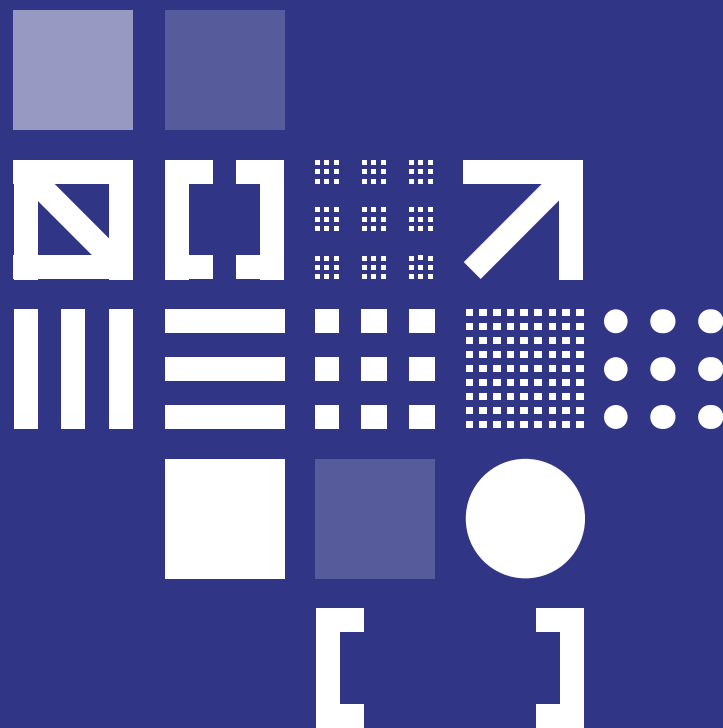




3^{ème} Édition

Baromètre de la cybersécurité 2025

Quelle maturité pour les entreprises françaises ?

L'édito



Olivier Vallet
Président Directeur Général



Si les usages numériques se diffusent massivement et ont désormais été intégrés à tous types d'organisations (entreprises de toute taille, Etat, collectivité...), les menaces cyber sont toujours plus fortes, plus rapides et plus industrialisées. En 2025, les rançongiciels restent massifs, tandis que le phishing et les malwares dopés à l'intelligence artificielle gagnent en crédibilité et en efficacité. Les grandes organisations ont consolidé leurs défenses, mais les écarts de maturité persistent : TPE, PME, ETI et collectivités, souvent limitées en ressources et en expertise, restent des cibles privilégiées.

Cette année, deux évolutions majeures sont à noter. D'une part, l'essor de l'IA élargit la surface d'attaque et impose de nouveaux réflexes de protection. D'autre part, l'intensification du cadre réglementaire – avec NIS2 et, pour certains secteurs, DORA – confirme que la cybersécurité est une condition de résilience, de continuité d'activité et de confiance, portée au plus haut niveau de gouvernance.

Cette troisième édition du baromètre, co-réalisée entre Docaposte et Cyblex Consulting, mesure les progrès, souligne la prise de conscience grandissante et l'importance croissante accordée à la souveraineté, mais rappelle aussi l'urgence : la menace ne faiblit pas. Ensemble, faisons de la cybersécurité un socle commun de confiance pour toutes les organisations françaises.



Christophe Vendran
Directeur Général



Trois ans après le lancement de ce baromètre, une chose est claire : le risque cyber n'est plus un sujet émergent, mais est un paramètre structurel du quotidien des organisations françaises. Les dépendances numériques se multiplient, les attaques se professionnalisent, les exigences réglementaires se renforcent... et au milieu de cette pression croissante, chacun doit arbitrer, prioriser, et surtout tenir dans la durée.

Cette 3e édition va au-delà de la simple photographie. Ces trois années de recul permettent désormais de mettre en lumière des tendances, de distinguer ce qui progresse réellement, ce qui stagne, voire ce qui recule. Nous voyons se dessiner un écart persistant entre la prise de conscience des risques, désormais largement partagée, et la capacité à mettre en place des actions concrètes, en particulier pour les TPE et PME, qui demeurent très exposées faute de moyens, qu'ils soient financiers ou humains.

Co-réalisé par les équipes de Cyblex Consulting et de Docaposte, ce baromètre de la cybersécurité se veut avant tout être un outil constructif qui dresse un état des lieux précis des menaces, permet de comprendre les évolutions et où concentrer les efforts pour permettre le développement d'une défense plus efficace, adaptée à ses enjeux et à ses capacités. La cybermaturité se construit dans le temps, notamment par des choix assumés et des investissements cohérents.

La cybersécurité est avant tout une responsabilité collective. En mettant à disposition ces enseignements riches, nous souhaitons contribuer à une meilleure compréhension des risques, mais aussi à la diffusion de bonnes pratiques. Ensemble, bâtissons un monde numérique plus résilient.

Un baromètre national pour mesurer l'évolution de la cybermaturité 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 cybermenaces, 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 cyberrisques.

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 cybermaturité des dirigeants et décideurs** français et d'en suivre l'évolution.

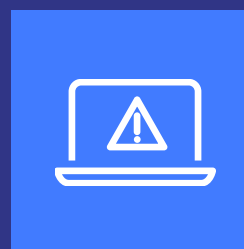
→ Sur la base d'un entretien téléphonique articulé autour d'une vingtaine de questions, trois thématiques sont abordées dans l'objectif d'appréhender la cybermaturité du décideur interrogé.



La connaissance des mesures mises en œuvre



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



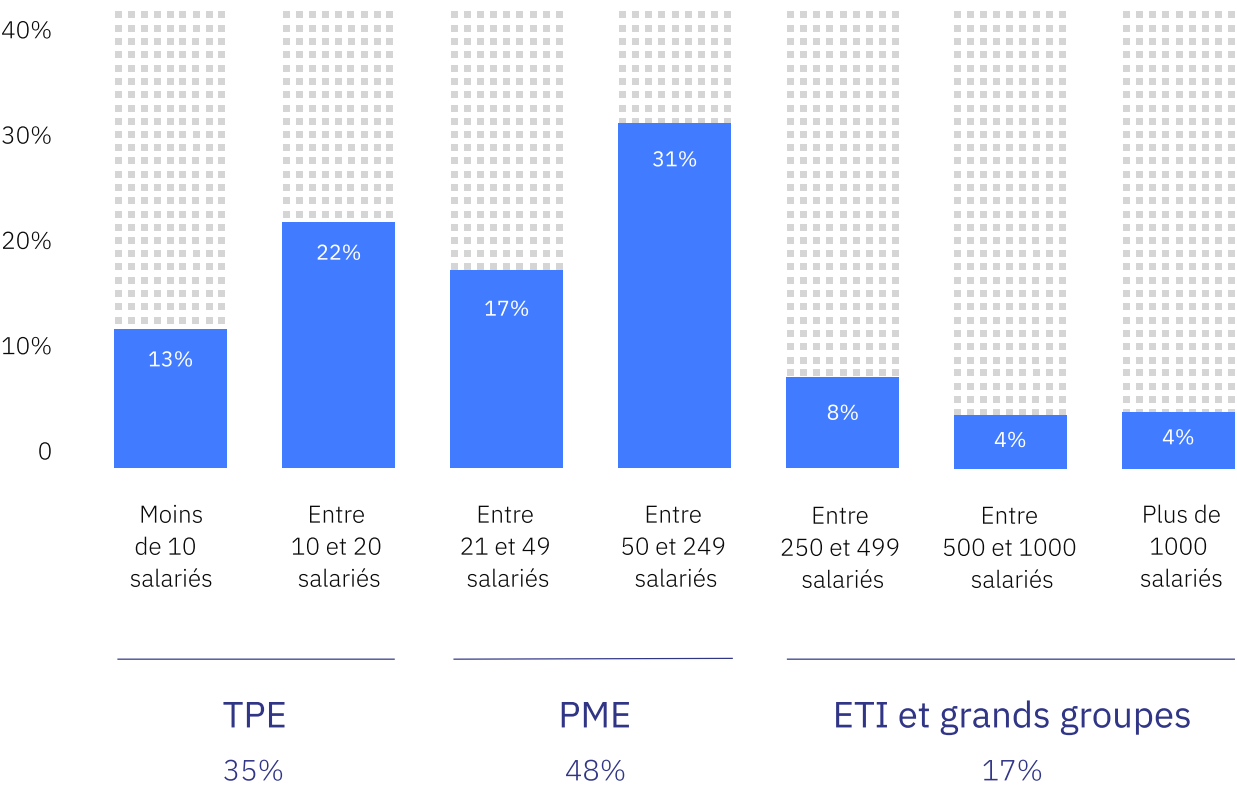
La perception du niveau de risque

L'échantillon de notre enquête

Le périmètre de l'enquête

Les PME sont majoritaires dans cette étude : **1 répondant sur 2.**

1/3 des personnes interrogées représentent une TPE.



