DOCAPOSTE

CYBLEX Consulting

2ème Édition

Baromètre de la cybersécurité 2024

Quelle maturité pour
les entreprises françaises ?

iteractii

L’édito

Olivier Vallet
Président Directeur Général

DOCAPOSTE

Les technologies numériques sont au centre des enjeux sociétaux, géopolitiques, environnementaux et économiques. En quelques années, leur développement massif a bouleversé le quotidien des citoyens, des entreprises, du secteur public et ce, quels que soient les domaines d’activités.

Ces évolutions majeures s’accompagnent d’une montée en puissance de la cybercriminalité, qui constituent aujourd’hui un défi pressant pour l’ensemble des acteurs. Tandis que la réalité de cette menace est désormais incontestable, les grandes entités ont réagi en conséquence en investissant massivement dans leur sécurité et en intégrant des technologies de pointe afin d’anticiper et de contrer les cyberattaques. Cependant, les acteurs de moindre envergure, les TPE, ETI, collectivités, dépourvus des ressources et de l’expertise nécessaires, se retrouvent démunis face à ces enjeux.

Le sujet de la cybersécurité deviendra encore plus crucial avec l’essor des technologies émergentes comme l’intelligence artificielle. Ces innovations, bien que prometteuses, élargissent la surface d’attaque des cybermenaces. Les plus petites entités, qui ne l'auront pas anticipé, seront particulièrement fragiles.

Afin de s’assurer une autonomie stratégique numérique, de se prémunir d’un risque tant économique que sécuritaire, nous devons accompagner ces structures moins bien protégées.

En effet, cette deuxième édition du baromètre, co-réalisé par Cyblex Consulting et Docaposte, révèle encore un fort besoin de sensibilisation de l’ensemble des collaborateurs et d’un accompagnement structuré pour identifier les solutions adaptées à leurs besoins. Il est à noter une progression importante quant à la prise de conscience des enjeux liés à l’importance de disposer de systèmes souverains. Nous devons poursuivre en ce sens. Il est important que cette prise de conscience se poursuive afin de limiter notre dépendance excessive à l’égard des géants technologiques étrangers pour maîtriser les infrastructures de cybersécurité, notamment lorsqu’il s’agit de données sensibles.

Christophe Vendran
Directeur Général

CYBLEX Consulting

Chaque année, les enjeux de la cybersécurité prennent une ampleur nouvelle, reflétant la complexité croissante d’un monde toujours plus interconnecté. Chaque incident, chaque attaque, chaque règlementation nous rappelle que le cyberespace est un terrain en perpétuelle mutation. Dans cet environnement complexe, les organisations, indépendamment de leur taille et leur secteur d’activité, doivent anticiper, comprendre les dynamiques qui transforment les risques en réalité et agir avec détermination.

L’édition 2024 du baromètre s’inscrit dans cette ambition. Cette publication annuelle s’est imposée comme un rendez-vous incontournable pour dresser un état des lieux précis des menaces, comprendre les évolutions, les enjeux mais aussi les réponses que nous devons apporter pour protéger ce qui nous est essentiel.

Une disparité notable persiste encore entre les grandes organisations souvent bien équipées, et les TPE/PME qui restent très vulnérables.

Aussi, ce baromètre, co-réalisé par les experts de Cyblex Consulting et Docaposte, invite chaque acteur à mesurer pleinement l’importance d’une posture proactive. De sorte à faire de la cybersécurité une priorité, non par obligation, mais par conviction et ainsi mettre en place des mesures de sécurité adaptées à ses besoins et à ses moyens financiers. Car élever son niveau de protection est devenu une condition essentielle pour bâtir des écosystèmes numériques durables et résilients.

Cette édition est une fois de plus riche d’enseignements qui méritent d’être partagés au plus grand nombre. Au-delà de l’analyse, elle porte un message essentiel : la sécurité grandit lorsqu’elle se partage. Ensemble, partageons ces connaissances et renforçons notre résilience face aux défis 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 mises en œuvre

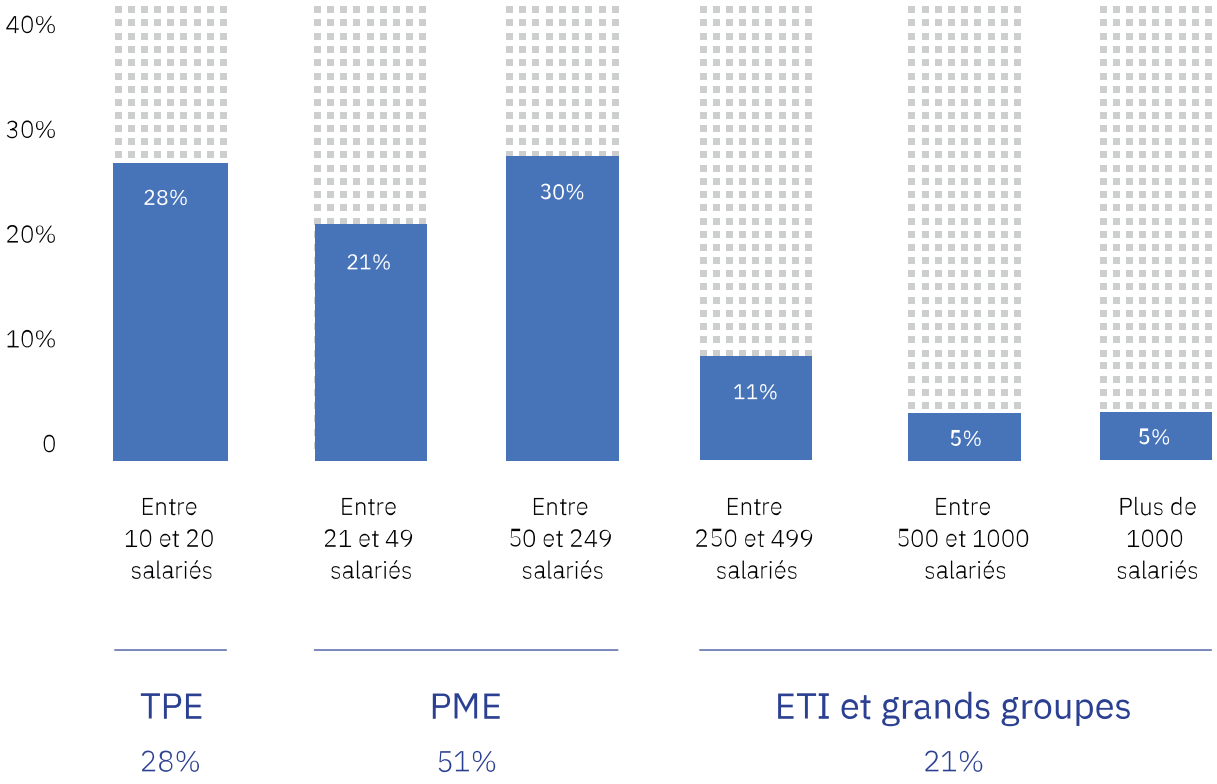
La perception du niveau de risque

L’échantillon de notre enquête

Le périmètre de l’enquête

Un échantillon qui fait la part belle aux PME : **50% des personnes interrogées.**

Une enquête résolument orientée décideurs d'entreprise : la moitié dans le domaine IT et l'autre en tant que DG et responsables administratifs et financiers.

