48%
Atteinte à l'image de l'entreprise, usurpation d'identité, confiance dégradée	19%
Perte de temps	10%
Fermeture de la société	2%
Procédures judiciaires, pénales	1%
Impact sur les données	**41%**
Destruction, perte de données	24%
Vol, piratage, détournement de données	20%
Impact financier	**26%**
Perte financière, chiffre d'affaires, piratage comptes bancaires	23%
Demande de rançon	5%
Autres conséquences (importante, grave, etc…)	7%
Aucun / Ne sait pas / Non-réponse	6% ↘ (2024 : 16%)
Nombre moyen de citations	**1,7**

↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 x% / x% : Résultat statistiquement supérieur ou inférieur au total

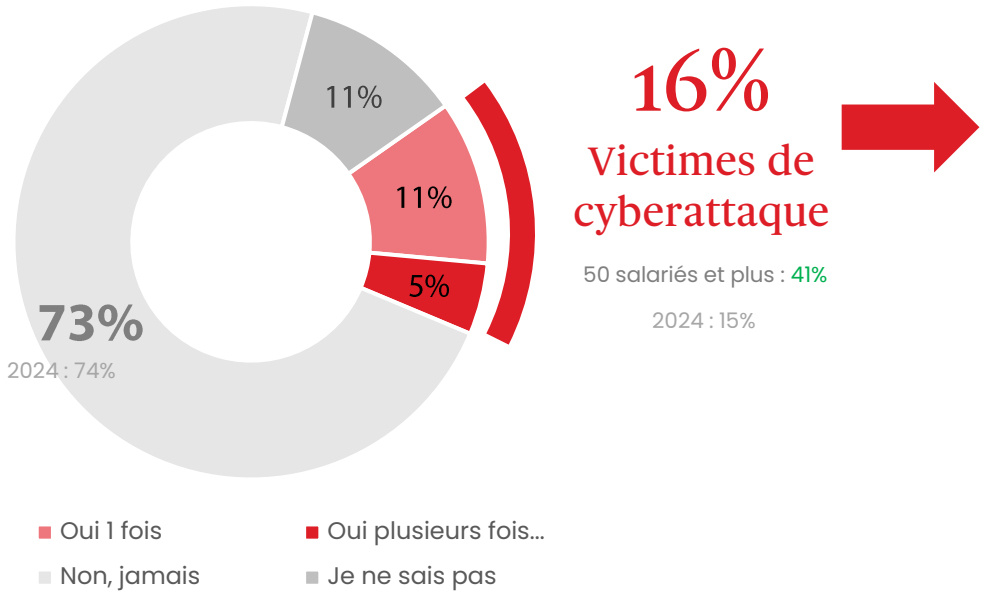
En cas de cyberattaque, plus de 9 entreprises sur 10 redoutent la destruction ou le vol de données, dont 6 sur 10 s'en inquiétant beaucoup. D'autres conséquences restent également très présentes dans les esprits : près de 9 sur 10 craignent une perte financière ou une interruption d'activité, tandis que 8 sur 10 appréhendent une atteinte à l'image de leur entreprise.

Q17. En cas de cyberattaque, dans quelle mesure redoutez-vous … ?
Base : Total répondants (588)



Finalement, 16 % des entreprises déclarent avoir déjà été victimes d'une cyberattaque. Parmi ces entreprises, l'hameçonnage reste l'attaque la plus fréquente, bien plus mise en avant par les entreprises interrogées cette année qu'en vague précédente. Viennent ensuite les failles de sécurité non corrigées et les virus téléchargés.

Q20. A votre connaissance, votre entreprise a-t-elle été victime d'un ou plusieurs incident(s) de sécurité informatique autre qu'une panne au cours des 12 derniers mois ? Base : Total répondants (588)

