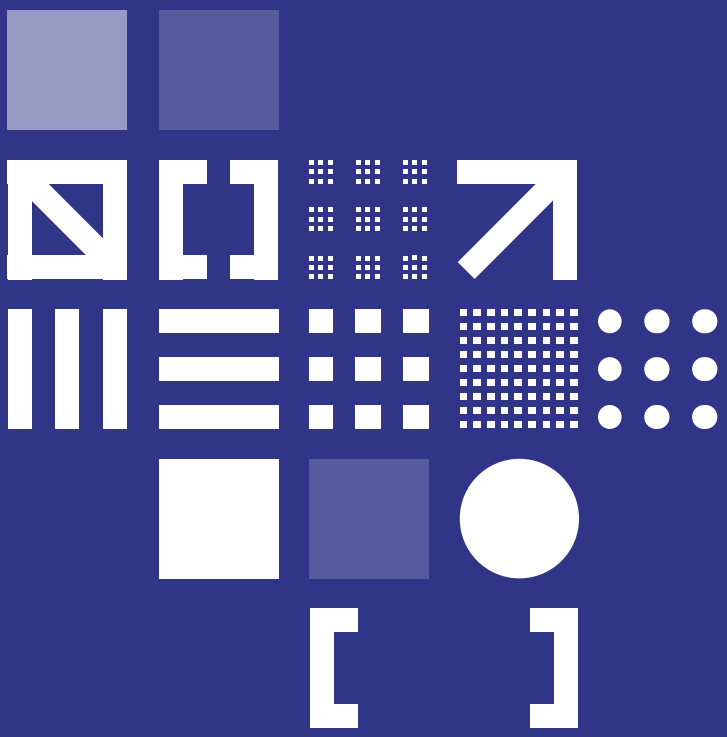


DOCAPOSTE

CYBLEX Consulting

# Baromètre de la cybersécurité 2023

Quelle maturité pour
les entreprises françaises ?

iteractii

# L’édito

**Olivier Vallet**
*Président Directeur Général*

DOCAPOSTE

**La montée en puissance de la cybercriminalité constitue aujourd'hui un défi pressant pour tous les acteurs, qu'ils soient publics ou privés, notamment les petites et moyennes entreprises et collectivités. La réalité de cette menace est désormais incontestable, amplifiée par une médiatisation fréquente des attaques. Les grandes entités ont réagi en conséquence au cours de la dernière décennie, investissant massivement dans leur sécurité, recrutant des experts et intégrant des technologies de pointe pour anticiper et contrer les cyberattaques.**

Cependant, pour les acteurs de moindre envergure, dépourvus des ressources financières et de l'expertise nécessaires, la question de la cybersécurité s'avère plus ardue. Malgré cela, des démarches accessibles et cruciales peuvent être entreprises. Tout d'abord, aborder les questions de cybersécurité au niveau de la gouvernance représente une étape fondamentale. Sensibiliser les collaborateurs aux bonnes pratiques de sécurité numérique constitue également une défense efficace, rendant les attaques plus complexes, même si elles ne les éliminent pas totalement. Souvent, cela suffit à détourner les menaces vers d'autres cibles.

Au-delà de la dimension humaine de la sécurité numérique, il est impératif de développer des solutions efficaces, faciles à acquérir et à utiliser, tout en restant financièrement abordables. Cet enjeu majeur vise à permettre à tous les acteurs, quelle que soit leur taille, d'élever leur niveau de protection cyber face à une menace qui ne montre aucun signe de faiblesse pour les années à venir.

Ce baromètre, co-réalisé par Cyblex Consulting et Docaposte nous montre que si les PME et les petites institutions sont aujourd’hui conscientes du risque cyber, l’écart reste encore important pour certaines d’entre les dispositifs mis en place et l’atteinte d’un niveau minimum de protection. Ses enseignements sont riches et méritent d’être partagés pour permettre le développement d'une défense plus efficace des petites organisations face à l'évolution incessante de la cybercriminalité.

**Christophe Vendran**
*Directeur Général*

CYBLEX Consulting

**Nous sommes dans un monde où le développement numérique a indéniablement révolutionné notre quotidien, façonnant notre manière de travailler, de communiquer et même de penser. Cependant, derrière cette avancée fulgurante se profile l'ombre grandissante de la cybermenace. Si l'intelligence artificielle constitue désormais un accélérateur de cette profonde transformation des environnements professionnels, son expansion suscite également des préoccupations grandissantes liées aux cyber risques.**

Ainsi, dans cet univers où le digital est ubiquitaire, la cybersécurité devient un enjeu crucial pour les entreprises et les organismes publics mais aussi de souveraineté nationale. La réalisation d'un baromètre dédié à l'observation de la maturité cyber se révèle être une boussole indispensable pour évaluer année après année l’état de l’évolution du risque cyber et de sa prise en compte dans les organisations indépendamment de leur taille et de leur secteur d’activité.

Ce baromètre, fruit d'une collaboration étroite entre les experts de Cyblex Consulting et de Docaposte a comme premier objectif de contribuer à une meilleure connaissance partagée de la compréhension des enjeux de la cybersécurité par les entreprises, de leur niveau de résilience numérique et de leur niveau actuel de maturité cyber. En partageant ce baromètre avec le plus grand nombre, Docaposte et Cyblex Consulting démontrent leur volonté de participer à une communauté informée et proactive face aux défis croissants de la cybercriminalité.

# Un baromètre national pour mesurer l'évolution de la maturité cyber des entreprises et organisations publiques

Ce baromètre permet d'avoir, année après année, une meilleure perception de la **compréhension par les décideurs des risques liés aux Cyber-menaces, des solutions qu'ils utilisent,** qu'ils **envisagent de déployer** ou qu'ils **aimeraient pouvoir déployer, des mesures mises en œuvre** dans leurs entreprises pour adresser ces Cyber-risques.

Sur la base des éléments recueillis et **en regard des recommandations de l'ANSSI** quant aux mesures à mettre en place, le baromètre vise à élaborer une **grille de Cyber-maturité des dirigeants et décideurs** français et d'en suivre son évolution dans la durée.

**Sur la base d'un entretien téléphonique articulé autour d'une vingtaine de questions, trois thématiques sont abordées dans l'objectif d'appréhender la Cyber-maturité du décideur interrogé.**

La connaissance des mesures mises en œuvre

La perception du décideur de l'efficacité et de la pertinence des mesures mise en œuvre

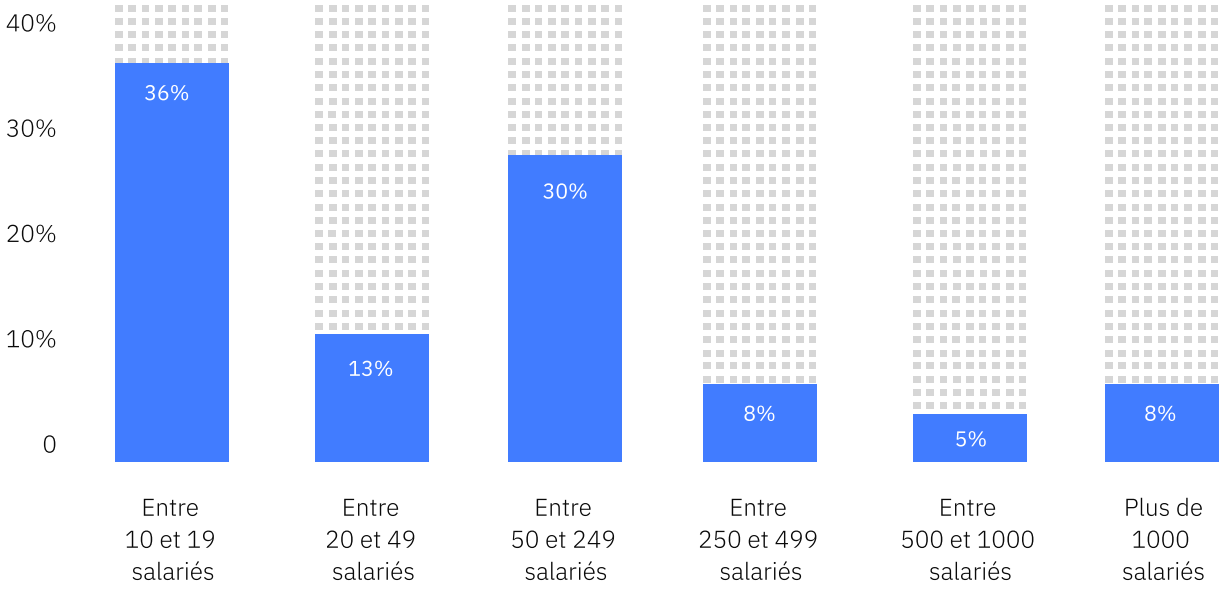
La perception du niveau de risque

# L’échantillon de notre enquête

## Le périmètre de l’enquête

Un échantillon au plus près de la **répartition des entreprises françaises dans le tissu économique et représentatif pour chaque segment.**

Une enquête orientée **décideurs : 3 répondants sur 4 ne sont pas spécialisés** dans les domaines de l’IT ou de la cybersécurité.