Secteur d'activité

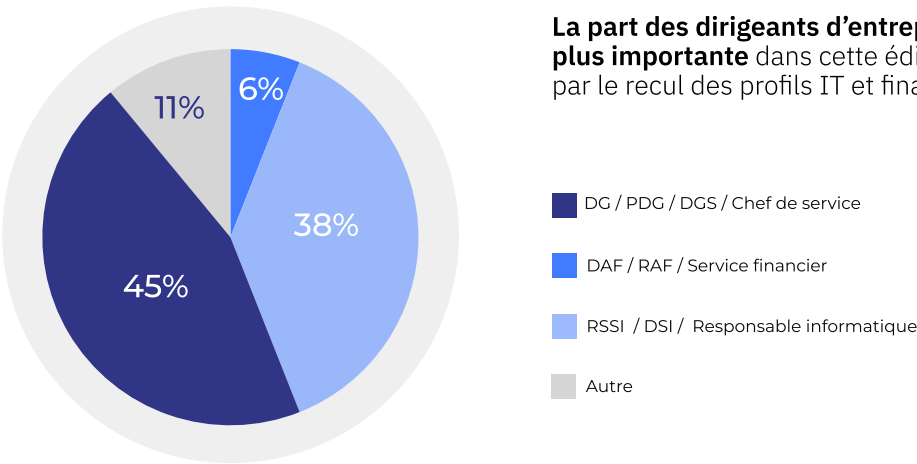
Cette année, une part plus importante a été accordée **aux acteurs du secteur public**.

Ainsi, avec 26% des répondants, cet échantillon permet une **analyse de ces organisations beaucoup plus solide**.



Fonction

La part des dirigeants d'entreprise est plus importante dans cette édition, portée par le recul des profils IT et financiers.



Executive summary - Quelques chiffres clés

→ Attaques

30% des organisations ont déjà subi une cyberattaque.

Les 3 attaques les plus récurrentes sont :

- Phishing (Hameçonnage)
- Ransomware (Rançongiciel)
- Vol et/ou perte de données

→ Management du risque

1/3 des répondants connaissent et appliquent les recommandations de l'ANSSI (+15pts).

Les répondants les plus informés sur les enjeux cyber sont issus de l'IT et des ETI.

91% des organisations estiment leur investissement en cybersécurité satisfaisant.

Une majorité d'organisations ont un budget en hausse.

3/4 des entreprises estiment faire suffisamment d'efforts en termes de cybersécurité.

Le sentiment d'exposition modéré entraîne une stabilisation des efforts budgétaires et organisationnels.

→ Organisation

65% des répondants font appel à une ressource externe pour être conseillés en cybersécurité.

La part de référents SSI (sécurité des SI) nommés en interne diminue (-11pts).

80% des organisations sont satisfaites ou très satisfaites de leur solution privilégiée (ressources internes ou partenariats externes)

1/2 répondant estime que la prise de conscience des enjeux cyber passe par des solutions et procédures imposées par le service IT.

→ Les écarts majeurs avec l'édition précédente

I

2x

plus d'organisations appliquent les recommandations du guide de l'ANSSI (+15pts).

II

+15%

des attaques subies étaient du phishing (+5pts).

III

41%

des répondants ont stabilisé leur budget de cybersécurité cette année. Cela représente 15% de plus que l'année précédente. (+10pts)

IV

+40%

ont été impactés par un vol et/ou une perte de données à la suite d'une cyberattaque (+6pts).

V

IT & DSI

sont les métiers de plus en plus impliqués dans les enjeux cyber. (+17pts).

VI

34%

des répondants nomment un référent SSI. Cela représente 25% de moins que l'année précédente (-11pts)

Le secteur public, plus inquiet mais aussi plus mature

→ Les acteurs publics allouent à la sécurité des systèmes d'information un budget supérieur aux entreprises : +15pts pour ceux qui déclarent un budget supérieur à 10K€/an.

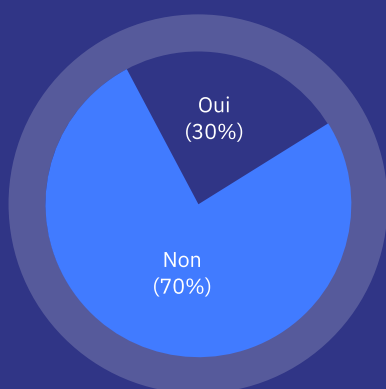
→ Le risque d'une attaque réussie est jugé plus élevé dans le secteur public que parmi les entreprises (+14pts). Alors que des deux, le secteur public déclare être moins attaqué (-5pts).

→ Les ressources extérieures sont davantage mobilisées dans le secteur public. C'est une cible qui accorde beaucoup d'importance à l'usage des systèmes souverains. (+18 pts)

→ Les acteurs publics surpassent de 14pts les entreprises en termes de connaissance et d'application des recommandations du guide d'hygiène de l'ANSSI.

Cyberattaques : des risques inégaux selon la taille des entreprises

→ Le nombre d'organisations ayant subi une cyberattaque n'a pas évolué depuis l'édition précédente.

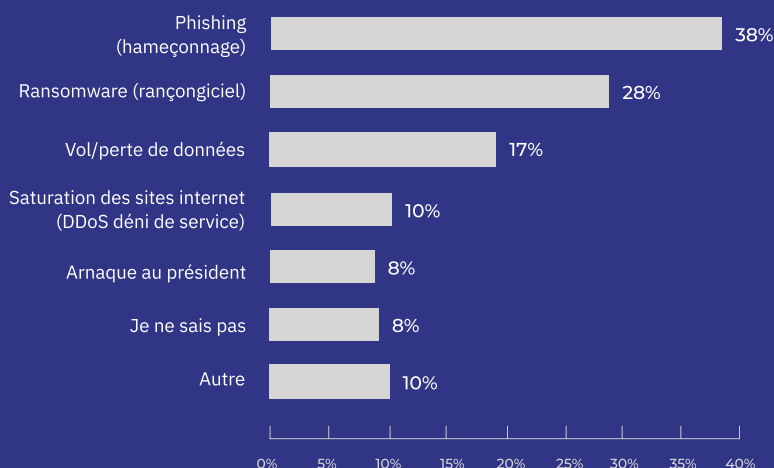


Focus géographique :

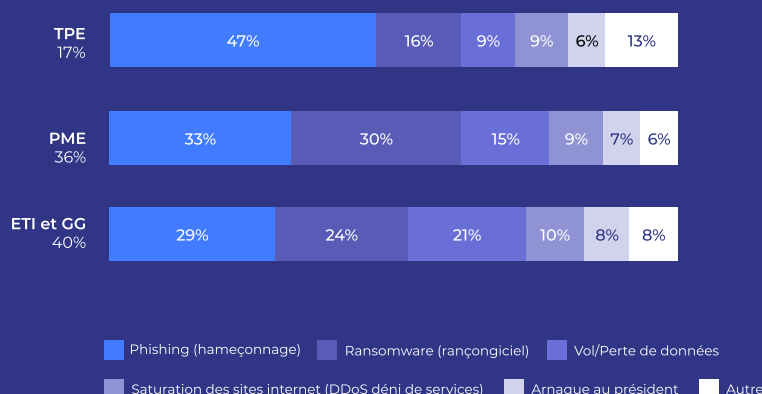
- Ile-De-France : 40%
- Sud-Est : 35%
- Nord-Ouest : 32%
- Sud-Ouest : 25%
- Nord-Est : 25%

La typologie des attaques n'a pas bougé depuis 2023 et la tête de liste est identique.

On retrouve une cohérence entre les types d'attaques et les craintes des répondants.



Focus sur les tailles d'organisation



Peu importe la taille des organisations, la hiérarchie des attaques subies est quasi identique.

