Une étude

harris interactive
ahead of what's next

pour

captain cyber
BE A CYBER HERO

Les salariés et la cybersécurité

Comment les salariés appréhendent-ils les enjeux liés à la cybersécurité ? Les entreprises les mettent-ils en situation d'appliquer les bonnes pratiques ?

Janvier 2020

Jean-Daniel Lévy, Directeur du Département Politique – Opinion
Gaspard Lancrey-Javal, Directeur d'études au Département Politique – Opinion
Morgane Hauser, Chef de groupe au Département Politique – Opinion

Sommaire

Méthodologie d’enquête

Enquête réalisée **en ligne** du **19** au **24 décembre** 2019.

Échantillon de **648** salariés d’entreprise de 50 salariés et plus travaillant au moins en partie sur un poste d’ordinateur, issu d’un échantillon représentatif de salariés d’entreprise de 50 salariés et plus.

Méthode des quotas et redressement appliqués aux variables suivantes : sexe et âge de l’interviewé, taille et secteur d’activité de l’entreprise.

Aide à la lecture des résultats détaillés :

- Les chiffres présentés sont exprimés en pourcentage.
- Les chiffres en italique sont ceux qui apparaissent significativement au-dessus de la moyenne.
- Afin de faciliter la lecture et dans le cadre de ce rapport, la mention « les salariés » désignera « les salariés d’entreprise de 50 salariés et plus travaillant au moins en partie sur un poste d’ordinateur », interrogés lors de l’enquête.

harris interactive
ahead of what’s next

captain cyber
BE A CYBER HERO

Intervalle de confiance

L'intervalle de confiance (parfois appelé « marge d'erreur ») permet de déterminer la confiance qui peut être attribuée à une valeur, en prenant en compte la valeur observée et la taille de l'échantillon. Si le calcul de l'intervalle de confiance concerne les sondages réalisés avec la méthode aléatoire, il est communément admis qu'il est proche pour les sondages réalisés avec la méthode des quotas.

Taille de l'échantillon	5% ou 95%	10% ou 90%	20% ou 80%	30% ou 70%	40% ou 60%	50%
100 interviews	4,4	6,0	8,0	9,2	9,8	10
200 interviews	3,1	4,3	5,7	6,5	6,9	7,1
300 interviews	2,5	3,5	4,6	5,3	5,7	5,8
400 interviews	2,2	3,0	4,0	4,6	4,9	5,0
500 interviews	2,0	2,7	3,6	4,1	4,4	4,5
600 interviews	1,8	2,4	3,3	3,8	4,0	4,1
800 interviews	1,5	2,1	2,8	3,2	3,4	3,5
1 000 interviews	1,4	1,8	2,5	2,9	3,0	3,1
2 000 interviews	1,0	1,3	1,8	2,1	2,2	2,3
3 000 interviews	0,8	1,1	1,5	1,7	1,8	1,8
4 000 interviews	0,7	0,9	1,3	1,5	1,6	1,6
6 000 interviews	0,6	0,8	1,1	1,3	1,4	1,4

harris interactive
ahead of what's next

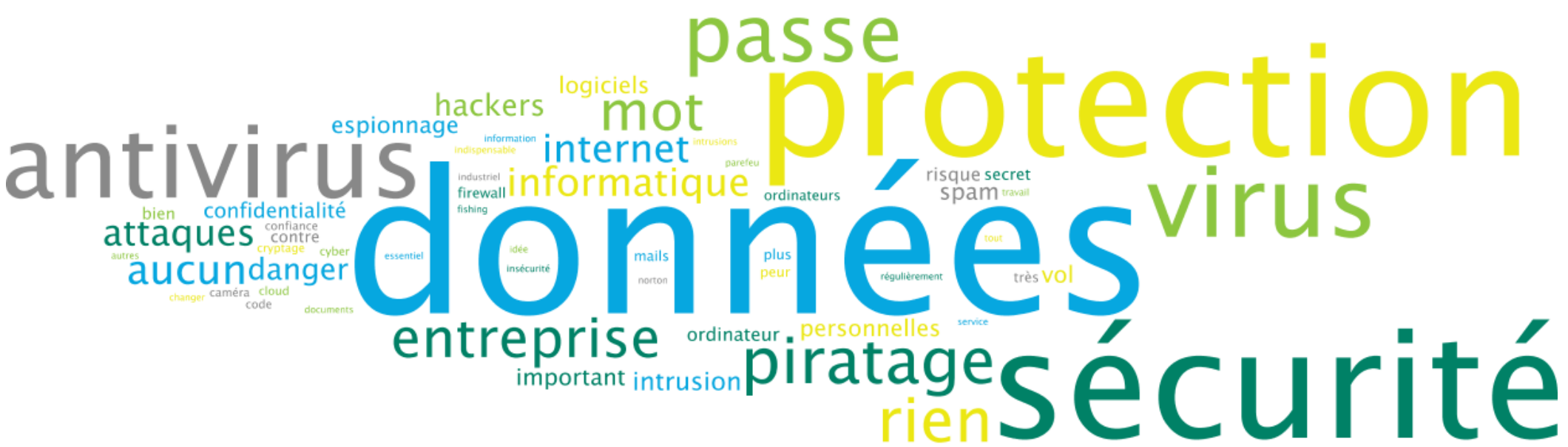
Note de lecture : **dans le cas d'un échantillon de 600 personnes**, si le pourcentage mesuré est de 10%, la marge d'erreur est égale à 2,4. Il y a donc 95% de chance que le pourcentage réel soit compris entre 7,6% et 12,4% (plus ou moins 2,4 points).