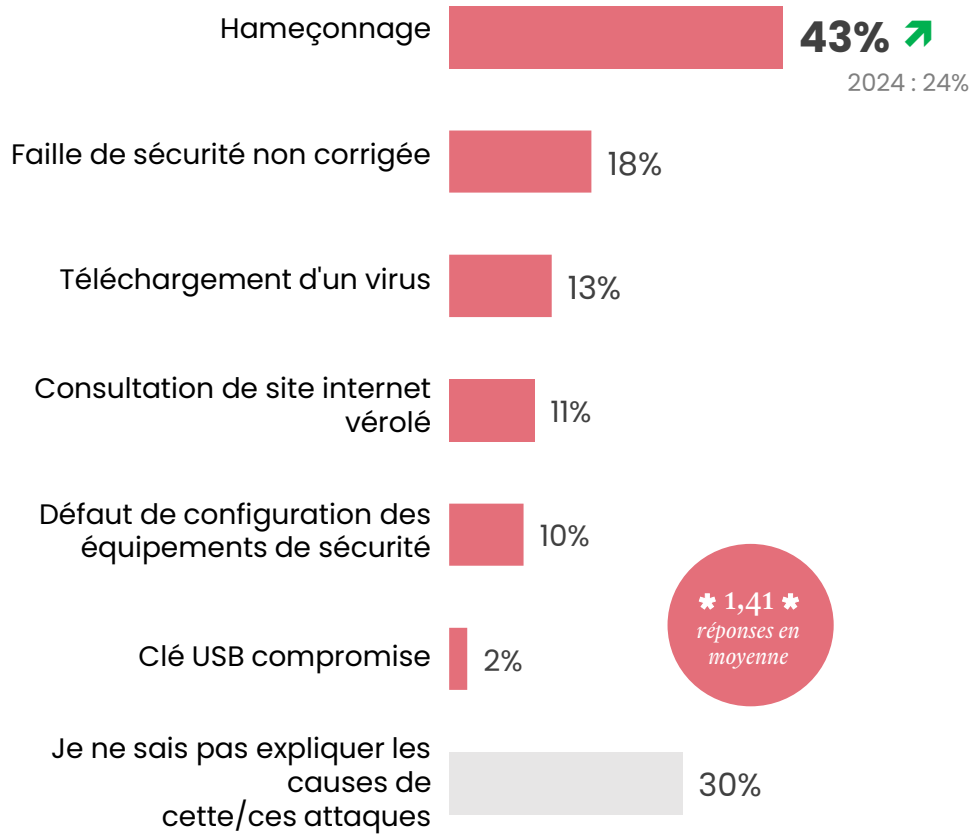


16%
Victimes de cyberattaque

50 salariés et plus : 41%

2024 : 15%

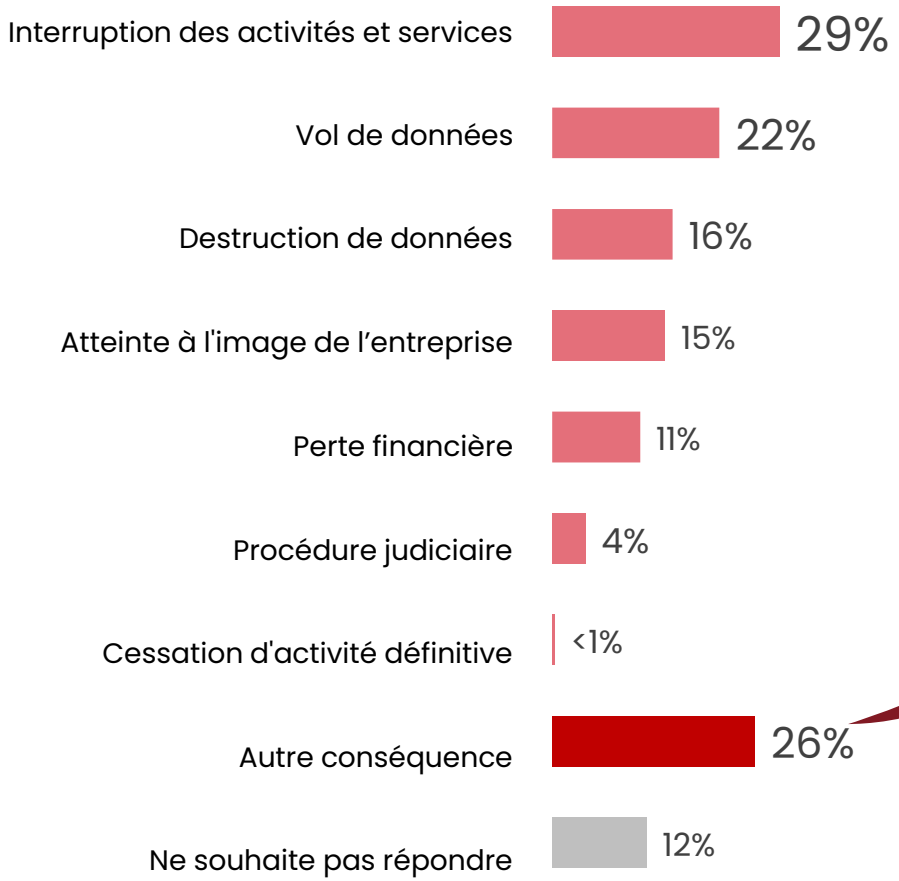
Q20b. A votre avis, à quoi ces attaques étaient-elles liées ? Base : Ont déclaré avoir été victimes d'un ou plusieurs incident(s) de sécurité informatique (94) - Plusieurs réponses possibles



Des attaques qui ont principalement entraîné des interruptions d'activité, la perte ou le vol de données, ainsi qu'une atteinte à la réputation.

Q20c. Et quelles ont été les conséquences de cet/ces incident(s) ?

Base : Ont déclaré avoir été victimes d'un ou plusieurs incident(s) de sécurité informatique (94) - Plusieurs réponses possibles



* 1,41 *
réponses en moyenne

« ***Piratage de réseaux sociaux pro et perso***

Fuite d'information

Usurpation RIB risque de perte financière arrêtée avant virement frauduleux

Arrêt de quelques heures pour restaurer les données

La tension nerveuse, la perte de temps

Réinstallation du système

Site avec informations hors sujet sans conséquences graves

Arrêt de la production durant 1 à 3 heures

Accès à notre boîte mail et envoi de mail à nos clients

Site internet piraté

Avertissement au collaborateur n'ayant pas respecté les règles de sécurité »