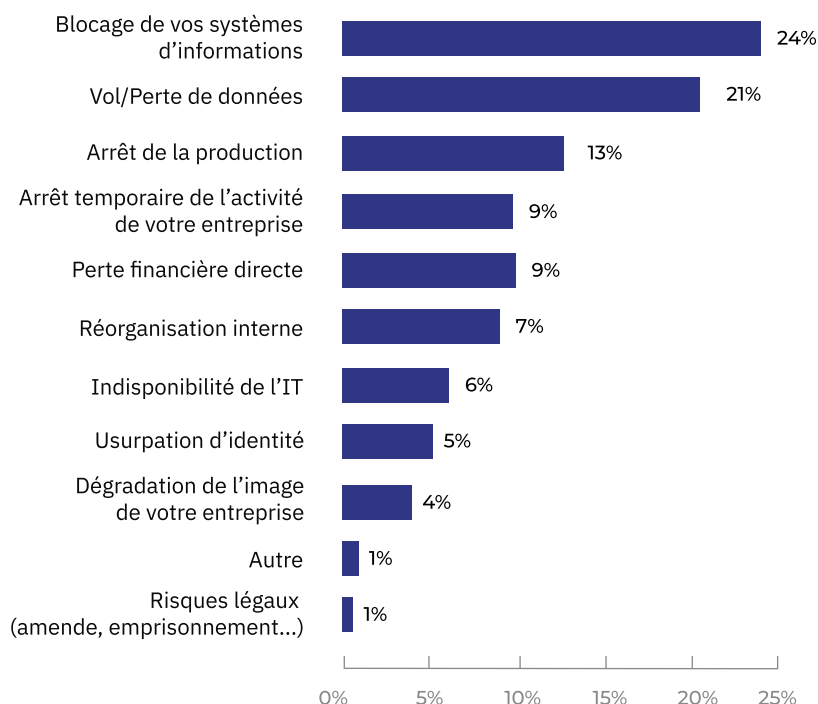
Le Phishing concerne presque 1 TPE sur 2.

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

Les 3 conséquences principales restent inchangées, et s'ancrent davantage :

- Blocage des systèmes d'information(+6pts)
- Vol et/ou perte de données (+6pts)
- Arrêt de la production (+3pts)

50% des organisations ont pu maîtriser leur attaque sans impact.



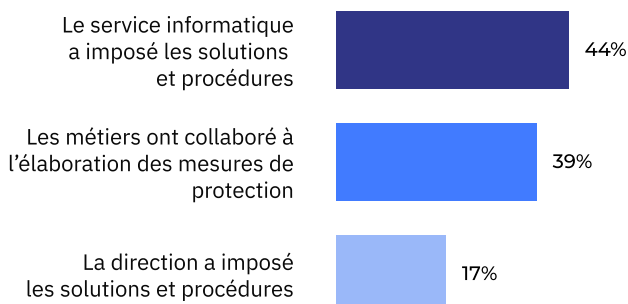
L'implication des métiers en progression pour une meilleure gestion du risque

Alors que le service informatique reste l'acteur majeur en termes de prise de conscience des enjeux cyber, **la coopération entre la DSI et les métiers progresse (+17pts)**. C'est un critère important concernant la maturité des organisations.

À l'inverse, l'implication de la direction est beaucoup moins citée cette année (-14pts).

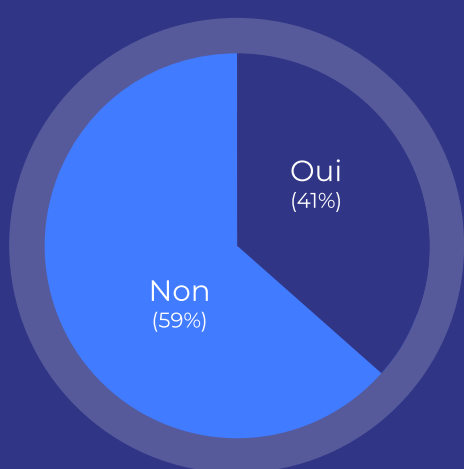
TPE : Les efforts de la direction, et surtout la collaboration, prennent largement le dessus sur le service IT.

- TPE : 15% IT / 57% collaboration
- PME : 53% IT / 33% collaboration
- ETI : 66% IT / 26% collaboration



Une évaluation de la menace et de l'exposition au cyberrisque qui varie selon les profils : taille, secteur, poste occupé

→ **41% estiment être une cible potentielle de cyberattaque**



Le sentiment d'exposition reste identique à 2024.

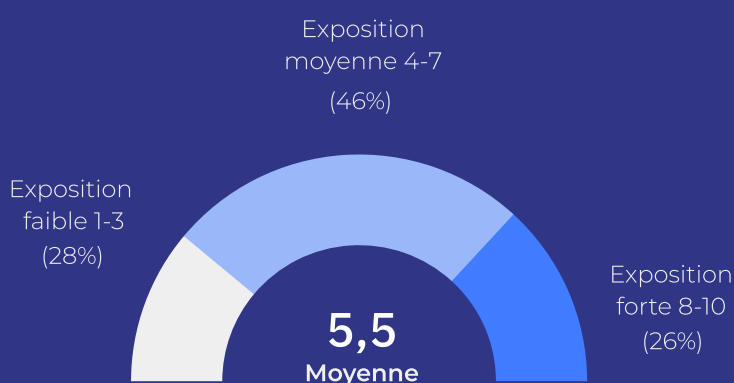
Les spécialistes IT sont les plus conscients du risque lié à leur activité : ils sont 54% (+6pts) à répondre OUI, contre 30% de DG.

50% des acteurs publics se sentent pris pour cible, cela concerne 37% des entreprises.

Le top 5 des secteurs qui se sentent le plus ciblés :

- Information, communication et digital : 62%
- Informatique et Télécoms : 60%
- Activité financière et d'assurance : 50%
- Activités et services administratifs de soutien : 49%
- Santé et action sociale : 47%

1 organisation sur 4 se sent très exposée



Le sentiment d'exposition faible gagne 9 points, alors que le sentiment d'exposition fort passe au second plan.

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

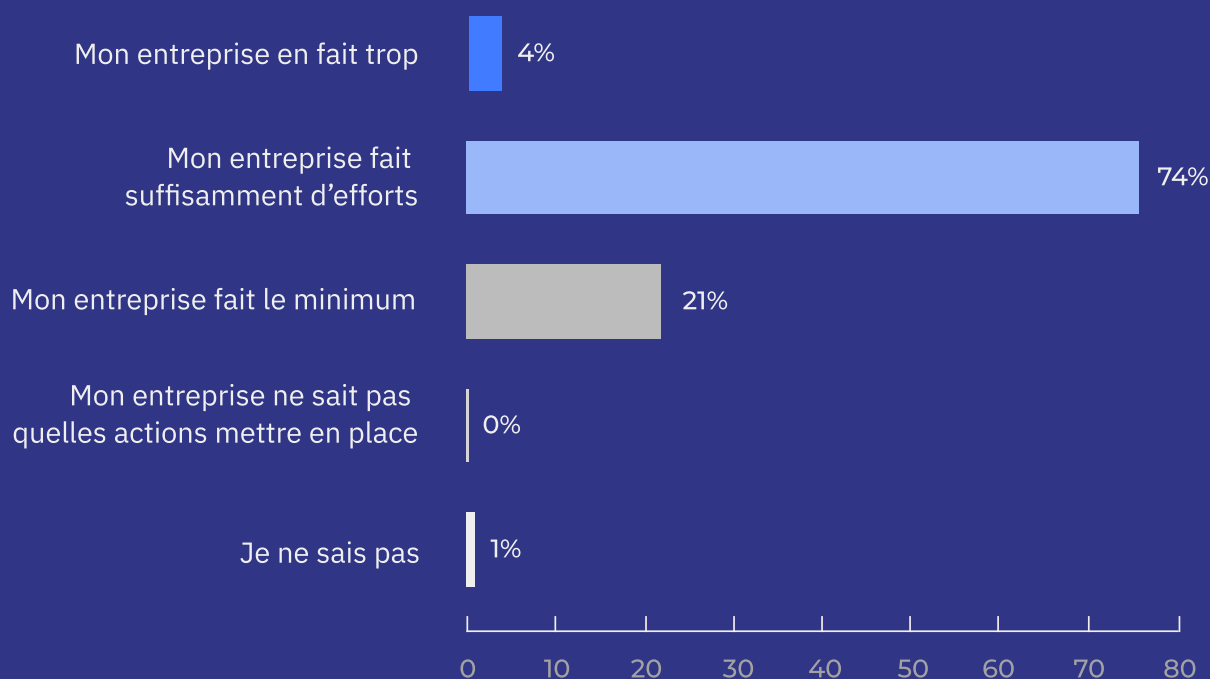
- 15% des TPE (moyenne 4,4/10)
- 28% des PME (moyenne 5,8/10)
- 45% des ETI (moyenne 6,7/10) : 3 fois plus inquiètes que les TPE (2 fois en 2024)

Du côté des individus : **19% des DG** estiment faire face à une exposition forte contre **36% des RSSI**.