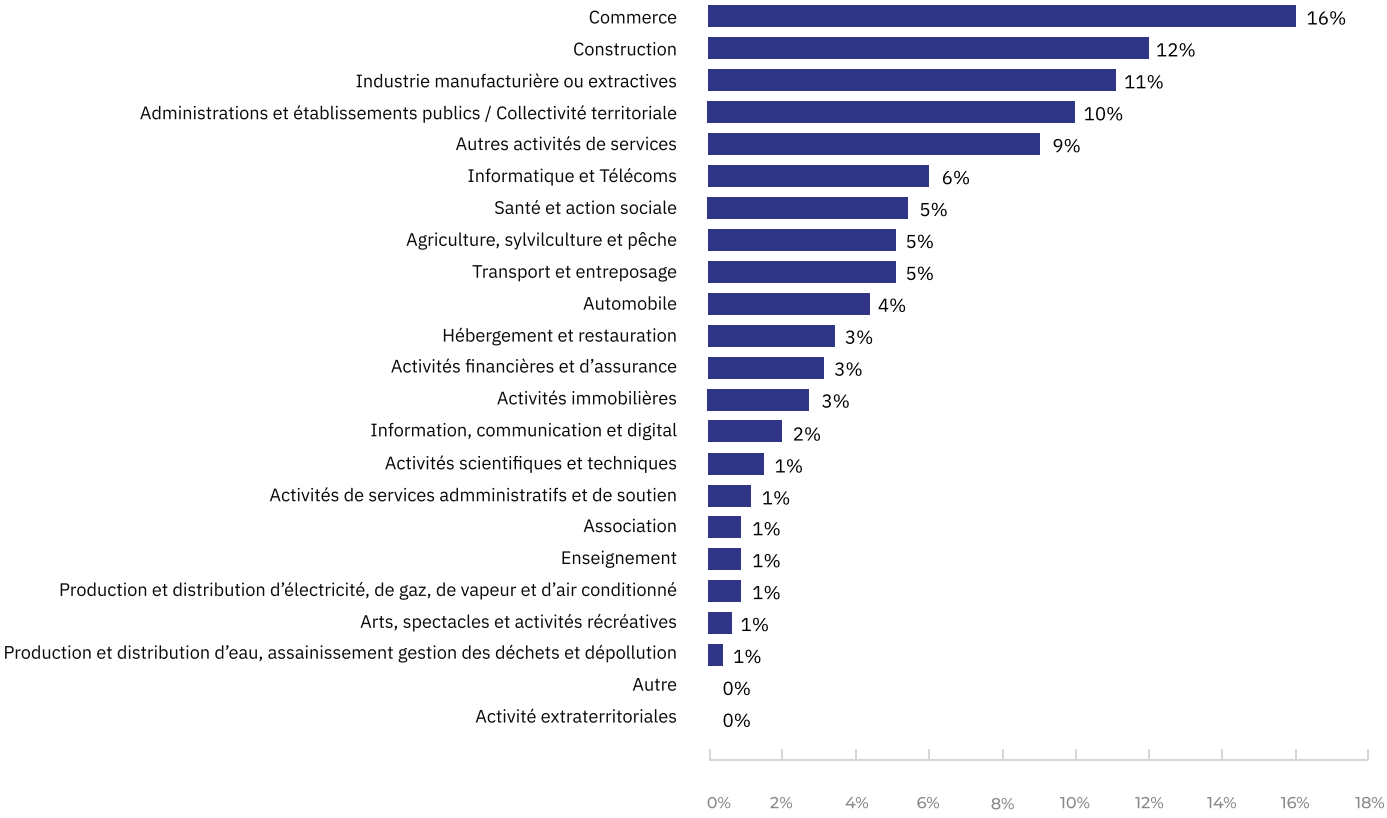



**TPE**
36%

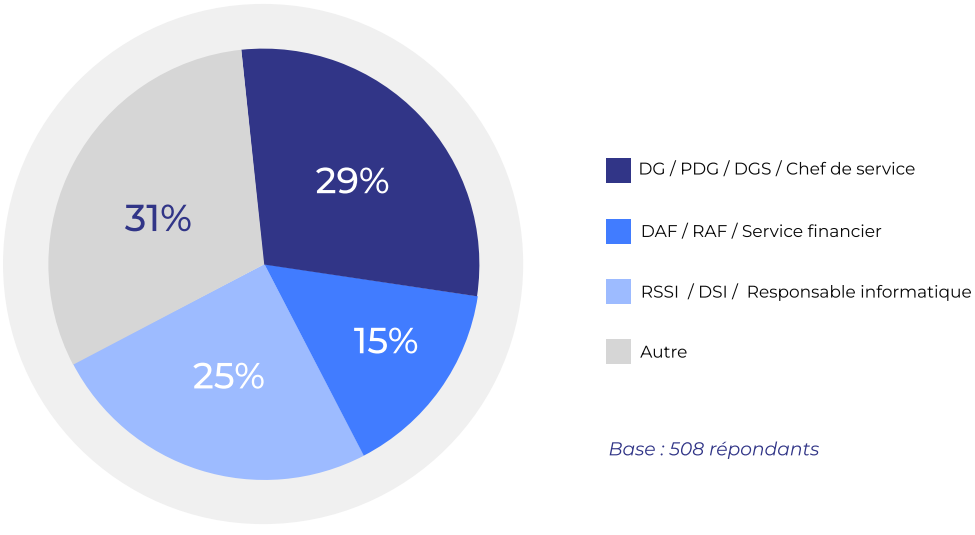
**PME**
43%

**ETI et grands groupes**
21%

# Le profil des répondants




*Base : 508 répondants*




*Base : 508 répondants*

**Les 3/4 des répondants ne sont pas spécialisés dans l'IT ou la cybersécurité**

Au-delà de la finance, il y a les fonctions administratives, commerciales, techniques et RH (dans 'Autres')

La population des DSI/RSSI est tout de même suffisamment importante pour identifier si des différences notables existent avec les autres fonctions.

# Executive summary - Quelques chiffres clés

## Baromètre de la cybersécurité 2023

Quelle maturité pour les entreprises françaises ?

DOCAPOSTE CYBLEX Consulting intuiti

## I

**Cyberattaques** : des disparités selon la taille des entreprises, des impacts hétérogènes

**1/5** des entreprises **ont déjà subi une cyberattaque**

## II

Une **évaluation de la menace et de l'exposition au risque** Cyber qui varie selon la typologie de l'entreprise

**31%** **se considèrent comme des cibles potentielles**

## III

Des **efforts en hausse pour réduire les risques**, des disparités budgétaires en fonction de la taille

**64%** des entreprises **pensent faire suffisamment d'efforts**

## IV

Des **craintes ainsi que des démarches mises en œuvre** qui varient en fonction de la taille

Pour **62%** de l'échantillon, la **perte de données est la première crainte cyber**

## V

Des **actions concrètes mises en œuvre**, ayant permis selon une majorité des répondants de **diminuer le risque d'une attaque**

**+1/3** des entreprises **n'ont pas confiance dans les actions mises en place**

## VI

Un nombre important d'entreprises qui semblent ne pas porter d'intérêt majeur aux **questions de Souveraineté**

**1/3** seulement des répondants **estiment ce sujet important**

## VII

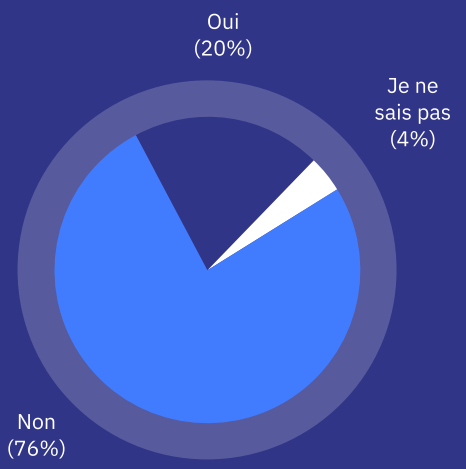
Au global, **une maturité plutôt moyenne** au regard des **préconisations de l'ANSSI mais un fort potentiel d'évolution**

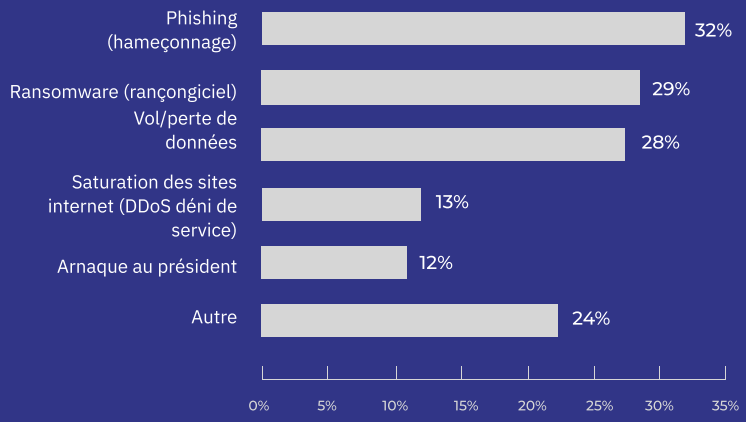
**66%** des entreprises n'appliquent pas les pratiques permettant d'atteindre le niveau essentiel

Près de **2/3** pourraient basculer au niveau supérieur

# Cyberattaques : des disparités selon la taille des entreprises, des impacts hétérogènes

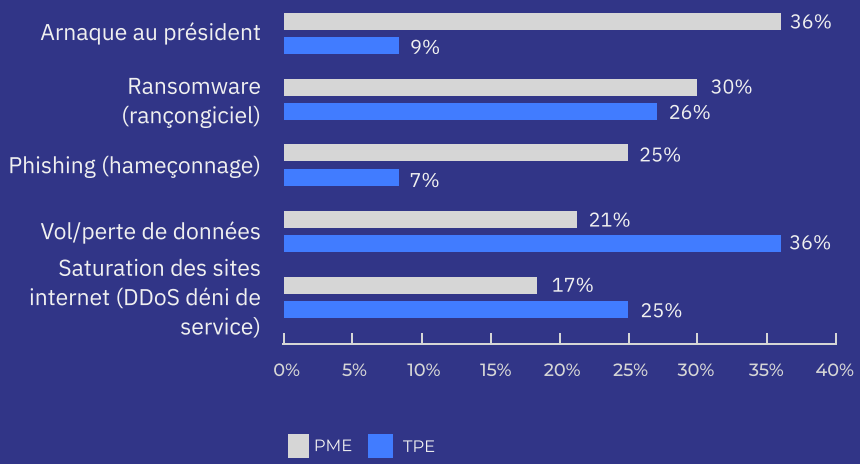
## → **1 entreprise sur 5** a déjà subi une cyberattaque




Phishing, Ransomware et Vol de données constituent l'essentiel des attaques subies par les entreprises.