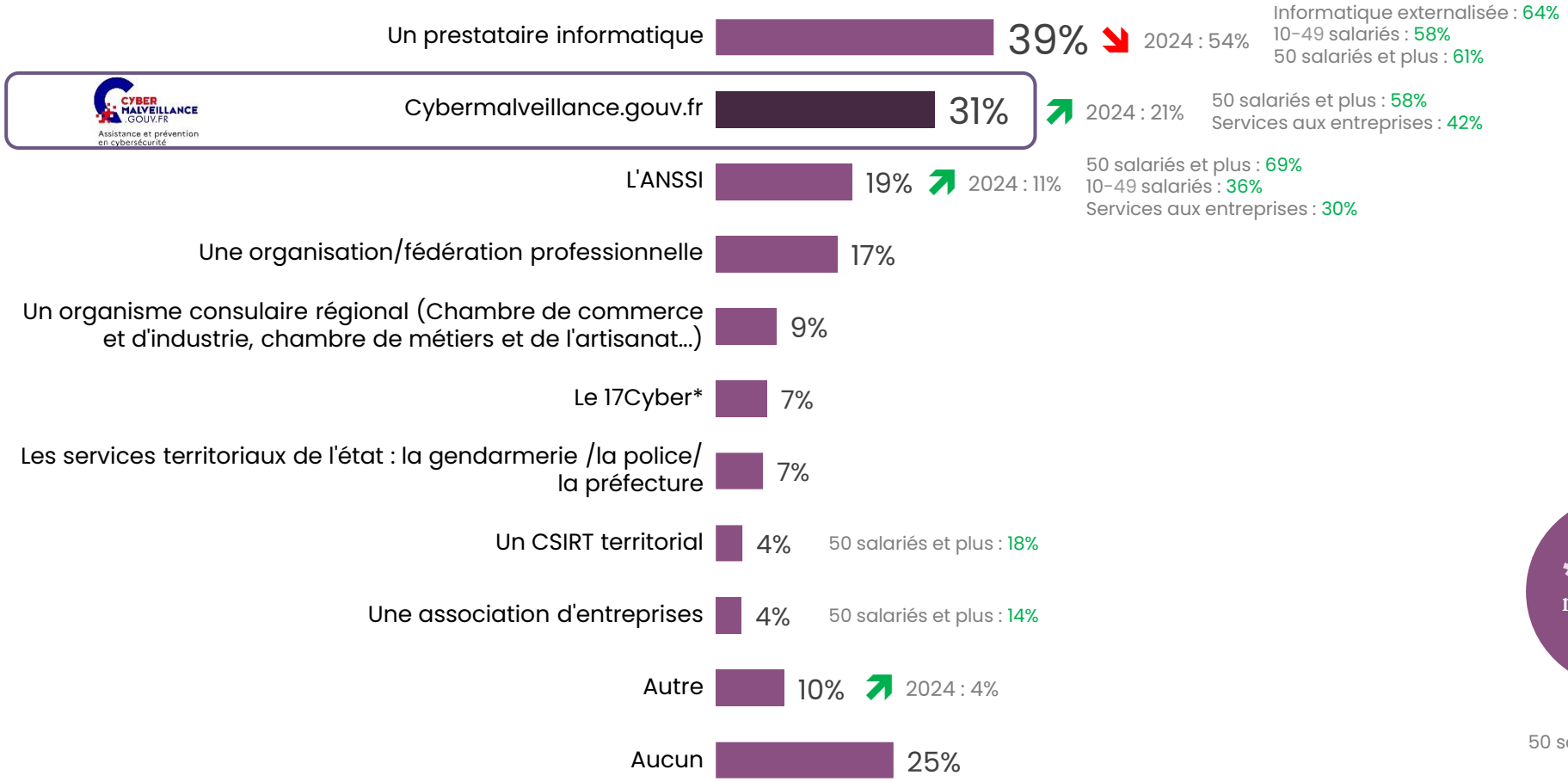
03

Cybersécurité : État des lieux des besoins

Pour s'informer ou se faire accompagner en matière de cybersécurité, près de 4 entreprises sur 10 font appel à des prestataires informatiques, qui restent les interlocuteurs privilégiés malgré un échantillon d'entreprises qui déclarent faire cette année moins appel à ces derniers. Cybermalveillance.gouv.fr, en progression cette année, maintient sa 2ème place, citée par 3 entreprises sur 10. L'ANSSI arrive en 3ème position mentionnée par 2 entreprises sur 10.

q24. Vers qui vous tournez-vous actuellement pour vous informer ou vous aider sur le sujet de la cybersécurité ?

Base : Total répondants (588)



* 1,94 *
réponses en moyenne

2024 : 1,68

50 salariés et plus : 2,68

*Nouvel item ajouté

Les plus grandes structures se tournent vers davantage d'interlocuteurs, mentionnant en moyenne 3 acteurs différents en cybersécurité.

q24. Vers qui vous tournez-vous actuellement pour vous informer ou vous aider sur le sujet de la cybersécurité ?

Base : Total répondants (588)