En France, les organisations fortement inquiètes sont majoritaires dans le Nord-Ouest et dans le Sud-Est.

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

➔ **74% des entreprises pensent faire suffisamment d'efforts**



Même si elles sont 1 sur 3 à se sentir fortement exposées, **3 organisations sur 4 estiment fournir suffisamment d'efforts et ont confiance en leurs moyens déployés en termes de cybersécurité.**

2 croissances à observer :

- Le nombre de grandes entreprises qui estiment faire trop d'effort (+11pts)
- Le nombre de TPE qui déclarent en faire le minimum (+4pts)

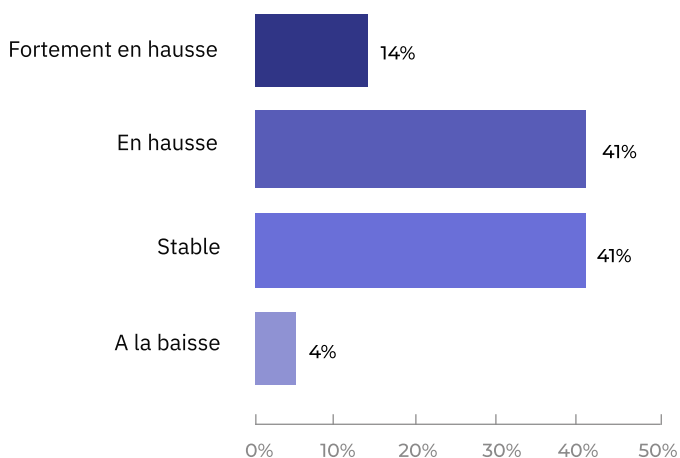
Des investissements jugés en hausse pour 55% des répondants

La croissance globale des budgets concerne une organisation sur deux. Les budgets "fortement en hausse" concernent davantage d'organisations cette année (+6pts).

Ils sont plus nombreux à stabiliser leur budget en 2025 (+10pts).

Plus l'organisation est grande, plus l'évolution est à la hausse.

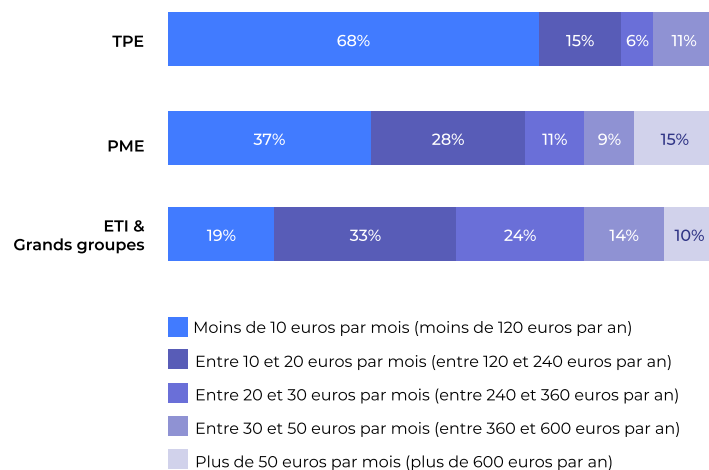
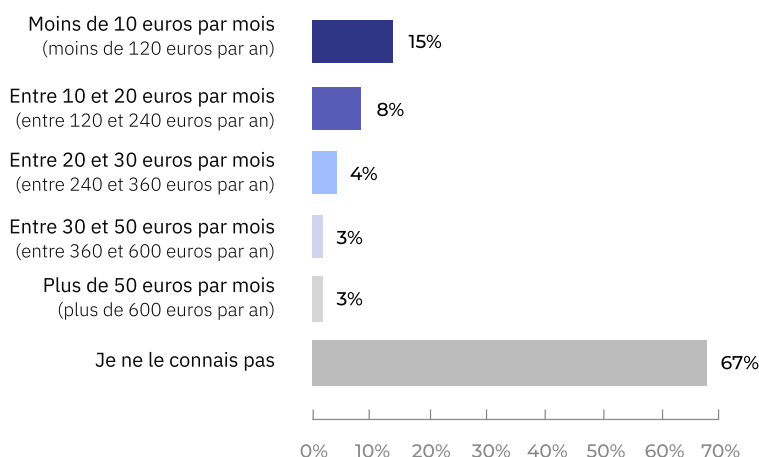
Les TPE sont deux fois plus nombreuses que les PME ou ETI à avoir stabilisé leur budget : +14pts de la moyenne.



Des dépenses par salarié et par mois restent stables autour des 10€

En 2025, la majorité des répondants se situe toujours dans la fourchette basse de moins de 10€ par mois par salarié.

Le détail du budget pour la cybersécurité n'est connu que par 34% des répondants.



Le détail du budget pour la cybersécurité est semblable à la répartition du budget global pour la sécurité des SI. **Plus l'organisation est grande, plus le budget est grand :**

- 83% des TPE dépensent moins de 20€ par salarié et par mois.
- Les ETI sont autant à dépenser au-dessus qu'en-dessous de 20€ par mois.

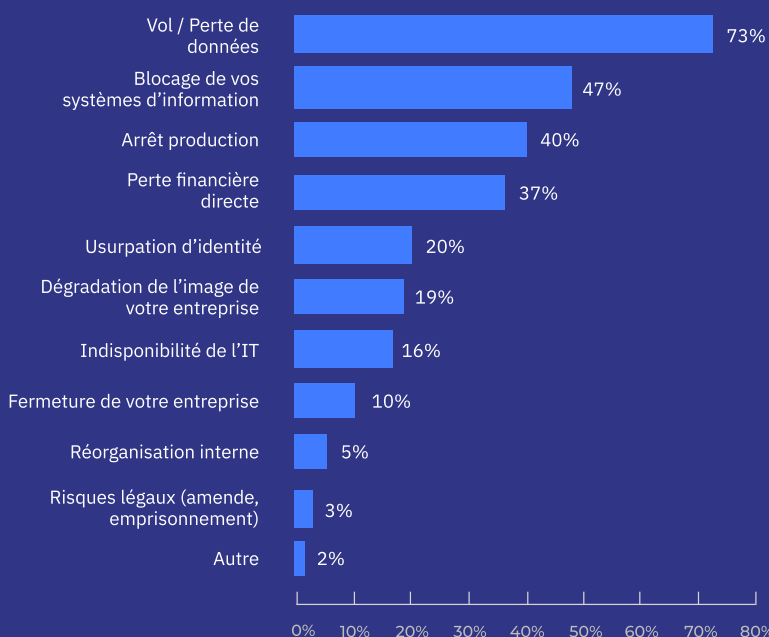
Des craintes ainsi que des démarches mises en oeuvre qui varient en fonction de la taille de l'organisation

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

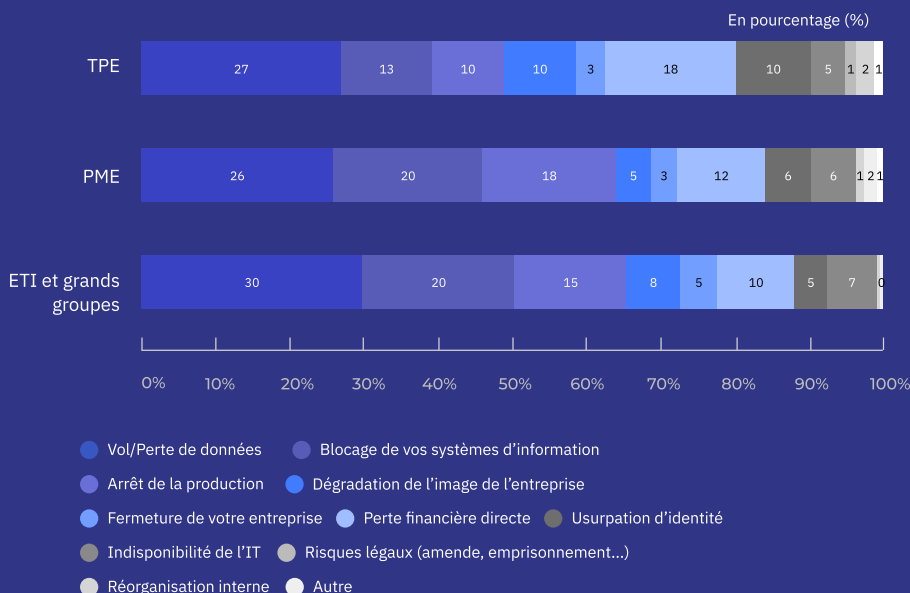
Le vol et/ou la perte de données creuse à nouveau l'écart avec les autres craintes exprimées par les répondants (+26pts vs 7pts en 2024). Elle a été citée par 3 répondants sur 4.