Perception spontanée de la cybersécurité

Les mots les plus utilisés spontanément par les salariés pour évoquer la cybersécurité

Quels sont tous les mots, toutes les représentations qui vous viennent à l'esprit lorsqu'on évoque la cybersécurité, et notamment la cybersécurité dans le cadre du travail ?
Question ouverte, réponses spontanées

- À tous -

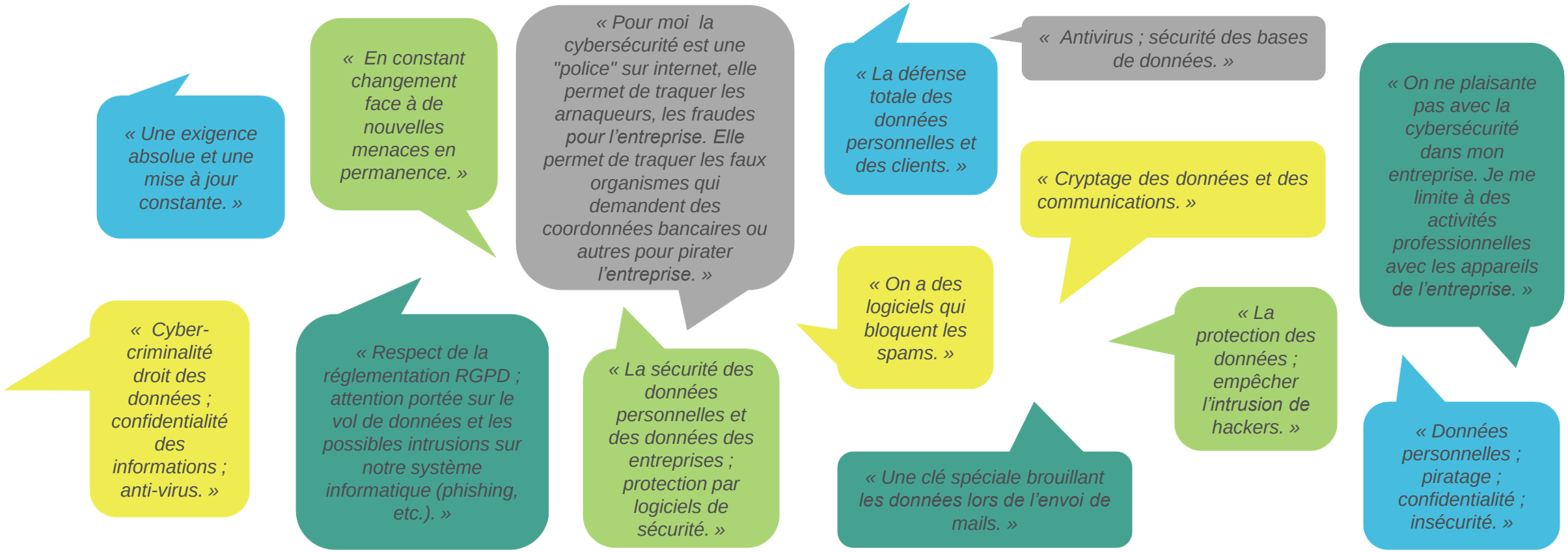


Le nuage de mots est automatiquement généré à partir de l'exhaustivité des réponses spontanées à la question ouverte. La taille d'un mot dans le visuel représente sa fréquence d'utilisation : le mot écrit en plus gros caractères est celui qui a été le plus utilisé par les sondés dans leurs réponses. L'emplacement d'un mot au sein du nuage n'a pas de signification particulière, pas plus que sa couleur.

Quelques exemples de *verbatim* spontanés de salariés sur la cybersécurité

Quels sont tous les mots, toutes les représentations qui vous viennent à l'esprit lorsqu'on évoque la cybersécurité, et notamment la cybersécurité dans le cadre du travail ?
Question ouverte, réponses spontanées

- À tous -



On nomme « cybersécurité » tous les moyens et toutes les pratiques qui permettent de protéger les personnes, les biens et les services (connectés directement ou indirectement à un réseau informatique) contre de multiples menaces : risques accidentels, malveillance, espionnage, manipulation de l'information, fraudes, etc.

harris interactive
ahead of what's next

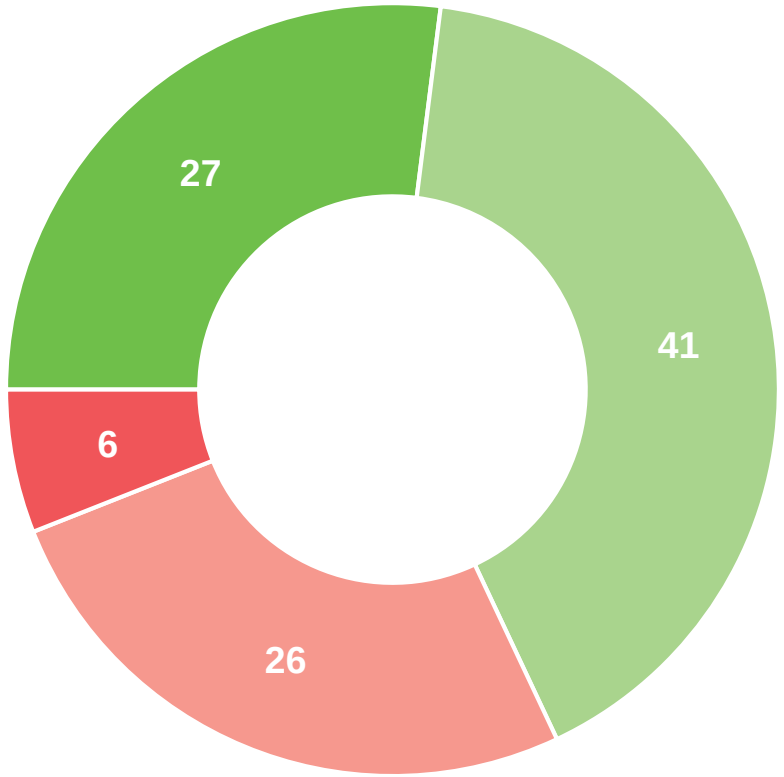
captain cyber
BE A CYBER HERO

Des salariés plutôt conscients des risques, mais aux pratiques encore très perfectibles