## Une typologie d'attaque qui varie en fonction de la taille de l'entreprise




**La typologie des attaques est quasi inversée entre les TPE et les PME**

Elles sont tout de même attaquées de manière identique sur le rançongiciel

## Des disparités de taille mais également sectorielles

- Les entreprises ayant été plus souvent cyber-attaquées que les autres sont davantage les petites ETI (+22 pts) et les grands comptes (+29 pts)
- Les entreprises de plus de 500 salariés subissent deux fois plus de phishing et 4 fois plus de déni de services
- L'arnaque au président est deux fois plus vécue par les entreprises entre 250 et 499 salariés

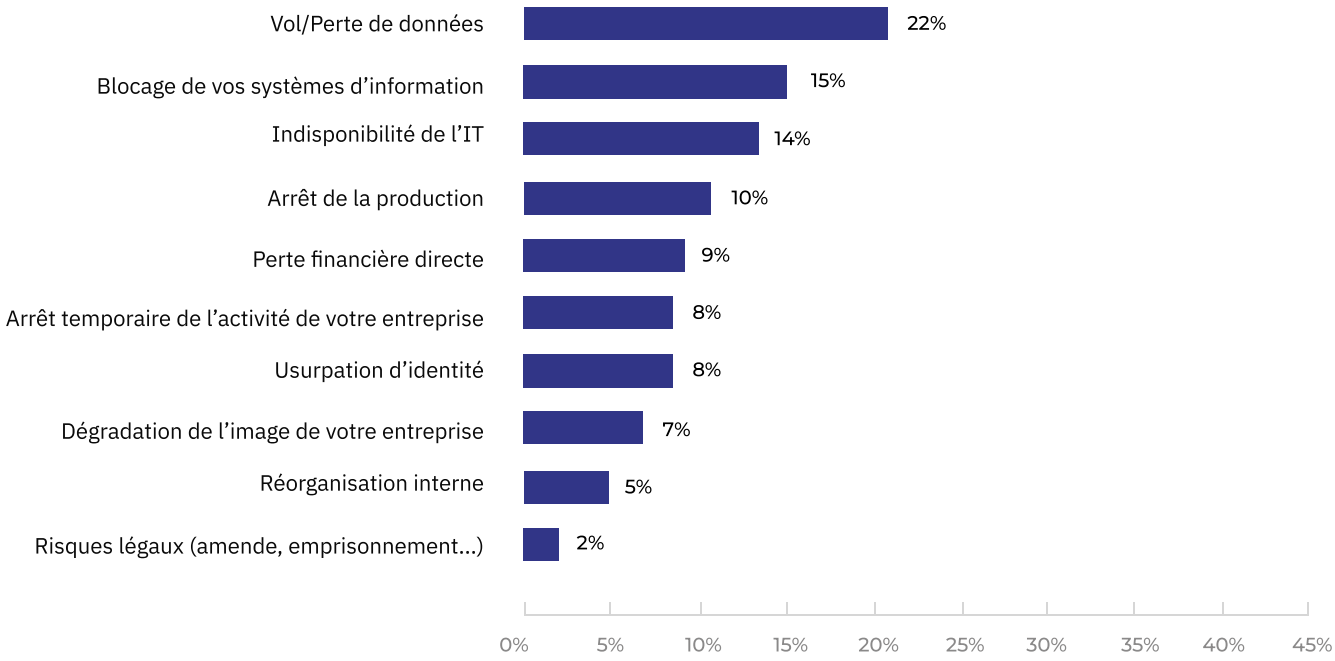
Les **3 secteurs** ayant le plus subi (au moins + de 30 pts au-dessus)

1 **Production et distribution d'eau, assainissement, gestion des déchets**

2 **Informations, communication et digital**

3 **Activités de services administratifs et de soutien**

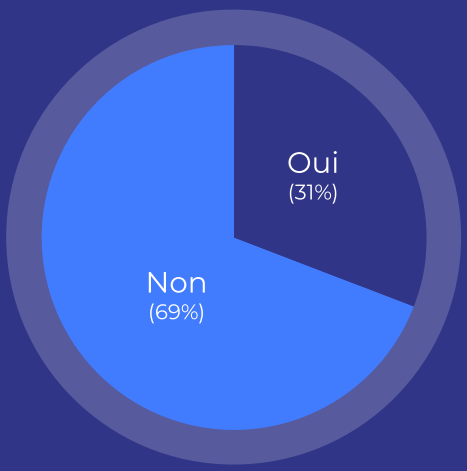
## Des impacts hétérogènes, le vol et de la perte de données en tête




*Base : 101 répondants*

# Une évaluation de la menace et de l'exposition au risque Cyber qui varie selon la taille de l'entreprise, son secteur d'activité et la fonction du répondant

**31% se considèrent comme des cibles potentielles**
avec un score plus élevé pour les répondants issus des fonctions IT



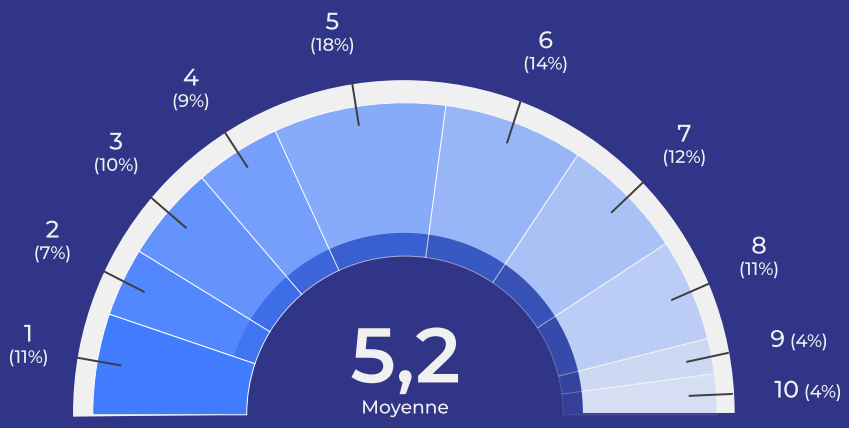

*Base : 508 répondants*

Sans surprise, **ceux qui ont répondu 'oui' sont à 44% des spécialistes IT**

Les 'non' sont surtout représentés par les autres fonctions (administratif, RH, commercial - à 36%) et la direction générale à 31%

**Les fonctions non IT se sentent deux fois moins une cible potentielle que les spécialistes IT**

## 19% pensent être très exposées

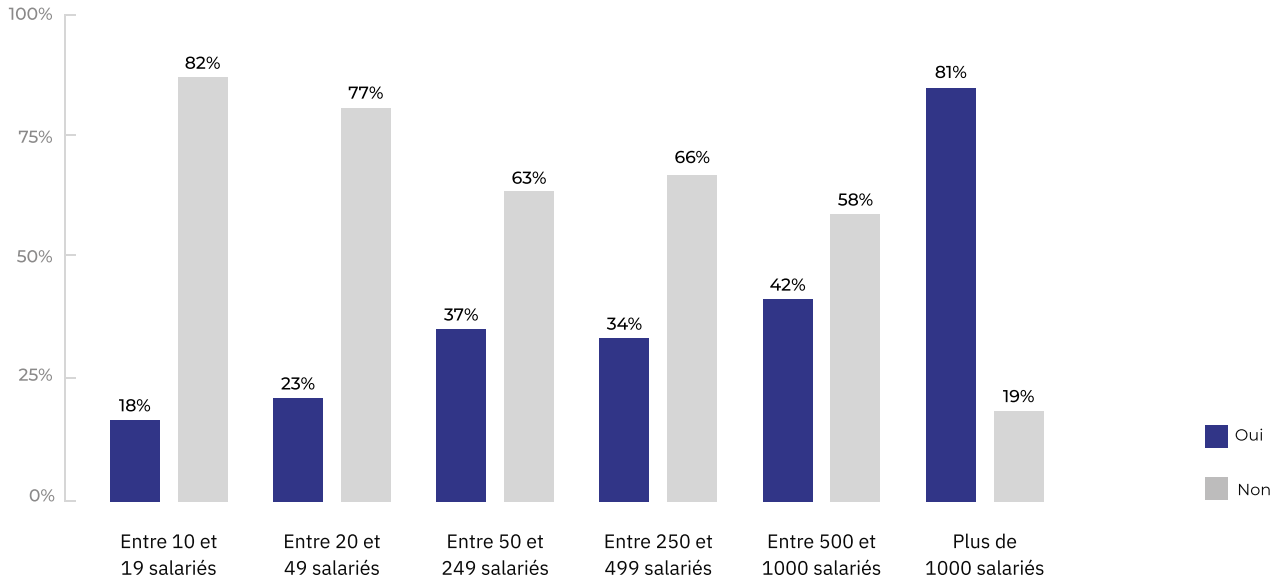



*L'exposition : 1 - peu exposée / 10 - très exposée*

**Moins d'un quart (19%) des entreprises pensent être très exposées au risque de cyberattaque** (notes de 8 à 10).

Elles sont plus nombreuses (28%) à penser qu'elles sont très peu exposées

## Plus l'entreprise est petite, moins elle se sent menacée




Des écarts assez importants : les TPE sont à 13 pts derrière alors que les + 1000 salariés sont quasiment 3 fois plus inquiètes que la moyenne

