ÉTUDE AUPRÈS DE SALARIÉS AUTOUR DE LA CYBERSÉCURITÉ

Rapport d'étude d'opinion

Septembre 2024

AGENDA

1. CONTEXTE, ENJEU & OBJECTIFS
2. APPROCHE METHODOLOGIQUE & DISPOSITIF DE L'ÉTUDE
3. RESULTATS CLES
4. RESULTATS DETAILLES
   - COMPORTEMENTS ET USAGE DES SALARIES
   - INFORMATIONS DES SALARIES QUANT AUX RISQUES DE CYBERCRIMINALITE
   - ENJEUX ET REPONSES FACE AUX CYBERATTAQUES
5. SYNTHESE & CONCLUSIONS

APPROCHE MÉTHODOLOGIQUE

Notre APPROCHE MÉTHODOLOGIQUE

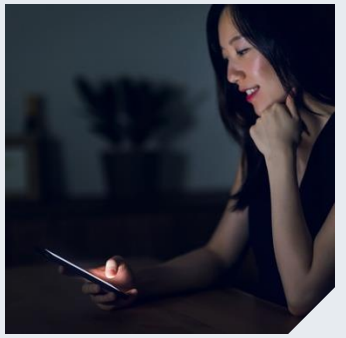
Une enquête d'opinion auprès des **salariés** en France travaillant sur **ordinateur.**

Une **enquête online** via notre panel Ipsos IIS, moyen de recueil fiable et rapide pour interroger les salariés.

Un échantillon robuste de 500 répondants, tout secteur d'activité confondu, avec des quotas sur le statut, âge, région et sexe, pour assurer une bonne mixité des résultats.

Un échantillon composé de salariés issus de tout **secteur d'activité**, avec 50% de l'échantillon issu d'entreprises industrielles et 50% d'entreprises spécialisées dans les services.

DISPOSITIF DE L'ÉTUDE



Rappel

MÉTHODE D'ÉCHANTILLONNAGE

- Tirage aléatoire dans la base des panélistes éligibles et désignation de la personne interrogée par la méthode des quotas.
- Panel propriétaire Ipsos IIS

CIBLE INTERROGÉE

- Cible : salariés français âgés de 18 à 65 ans issus de PME & ETI, travaillant sur ordinateur
- 500 salariés répartis en:
  - ✓ 200 employés
  - ✓ 200 prof. intermédiaires
  - ✓ 100 cadres
  - ✓ 50% de l'échantillon travaillant dans le secteur de l'industrie et 50% dans le secteur des services

COLLECTE

- On-line via l'Access panel d'Ipsos
- Terrain : du 2 au 9 septembre 2024
- Durée du questionnaire : 12 min
- Taille échantillon : 500 interviews

TRAITEMENT STATISTIQUE

- Echantillon pondéré
- Quotas sur genre, âge, région et activité professionnelle pour assurer une bonne mixité des résultats
- Méthode de pondération utilisée : calage sur marge
- Lecture par sous-cibles (statut, secteur d'activité, tranches d'âge, effectif salariés…)

Compléments d'informations méthodologiques disponibles sur demande

RÉSULTATS DÉTAILLÉS

Pratiques et usage des salariés

La pratique du télétravail

Un peu plus de la moitié des salariés interrogés pratique le télétravail. Les cadres, les habitants de la Région Parisienne et les 18-34 ans y ont davantage recours.

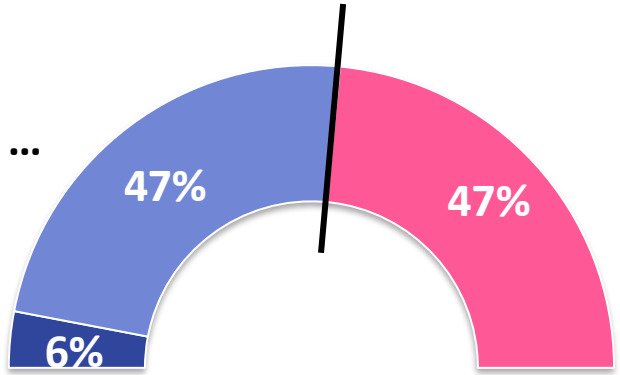
Télétravail

53% des salariés font du télétravail dont …

75% cadres

70% Région Parisienne

66% 18-34 ans



- Oui, complètement en télétravail
- Oui, quelques jours par semaine ou par mois en télétravail
- Non, je suis tout le temps sur site