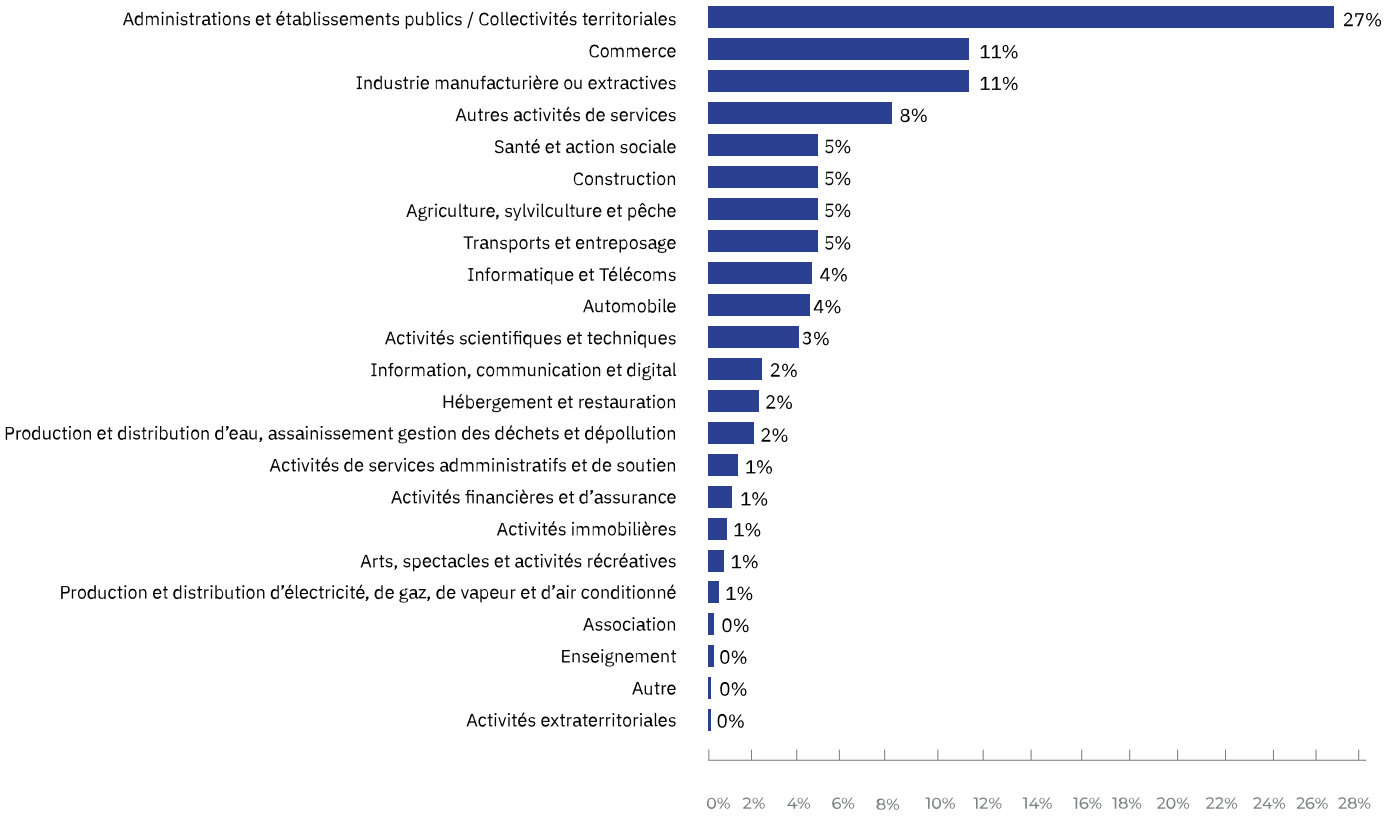


Base : 457 répondants

Secteur d'activité

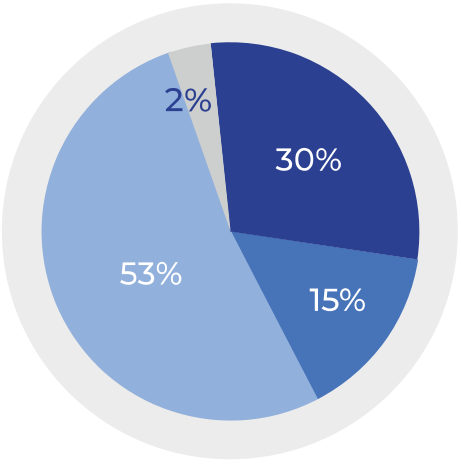
Cette année, une part plus importante a été accordée **aux acteurs du secteur public.**

Ainsi, avec 27% des répondants cet échantillon permet une **analyse de ces organisations beaucoup plus solide.**



Base : 457 répondants

Fonction



La part des dirigeants d'entreprise et des responsables administratifs et financiers a été maintenue pour cette 2ème édition.

- DG / PDG / DGS / Chef de service
- DAF / RAF / Service financier
- RSSI / DSI / Responsable informatique
- Autre

Base : 457 répondants

Executive summary - Quelques chiffres clés

Baromètre de la cybersécurité 2024

Quelle maturité pour les entreprises françaises ?

DOCAPOSTE CYBLEX Consulting intuiti

I **les entreprises se sentent davantage menacées** (+10pts) que l'année dernière

4/10 des entreprises **se sentent menacées**

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

72% **des répondants pensent faire suffisamment d'efforts** (+8pts)

III Une proportion d'entreprises cyber attaquées **en hausse** (+11 pts)

1/3 des entreprises **ont déjà subi une cyberattaque au cours des 12 derniers mois**

IV **La mise en doute de l'efficacité des actions** reste identique

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

V **L'intérêt des entreprises vis-à-vis d'un système souverain** augmente nettement

1/2 **jugent important ou très important** d'en disposer d'un

---

VI L'accompagnement par un partenaire spécialisé **devient majoritaire**

2/3 des entreprises **font appel à une ressource externalisée**

VII **Le Cloud reste encore en dehors du scope de cybersécurité** pour la majorité des entreprises

1/3 des entreprises **étendent au Cloud leurs actions de cybersécurité**

→ Les écarts majeurs entre les 2 éditions

I

+33%

d'organisations **qui se sentent menacées**

II

+50%

d'entreprises **ayant subi une cyber attaque**

III

+46%

des entreprises **ont leur budget cybersécurité en hausse**

IV

+63%

des entreprises **jugent très important de disposer d'un système souverain**

V

x2

plus d'entreprises **font appel à une ressource externalisée**

VI

x2

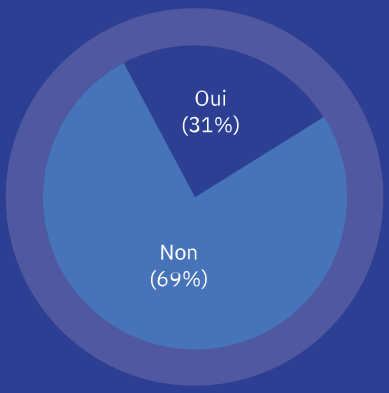
plus d'entreprises **consultent les sites d'organismes officiels**

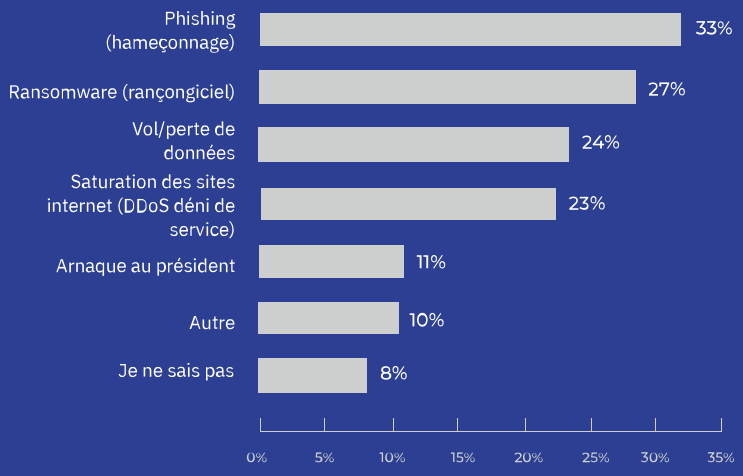
Le secteur public apparaît davantage mature

- **Les acteurs publics déclarent avoir subi moins de cyberattaques que les entreprises** (-6 pts)
- **Les budgets en cybersécurité ont davantage augmenté** (+13 pts)
- **Les acteurs publics surpassent** de 5 à 17 pts **les entreprises dans les actions concrètes mises en place**
- **Les acteurs publics appliquent davantage les recommandations du guide de l'ANSSI** (+14 pts)