*Base : 508 répondants*

## Avec des disparités sectorielles nettes

Les secteurs qui se sentent les **plus exposés**

**60%** — **Secteur financier**

**60%** — **Secteur informatique et digital**

**42%** — **Secteur industriel**

**40%** — **Établissements publics**

Les secteurs qui se sentent les **moins exposés**

**12%** — **Hébergement/ Restauration**

**16%** — **Commerce**

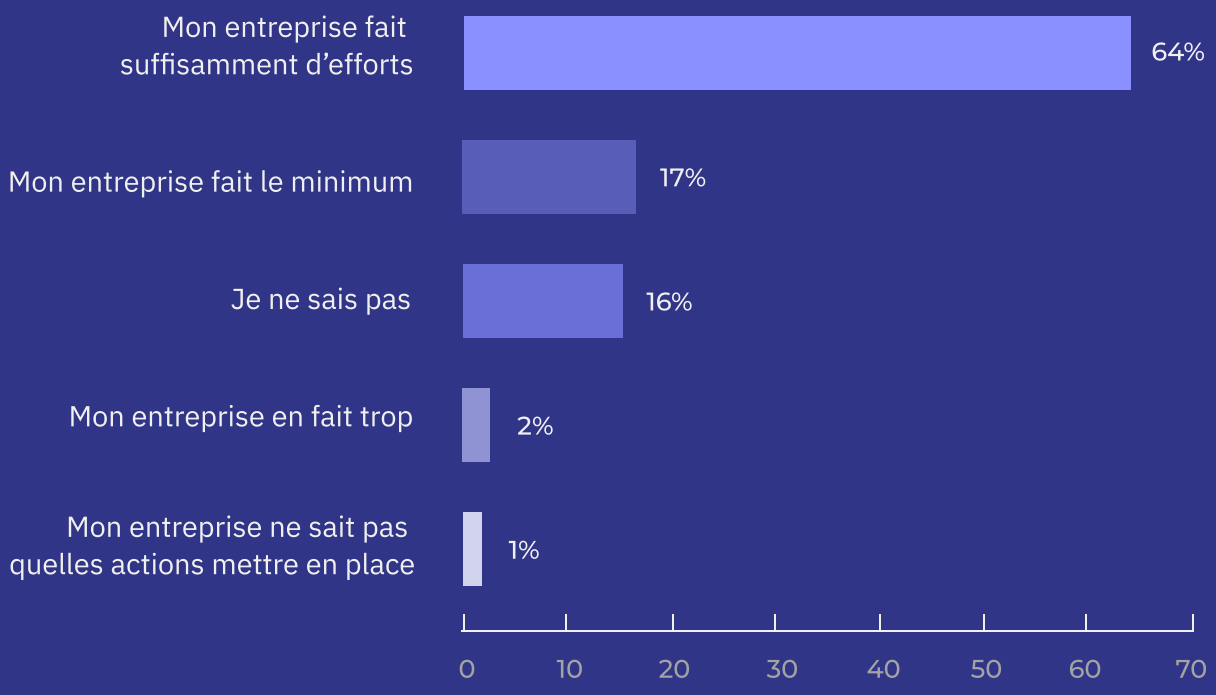
**18%** — **Secteur agricole**

**19%** — **Construction/ Automobile**

Moyenne : **31%**

# Des efforts en hausse pour réduire les risques, des disparités budgétaires en fonction de la taille de l'entreprise

## 64% des entreprises pensent faire suffisamment d'efforts



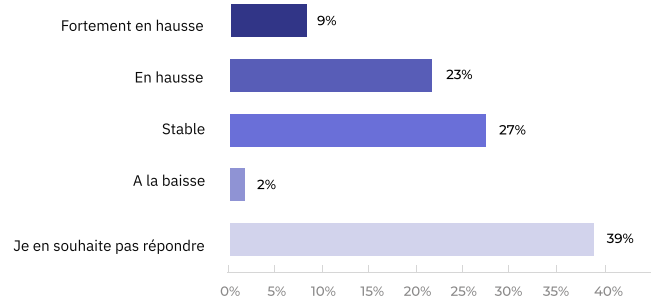

*Base : 508 répondants*

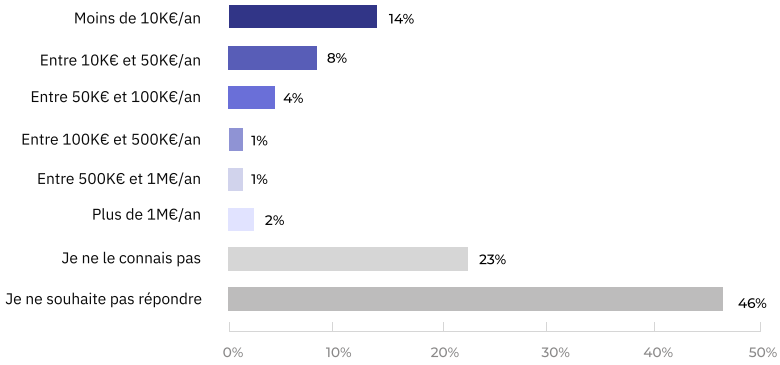
**La taille de l'entreprise impacte cette perception :**

- les entreprises de plus de 1000 salariés pensent à 81% en faire suffisamment
- contre 49% pour celles de moins de 50 salariés

# Un tiers des entreprises affirment notamment que leur budget est en hausse

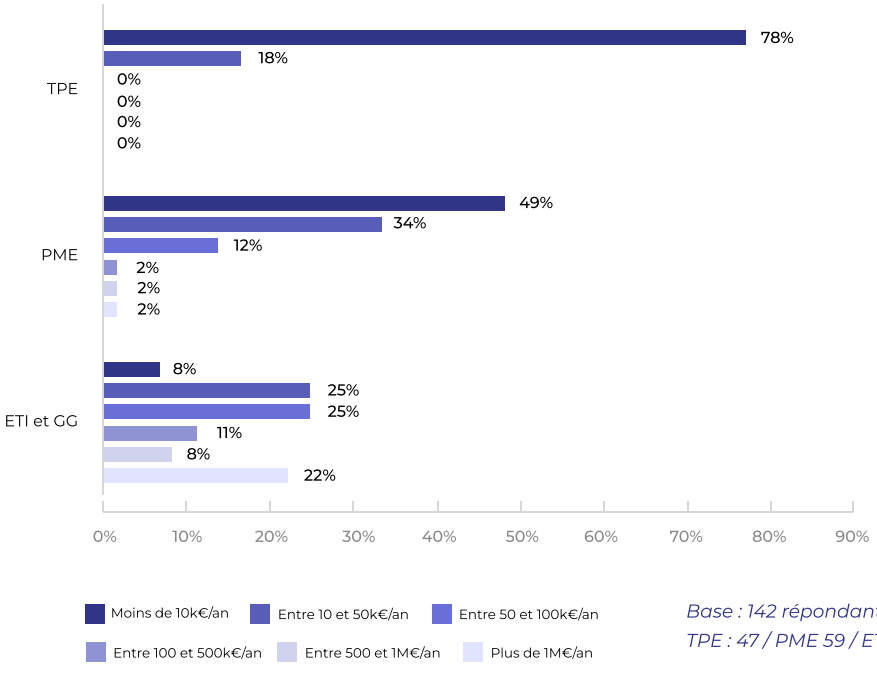
- **Parmi les entreprises qui affirment avoir un budget cybersécurité en forte hausse, la plus grosse part (15%) a un budget de plus de 1M d'euros/an**
- Celles qui affirment avoir un budget cybersécurité en hausse, disposent d'un montant entre 10 et 100K/an
- Concernant la connaissance du budget : on constate 5 pts d'écart avec la fonction DSI ou le service financier.
  *Note : près de la moitié des professionnels n'a pas souhaité répondre*




*Base : 508 répondants*

# Les plus petites entreprises accordent majoritairement moins de 10K€ par an au budget de cybersécurité



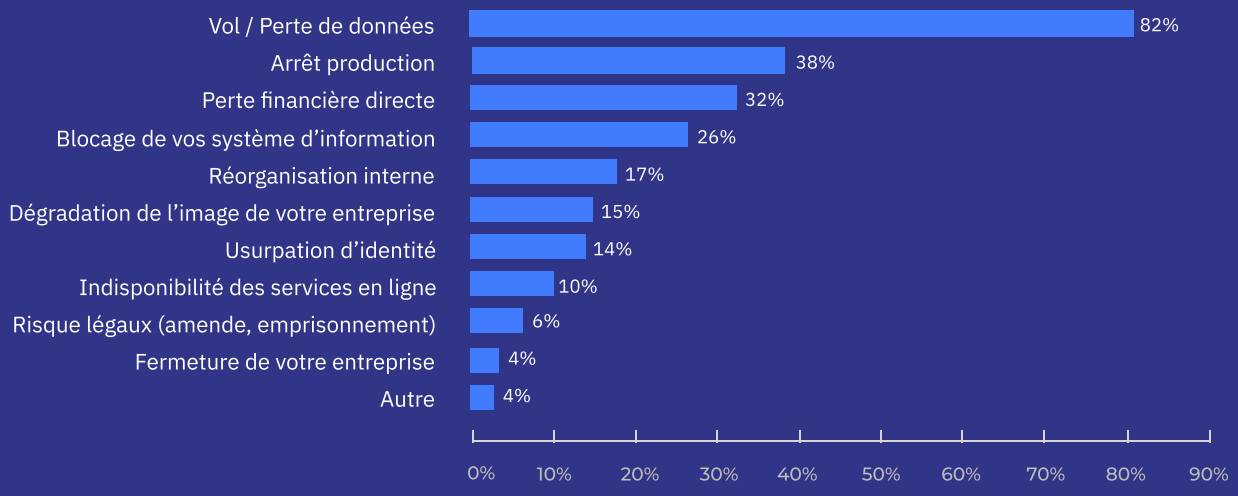

*Base : 142 répondants*
*TPE : 47 / PME 59 / ETI et GG : 36*

On constate même que **78% des TPE ont un budget de moins de 10K€ par an et jamais plus de 50K€**

Concernant les PME entre 20 et 49 salariés, elles sont même 82% à disposer d'un budget de moins de 10K€ par an