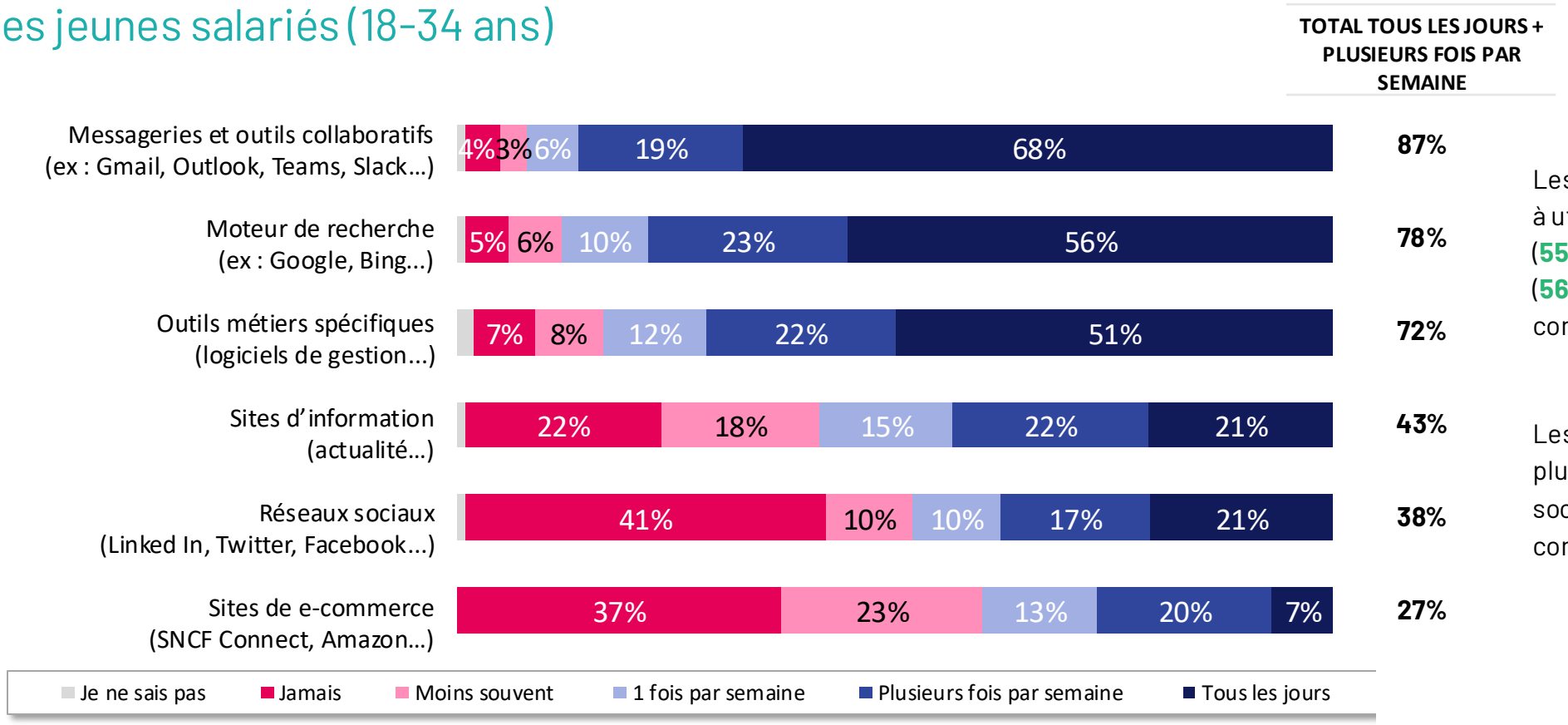
Base: 500 personnes - Ensemble

A3. Exercez-vous votre activité professionnelle en télétravail ?

xx% / xx% = différence significativement supérieure / inférieure au total

Utilisation sites Internet

Les messageries et outils collaboratifs ainsi que les moteurs de recherche sont des outils transversaux, utilisés de façon hebdomadaire ou quotidienne par la plupart des salariés. L'usage des sites d'information, des Réseaux sociaux et des sites de e-commerce est plus développé auprès des cadres ou des jeunes salariés (18-34 ans)



Les **cadres** sont plus nombreux à utiliser les sites d'information (**55%**), les réseaux sociaux (**56%**), et les sites de e-commerce (**35%**)

Les **18-34 ans** sont également plus présents sur les réseaux sociaux (**48%**) et les sites de e-commerce (**42%**)