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

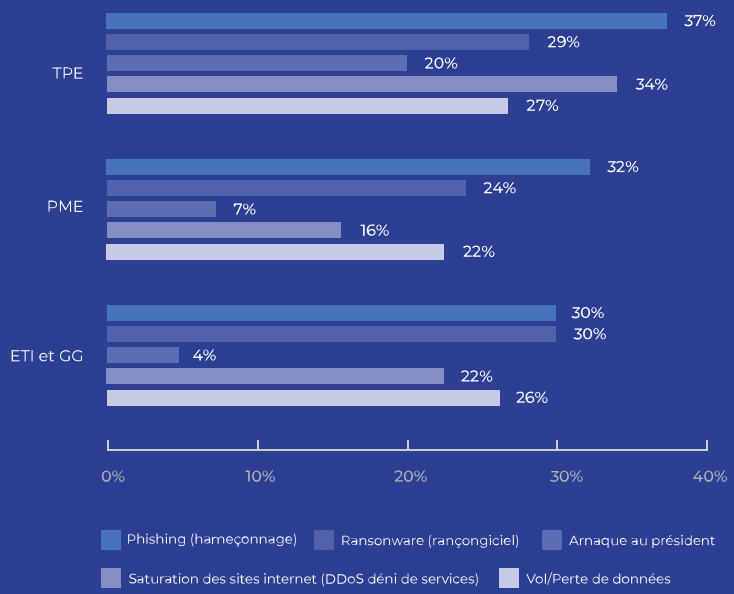
Le nombre d'entreprises ayant subi une cyberattaque **est plus élevé que l'année dernière (+11 pts)**





Contrairement aux craintes précédemment recueillies, la perte de données n'est pas le premier type d'attaque ayant été subie même s'il est dans le top 3.

Focus sur les cyberattaques



Les TPE et PME ont une hiérarchie des attaques subies quasi identique.

Les ETI et grands groupes se distinguent sur 2 attaques qu'ils subissent davantage : "Arnaque au président" (3 fois plus que les autres types d'entreprises) et "Saturation des sites Internet".

Base : 142 répondants

Des disparités de taille mais également sectorielles

Les entreprises ayant été plus souvent cyber-attaquées que les autres sont davantage les entreprises de plus de 500 salariés (+12 à +26 pts).

Le top 5 des secteurs qui se sentent le plus être une cible (qui répondent oui pour au moins 50% d'entre eux) :

1 **Activités financières et d'assurance**

2 **Activités de service administratif et de soutien**

3 **Hébergement et restauration**

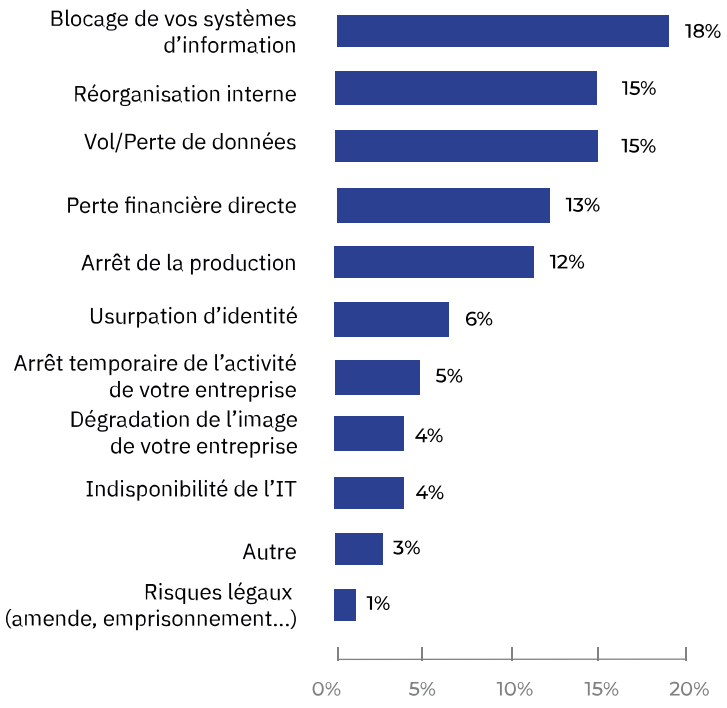
4 **Production et distribution d'eau/d'électricité**

4 **Acteurs publics**

Des impacts hétérogènes, le blocage des systèmes d'information en tête

Le vol de données n'est plus le principal impact qui se dégage des autres. Cette 2ème édition voit la montée de 2 conséquences dans le top 3 :

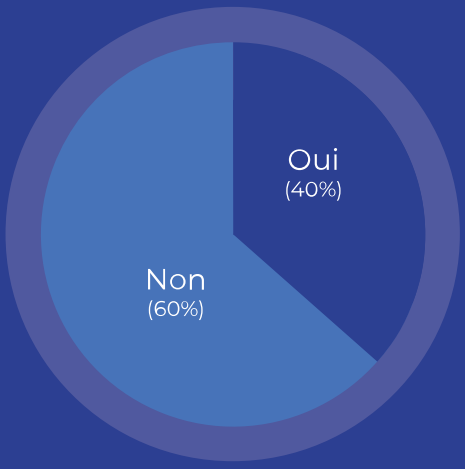
- Blocage des systèmes d'information **(+3 pts)**
- Réorganisation interne **(+10 pts)**



Base : 142 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

→ 48% se considèrent comme des cibles potentielles
avec un score plus élevé pour les répondants issus des fonctions IT



Base : 457 répondants

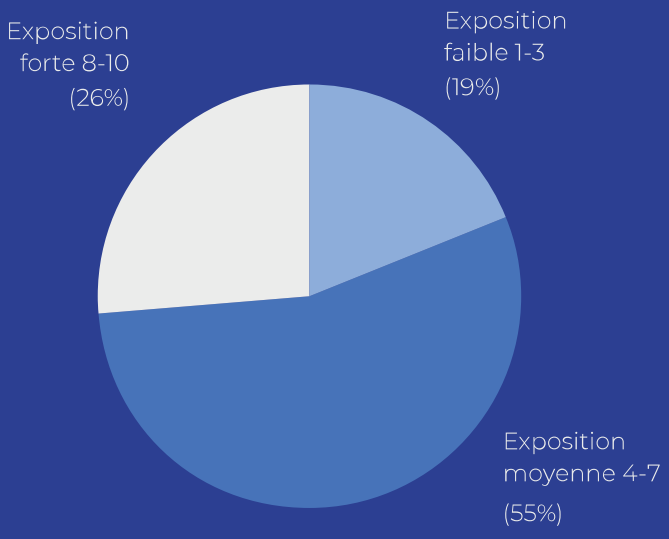
Les entreprises s'estiment être davantage la cible que l'année dernière : 9 pts de plus.

Les spécialistes IT semblent avoir davantage conscience de l'attractivité de leurs données : ils sont 48% à répondre oui.

Le top 5 des secteurs qui se sentent le plus être une cible (qui répondent oui pour au moins 50% d'entre eux) :

- Activités financières et d'assurance
- Activités de service administratif et de soutien
- Hébergement et restauration
- Production et distribution d'eau/d'électricité
- Acteurs publics (ex-aequo)

26% pensent être très exposées



Base : 457 répondants

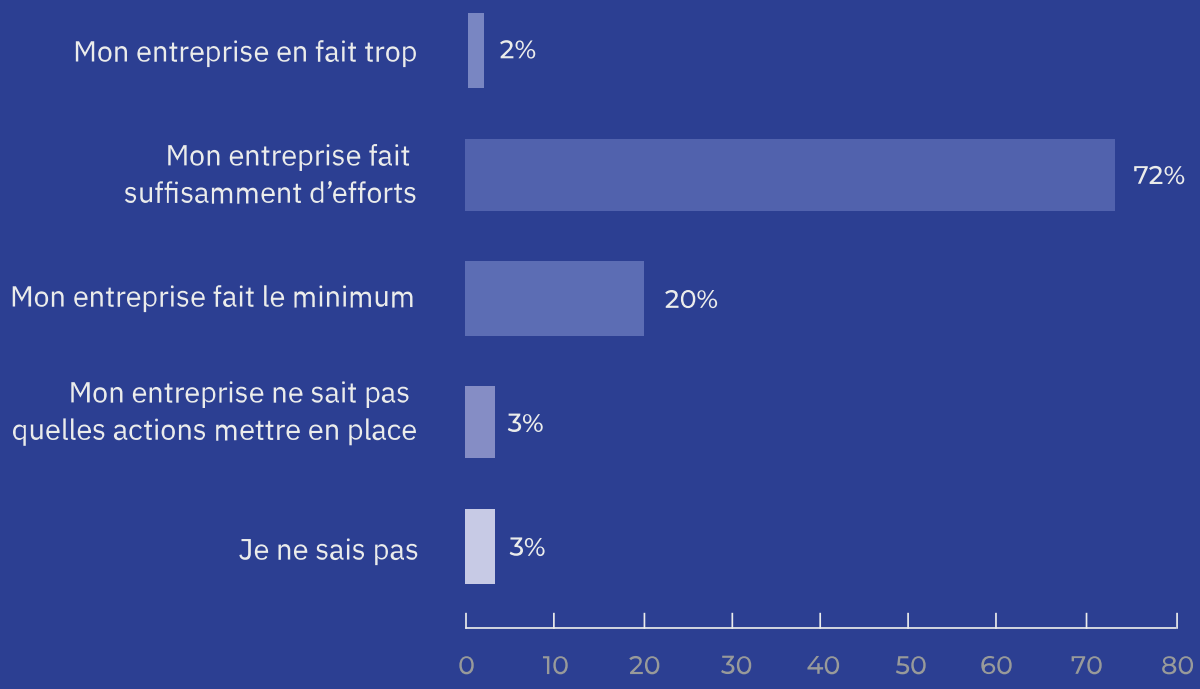
Les entreprises ont davantage le sentiment d'être exposées que de l'être faiblement (7 pts d'écart). La tendance s'est inversée depuis l'année dernière.