La salariés de bureau déclarent en majorité s’intéresser aux enjeux de cybersécurité dans leur entreprise, mais seul un quart déclare prendre ces enjeux à cœur

Personnellement, diriez-vous que les enjeux liés à la cybersécurité dans votre entreprise vous intéressent… ?

- À tous, en % -



Beaucoup / Assez : 68%

Hommes : 74%
18-29 ans : 79%
Cadres : 81%
Managers : 84%
Occupent des fonctions commerciales (79%) ou de pilotage (78%)
Salariés d’ETI : 71%

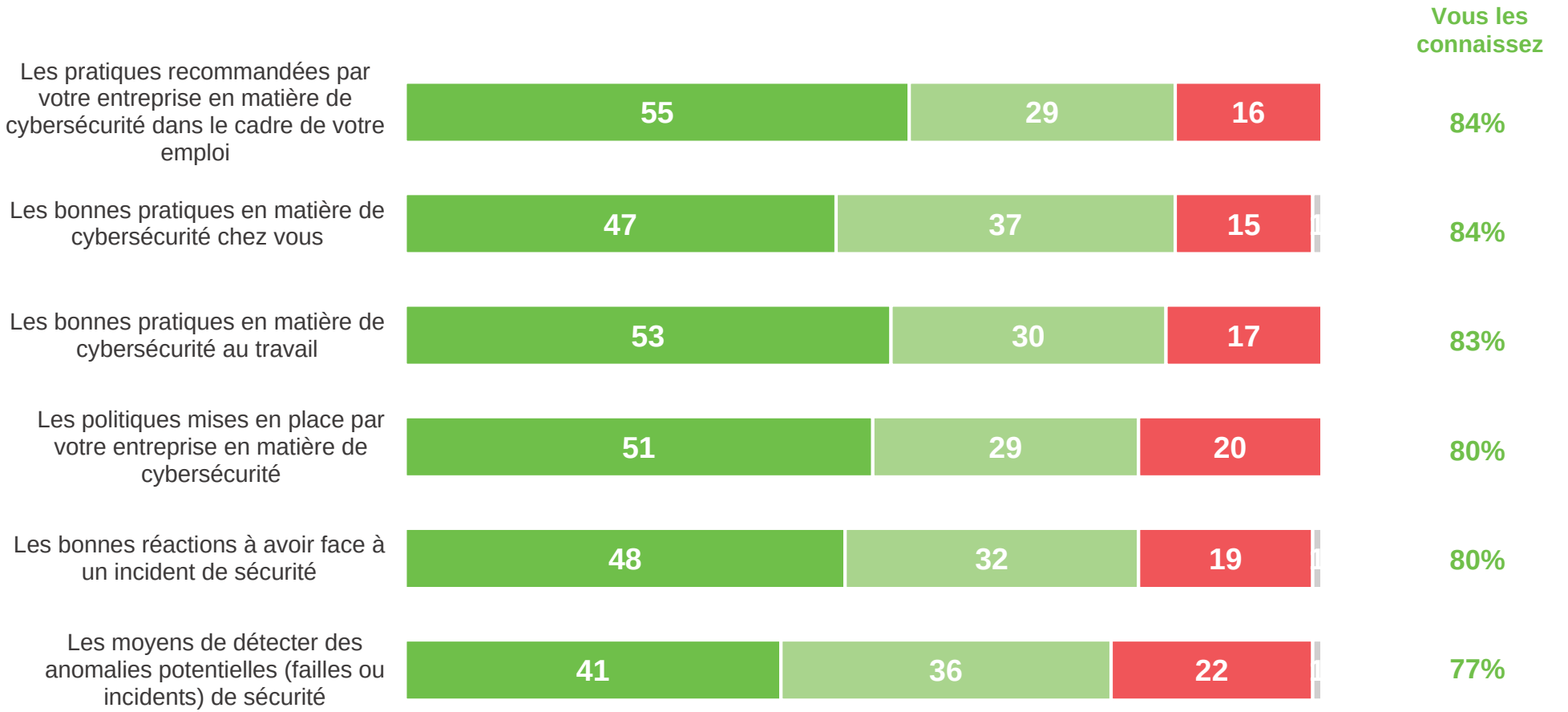
Peu / Pas du tout : 32%

Femmes : 38%
50 ans et plus : 40%
Salariés de grandes entreprises : 41%
N’occupent pas de fonction de management : 51%

Les salariés déclarent très majoritairement connaître différents enjeux associés à la cybersécurité, mais seule une moitié d'entre eux déclare les appliquer au quotidien

Pour chacun des éléments suivants, diriez-vous plutôt que : vous le connaissez et l'appliquez au quotidien ; vous le connaissez mais ne l'appliquez pas vraiment au quotidien ; ou que vous ne le connaissez pas et ne l'appliquez pas au quotidien.