Les autres risques relevés sont toujours très ventilés.

Quelques évolutions de citation par rapport à 2024, mais la hiérarchie des craintes reste identique.



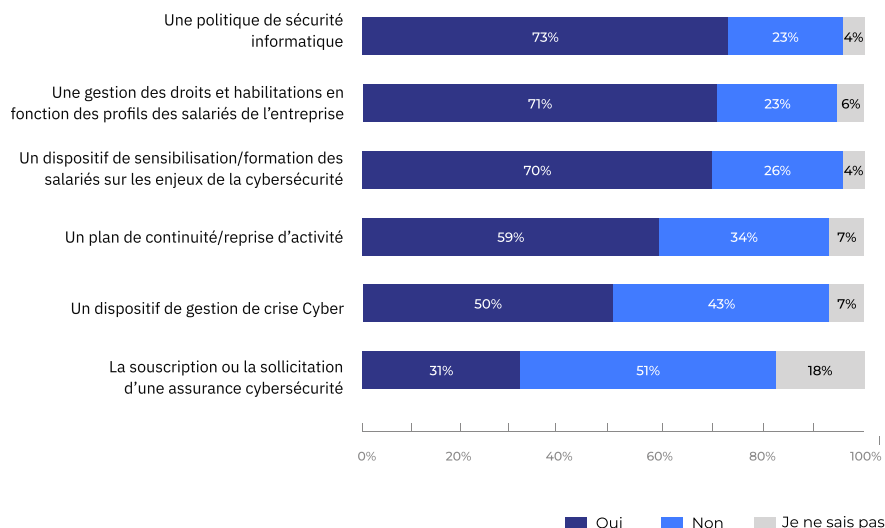
Pour les TPE, la hiérarchisation des impacts est différente : le risque de perte financière a une place non négligeable



Alors que la répartition des réponses des PME et des ETI est très similaire et principalement axée sur le top 3, **Les TPE ont d'autres préoccupations :**

- La perte financière inquiète ces organisations au point d'être en 2e place (4e place pour les PME et ETI)
- L'usurpation d'identité a été aussi notablement citée et occupe la 4e place.
- La dégradation de l'image de l'entreprise est une crainte importante pour les TPE (2 fois plus que les autres profils)

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



La hiérarchisation des actions est identique à 2024, le top 3 se distingue des autres.

3 démarches sont en progression :

- Un plan de continuité/reprise d'activité (+8pts)
- Un dispositif de gestion de crise cyber (+7pts)
- Un dispositif de sensibilisation des salariés (+3pts)

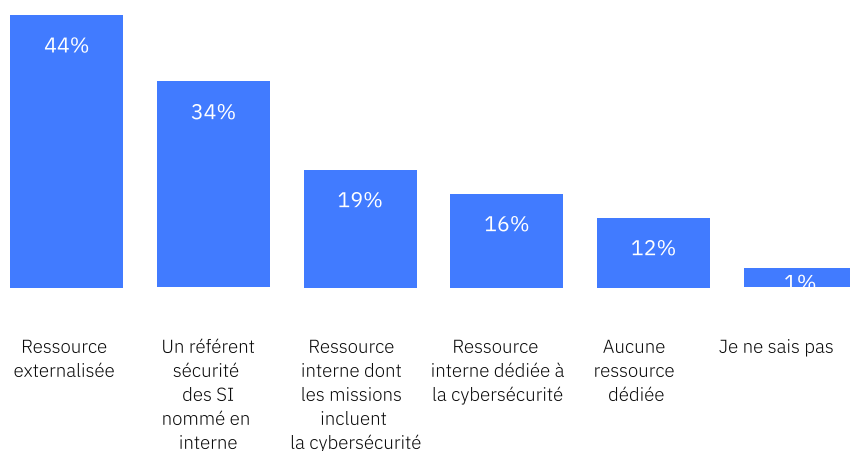
La souscription à une assurance cybersécurité est très en retrait pour tous les profils.

D'un point de vue sectoriel : les acteurs publics sont en avance sur les autres secteurs (le top 3 est réalisé au moins à 75%).

Une organisation sur trois a désigné un référent SSI pour mettre en place ces démarches

La prise de conscience qui semblait émerger l'année dernière perd quelque peu ses indicateurs.

- Malgré les recommandations de l'ANSSI, on observe une diminution de la part des référents SSI nommés en interne (-11pts)
- La part de ressources externalisées a aussi notablement diminué cette année (-22pts)
- Il y a 12% de répondants qui n'ont aucune ressource dédiée (+8pts) : on y retrouve principalement des TPE et les profils de DG.



Des actions et solutions concrètes ont été mises en place

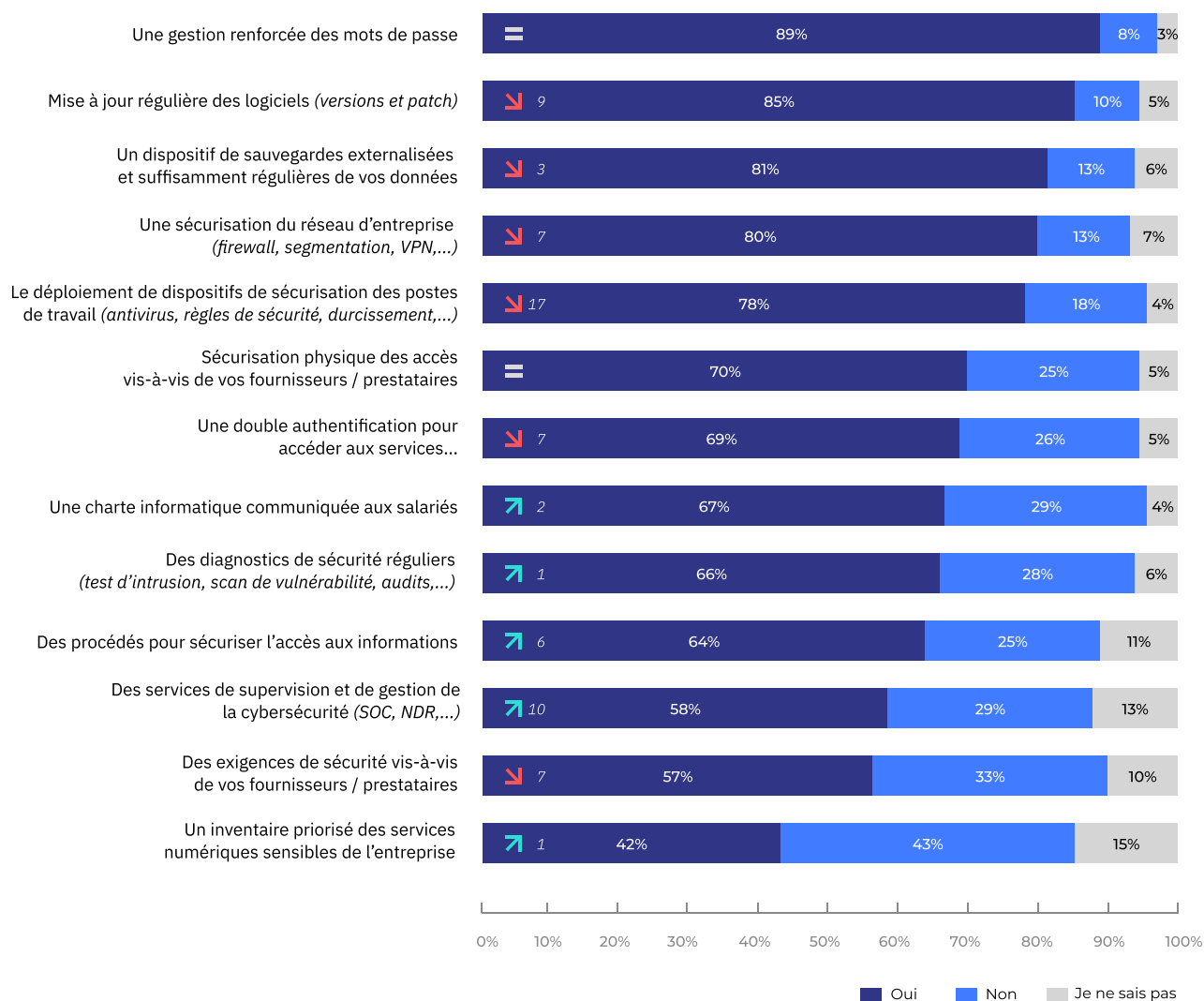
Le top 3 des actions et solutions mises en place :

- Une gestion renforcée des mots de passe
- Une mise à jour régulière des logiciels
- Un dispositif de sauvegardes externalisées et régulières des données (nouveau dans le top 3)

6 actions sur les 13 proposées voient une diminution par rapport à l'année dernière :

- Mise à jour des logiciels
- Un dispositif de sauvegardes externalisées
- Une sécurisation du réseau
- La sécurisation des postes de travail
- Une double authentification
- Des exigences de sécurité vis-à-vis des fournisseurs

Les répondants au profil IT déclarent mettre davantage d'actions en place, surtout celles pour lesquelles les managers avouent ne pas savoir si l'entreprise l'a mise en place ou pas.