Plus l'entreprise est grosse, plus elle se sent exposée (notes 8-10)

- 29% entre 50 et 249 salariés : +3 pts
- 38% entre 250 et 499 salariés : +19 pts
- 48% entre 500 et 1000 salariés : +29 pts
- 57% plus de 1000 salariés : +38 pts

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

72% des entreprises pensent faire suffisamment d'efforts



Base : 457 répondants

Le sentiment de faire des efforts est partagé par quasiment les ¾ des entreprises. Elles sont davantage confiantes qu'il y a un an (+8 pts).

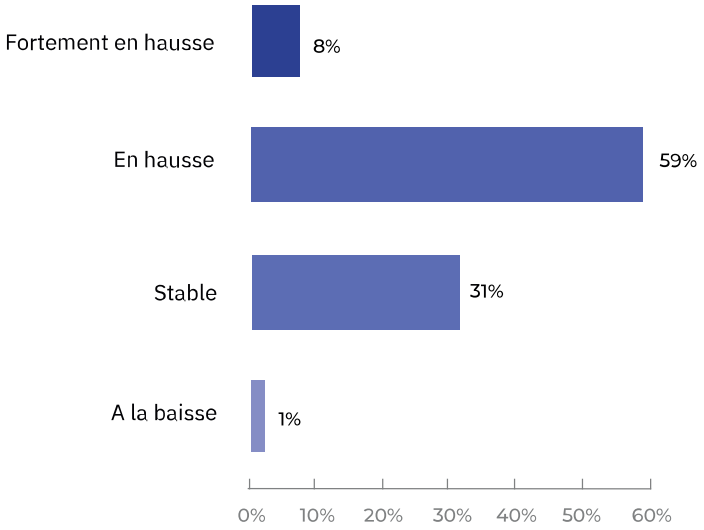
Les entreprises de plus de 500 salariés sont celles qui affirment le plus en faire suffisamment (+6 pts).

Ce sentiment est cependant moins partagé (-6 pts) par les plus petites entreprises qui disent en faire le minimum (+6 pts).

Deux tiers des entreprises affirment notamment que leur budget est en hausse

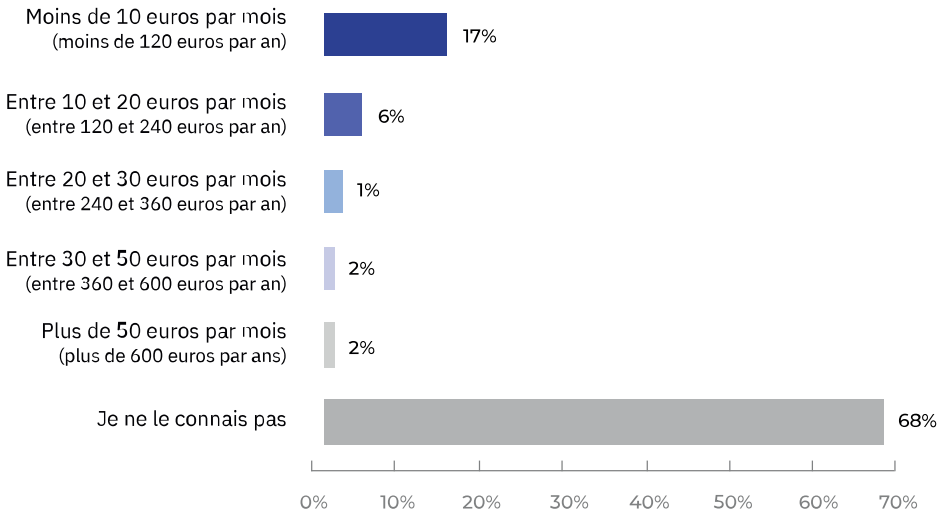
Des efforts supplémentaires ont été réalisés car la hausse du budget concerne beaucoup plus d'entreprises que lors de la dernière édition : +21 pts.

- Ce budget en hausse est surtout porté par les entreprises de plus de 50 salariés.
- Cette hausse a surtout concerné des montants entre 20 et 50 euros par mois par salarié.
- Si l'item "fortement en hausse" baisse de 7 pts, il concerne surtout les entreprises de plus de 1000 salariés (+17 pts par rapport à la moyenne).
- A noter que les TPE, davantage que les autres, se sont contentées de garder stable leur budget (+15 pts que la moyenne).



Base : 457 répondants

La moyenne des dépenses par salarié par mois est de 15 euros



- Les entreprises de moins de 250 salariés dépensent moins de 20 euros par mois.
- A partir de 500 salariés, les entreprises dépensent au moins 30 euros.
- Au global, la moyenne des montants investis par salariés par mois est d'environ 15 euros.
- Précisons que sur cette question, 10% de l'échantillon n'a pas souhaité y répondre.

Base : 411 répondants

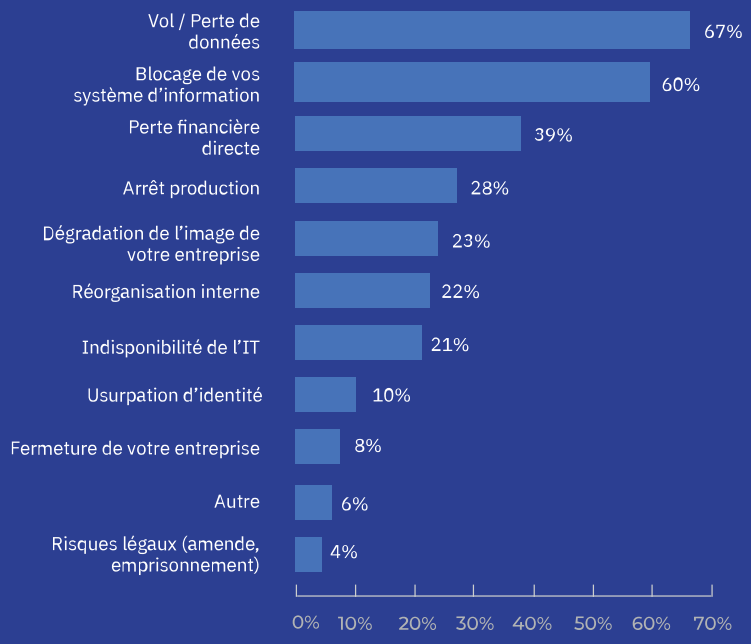
Des craintes ainsi que des démarches mises en œuvre qui varient en fonction de la taille de l'entreprise