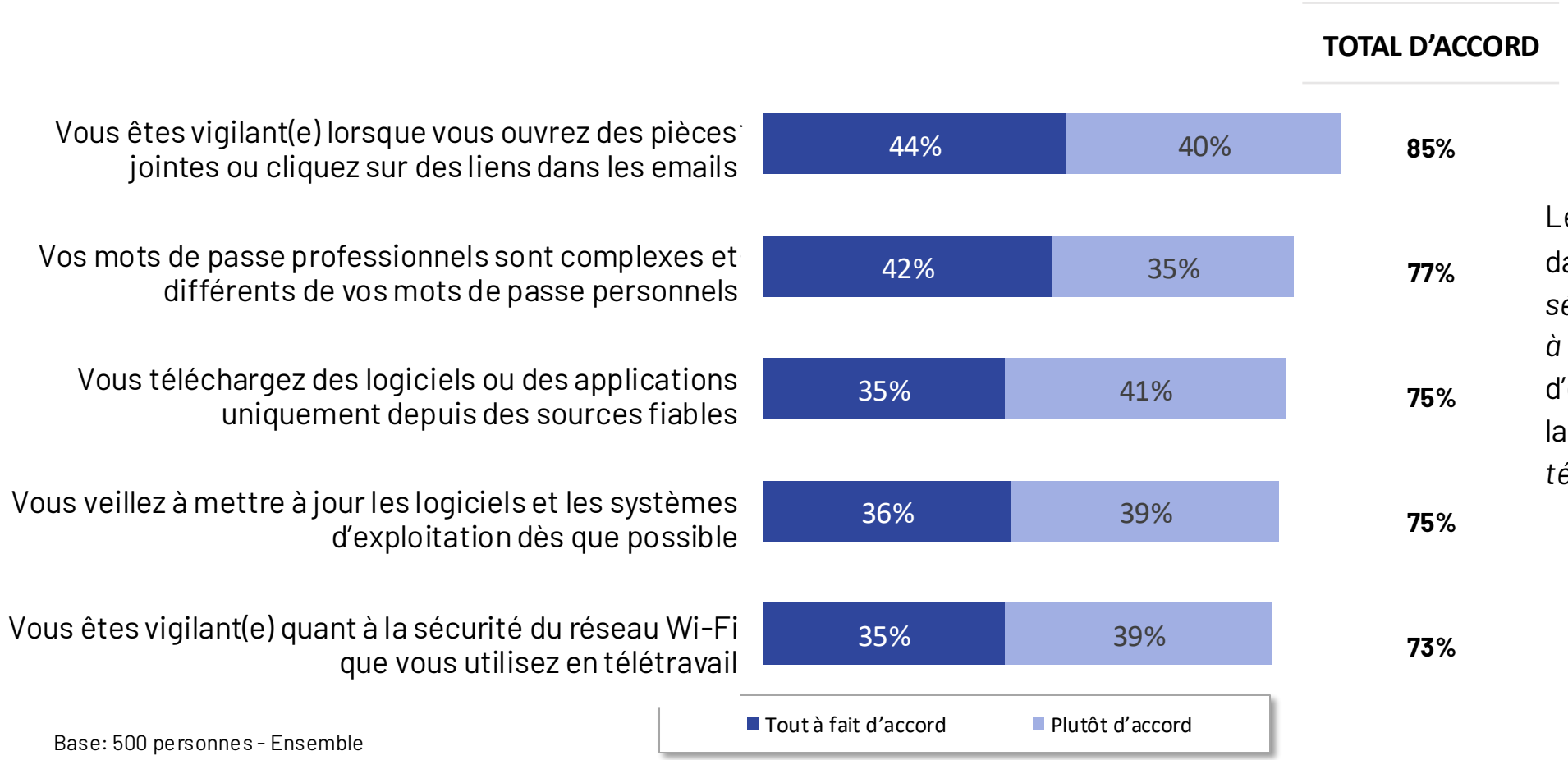
Base: 500 personnes - Ensemble

xx% / **xx%** = différence significativement supérieure / inférieure au total

A1. Dans quelle mesure utilisez-vous les sites suivants dans le cadre de votre travail ?

Les bonnes pratiques des salariés

Les bonnes pratiques sont plutôt acquises par les salariés (vigilance quant aux PJ, changement et complexité des mots de passe…). Les cadres y sont davantage sensibilisés que le reste des salariés.



Les **cadres** se disent davantage *vigilants quant à la sécurité du Wifi* (**84%**), à la *mise à jour* des logiciels et système d'exploitation (**85%**) ou encore à la *fiabilité des sources de téléchargement* (**86%**)

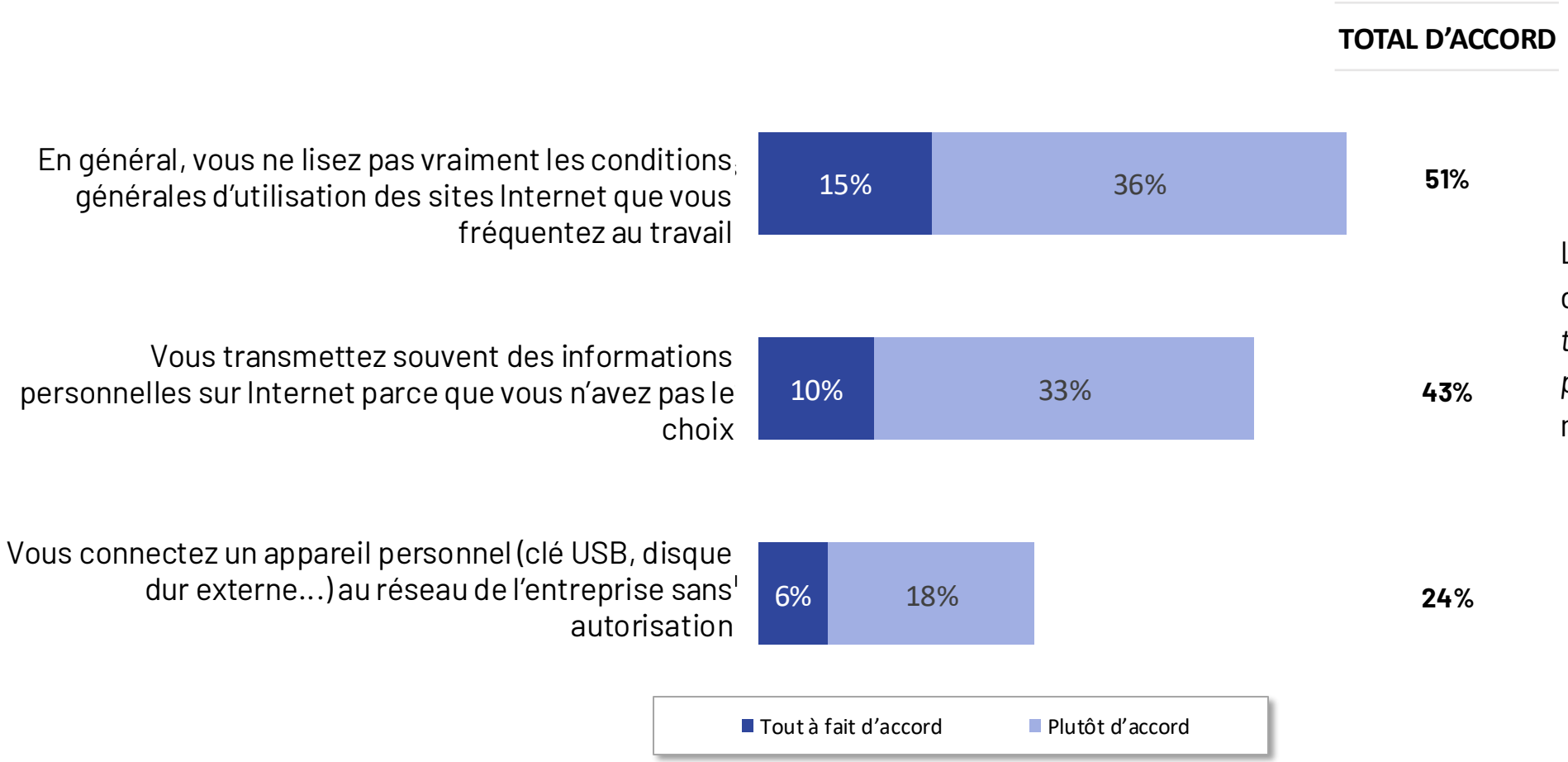
Base: 500 personnes - Ensemble

A4. Dans quelle mesure êtes-vous d'accord ou non avec chacune des opinions suivantes ?

xx% / **xx%** = différence significativement supérieure / inférieure au total

Des risques pris par les salariés subsistent…

Notamment concernant la non lecture des conditions générales d'utilisation ou encore la transmission d'informations personnelles.