- À tous, en % -

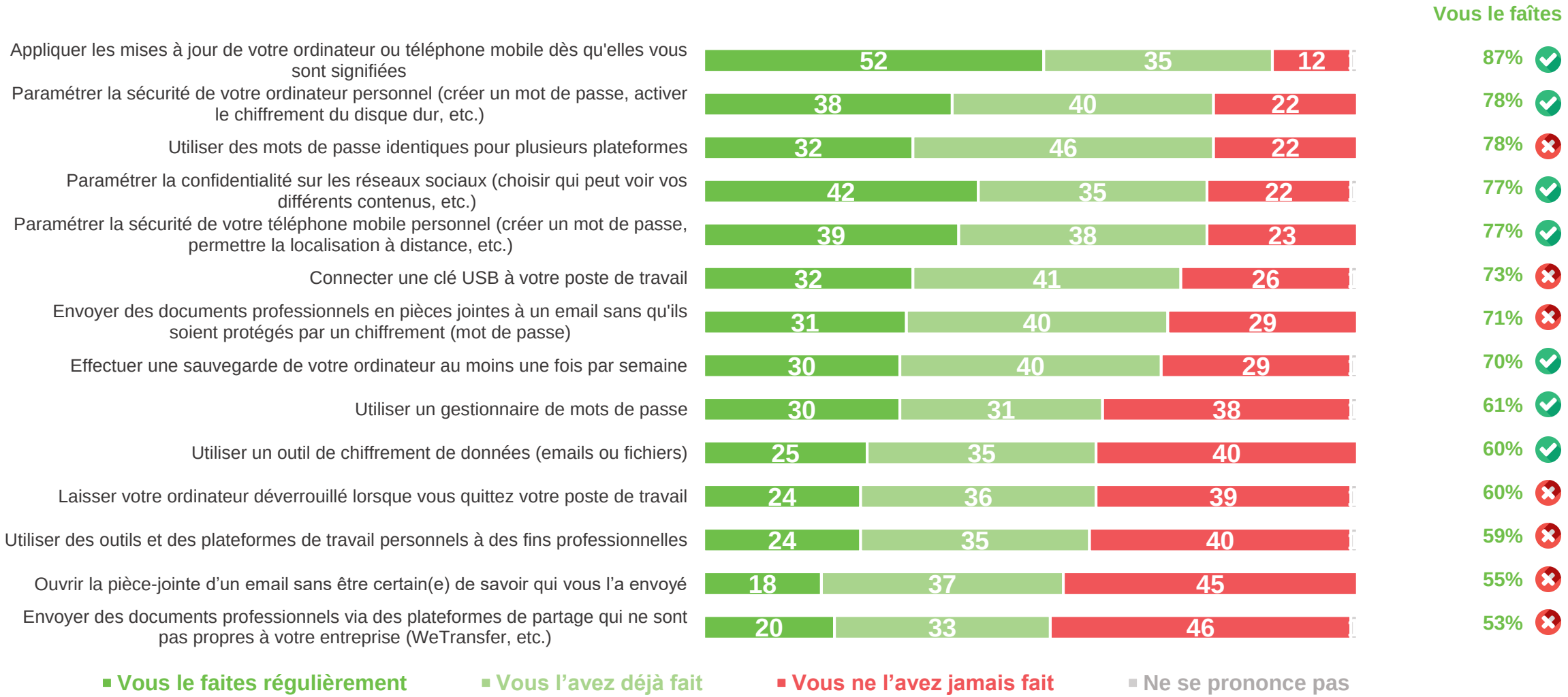


Les hommes, les salariés qui occupent des fonctions d'encadrement ou de management ainsi que ceux pour qui le digital a une grande importance au quotidien (pour leur poste ou leur entreprise), se montrent largement plus convaincus de connaitre et d'appliquer les différentes mesures liées à la cybersécurité.

Dans les faits, les salariés mélangent largement bonnes et mauvaises pratiques en matière de cybersécurité au quotidien et dans le cadre de leur emploi

Pour chacun des éléments suivants, diriez-vous plutôt que : vous le connaissez et l'appliquez au quotidien ; vous le connaissez mais ne l'appliquez pas vraiment au quotidien ; ou que vous ne le connaissez pas et ne l'appliquez pas au quotidien.