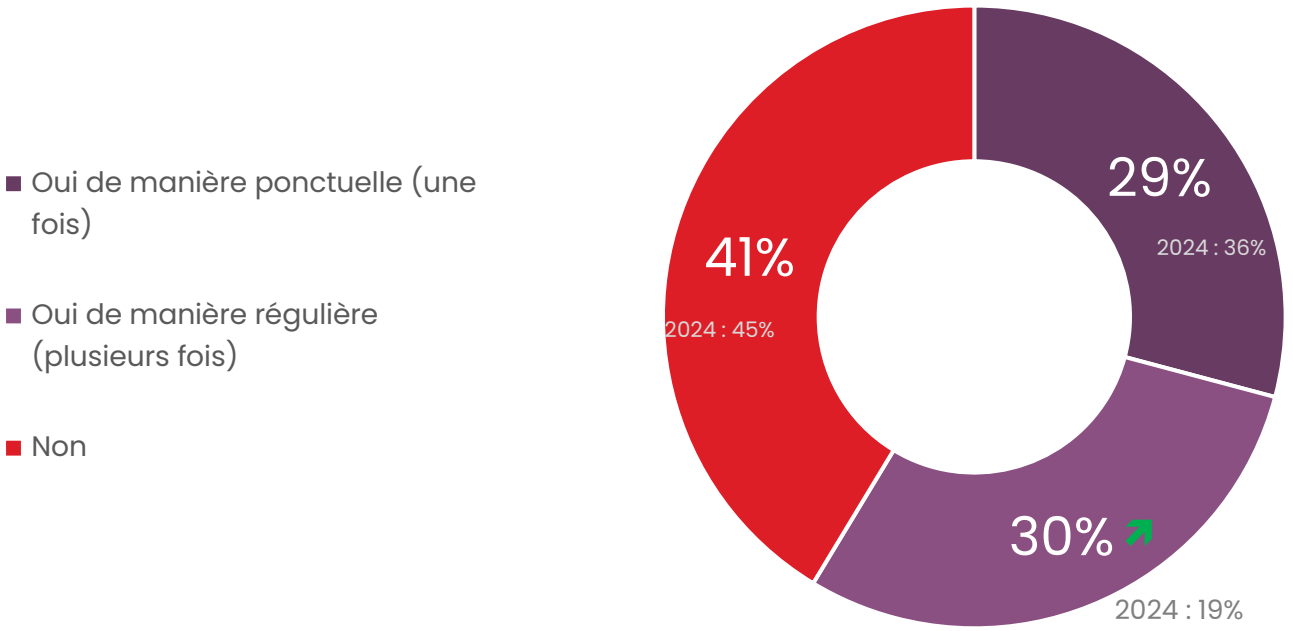
		Tailles des entreprises				Secteur d'activité				
	TOTAL	0 salarié	1 à 9 salariés	Entre 10 et 49 salariés	50 salariés et plus	Agriculture / Industrie / BTP	Commerce / HCR	Services aux entreprises	Administration / Santé / Enseignement	Services aux particuliers
Base (non pondéré)	*588*	*152*	*225*	*103*	*108*	*127*	*68*	*185*	*69*	*139*
Un prestataire informatique	39%	30%	43%	**58%**	**61%**	45%	35%	35%	39%	44%
Cybermalveillance.gouv.fr	31%	30%	30%	33%	**58%**	23%	29%	**42%**	22%	34%
L'ANSSI	19%	20%	16%	**36%**	**69%**	14%	10%	**30%**	15%	26%
Une organisation/fédération professionnelle	17%	15%	19%	12%	9%	23%	17%	12%	15%	15%
Un organisme consulaire régional (Chambre de commerce et d'industrie, chambre de métiers et de l'artisanat…)	9%	6%	10%	5%	3%	10%	13%	5%	7%	7%
Le 17Cyber*	7%	5%	8%	6%	7%	4%	6%	11%	5%	9%
Les services territoriaux de l'état : la gendarmerie /la police/ la préfecture	7%	6%	7%	11%	8%	9%	6%	6%	3%	7%
Un CSIRT territorial	4%	4%	3%	4%	**18%**	2%	4%	6%	3%	3%
Une association d'entreprises	4%	4%	3%	3%	**14%**	3%	0%	4%	9%	5%
Autre	10%	16%	6%	14%	14%	10%	8%	13%	3%	10%
Aucun	25%	25%	27%	**7%**	**3%**	26%	28%	20%	33%	22%
MOYENNE	1,94	1,81	1,98	1,95	**2,68**	1,91	1,78	2,08	1,83	2,05

*Nouvel item ajouté

Et près de 6 entreprises sur 10 déclarent avoir déjà été sensibilisées à la cybersécurité, notamment celles déclarant être préparées en cas d'attaque. 4 sur 10 n'ont ainsi pas bénéficié de sensibilisation au cours des 12 derniers mois.

q21. Avez-vous, dans un cadre professionnel, été sensibilisé(e) à la cybersécurité au cours des 12 derniers mois ?

Base : Total répondants (588)



59% 2024 : 55%

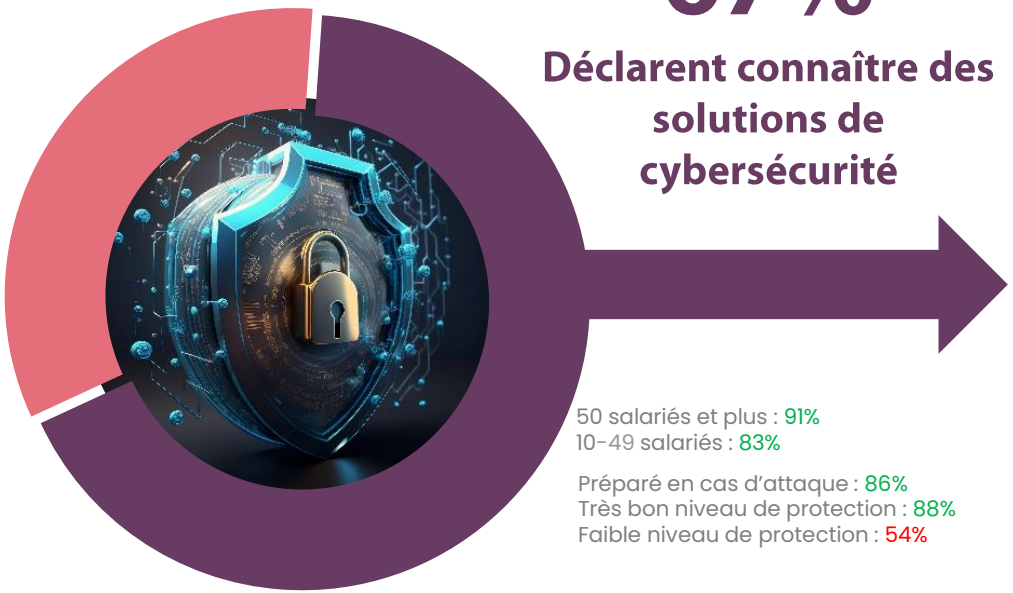
Ont déjà été sensibilisées au moins une fois à la cybersécurité