Les **cadres** ont par ailleurs davantage tendance à *transmettre des informations personnelles* sur internet par manque de choix (**53%**)

Base: 500 personnes - Ensemble

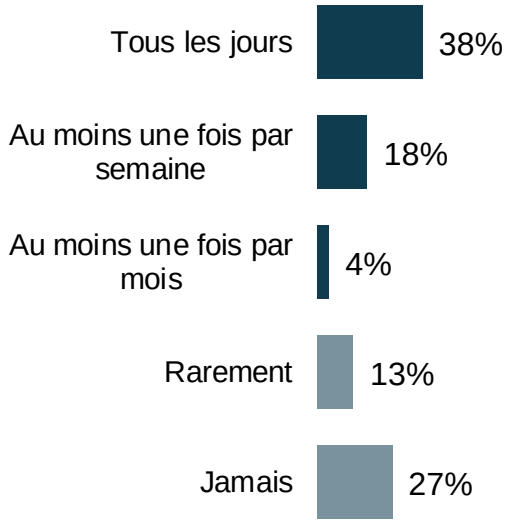
A4. Dans quelle mesure êtes-vous d'accord ou non avec chacune des opinions suivantes ?

xx% / xx% = différence significativement supérieure / inférieure au total

L’utilisation des appareils personnels

60% des salariés ont recours à leurs appareils personnels pour effectuer des tâches professionnelles.
Un usage renforcé chez les 18-34 ans, les cadres ou encore les salariés travaillant dans les services.

Fréquence d’utilisation des appareils personnels



60% Utilisent leurs appareils personnels **au moins une fois par mois**

75% 18-34 ans

71% cadres

64% Secteur des services

Base: 500 personnes - Ensemble

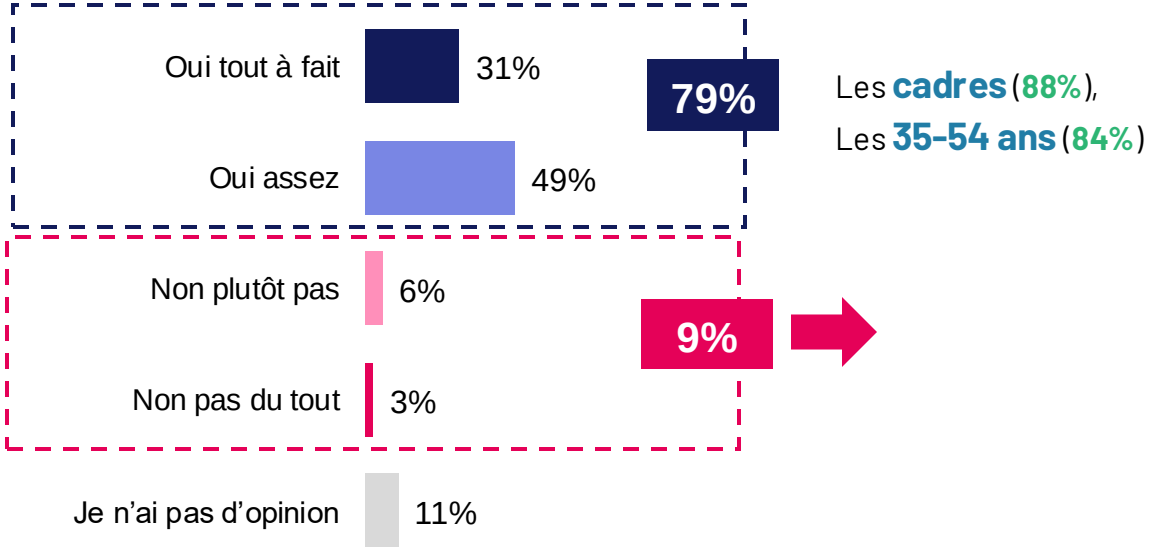
A2. Utilisez-vous des appareils qui vous appartiennent personnellement, tels que des smartphones, des tablettes, des ordinateurs portables ou des ordinateurs de bureau, pour effectuer des tâches professionnelles ?

xx% / xx% = différence significativement supérieure / inférieure au total

La sécurité des données, une affaire de tous !

Près de 8 salariés sur 10 pensent avoir leur part de responsabilité dans la sécurité des données de leur entreprise. Un sentiment de responsabilité supérieur est observé chez les cadres et les 35-54 ans.

Sentiment de responsabilité des salariés



Les **cadres** (88%),
Les **35-54 ans** (84%)

Base: 500 personnes - Ensemble

Raisons de non-sentiment de responsabilité

1. Responsabilité entreprise / employeur

« C'est à l'employeur d'assurer la sécurité »
« C'est l'entreprise qui doit s'en occuper »

2. Des services dédiés

« Le service informatique s'en occupe »
« C'est n'est pas à moi de gérer ce genre de choses »

3. Des compétences limitées

« Il y un des personnes qui s'occupe de ça dont c'est le travail car mes compétences en termes de sécurité des outils informatique sont limitées »