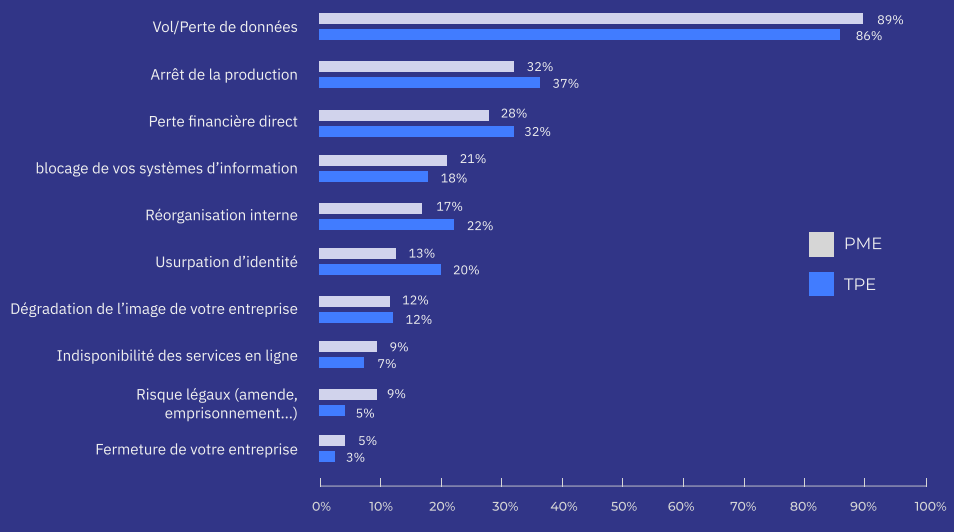
# Des craintes ainsi que des démarches mises en œuvre qui varient en fonction de la taille de l'entreprise

## De manière spontanée, la perte de données est la première crainte




*Base : 508 répondants*

## Le top 3 des craintes des TPE-PME converge avec l'ensemble des entreprises

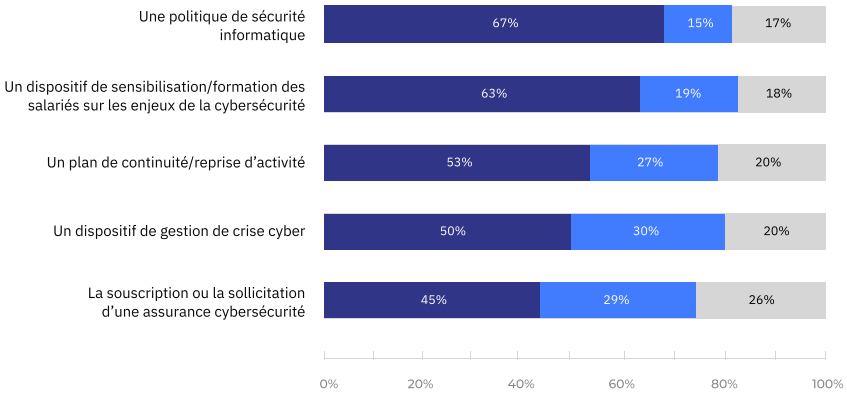



*Base : 384 répondants*

On constate que le top 3 des craintes pour les TPE-PME est identique à l'ensemble des entreprises interviewées.

*A noter que le vol de données est une crainte encore plus forte chez les PME : +7 pts par rapport à la moyenne.*

# Différentes typologies de démarches sont mises en place pour réduire les risques cyber




*Base : 508 répondants*

**Les entreprises qui pensent faire suffisamment d'efforts semblent effectivement en faire davantage que les autres, sur toutes les démarches :**

- Politique de sécurité : +16 pts
- Sensibilisation/formation : +16 pts
- PCA/PRA : +15 pts
- Gestion de crise : +16 pts
- Assurance : +11 pts

# Le top 3 des démarches mises en place

## PME et TPE ont en commun la mise en oeuvre

**↘ 01**

D'une politique de sécurité informatique

**↘ 02**

D'un dispositif de sensibilisation/formation des salariés

## Et divergent sur la troisième mesure

**↘ 03**

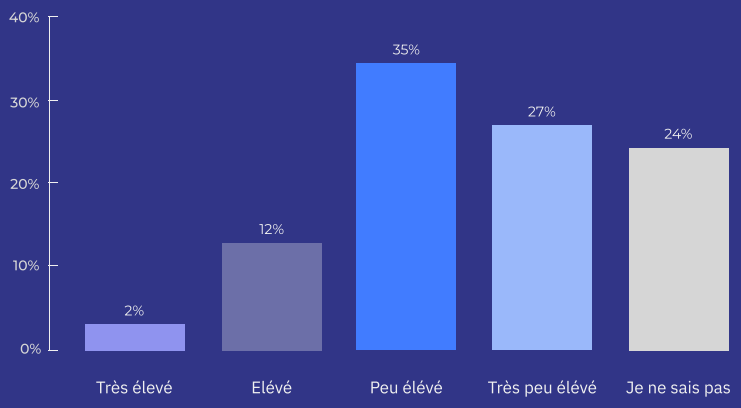
Un dispositif de gestion de crise cyber (+15pt par rapport à l'ensemble des répondants )

**↘ 03**

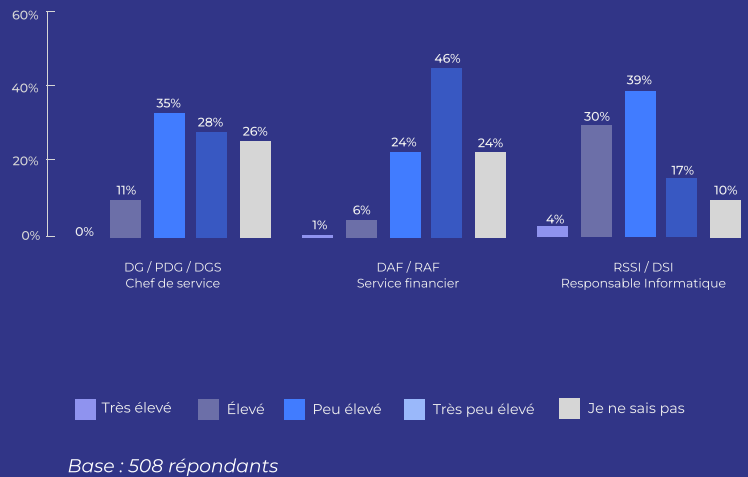
Un plan de continuité/ reprise d'activité

# Des actions concrètes mises en œuvre, ayant permis selon une majorité des répondants de diminuer le risque d'une attaque

## Néanmoins, plus d'un tiers des entreprises n'ont pas confiance dans les actions mises en place




**Un quart des entreprises interviewées ne savent pas si leurs mesures seront efficaces et 14% estiment toujours que le risque est élevé ou très élevé**

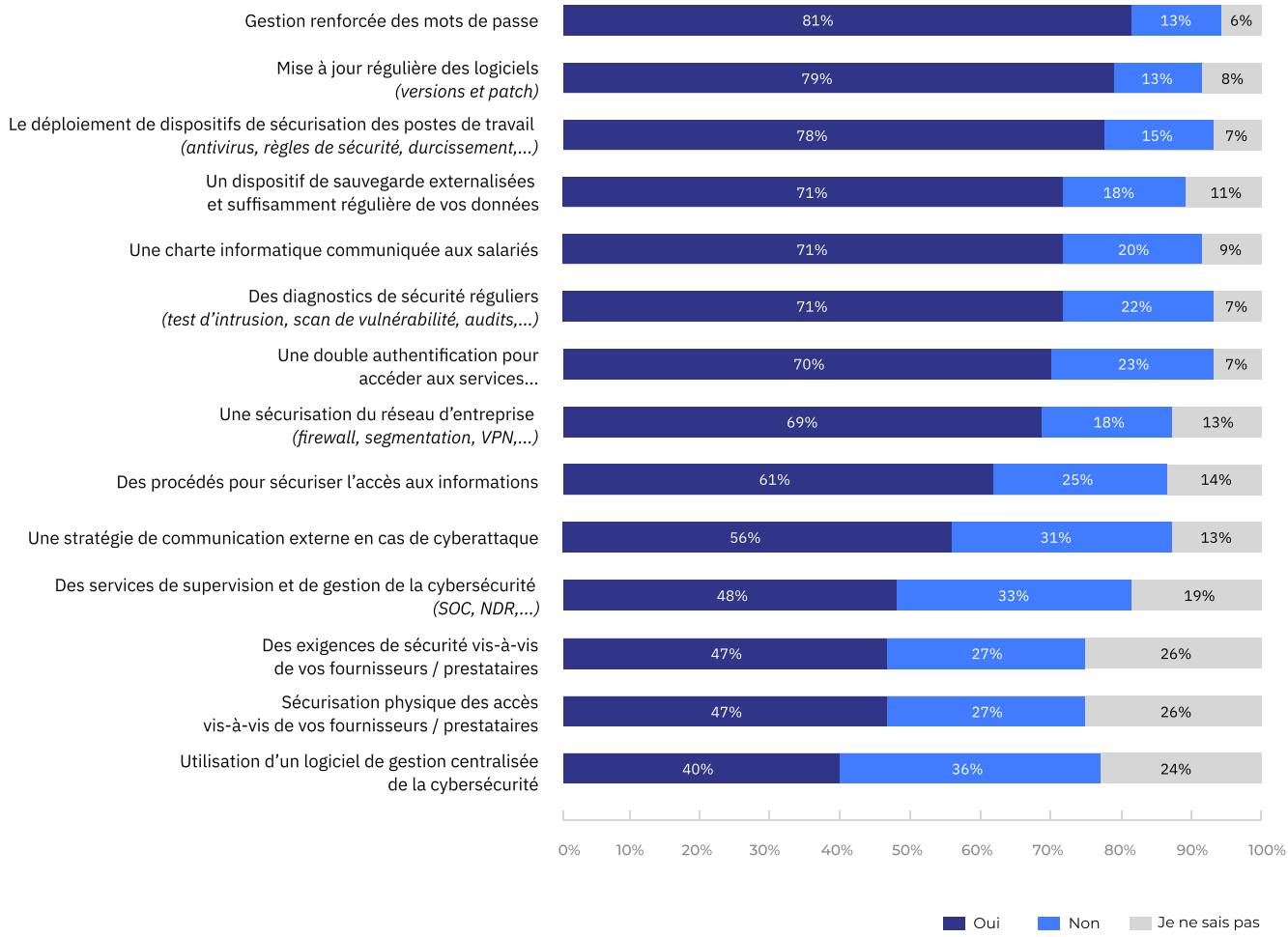



**Les fonctions IT restent trois fois plus sceptiques que la moyenne sur l'efficacité des actions mises en place**

Si les fonctions financières sont les plus confiantes on constate que les dirigeants sont dans la moyenne avec un tiers qui n'est pas sûr de l'efficacité des actions