- À tous, en % -

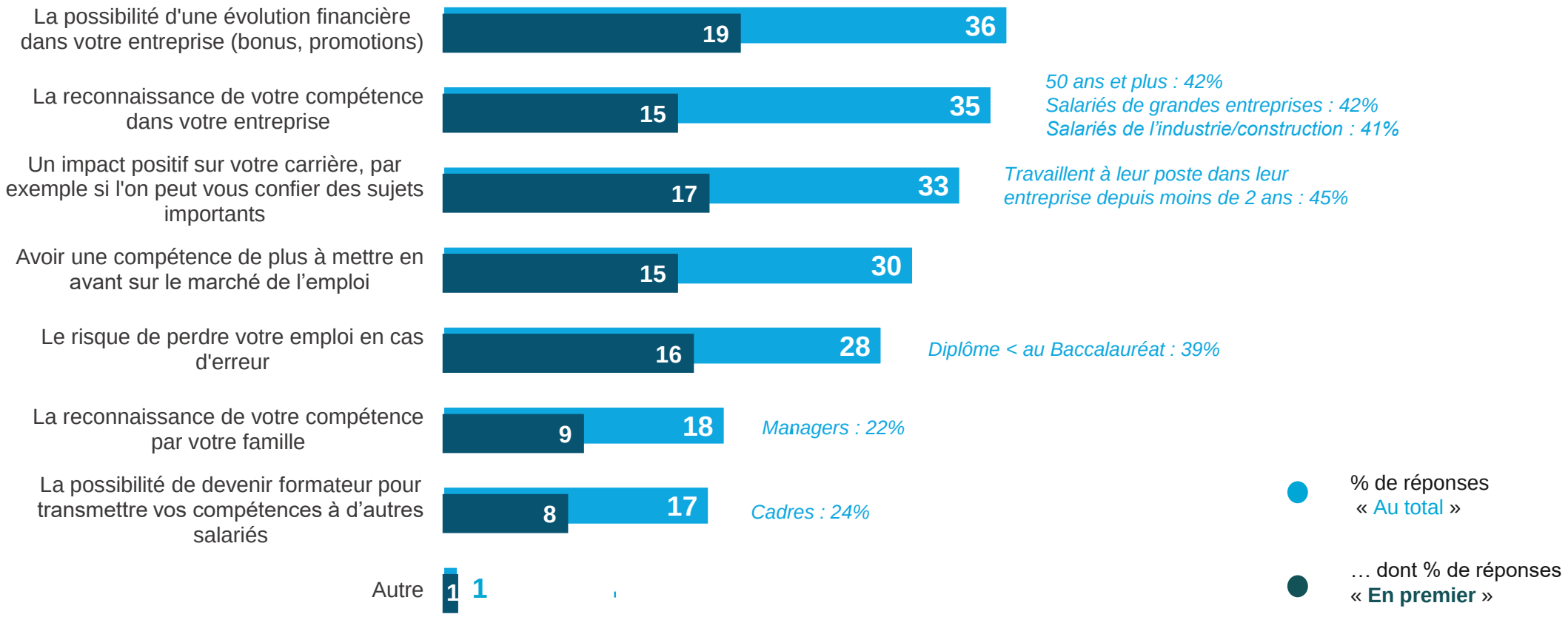


Aucune population n'est à l'abri des risques en matière de cybersécurité : celles qui adoptent le plus des comportements sécurisés (jeunes, cadres, etc.), sont aussi celles qui témoignent le plus avoir des pratiques à risque.

Pour mieux s’impliquer dans les enjeux de cybersécurité, les perspectives de gains financiers et la possibilité de gagner en reconnaissance et en expertise s’avèrent des leviers majeurs

Parmi les motivations suivantes, quelles sont celles qui pourraient le plus vous amener à vous intéresser à la cybersécurité de façon générale ?

- À tous, en % -

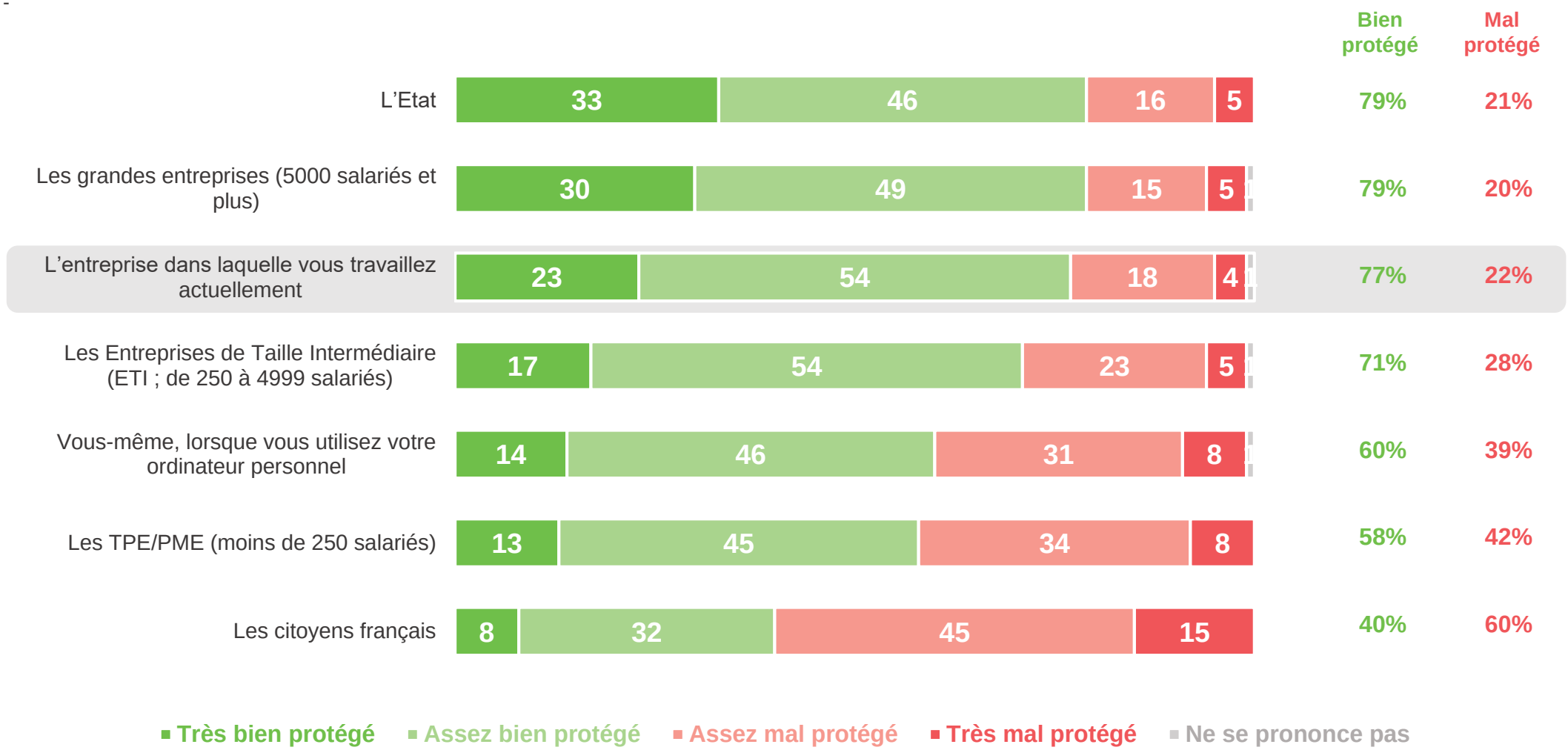


Une relative confiance dans l’entreprise en matière de cybersécurité

Plus une structure est de taille importante, mieux les salariés estiment qu'elle est protégée en matière de cybersécurité ; les salariés se déclarant davantage sereins concernant leur entreprise ou pour eux-mêmes que pour les autres

Personnellement, avez-vous le sentiment que chacun des acteurs suivants est aujourd'hui bien protégé ou non en matière de cybersécurité ?