Base: 46 personnes – Non responsables de la sécurité

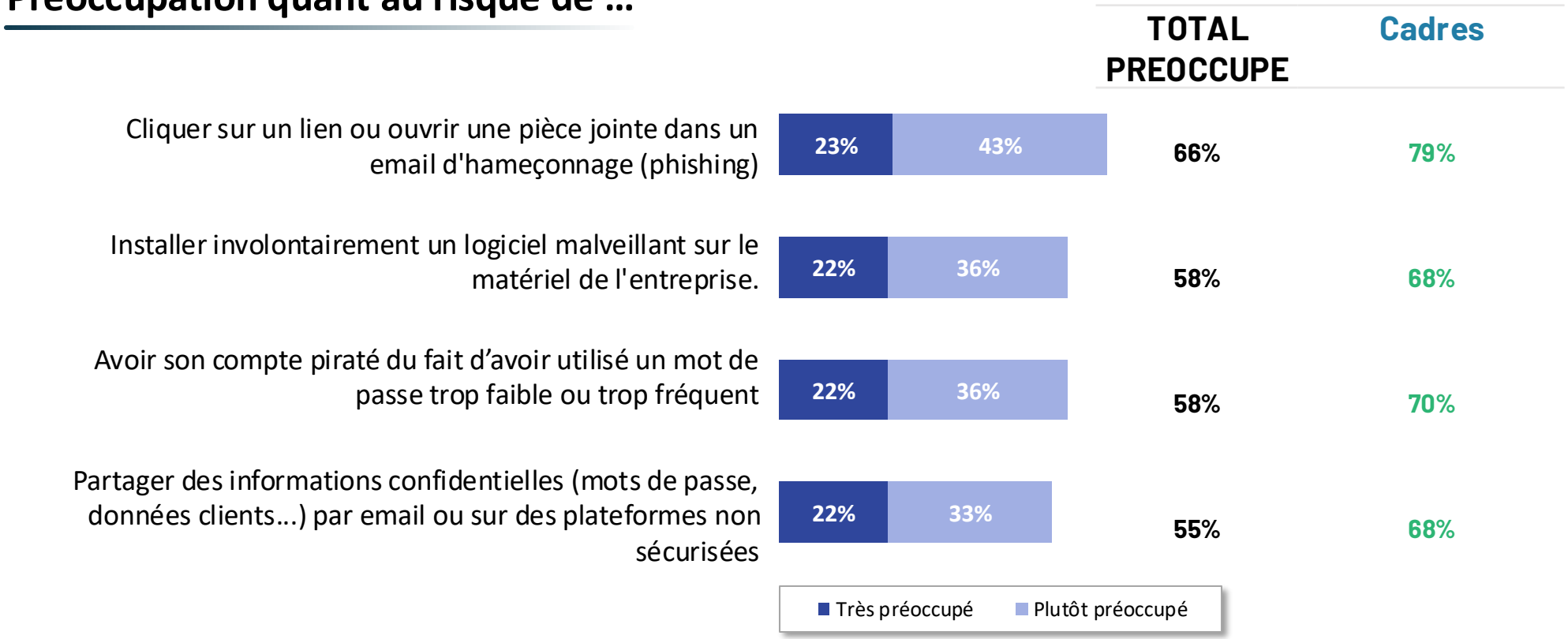
xx% / xx% = différence significativement supérieure / inférieure au total

A5. Pensez-vous que la sécurité des données de votre entreprise est également de votre responsabilité ?
A5.1. Pour quelle(s)raison(s) pensez-vous que la sécurité des données de votre entreprise n'est pas de votre responsabilité ?

Préoccupation des salariés face aux risques d'attaque

Les salariés sont assez préoccupés par les risques majeurs de cyberattaques, notamment par la crainte de phishing. Un enjeu d'autant plus fort chez les cadres qui subissent une plus forte pression.

Préoccupation quant au risque de …



Base: 500 personnes - Ensemble

A6. Dans le cadre de votre activité professionnelle, êtes-vous préoccupé par les risques suivants ?

xx% / xx% = différence significativement supérieure / inférieure au total

Signalement des risques de cybersécurité

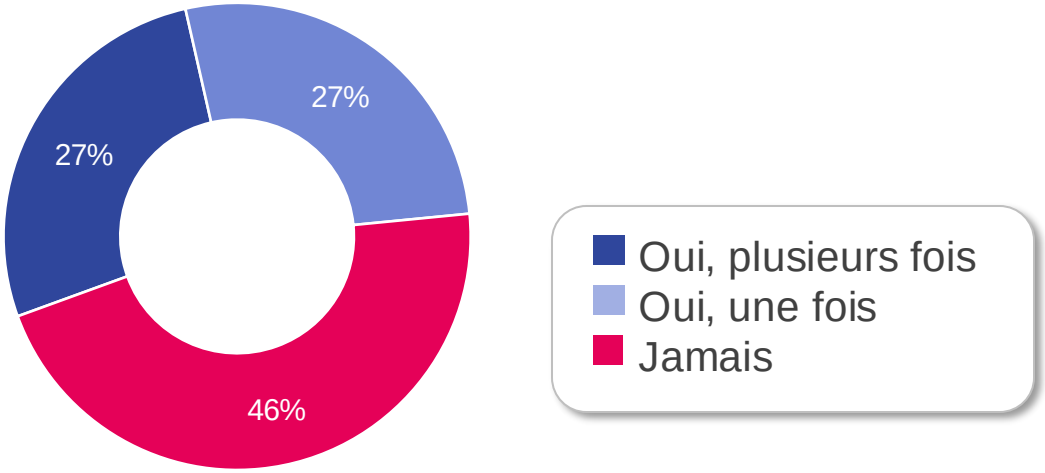
Plus d'un répondant sur 2 a d'ailleurs déjà signalé un risque à son entreprise. Les hommes et les salariés issus du secteur de l'industrie sont plus nombreux à avoir fait remonter un incident.