*Base : 508 répondants*

# Des actions et solutions concrètes ont été mises en place, des PME plus volontaires




**Les entreprises qui pensaient faire suffisamment d'efforts ont aussi davantage mis en place des actions que les autres, à tous les niveaux :** entre 8 et 13 points de plus

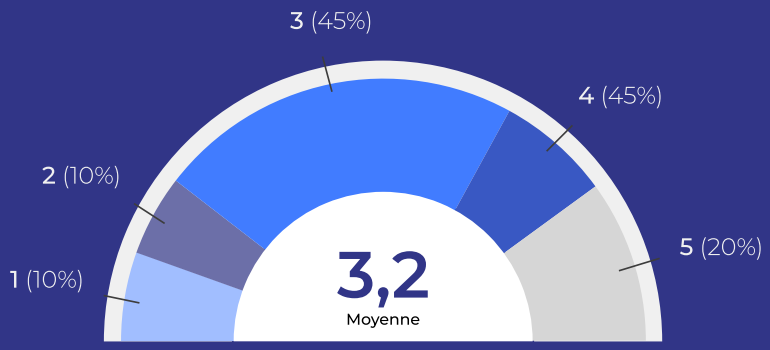
**Par ailleurs, la taille d'entreprise est aussi un facteur majeur :**

- Les TPE ont moins agi (entre -12 et -20 pts par rapport à la moyenne).
- Alors que les PME (50 à 249 sal.) font davantage d'efforts que la moyenne : +6 à +12 pts de plus

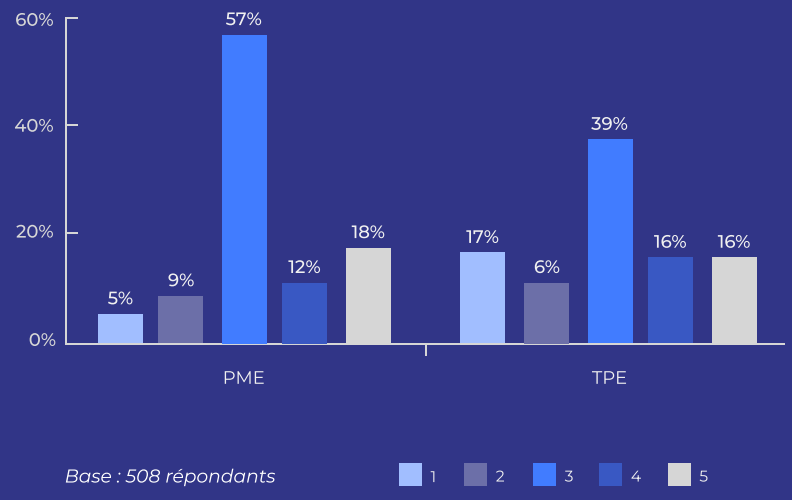
# Un nombre important d'entreprises qui semblent ne pas porter d'intérêt majeur aux questions de Souveraineté

## Néanmoins, 1/3 des répondants estiment ce sujet important à très important

A quel point l'usage de systèmes de cybersécurité souverains (français ou européen) est-il important dans vos choix ?
1= très peu important ; 5 = très important




Si 45% semblent éloignés du sujet en exprimant aucun avis, les **entreprises jugeant que ce critère est très important sont deux fois plus nombreuses** que celles qui le jugent peu important

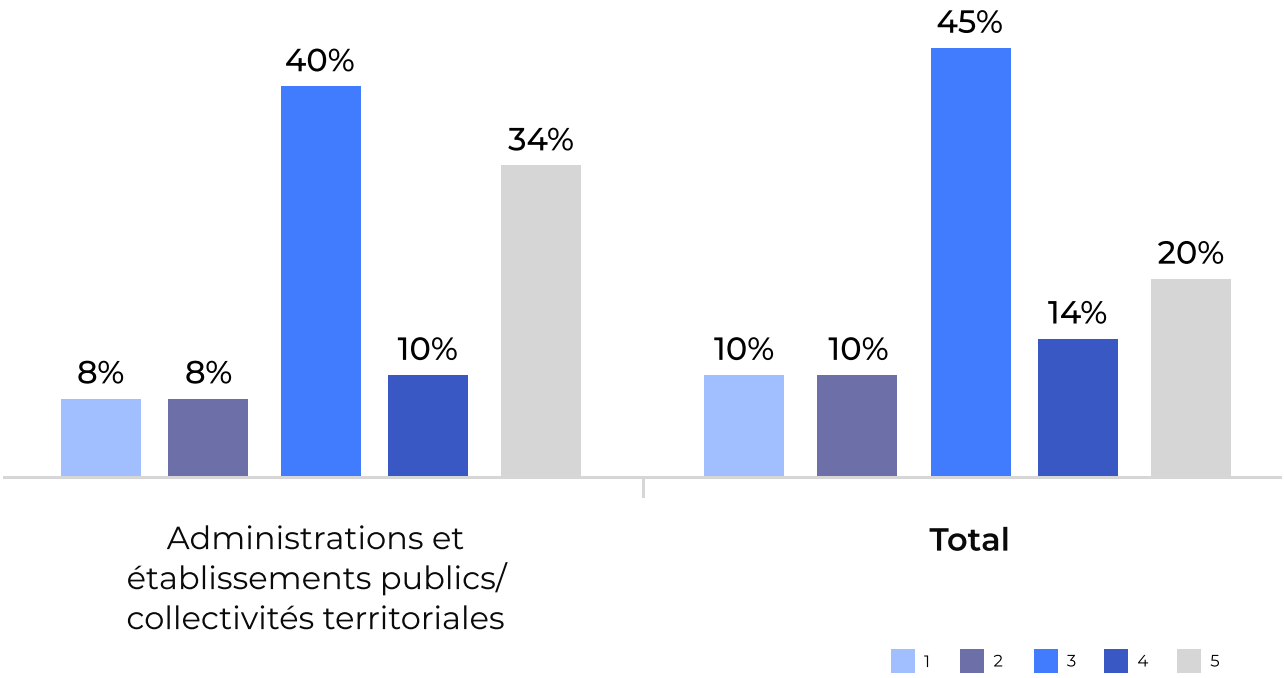



L'intérêt de la souveraineté pour les TPE-PME est légèrement plus basse que les autres entreprises

*Base : 508 répondants*

# La Souveraineté, un intérêt particulier émis par les établissements publics

**A quel point l'usage de systèmes de cybersécurité souverains (français ou européen) est-il important dans vos choix ?**
*1= très peu important ; 5 = très important*



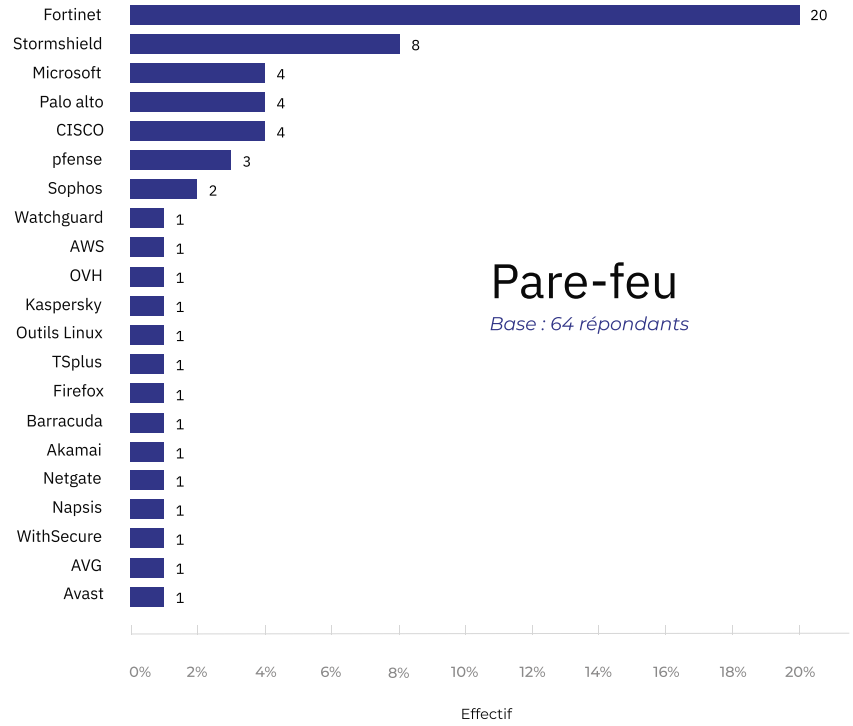

*Base : 508 répondants*

Si **les établissements publics** sont à peine plus concernés par la souveraineté que la totalité des répondants (+4pts sur les notes 3, 4 et 5), ils **sont davantage enclins à mettre de fortes notes** : +14pts sur la note 5/5 et +4 pts sur la note 4/5

# Les choix de logiciels utilisés, reflet des tendances

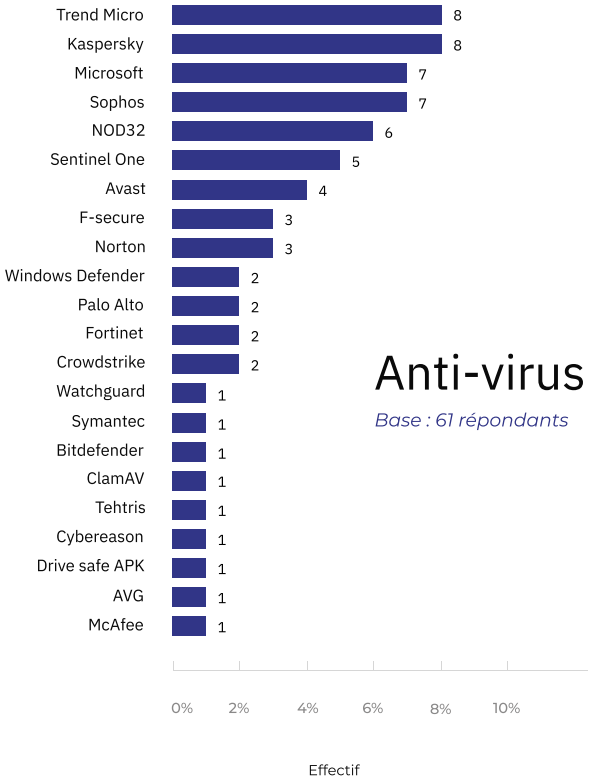
**Les logiciels les plus souvent cités sont d'origine étrangère**.
Avec une exception pour les pare-feux, Stormshield, le 2e cité est français.