- À tous, en % -

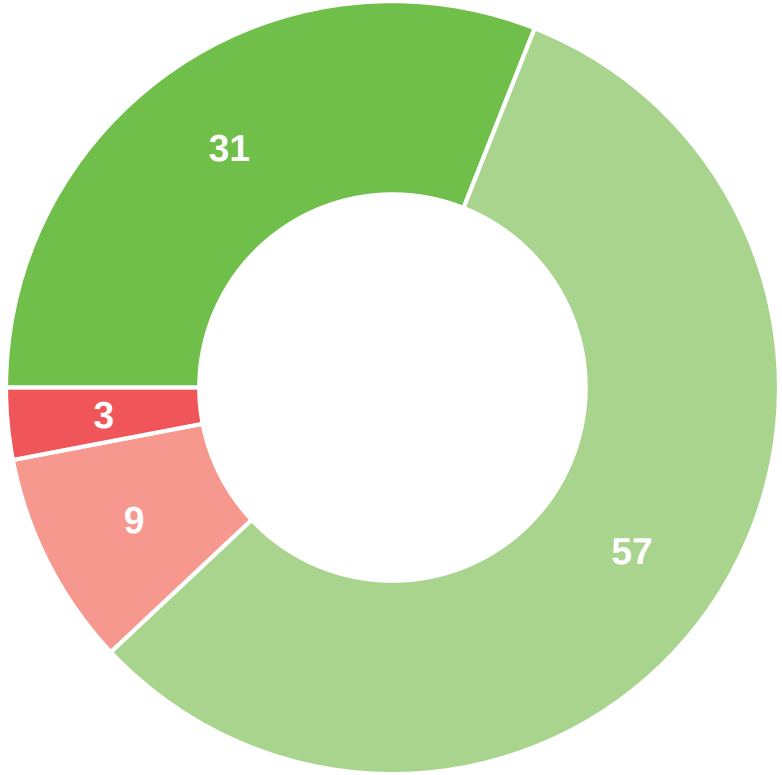


Les salariés dont le poste ou l'entreprise ont un rapport important avec le digital ont davantage le sentiment que les différents acteurs sont bien protégés concernant les enjeux de cybersécurité.

Les salariés font quasi-unanimement confiance à la personne responsable de la cybersécurité au sein de leur entreprise, même si cette confiance reste relativement peu intense (moins d'un tiers « tout à fait confiance »)

Personnellement, faites-vous confiance ou pas confiance au responsable chargé de la cybersécurité dans votre entreprise ?