Signalement des risques de cybersécurité

54% des salariés ont déjà signalé un risque potentiel

60% Dans l'industrie

60% Hommes



Base: 500 personnes - Ensemble

A7. Avez-vous déjà pris l'initiative de signaler un risque potentiel de cybersécurité à votre hiérarchie ou au service informatique (ex : mail malveillant, etc...) ?

xx% / xx% = différence significativement supérieure / inférieure au total

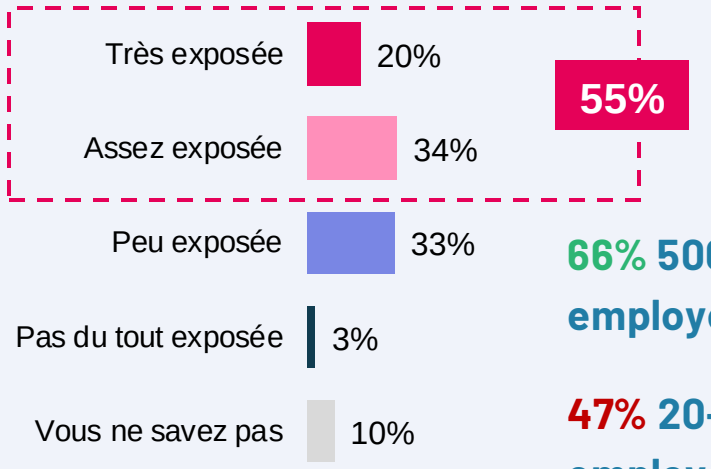
RÉSULTATS DÉTAILLÉS

CYBERCRIMINALITE

Des entreprises exposées aux risques de cybersécurité

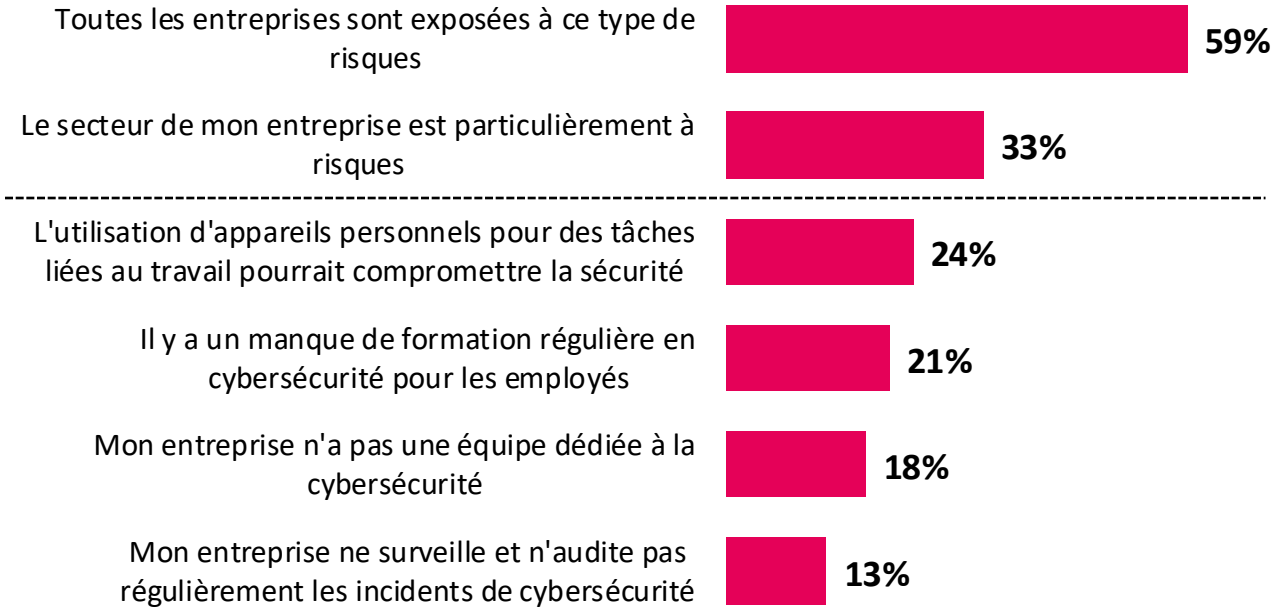
Pour 55% des salariés, leur entreprise peut être exposée à un risque potentiel de cybercriminalité. Un risque qui s'accroit avec la taille de l'entreprise.

Entreprise exposée aux risques



Base: 500 personnes - Ensemble

Raisons d'exposition



Base: 274 personnes - Exposées

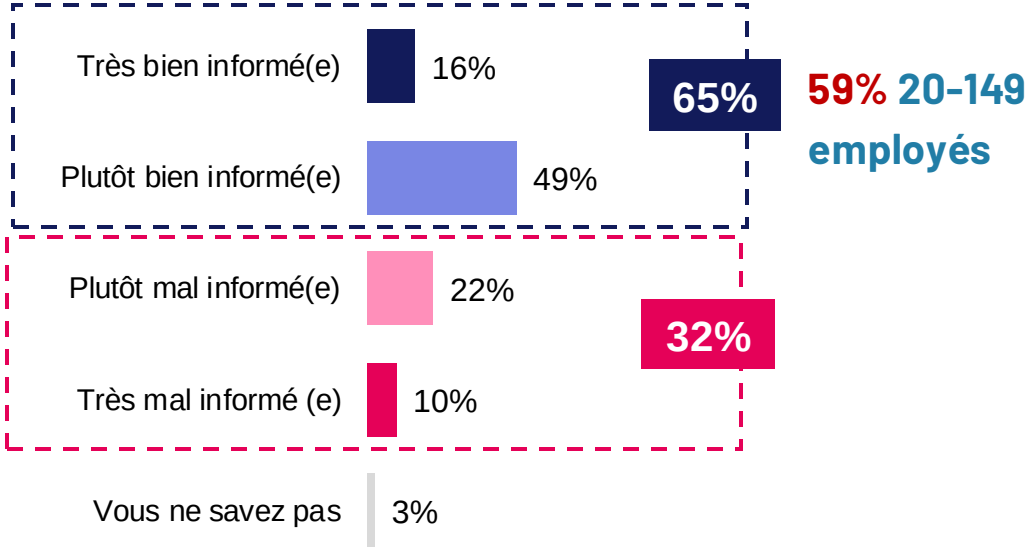
B1. A quel niveau diriez-vous que votre entreprise est exposée aux risques de cybercriminalité (ex : fuite de données, extorsion, ransomware, etc...) ?
B1bis. Pour quelle(s) raison(s) pensez-vous que votre entreprise est exposée aux risques de cybercriminalité ?

xx% / xx% = différence significativement supérieure / inférieure au total

Information & politiques de sécurité informatique

Par ailleurs, près de 2/3 des répondants estiment être bien informés concernant les risques et bonnes pratiques. Un peu moins de 60% ont d'ailleurs connaissance des politiques de sécurité de leur entreprise.