Le reste des réponses est réparti de manière assez équilibrée entre les personnes qui ne savent pas ou qui ne veulent pas répondre (par souci de confidentialité).



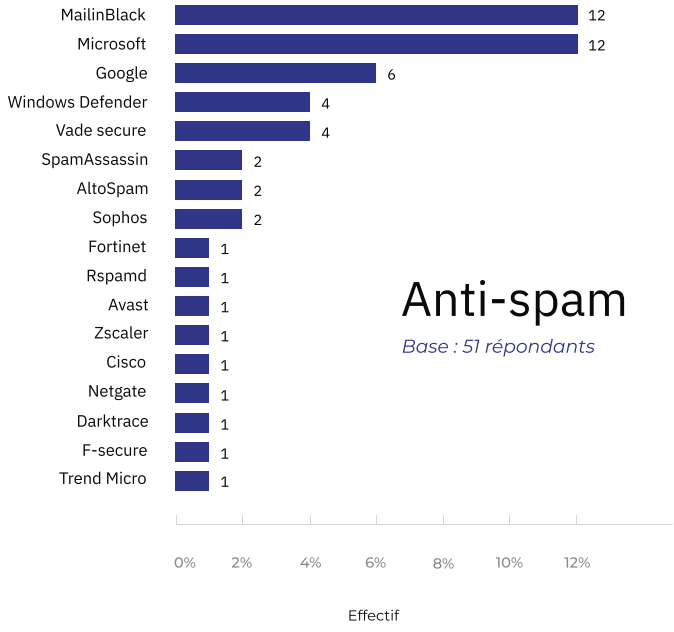

## Pare-feu

*Base : 64 répondants*




## Anti-virus

*Base : 61 répondants*




## Anti-spam

*Base : 51 répondants*

# L'élaboration de la grille de maturité et des critères associés s'appuie sur les recommandations de l'ANSSI au travers du « Guide des mesures Cyber préventives prioritaires » et du « Guide d'hygiène informatique »

**4 Niveaux ont ainsi été définis dans cette grille s'appuyant sur le respect ou non d'un sous-ensemble de recommandations présentes dans ces guides**

## Niveau critique

**Toutes les entreprises** qui se positionnent **en dehors des trois autres niveaux** et qui sont donc considérées comme **n'ayant pas déployé l'ensemble des mesures essentielles** qui leur permettent d'espérer une continuité de ses activités suite à une cyberattaque.

## Niveau essentiel

Les entreprises expriment le fait qu'elles ont mis en œuvre **les mesures essentielles** préconisées par l'ANSSI **qui permettent de limiter la probabilité** d'une cyberattaque à court-terme et d'en **réduire ses potentiels effets**.

## Niveau standard

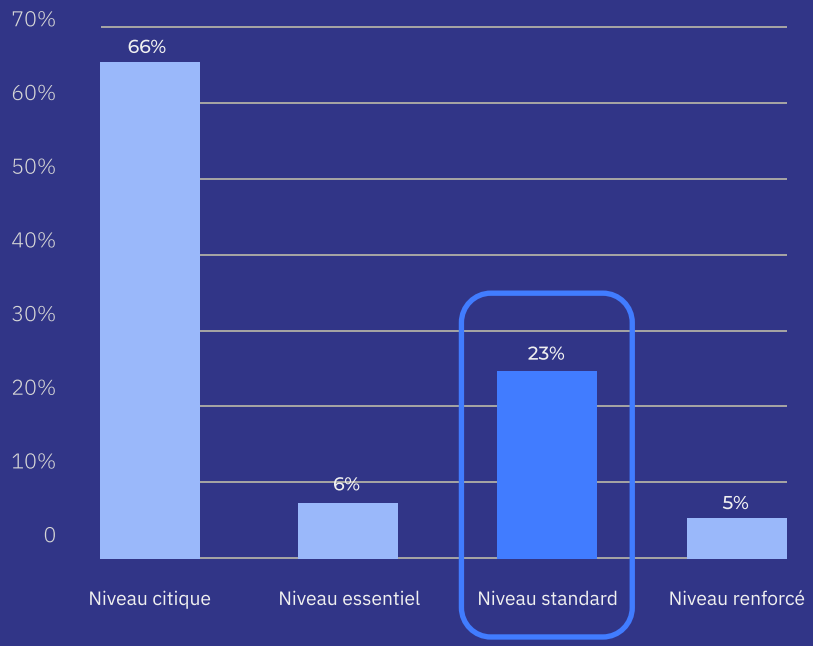
Les entreprises s'inscrivent dans une démarche de **mise en œuvre des mesures d'hygiène informatique** préconisées par l'ANSSI **afin d'assurer la sécurité de leurs systèmes d'information** que ce soit en termes d'outils, d'organisation ou de processus. Les mesures préconisées pour ce niveau standard visent à **apporter à l'entreprise les mécanismes d'amélioration continue nécessaires à un maintien à l'état de l'art dans ses mesures de protection**.

## Niveau renforcé

Les entreprises ont complété les mesures nécessaires à atteindre le niveau standard avec **la mise en œuvre d'une approche globale de maîtrise des risques et la mise en place d'une gouvernance globale** permettant d'appréhender et maîtriser les risques liés à la cybermalveillance. Ce niveau renforcé est particulièrement adapté pour les entités plus exposées aux risques cyber ou de secteurs essentiels.

# Une maturité des entreprises plutôt moyenne au regard des préconisations de l'ANSSI, mais un fort potentiel d'évolution

## 66% des entreprises n'appliquent pas les pratiques permettant d'atteindre le niveau essentiel




Près des 2/3 de l'échantillon pourrait basculer au niveau supérieur avec un bon accompagnement et une mise en perspective du degré d'importance des mesures à mettre en place

Sur les 23% d'entreprises qui ont complété le niveau standard, on retrouve : 1/4 ETI et grands groupes contre 3/4 TPE et PME

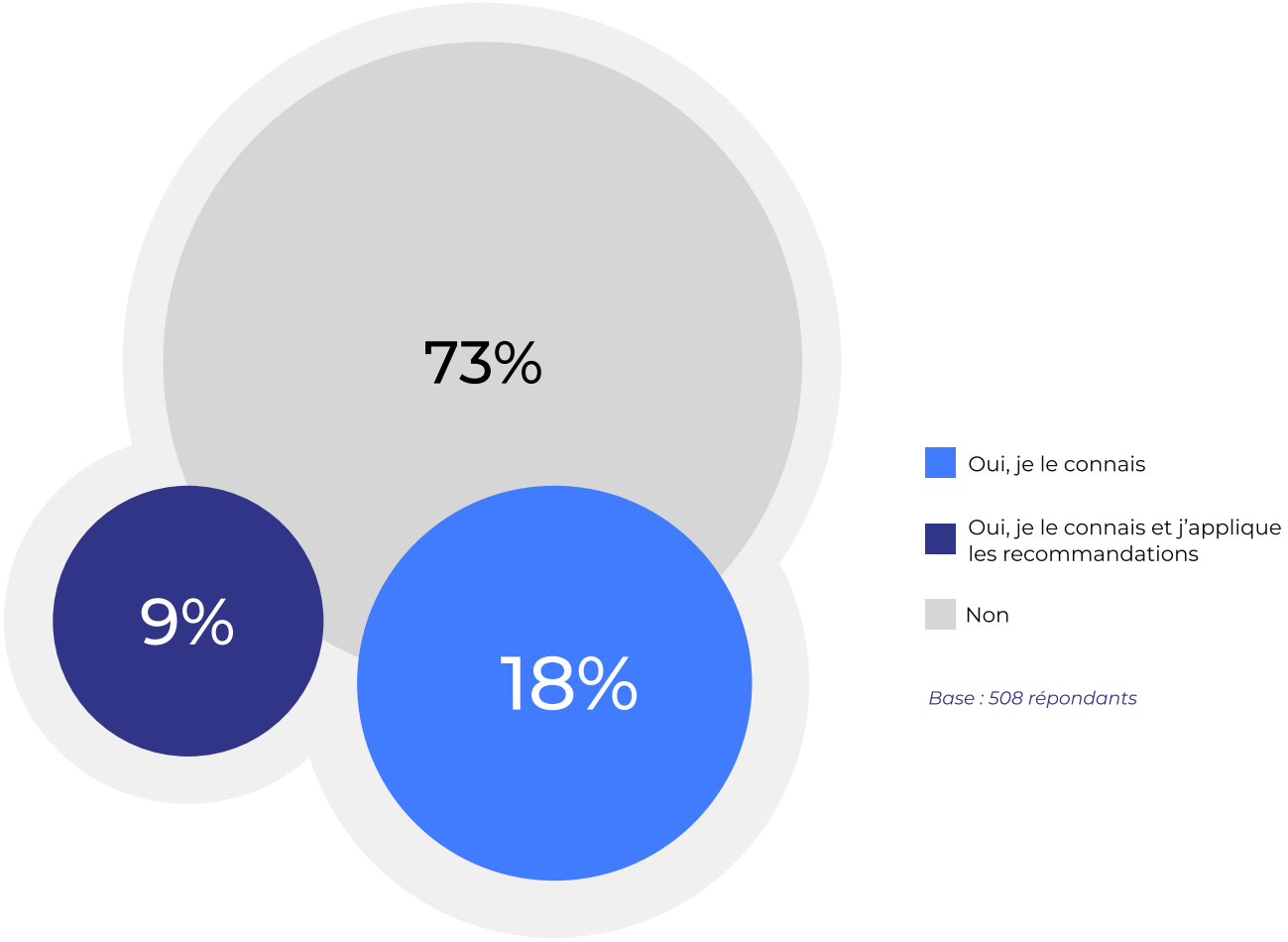
Deux principaux manques sont exprimés :