Connaissent la procédure en cas d'attaque: 89%
Préparé en cas d'attaque : 88%

50 salariés et plus : 94%
10-49 salariés : 86%
Services aux entreprises : 71%

Si 2 tiers des entreprises déclarent connaître les solutions de cybersécurité disponibles sur le marché, près de la moitié les jugent adaptées à leurs besoins.

Q22. Connaissez-vous des solutions de cybersécurité actuellement proposées sur le marché (exemples : firewall, antivirus, EDR-XDR…) ?
Base : Total répondants (588)



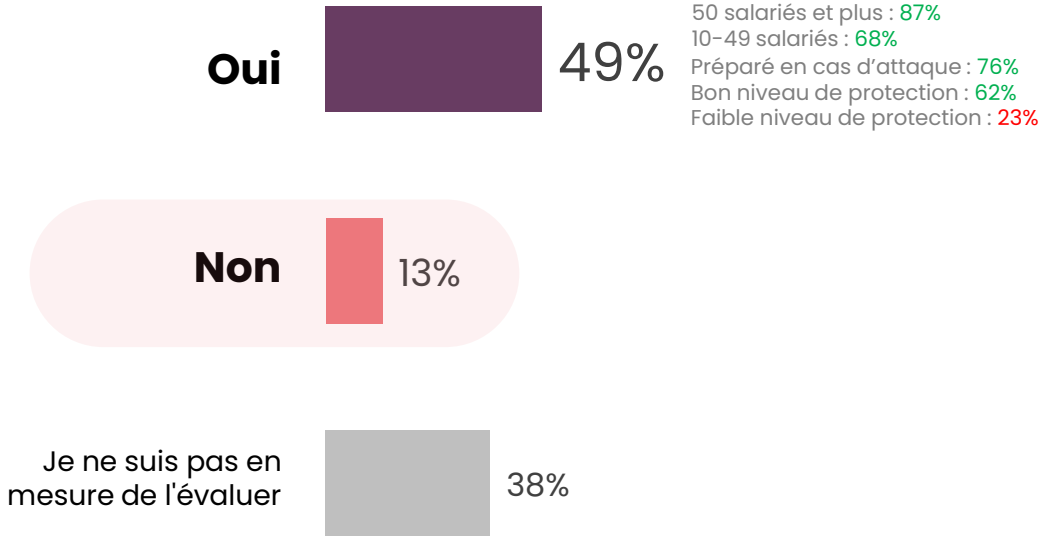
67%

Déclarent connaître des solutions de cybersécurité

50 salariés et plus : 91%
10-49 salariés : 83%

Préparé en cas d'attaque : 86%
Très bon niveau de protection : 88%
Faible niveau de protection : 54%

Q22b. Pensez-vous qu'elles soient adaptées aux besoins de votre entreprise… ? Base : Ont déclaré connaitre des solutions de cybersécurité (394)