Information sur les risques & bonnes pratiques

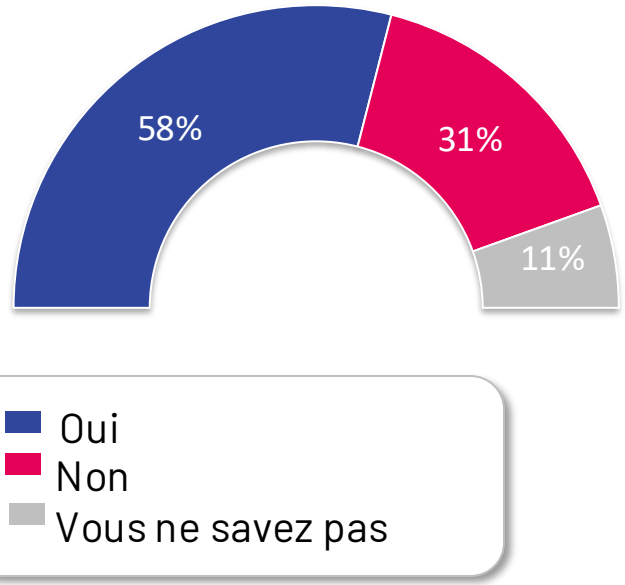


59% 20-149 employés

Connaissance des politiques de sécurité informatique

49% 20-149 employés

66% 150-499 employés



Base: 500 personnes - Ensemble

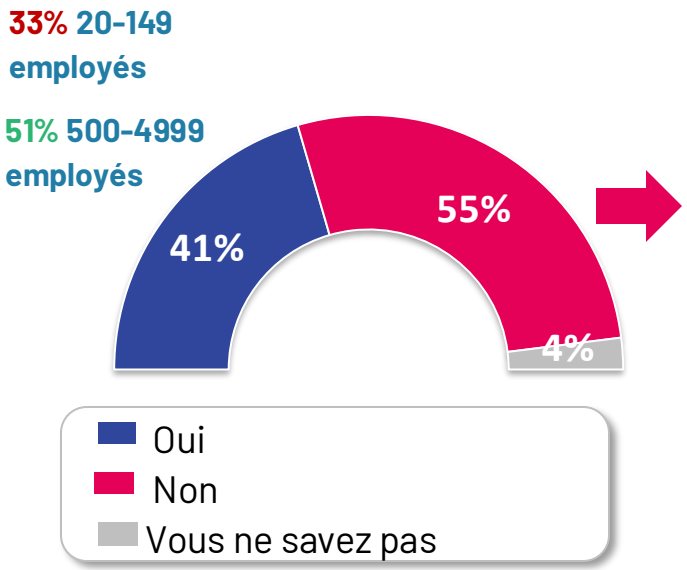
B2. Diriez-vous que vous vous sentez bien informé(e) par votre employeur sur les risques de cybercriminalité et les bonnes pratiques à adopter pour s'en protéger ?
B3. Avez-vous connaissances des politiques de sécurité informatique mises en place dans votre entreprise ?

xx% / xx% = différence significativement supérieure / inférieure au total

Formation & besoins en formation

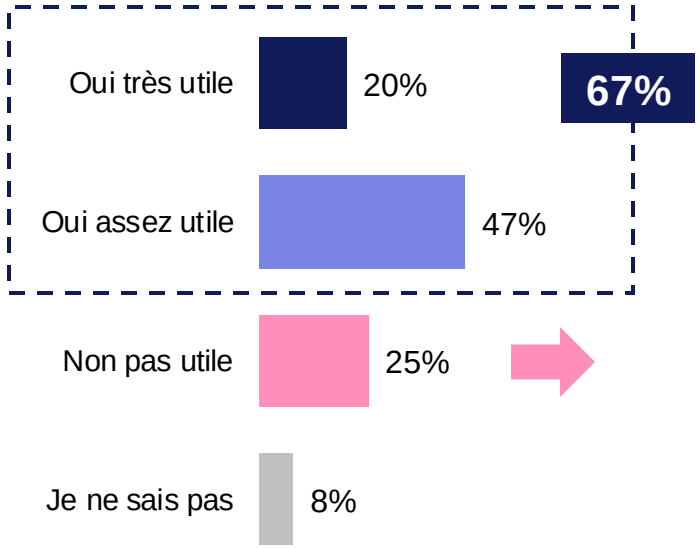
4 salariés sur 10 ont suivi une formation au cours des 24 derniers mois. Formation pourtant jugée utile pour une majorité. Les grandes entreprises sont plus enclines à former leurs salariés.