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

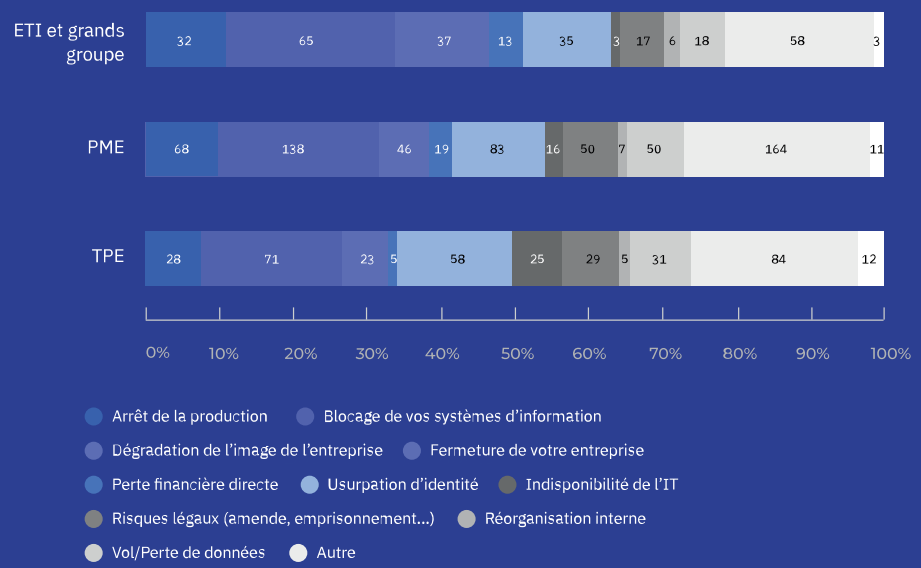
Le vol et/ou la perte de données reste en tête des craintes exprimées par les entreprises (surtout les PME) mais **son écart avec la 2ème crainte est moins flagrant** (6 pts vs. 44 pts en 2023).

- On constate de manière générale des réponses davantage ventilées entre les différents risques.
- Notons cependant que la typologie des types d'attaques subies n'a pas bougé depuis 1 an.

Base : 457 répondants



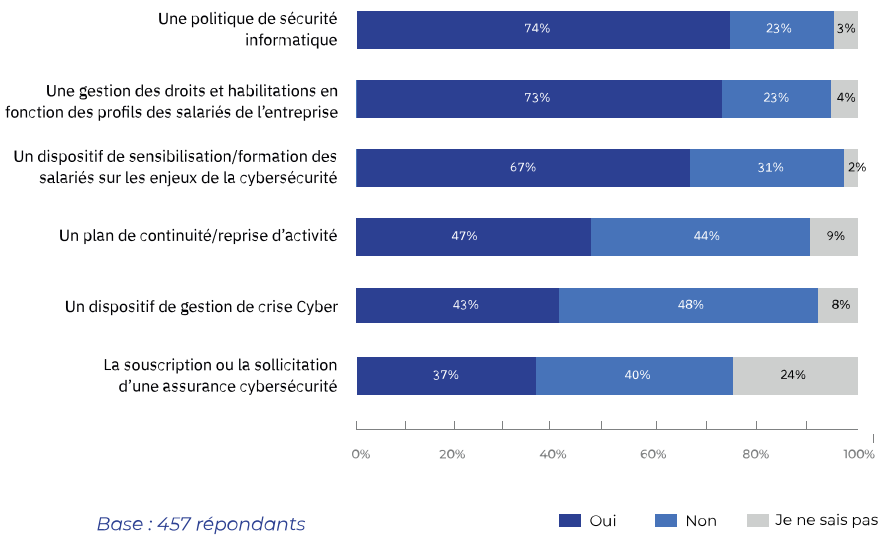
Le top 3 des craintes des TPE-PME sont similaires à celles de l'ensemble des entreprises



Si le top 3 concerne globalement l'ensemble des entreprises, on constate trois écarts significatifs :

- La dégradation de l'image de l'entreprise est davantage une préoccupation des ETI et grands groupes (+25 pts).
- L'usurpation d'identité concerne surtout les TPE (2 fois plus).
- Et la crainte du déni de services concerne surtout les entreprises de plus de 1000 salariés.

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



Base : 457 répondants

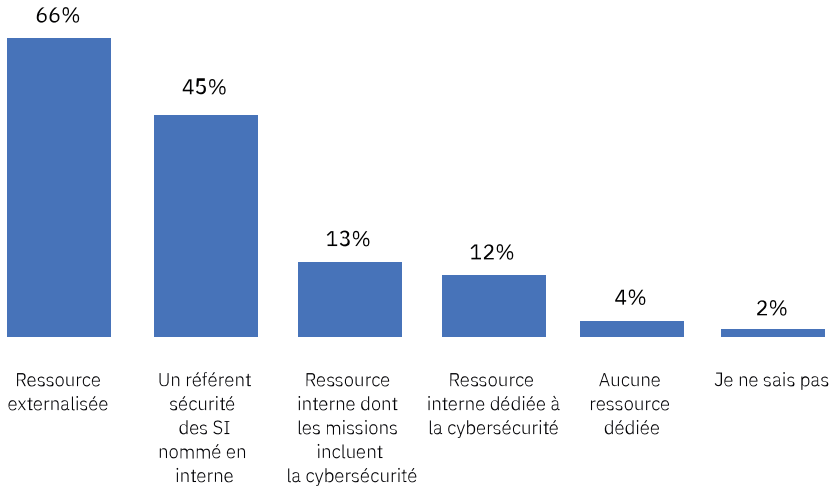
L'écart se creuse entre les 3 premières actions et les suivantes

- En effet, la politique de sécurité informatique et la sensibilisation des salariés progressent respectivement de 7 et 4 points par rapport à 2023.
- Et le nouvel item de cette édition (la gestion des droits selon les profils) entre directement à la 2ème place.
- A l'inverse, le niveau des actions les moins souvent mises en place baisse (-7 pts environ). Cela est d'autant plus un réel souci sur les deux derniers qu'elles sont des recommandations essentielles de l'ANSSI.

Une entreprise sur deux a désigné un référent sécurité pour mettre en place ces démarches

Deux tiers des entreprises font appel à des ressources externalisées (c'est 2 fois plus que l'année dernière).

- Elles sont pour moitié à se doter d'un référent sécurité en interne (cette recommandation ANSSI largement relayée par les différentes communication de l'agence ou de cybermalveillance semble porter ses fruits).
- L'autre élément qui atteste cette prise de conscience est la très faible part des répondants qui n'ont aucune ressource dédiée (-7 pts par rapport à l'année dernière).



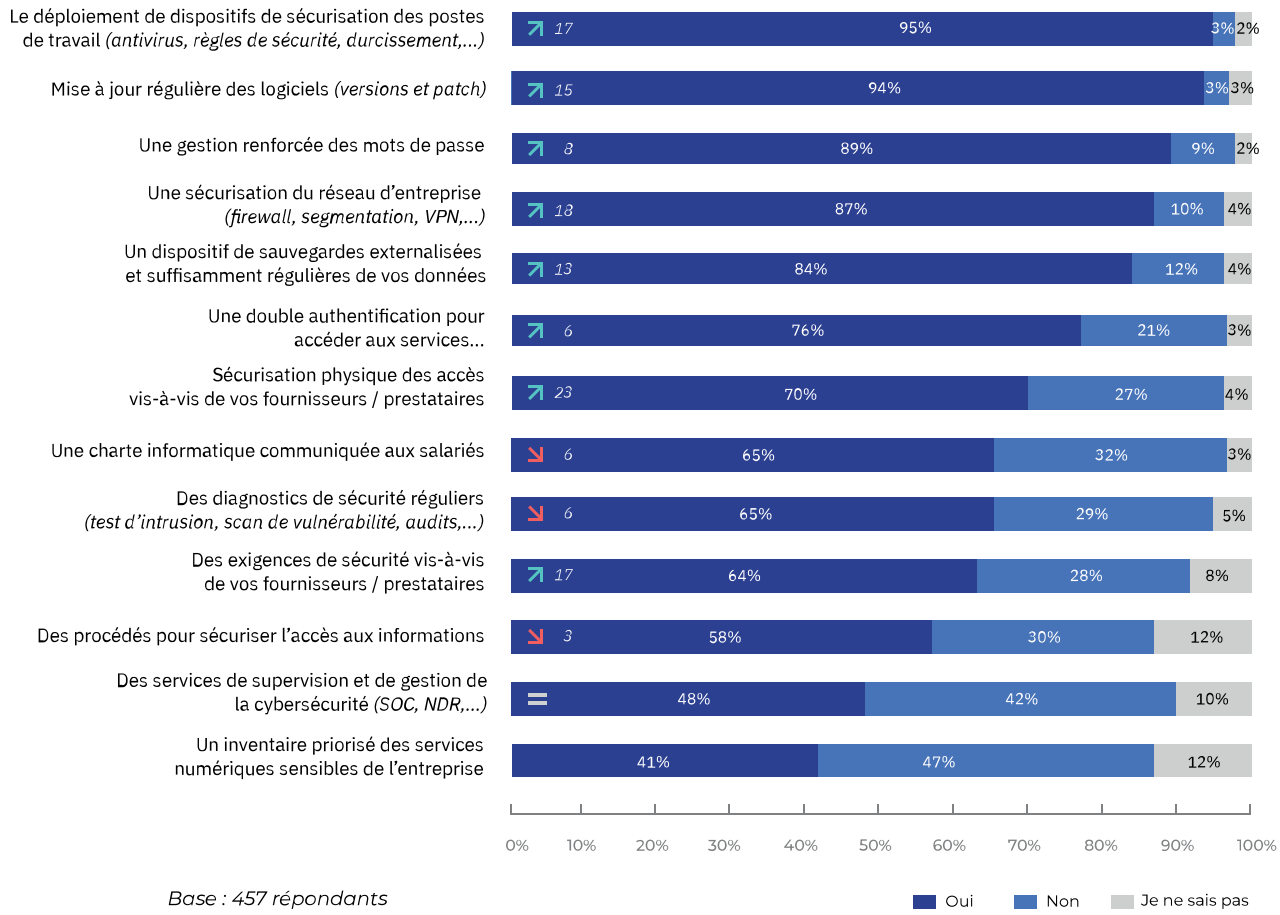
Des actions et solutions concrètes ont été mises en place