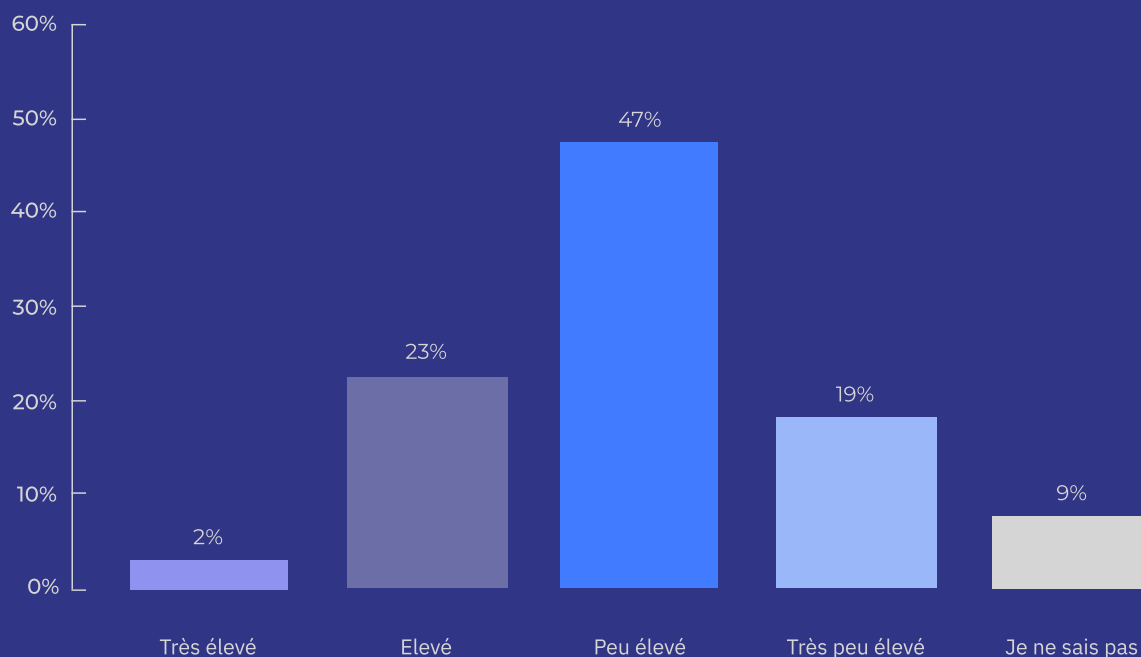


Pour 2 répondants sur 3, le risque serait moins important grâce à la mise en œuvre d'actions concrètes

➔ **Presque 1 organisation sur 2 estime le risque d'une cyberattaque réussie comme peu élevé**

Cette perception est cohérente avec un sentiment d'exposition globalement modéré (5,5/10), les répondants ne sont pas alarmés par le risque cyber. Cela explique aussi la part des démarches mises en places qui a peu évolué depuis 2024.

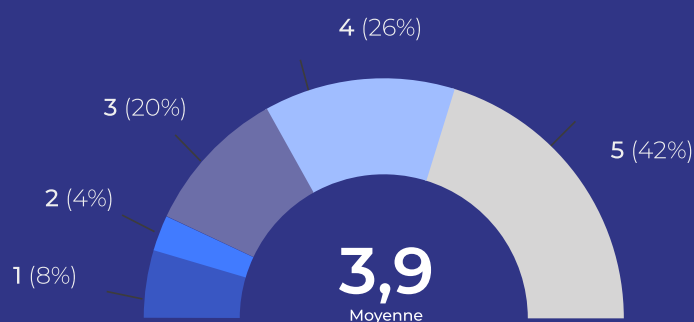
1/4 des organisations y voient toujours un risque important.
Parmi les profils pour qui les mesures appliquées ne sont pas suffisantes, on retrouve : les responsables IT (31% risque élevé et très élevé), les acteurs publics (37%) et les ETI (35%).



L'usage de systèmes souverains est un critère de plus en plus important pour les acteurs publics

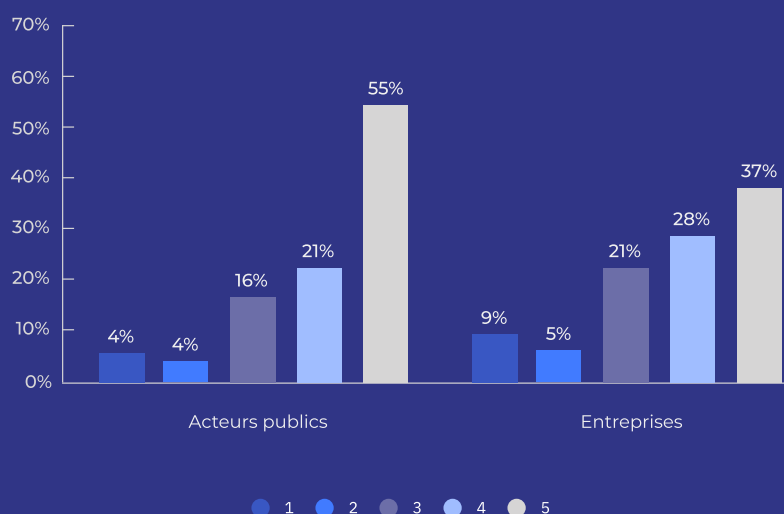
➔ Néanmoins 68% des entreprises situent l'importance de l'usage de systèmes souverains à 4/5 voire plus

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



Pour rappel, la proportion de la note 5/5 a doublé par rapport à 2023.

Une disparité est notée sur les tailles d'organisations : la note de 5/5 est attribuée par 55% des répondants représentant une ETI et 37% de répondants issus d'une TPE (PME 42%).



Les acteurs publics accordent une plus grande importance à l'usage de systèmes souverains : ils sont 55% à attribuer la note de 5/5 à ce sujet.

A l'inverse, les entreprises qui avaient gagné en maturité l'édition précédente ne sont que 37% à attribuer 5/5.

La moyenne par secteurs oscille entre 4,2 (+0,1) et 3,8 (-0,1)

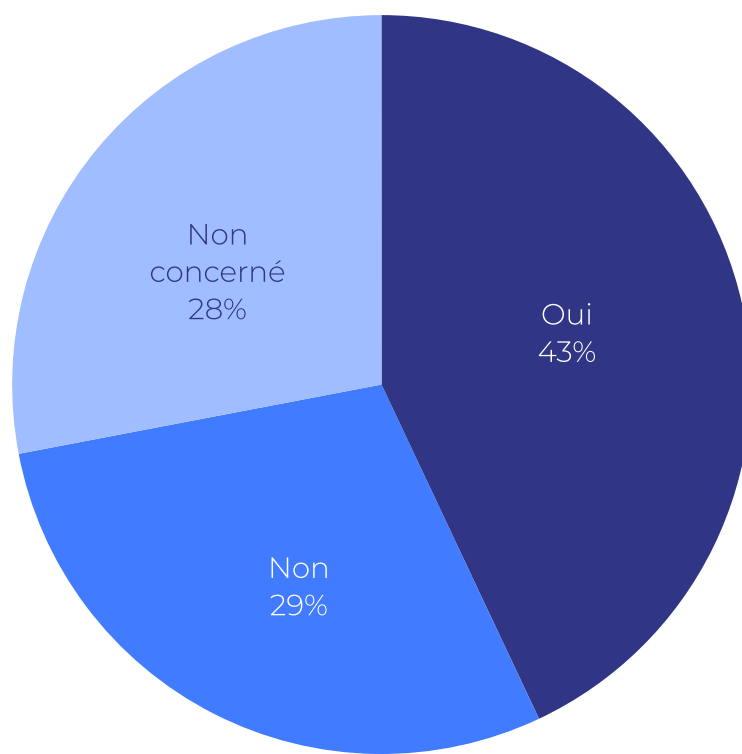
Les solutions packagées proposées par les partenaires sont préférées

43% des répondants préfèrent une solution packagée pour lutter contre les cyberattaques.