- À tous, en % -



Confiance : 88%

Managers : 91%

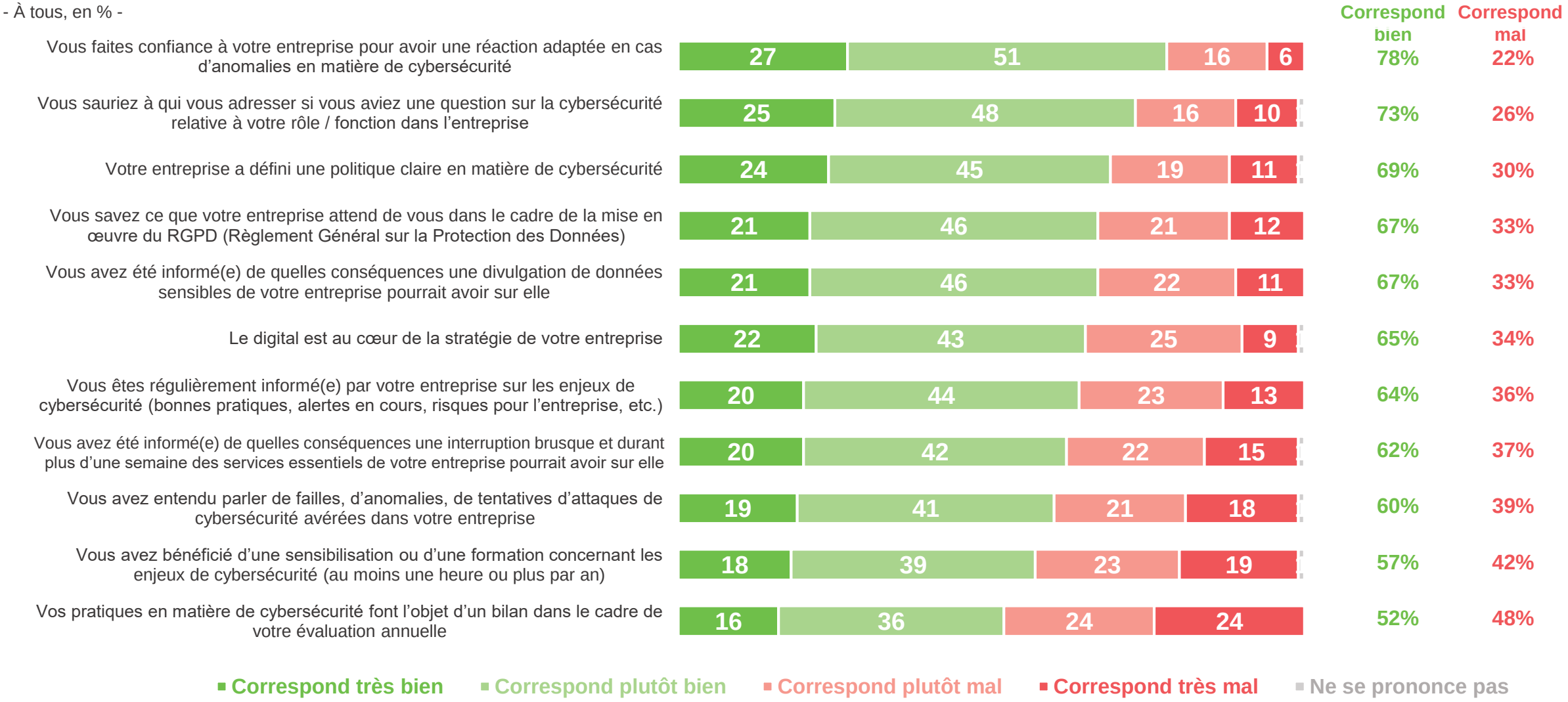
Pas confiance : 12%

■ Tout à fait confiance ■ Plutôt confiance ■ Plutôt pas confiance ■ Pas du tout confiance

Les salariés expriment une certaine confiance envers leur entreprise, qu'ils prennent comme référence sur les questions liées à la cybersécurité, même s'ils témoignent de quelques insuffisances en matière d'information

Diriez-vous que chacune des affirmations suivantes correspond bien ou mal à votre situation concernant la cybersécurité au sein de votre entreprise… ?

- À tous, en % -

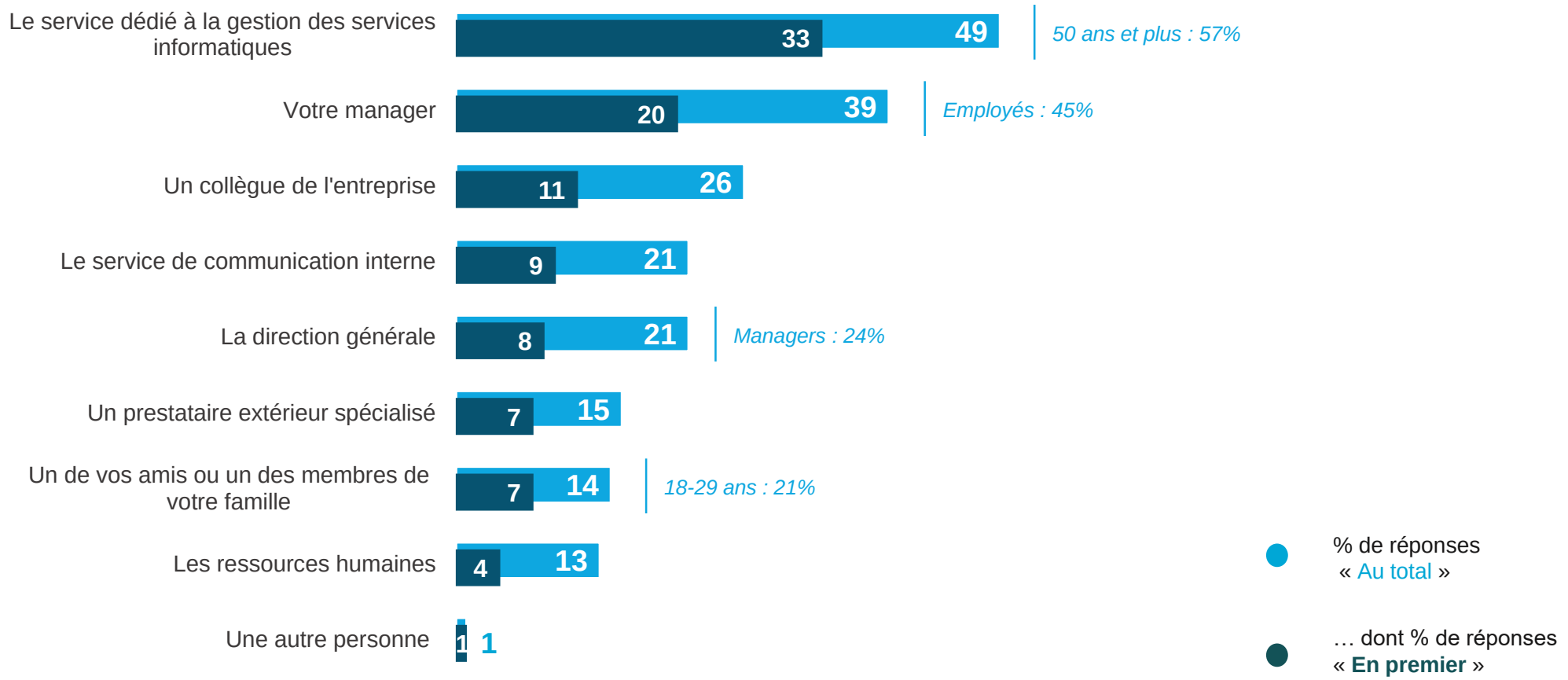


Les salariés de région parisienne, les cadres ou managers et ceux pour qui le digital occupe une grande importance (dans leur poste ou dans leur entreprise), se sentent dans l'ensemble bien plus concernés par ces différentes affirmations

Moins d’un salarié sur deux se tourne en premier lieu vers le service dédié à la gestion des services informatiques lorsqu’il a besoin d’information ou d’aide sur des questions relatives à la cybersécurité dans le cadre de leur travail

Quel(s) interlocuteur(s) consultez-vous le plus souvent lorsque vous avez besoin d’information ou d’aide sur des questions relatives à la cybersécurité dans le cadre de votre travail ?