L'ensemble des solutions listées sont davantage appliquées par les entreprises interrogées (+5 à 23 pts).

Le top 3 des augmentations d'actions mises en place sont :

1. la sécurisation physique des accès aux zones sensibles,
2. la sécurisation du réseau d'entreprise (firewall…),
3. la sécurisation des postes de travail et les exigences vis-à-vis des fournisseurs (à égalité)

Uniquement 3 actions sont en baisse.



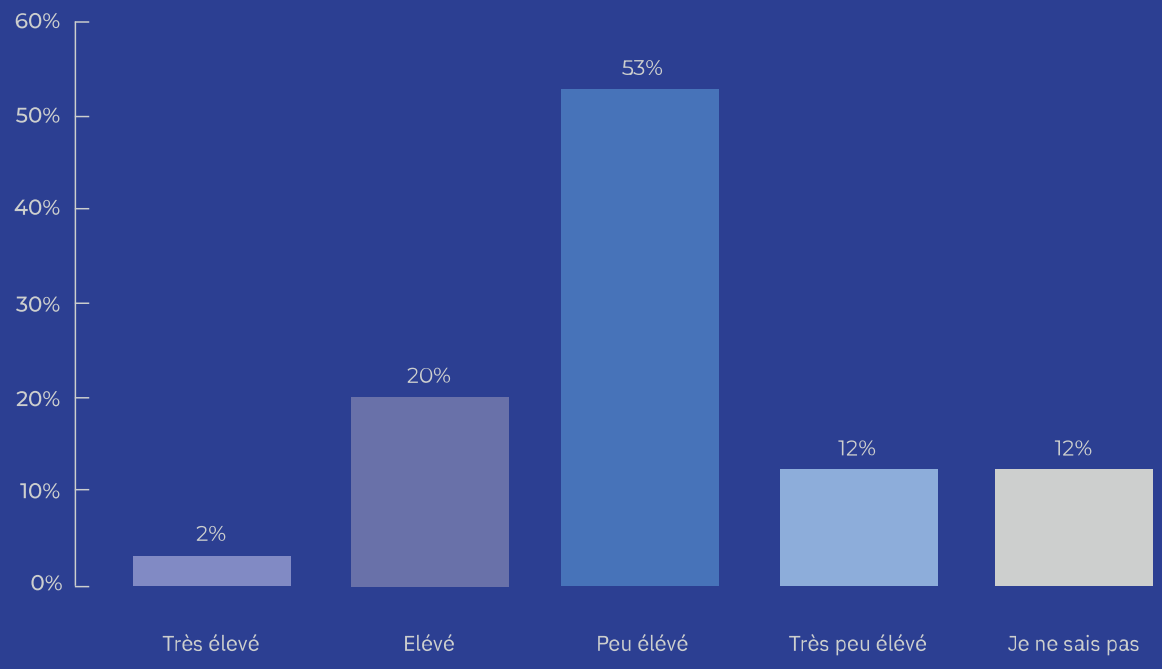
Base : 457 répondants

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

Les avis semblent davantage polarisés cette année. Si la part d'indécis a été divisée par deux, les entreprises expriment davantage leur manque de confiance sur l'efficacité des actions : 22% (au lieu de 14) estiment que le risque d'une cyberattaque réussie reste élevé ou très élevée. Malgré toutes les actions davantage faites que l'année dernière, les entreprises expriment un manque de confiance : est-ce une prise de conscience de démarche pas tout à fait guidée par une politique de cybersécurité solide ?

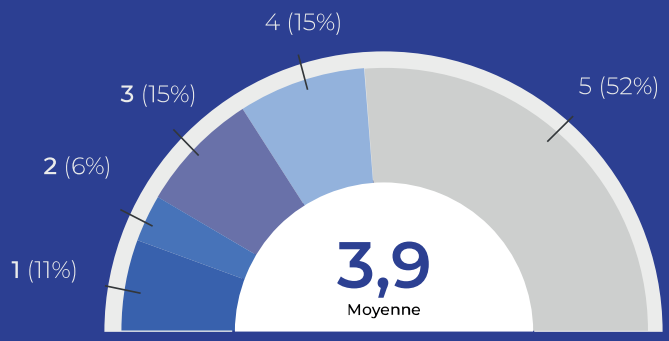
Les différentes fonctions sollicitées sont d'ailleurs sur la même longueur d'onde : pas de différence entre les fonctions IT et les autres.



L'intérêt de la question de la Souveraineté est en nette progression

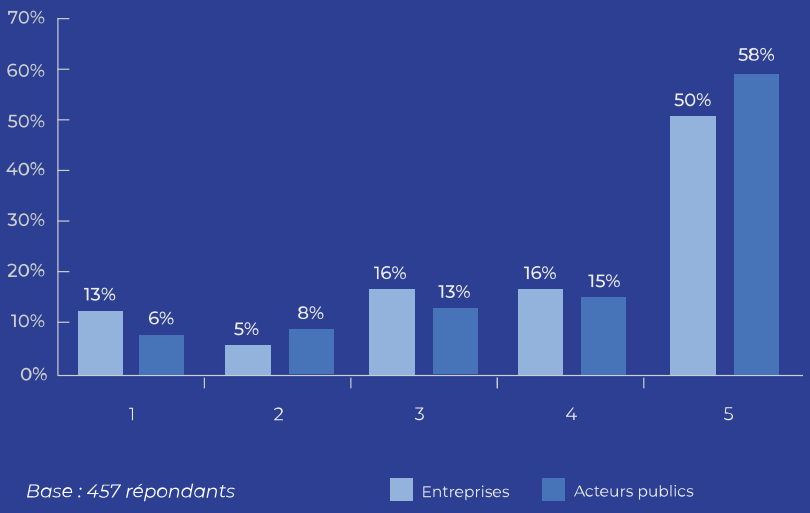
A noter que ce sujet semble susciter un intérêt légèrement plus élevé de la part du secteur public

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



On constate que 52% des répondants ont donné la note maximale de 5/5 (vs. 20% en 2023).

Cela donne une moyenne qui progresse de 3,2 à 3,9.



Base : 457 répondants

Les acteurs publics jugent les systèmes de cybersécurité souverains davantage très importants que les entreprises (+8 pts). Cela donne une moyenne plus élevée également (4,1 vs. 3.9).

L'écart est cependant moins important que l'année dernière, preuve d'une prise de conscience plus forte auprès des entreprises.