**01**
Des services de supervision et de gestion de la cybersécurité

**02**
Un dispositif de gestion de crise cyber

Traiter ces deux manques permettrait à près de 50 % de ces entreprises de passer au niveau essentiel

# Moins d’1/3 des répondants (27%) connaissent le guide de l’ANSSI

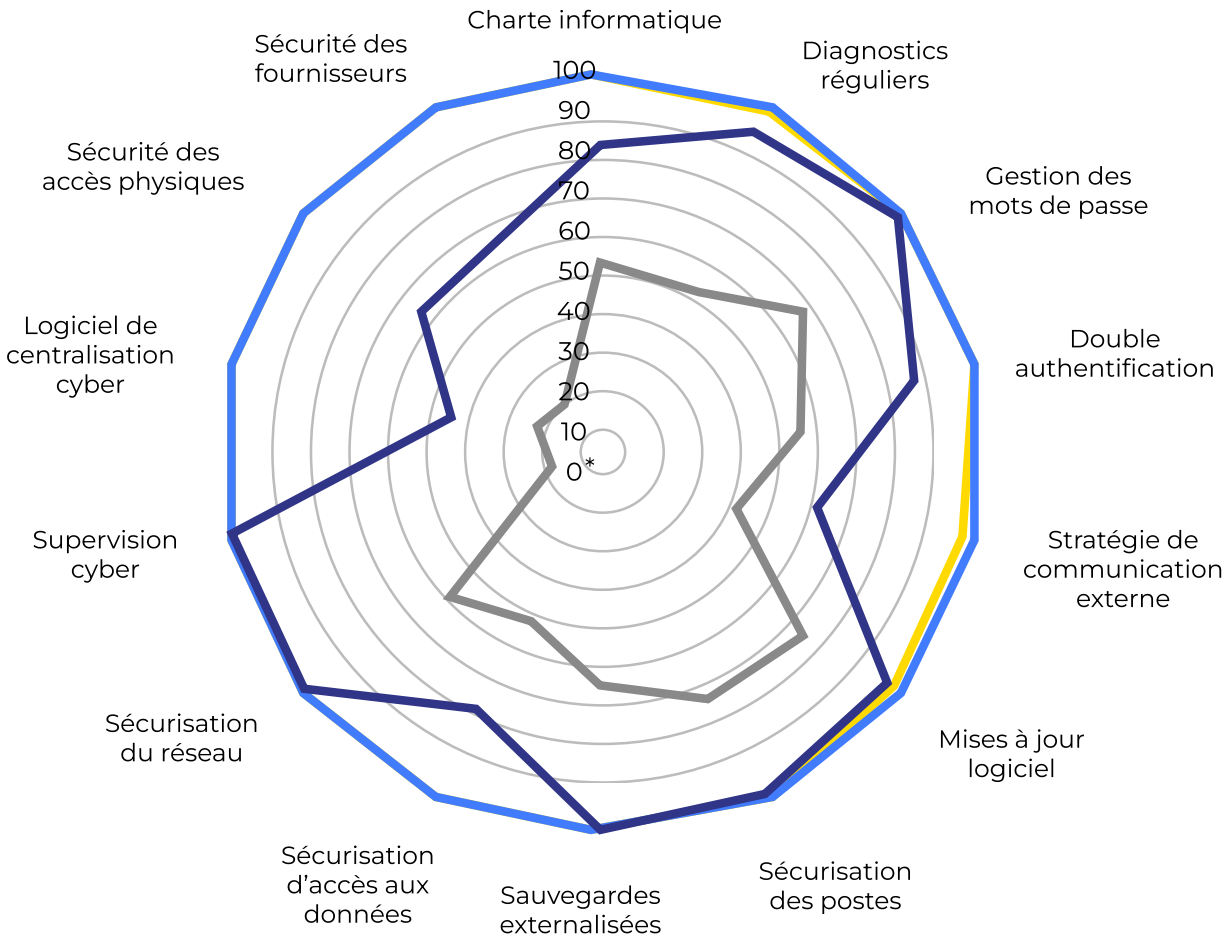



**Parmi le tiers des répondants qui connaissent le guide, seuls 9% mettent en place des recommandations**

**Les entreprises de 250-499 salariés et celles de plus de 1000 salariés connaissent 2 fois plus le guide que les autres tailles d’entreprises et l’appliquent 3 fois plus**

Sans surprise celles de moins de 50 salariés sont celles qui le connaissent le moins (au moins 11 pts d’écart avec la moyenne)

# Le radar de maturité montre néanmoins de gros écarts entre les entreprises du niveau critique et les autres




** En pourcentage des entreprises des différents niveaux ayant mis en place les actions*

DOCAPOSTE

Référent de la confiance numérique en France et filiale du groupe La Poste, Docaposte accompagne toutes les entreprises – des PME aux grands-comptes – ainsi que les institutions publiques dans leur transformation et leur permet de l'accélérer, en confiance. Expert dans le traitement de données sensibles et Tiers de confiance, Docaposte bénéficie d'un positionnement unique sur le marché qui lui permet de répondre de bout en bout à l'intégralité d'un besoin client, dans le respect des réglementations et avec l'assurance d'une donnée hautement sécurisée. Leader des solutions numériques de confiance (vote électronique, lettre recommandée électronique, signature électronique, archivage numérique) et premier opérateur de données de santé en France avec plus de 45 millions de dossiers médicaux, Docaposte apporte son expertise dans la conception et la gestion de plateformes numériques sur mesure.

Ses savoir-faire industriels et de délégation de gestion lui permettent de répondre à tous les besoins de ses clients. Avec près d'1 milliard de CA à fin 2023, Docaposte compte plus de 40 000 entreprises et administrations clientes et 7 500 collaborateurs répartis sur près de 86 sites en France et à l'international.

**Contributeurs Docaposte**
Marion DUMESNIL, Christophe HÉRAULT, Stéphane INGRASSIA, Smara LUNGU, Gwenaelle MARTINET, Muriel POLITANO, Guillaume POUPARD, Morgane TUILLIER

---

CYBLEX Consulting

Cyblex Consulting est un cabinet spécialiste du conseil et de l'audit en cybersécurité, construit autour de la conviction que la cybersécurité est une des clés de la résilience dans un monde de plus en plus digitalisé et que la compétence doit être partagée. Il intervient depuis les phases d'évaluation de la maturité jusqu'à la mise en place et l'amélioration continue du SMSI. Cyblex Consulting est une filiale d'IMS Networks, groupe français spécialisé depuis plus de vingt-cinq ans dans le déploiement, l'infogérance et la sécurité d'infrastructures et de services numériques critiques. Cela a permis à Cyblex Consulting de développer une approche approfondie de l'ensemble de la chaîne de la sécurité des systèmes d'information.

Nos consultants Cybersécurité s'appuient sur leurs expériences individuelles dans une grande variété de secteurs : banque & assurance, santé, télécom, agro-alimentaire, aéronautique et spatial, énergie, services publics...

**Contributeurs Cyblex Consulting**
Thierry BARDY, Christophe VENDRAN, Stéphane CHMIELEWSKI, Fabrice VERNEZOUL, Lucie GOUIRY, Mathieu RIGOTTO, Matthieu HUC, Antoine DERAIN

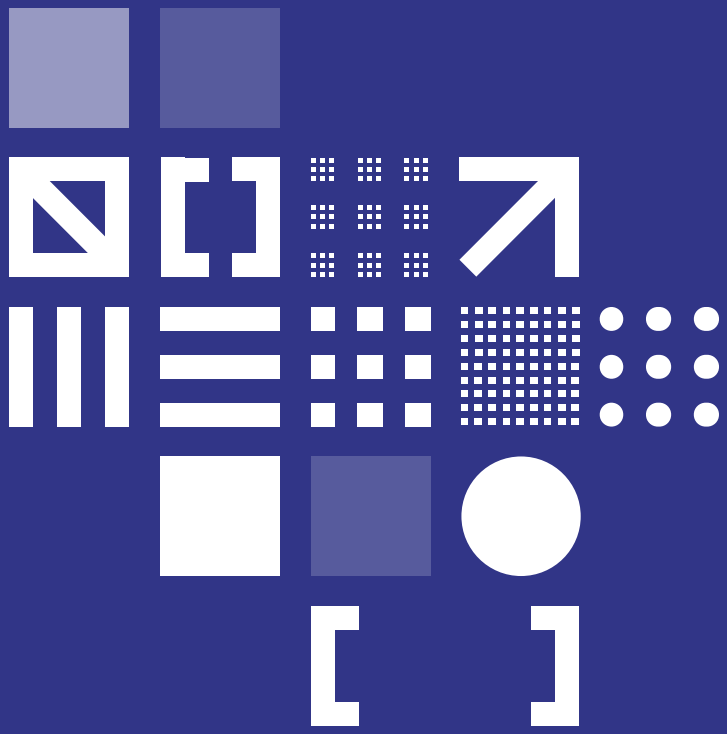
---

iteractii

Depuis notre création en 2021, notre mission chez Iteractii est de façonner des expériences client inégalables, définies par l'innovation et une connaissance pointue des besoins du marché. Établis dans cinq métropoles françaises, nos 300 collaborateurs dédiés donnent le meilleur d'eux-mêmes chaque jour pour répondre aux exigences de 120 clients majeurs, générant un chiffre d'affaires de 15 millions d'euros.

Imaginez le conseil et la mise en œuvre pilotés avec la vivacité d'une start-up et l'expertise d'un grand groupe. C'est là l'essence d'Iteractii, votre partenaire agile et rigoureux dans la conquête d'un parcours client exceptionnel.

**Contributeur Iteractii**
Nabil THALMANN



DOCAPOSTE

CYBLEX Consulting

iteractii