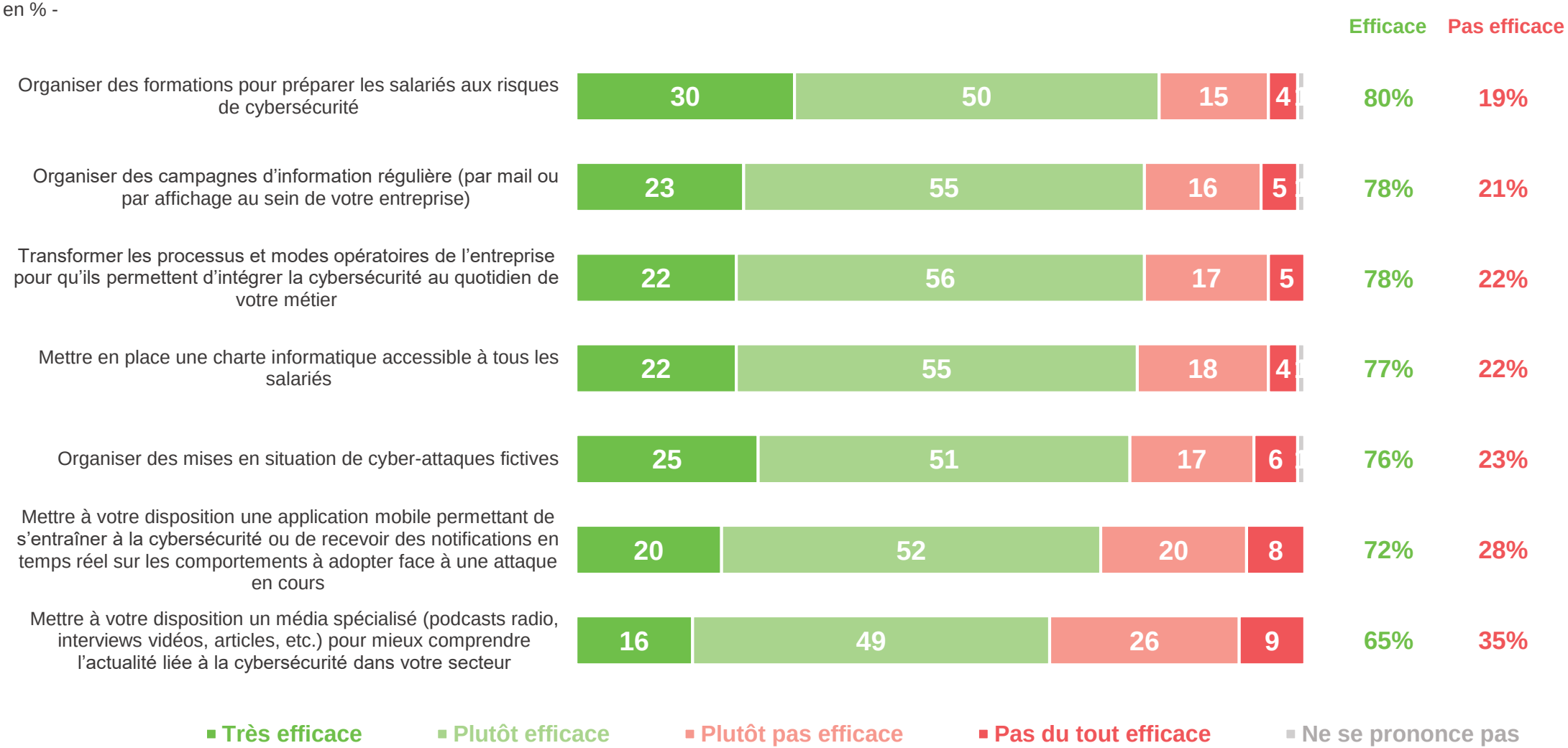
- À tous, en % -



Dans l’ensemble, les salariés se montrent favorables à la mise en place de nombreuses solutions d’information en matière de cybersécurité, les jugeant pour la plupart efficaces

Et, toujours pour vous informer et vous aider sur les questions de cybersécurité dans le cadre professionnel, chacun des moyens suivants serait-il selon vous efficace ou pas efficace de la part de votre entreprise ?

- À tous, en % -



Contacts

Merci de noter que toute **diffusion de ces résultats**
doit être accompagnée des éléments techniques suivants :
le **nom de l'institut**, le **nom du commanditaire de l'étude**,
la **méthode d'enquête**, les **dates de réalisation** et la **taille de l'échantillon**.

Suivez l'actualité de Harris Interactive sur :

www.harris-interactive.com

Facebook

Twitter

LinkedIn

Contacts Harris Interactive en France :

Jean-Daniel Lévy – Directeur du Département Politique & Opinion - 01 44 87 60 30 - jdlevy@harrisinteractive.fr

Laurence Lavernhe – Responsable de la communication - 01 44 87 60 94 - 01 44 87 60 30 - llavernhe@harrisinteractive.fr

Contacts CaptainCyber (Cyberbrief SAS) :

Sylvan Ravinet – Fondateur – sylvan@captaincyber.com

Leslie Toledano – Relations presse – 06 10 20 79 60 – presse@captaincyber.com

ahead of what's next