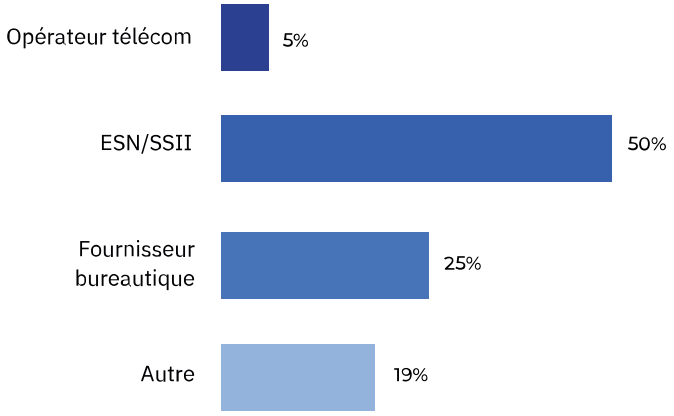
Une entreprise sur 2 choisit une ENS/SSII comme partenaire en cybersécurité

Précisons que le choix d'un prestataire est identique sur les 3 grandes étapes d'un projet : le conseil, la mise en oeuvre et le pilotage

- ESN > fournisseur bureautique > opérateur telecom

Les acteurs cités dans "Autre" sont souvent les mêmes :

- L'équipe en interne ou le groupe auquel appartient l'entreprise
- Des organismes officiels (gendarmerie, ENEDIS, ANSSI, CCI)
- Des prestataires informatiques plus ou moins spécialisés (Waybox, Wesecure)
- Des cabinets de consulting



Base : 457 répondants

Les réponses spontanées montrent une diversité de solutions avec un mélange d'approches internes et externes, de grands acteurs du secteur de la cybersécurité à côté de prestataires régionaux et des solutions spécifiques.

Les solutions les plus citées sont par exemple Orange Cyber Défense, Microsoft, ESET et Mail in Black.

Suivies par d'autres prestataires spécialisés tels que Palo Alto, Sophos, Fortinet, Prodware, OVH, IMS Networks ou Stormshield.

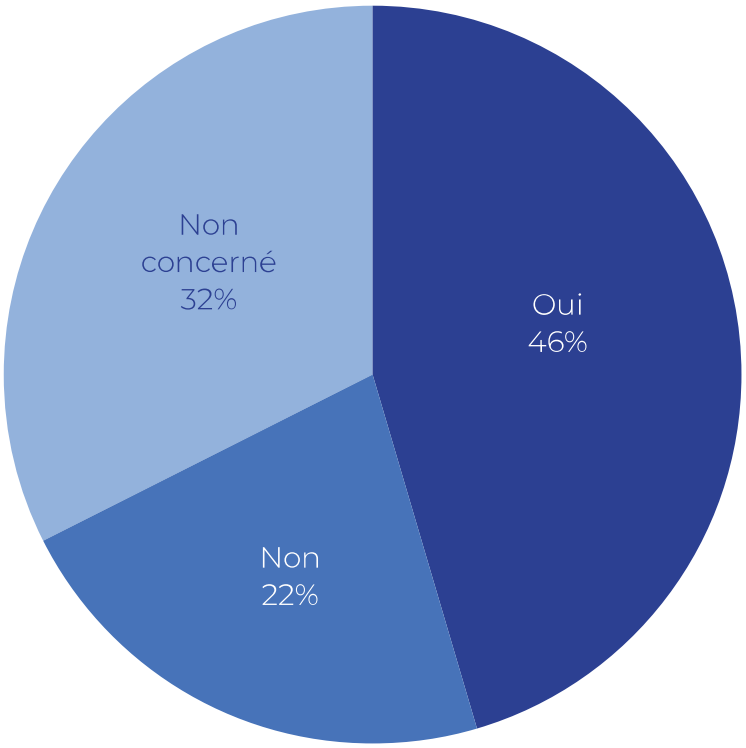
A noter que 1 entreprise sur 5 n'a pas souhaité donner de noms précis.

Une solution packagée proposée par un partenaire spécialisée est préférée

On constate qu'une offre packagée est préférée par la moitié des répondants.

Si l'on exclut les "non concernés", ce sont les 2/3 qui sont en faveur de ce type d'offre (68%).

Afin de faciliter l'implémentation et la gestion de ce type de solution, la préférence tend vers le fait d'avoir un interlocuteur unique et un expert qui sait avoir une vision systémique de cette problématique.



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.

Par ailleurs, nous avons aussi souhaité distinguer les efforts de chaque entreprise afin d'identifier celles qui se rapprochaient le plus du niveau supérieur par leurs actions

Ainsi nous avons distingué les 2 nuances suivantes :

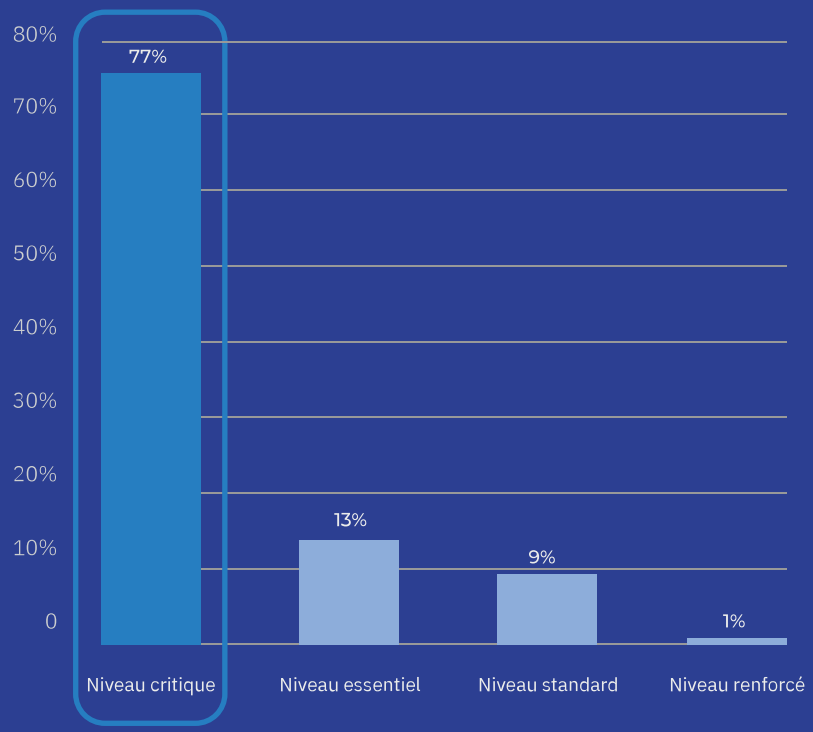
↘ **L'appellation "partiel" indique que plus de la moitié des actions du niveau a été réalisée.**

↘ **L'appellation "non atteint" indique que moins de la moitié des actions du niveau a été réalisée.**

Cela nous permet de mieux évaluer les entreprises qui sont proches d'atteindre le niveau supérieur : celles qui ont rempli partiellement les actions requises pour ce niveau

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

77% des entreprises n'appliquent pas les pratiques permettant d'atteindre le niveau essentiel



De manière générale, plus l'entreprise est petite et plus elle se situe au niveau critique. Une part importante de chaque taille d'entreprise s'y trouve :