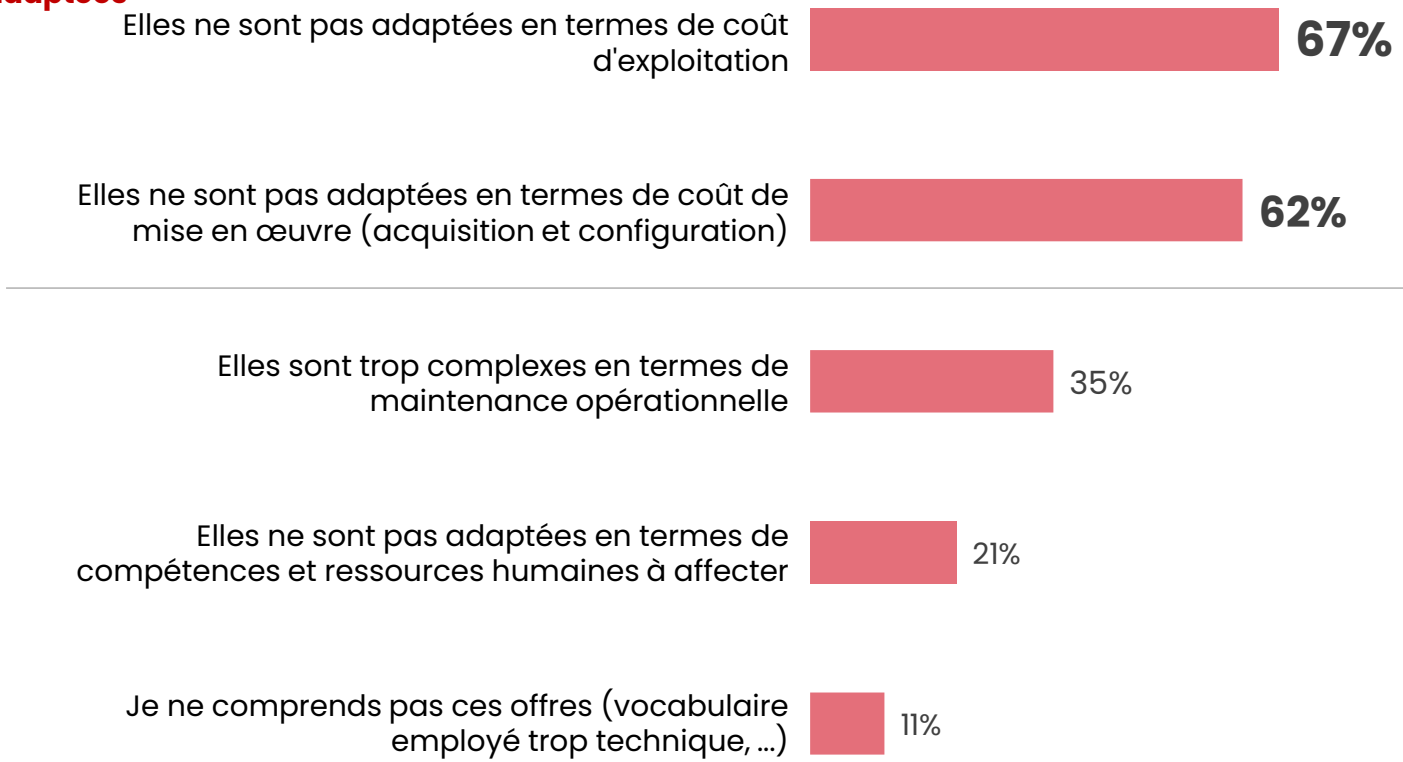


Parmi celles qui les considèrent inadaptées, plus de 6 entreprises sur 10 estiment que ces solutions ne conviennent pas, principalement en raison des coûts d'exploitation et de mise en œuvre. La complexité de maintenance opérationnelle constitue également un frein pour un tiers d'entre elles.

Q22c. Pourquoi indiquez-vous que ces solutions de cybersécurité proposées sur le marché ne sont pas adaptées aux besoins de votre entreprise … ?

Base : Ont déclaré que les solutions de cybersécurité proposées sur le marché ne sont pas adaptées (51)

13%
Pensent que les solutions proposées sur le marché ne sont pas adaptées

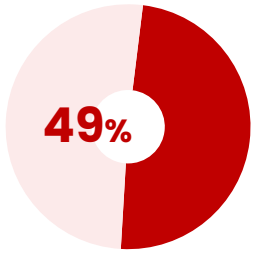


* 1,95 *
réponses en moyenne

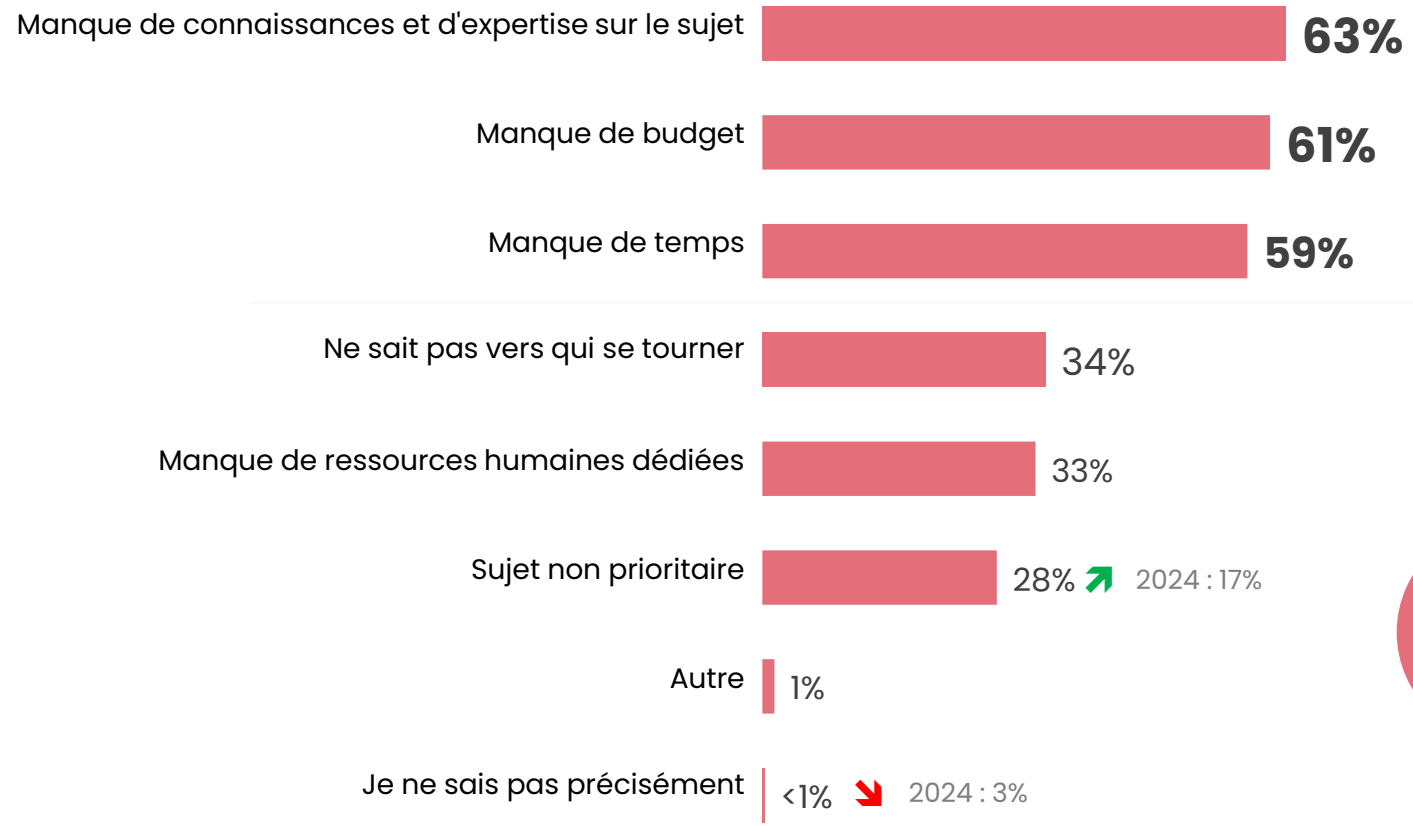
x% / x% : Résultat statistiquement supérieur ou inférieur au total