Parmi les répondants qui se sentent concernés (ayant répondu « Oui » ou « Non »), plus de 60% préfèrent une solution packagée.

Ce sont des solutions privilégiées par les petites organisations, qui ont tendance à davantage externaliser leurs ressources.

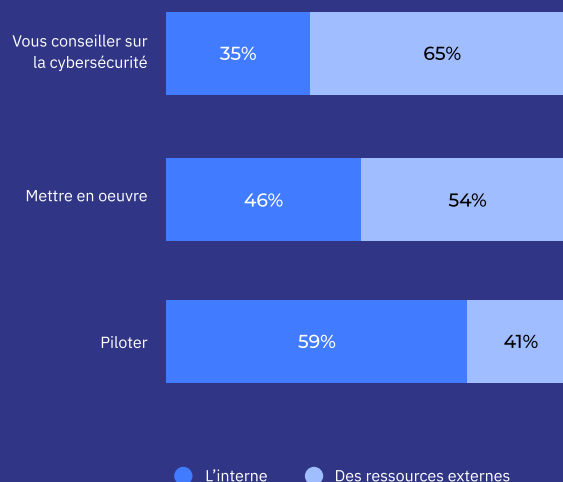
- TPE : 66% OUI
- PME : 62% OUI
- ETI : 42% OUI



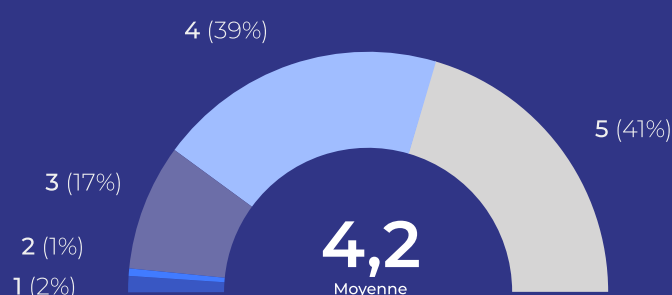
Alors que le conseil est externalisé, le service interne est privilégié pour le pilotage des actions

- Les organisations font davantage appel à des ressources externes pour chercher du conseil sur la cybersécurité.
- La mise en œuvre est partagée et notamment externalisée pour les petites organisations (60%).
- Lorsqu'il s'agit de pilotage, elles sont une majorité à internaliser les pratiques.

Les réponses sont dissonantes en fonction du poste occupé. **Les responsables IT déclarent davantage internaliser ces pratiques : +10pts** par rapport aux résultats globaux et aux réponses des DG pour chacune des missions.



➔ Partenaires ou solutions internes, la satisfaction semble unanime



Le taux de satisfaction concernant le prestataire ou la solution choisie est très bon : moyenne de 4,2/5. (idem en 2024)

La satisfaction est commune à tous les répondants, la taille, le secteur et le poste occupé n'ont pas d'influence sur le résultat.

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 leurs 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.

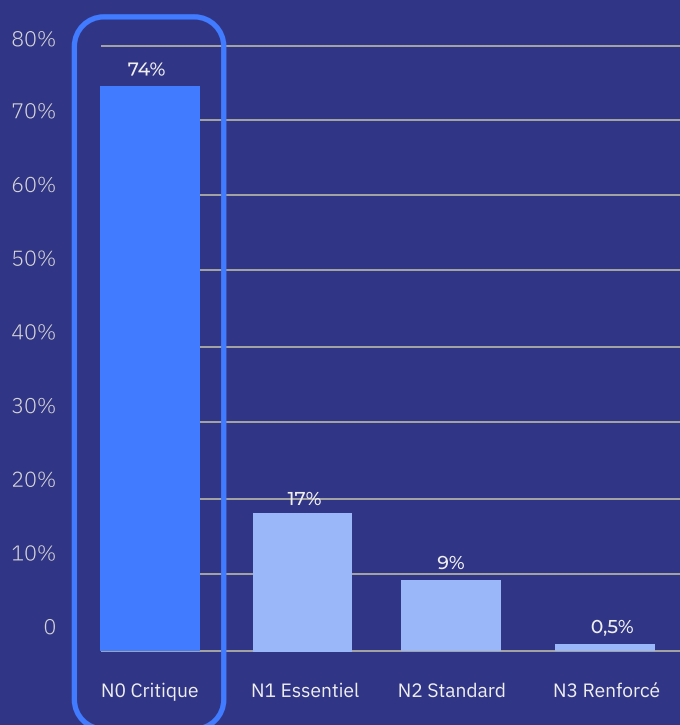


L'appellation "non atteint" indique que moins de la moitié des actions du niveau a été réalisée.

Cela nous permet de mieux évaluer les entreprises qui sont proches de basculer au niveau supérieur : celles qui ont rempli partiellement les actions du niveau supérieur.

Un niveau de maturité des organisations stable avec un fort potentiel d'amélioration

➔ **74% des entreprises françaises n'appliquent pas les pratiques pour atteindre le niveau essentiel recommandé par l'ANSSI :**



Elles ne sont actuellement pas suffisamment protégées.

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.

On constate sans surprise que plus l'organisation est petite, et plus elle est au niveau Critique.

Une part importante des organisations reste toujours au niveau Critique.

- 90% des TPE (-4pts /2024)
- 69% des PME (-6pts /2024)
- 57% des ETI (-3pts /2024)

Les marges de progression

Du niveau Critique vers l'Essentiel :

- Un dispositif de gestion de crise cyber
- Un inventaire priorisé des services numériques sensibles
- Un dispositif de sauvegardes externalisées et régulières des données

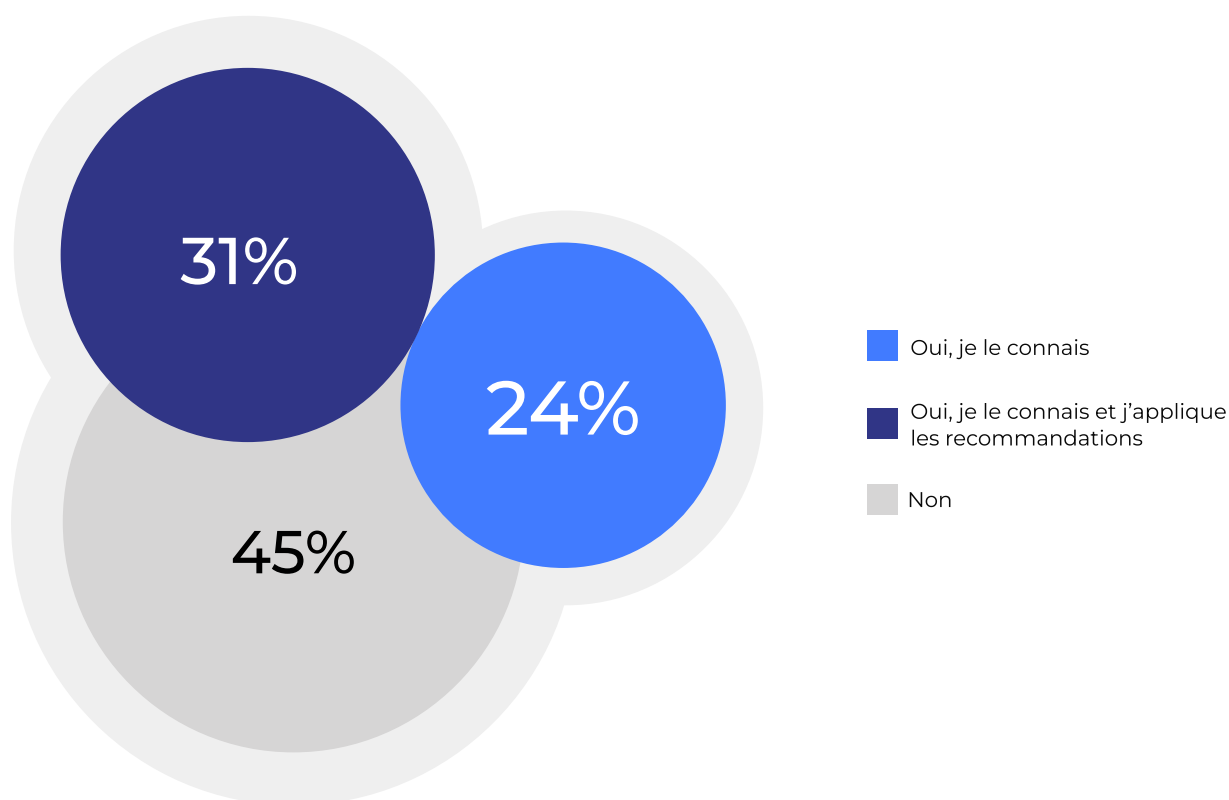
➤ Traiter ces 3 axes permettrait à 30% du niveau Critique de basculer au niveau Essentiel.