- 60% des ETI et grands groupes
- 75% des PME
- 94% des TPE

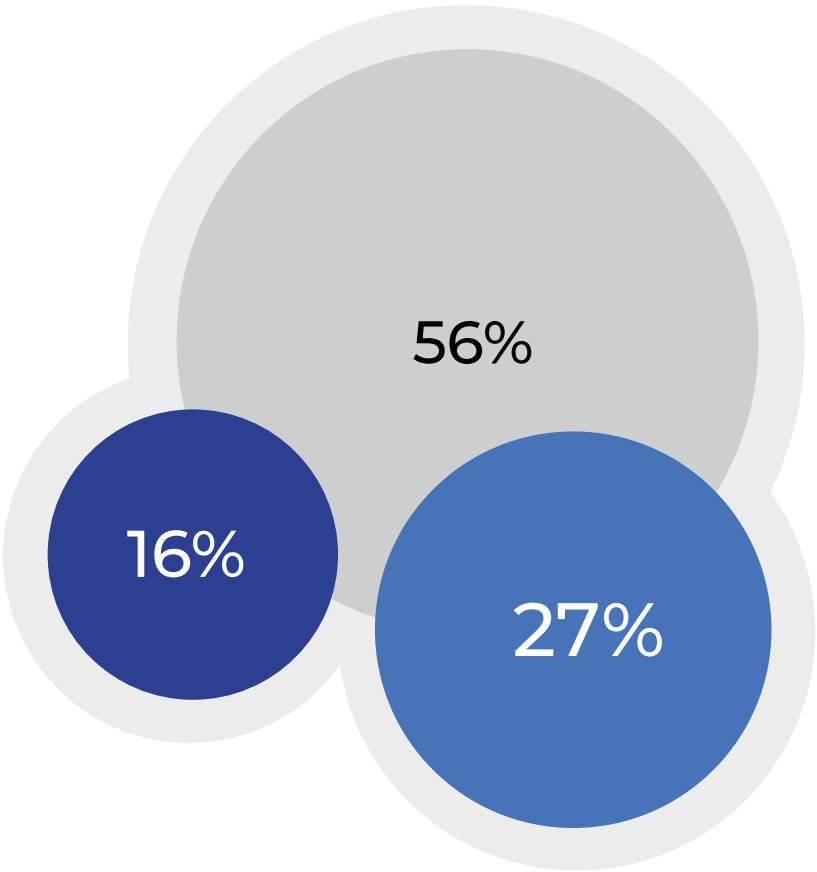
Un tiers de l'échantillon pourrait basculer au niveau supérieur avec un bon accompagnement et une mise en perspective du degré d'importance des mesures à mettre en place.

Les marges de progression

Du niveau critique vers l'essentiel
- Un inventaire priorisé
- Supervision et gestion de la cybersécurité (SOC)
- Un dispositif de sauvegarde externalisée et régulière

Traiter ces 3 axes permettrait à 27% du niveau critique de basculer au niveau essentiel.

Près d’un répondant sur 2 connaît le guide de l’ANSSI

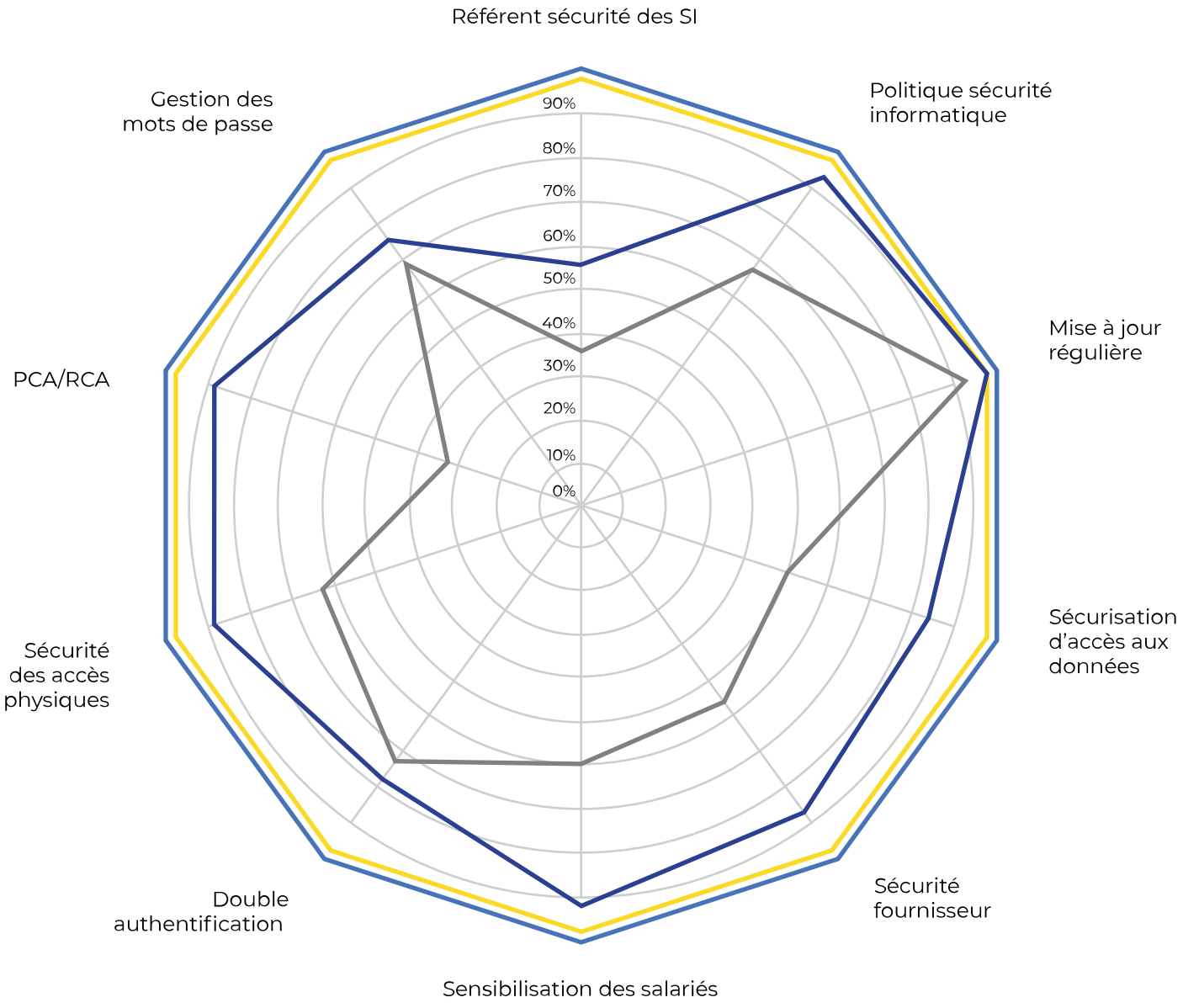


Base : 457 répondants

Nous constatons une nette progression de la notoriété du guide d’hygiène de l’ANSSI : 43% des entreprises interrogées le connaissent (+16 pts).

- Sans surprise, plus l’entreprise est grande, plus la fonction dirigeante connaît le guide de l’ANSSI et applique ses recommandations.
- A l’inverse, 9 TPE sur 10 et 7 petites PME sur 10 ne le connaissent pas.
- Les collectivités territoriales et établissements publics l’appliquent aussi davantage (+11 pts).

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*

- Niveau critique
- Niveau essentiel
- Niveau standard
- Niveau renforcé

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
Smara LUNGU, Stéphane INGRASSIA, Judith MEHL, Marion DUMESNIL

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, Antoine DERAIN

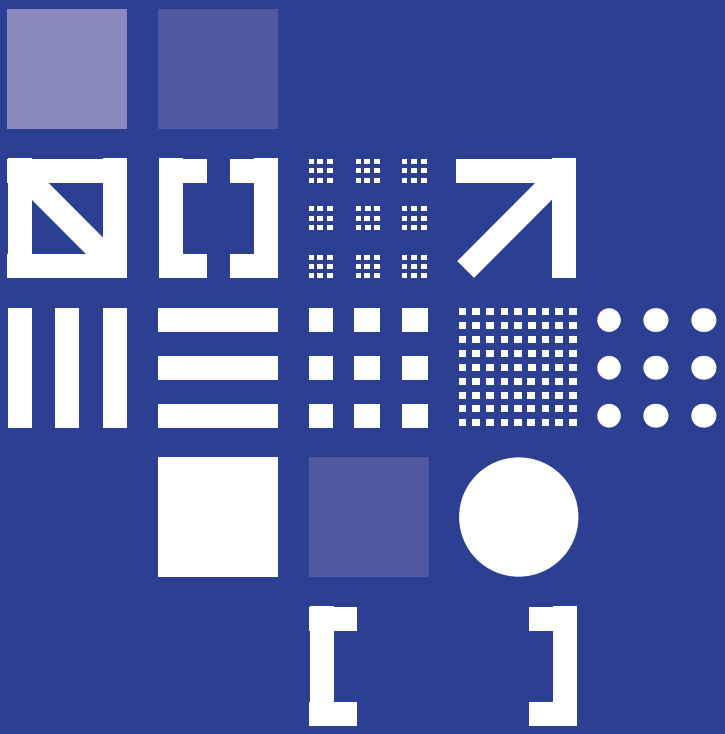
---

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