Les principaux obstacles à un niveau satisfaisant de sécurité informatique sont un manque de connaissances et d'expertise, des contraintes budgétaires, ainsi qu'un manque de temps. À noter que près de 3 entreprises sur 10 considèrent ce sujet comme non prioritaire, un chiffre qui augmente auprès des entreprises répondantes cette année.

q18b. Selon vous, quels sont les freins qui empêchent votre entreprise d'atteindre le bon niveau de sécurité informatique ?
Base : Ont déclaré que leur entreprise n'était pas préparée en cas d'attaque (289) - Plusieurs réponses possibles



Déclarent que leur entreprise n'est pas suffisamment préparée en cas d'attaque informatique
(rappel)



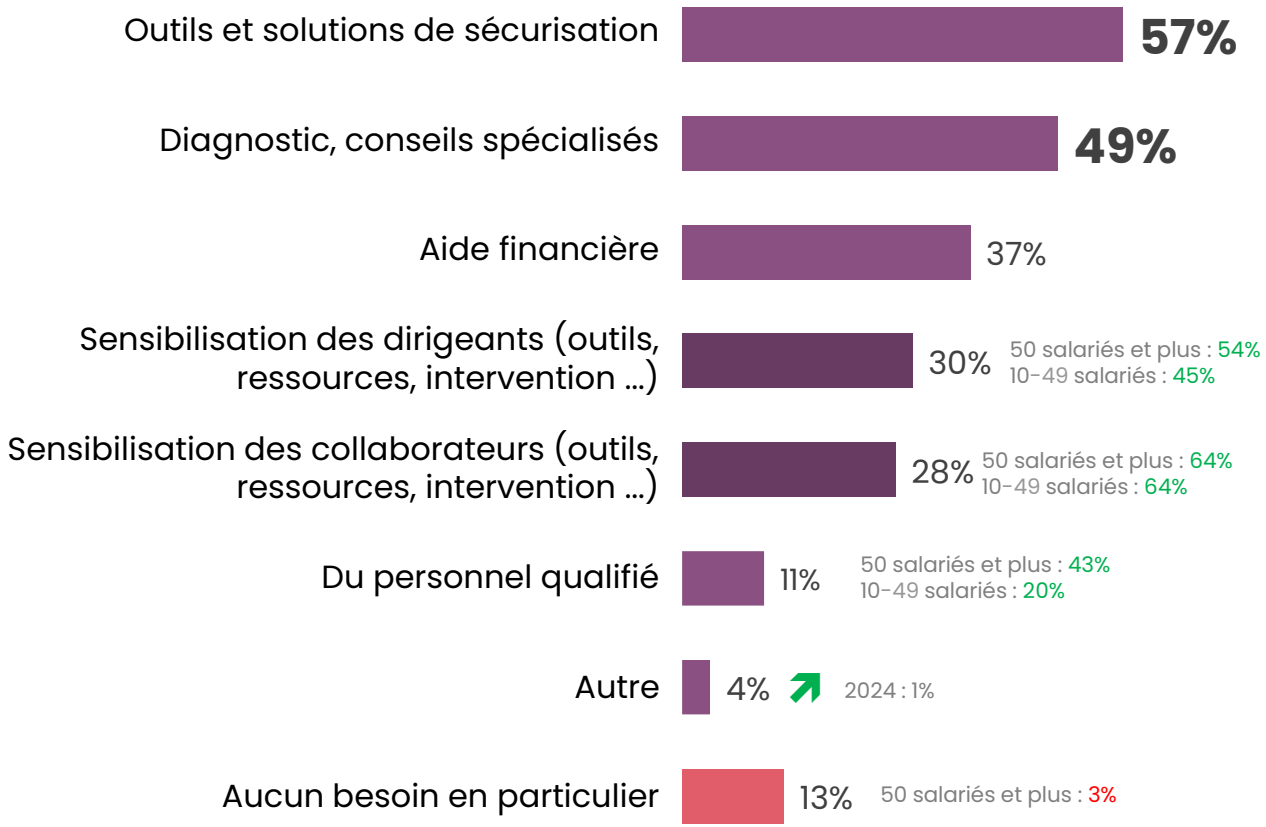
100% ↗
Au moins un frein cité
2024 : 97%