Du niveau Essentiel vers le Standard :

- La nomination d'un référent sécurité des SI
- Une gestion des droits et habilitations en fonction des profils
- La sécurisation physique des accès aux zones sensibles

➤ Traiter ces 3 axes permettrait à 60% du niveau Essentiel de basculer au niveau Standard

1/3 des répondants connaissent et appliquent le guide de l'ANSSI, 2 fois plus qu'en 2024.



En 2025, non seulement la notoriété du guide de l'ANSSI progresse mais il y a aussi une nette évolution de l'application de ses recommandations : on passe de 16% à 31% (+15pts).

On note que 1 responsable IT sur 2 connaît et applique les recommandations. C'est aussi le cas de 60% des ETI (35% des PME et 11% des TPE) .

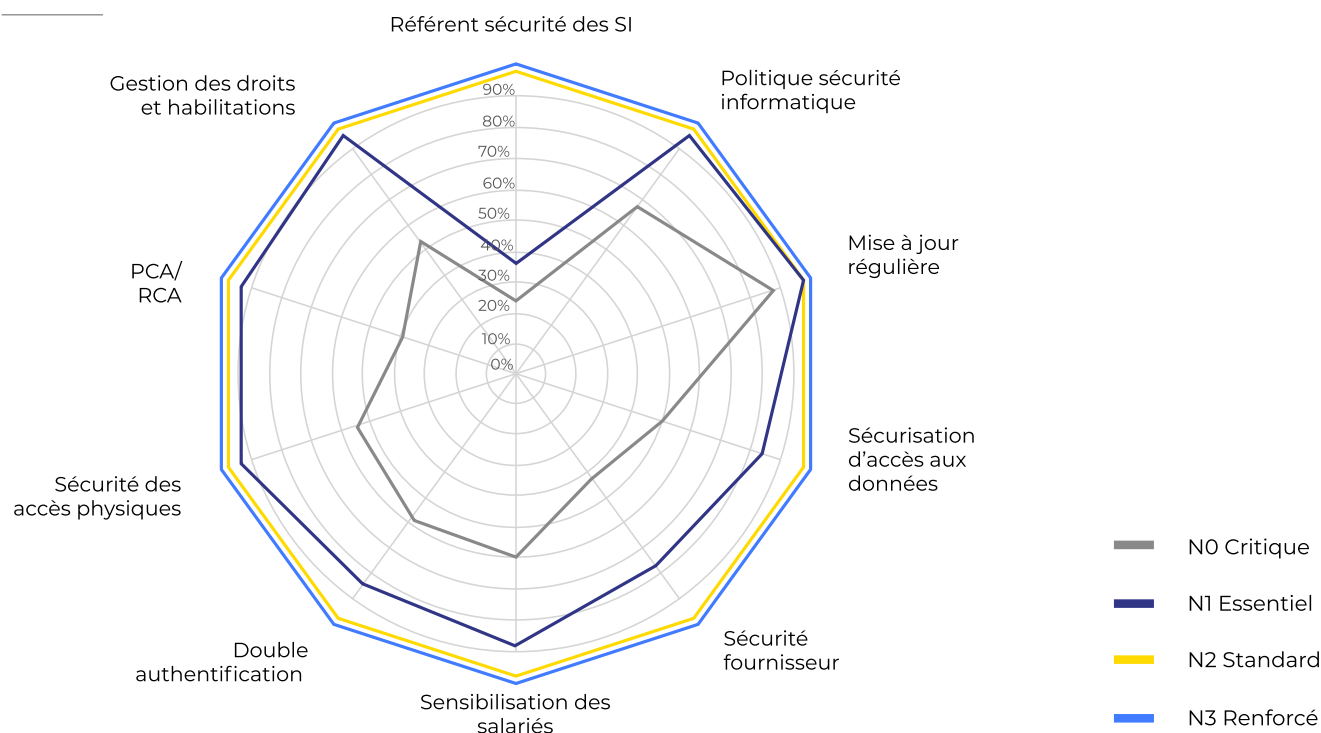
Le guide de l'ANSSI est davantage connu et surtout appliqué par les acteurs publics (+14pts). On observe cette application à travers la mise en place des actions recommandées.

Parmi les entreprises qui répondent toujours "Non", on retrouve 72% de TPE et 58% de fonctions dirigeantes, ce sont les profils les moins en éveil sur ce sujet.

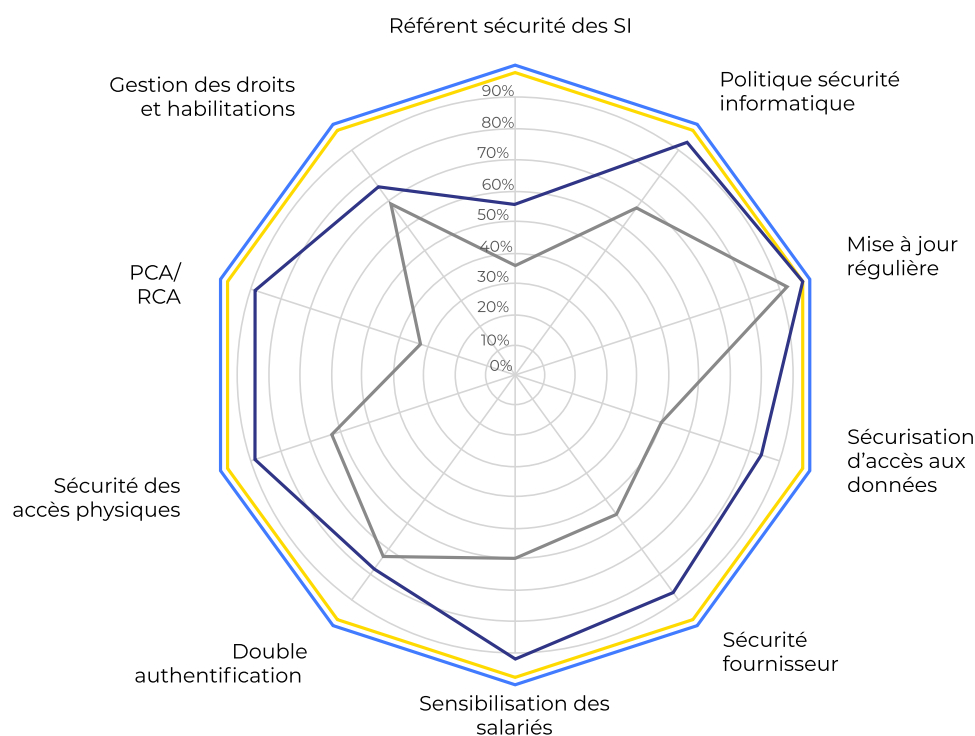


Le radar de maturité montre néanmoins de gros écarts entre les entreprises du niveau Critique et les autres

2025



Rappel 2024



Hormis le plan de continuité/ de reprise d'activité qui enregistre une légère hausse (+6pts), on constate une régression sur les autres axes du niveau Critique.

Le niveau Essentiel progresse globalement mais l'axe du référent sécurité SI diminue de 19pts.



Filiale numérique du groupe La Poste et référent de la confiance numérique, Docaposte accompagne les entreprises et institutions publiques dans leur transformation sur trois marchés prioritaires : le secteur public, la santé et la finance. Éditeur de logiciels et de solutions numériques de confiance, intégrateur et opérateur de plateformes et expert en conseil data-IA, Docaposte s'appuie sur ses propres briques technologiques et ses actifs dans le cloud, la cybersécurité et l'IA pour concevoir, développer et opérer des parcours numériques complets centrés sur l'expérience client, dans le respect des réglementations les plus exigeantes et avec un haut niveau de protection des données.

Leader des solutions de confiance (signature et vote électroniques, archivage numérique), premier opérateur de données de santé (49 millions de dossiers médicaux) et de données scolaires (18 millions d'utilisateurs de Pronote), Docaposte dispose d'un positionnement unique sur le marché, alliant souveraineté technologique et intérêt général et s'engage pour un numérique citoyen, éthique, responsable et accessible à tous.

Docaposte compte plus de 50 000 clients et plus de 6 500 collaborateurs répartis sur 66 sites en France et à l'international et a réalisé 879 M€ de chiffre d'affaires en 2024.

Contributeurs Docaposte

Smara LUNGU, Stéphane INGRASSIA, Marion DUMESNIL



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



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.