* 2,81 *
réponses en moyenne

↗ ↘ : Résultat statistiquement supérieurs ou inférieurs à la vague 2024 x% / x% : Résultat statistiquement supérieur ou inférieur au total

En matière de cybersécurité, les principaux besoins sont les outils de sécurisation et les conseils spécialisés. Si 57 % et 49 % mettent respectivement en avant ces éléments, 4 sur 10 soulignent l'importance de sensibiliser les dirigeants ou les collaborateurs. L'aide financière demeure également un levier important, sollicitée par plus d'un tiers des entreprises.

q23. Quels sont vos besoins prioritaires en matière de sécurité informatique ?
Base : Total répondants (588)



87%
Au moins un besoin

50 salariés et plus : 97%
Non préparé en cas d'attaque : 93%
Faible niveau de protection : 96%
Très bon niveau de protection : 74%

40%
Sensibilisation des dirigeants ou collaborateurs

50 salariés et plus : 73%
10-49 salariés : 72%

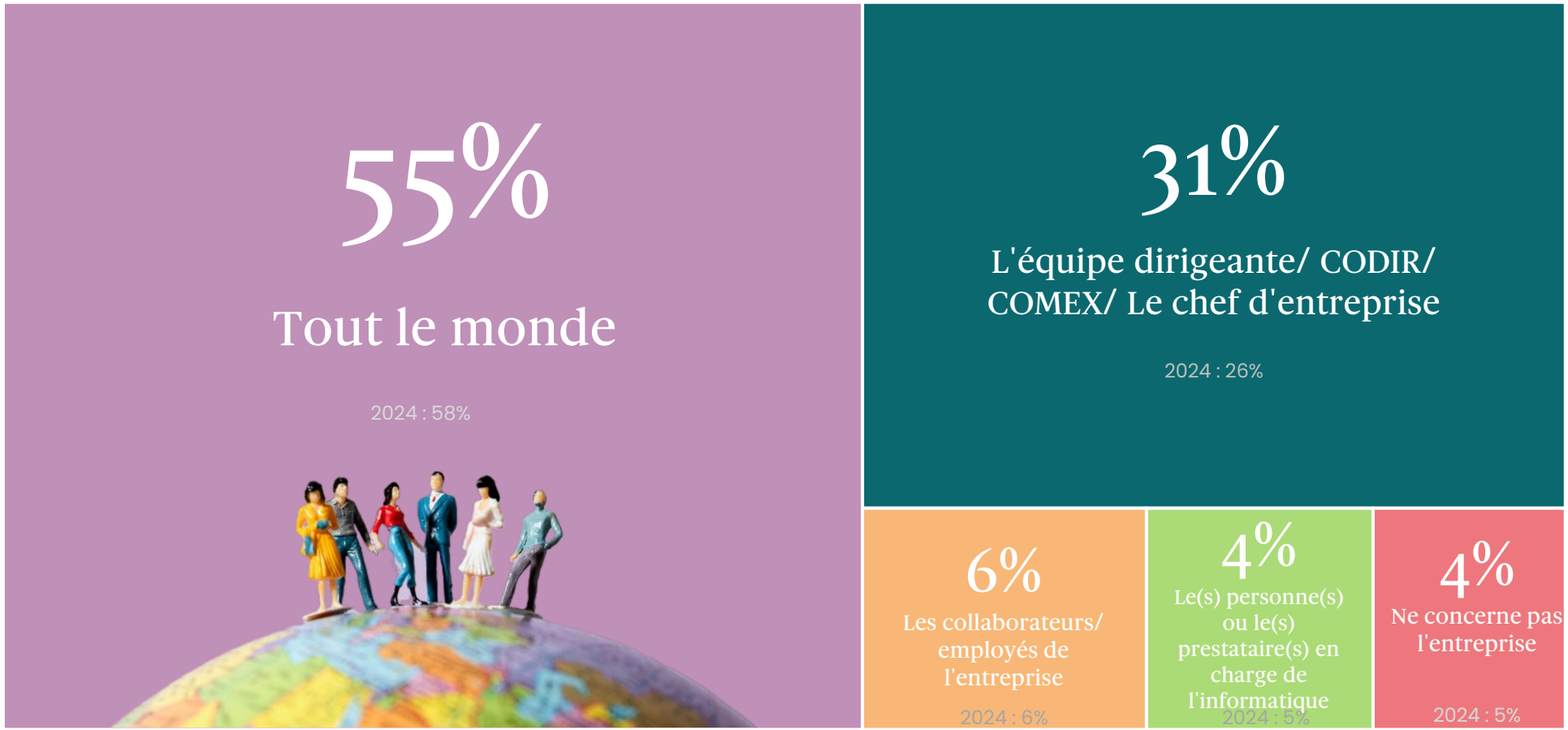
*** 2,48 ***
réponses en moyenne

50 salariés et plus : 3,12
10-49 salariés : 2,85

Finalement, si la majorité des Français estiment que la sécurité informatique concerne tout le monde, près d'un tiers estime que celle-ci implique en priorité les équipes dirigeantes.

q11. Selon vous, la sécurité informatique de l'entreprise doit impliquer en priorité…

Base : Total répondants (588)



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 25 Corporate

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

Maéva Nestor
Cheffe de projet
mnestor@opinion-way.com

Larissa Xia
Analyste
lxia@opinion-way.com

Ad'Vanced opinionway Enable *today*, shape *tomorrow*
#quant #analytics #multi-sector