Formation



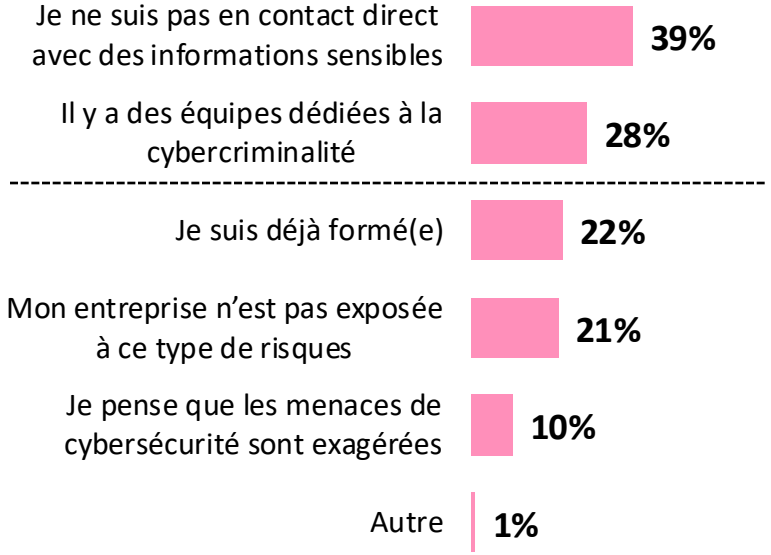
Base: 500 personnes - Ensemble

Besoins en formation



Base: 295 personnes - N'a pas bénéficié de formation au cours des 24 derniers mois

Raisons non-besoins en formation



Base: 72 personnes - N'a pas besoin de formation

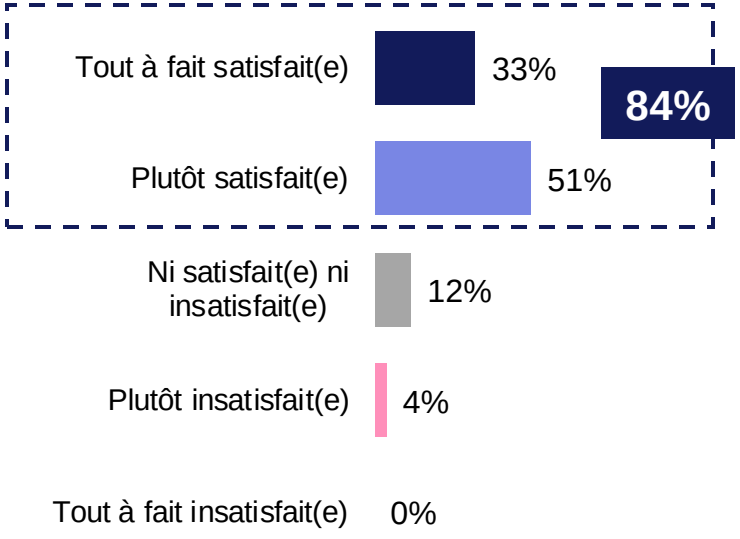
B4. Au cours des 24 derniers mois, avez-vous bénéficié d'une formation ou sensibilisation aux risques de la cybersécurité dispensée par votre entreprise ?
B5. Pensez-vous qu'une formation en cybersécurité pourrait vous être utile dans le cadre de votre travail ?
B5bis. Pour quelle(s)raison(s) ne ressentez-vous pas l'utilité d'être formé(e) en cybersécurité ?

xx% / xx% = différence significativement supérieure / inférieure au total

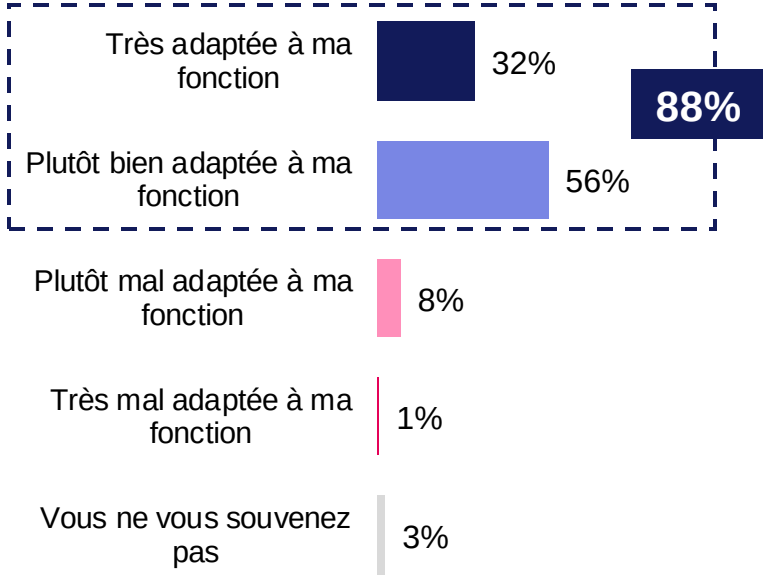
Satisfaction formation, ciblage & contenu

Les salariés ayant bénéficié d'une formation au cours des 24 derniers moins sont globalement satisfaits de leur formation, qui est perçue comme bien adaptée à leur fonction. Le sujet de la sensibilisation aux risques et bonnes pratiques générales est le plus repondu.

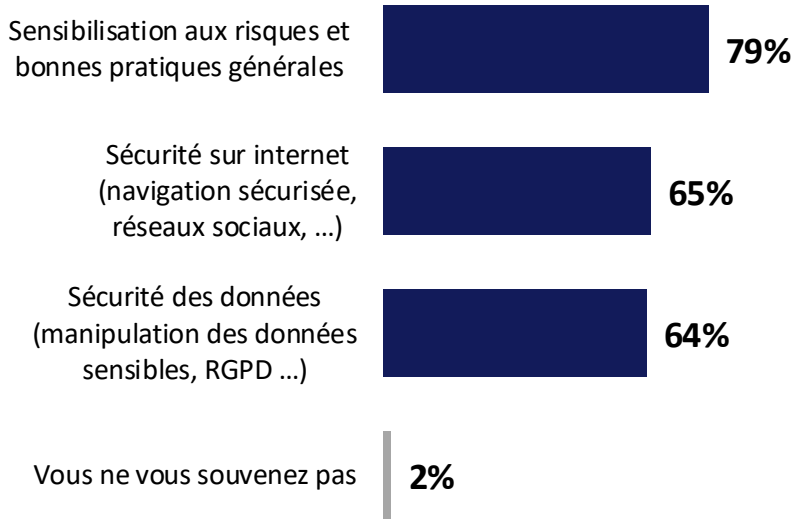
Satisfaction formation



Ciblage formation



Contenu formation

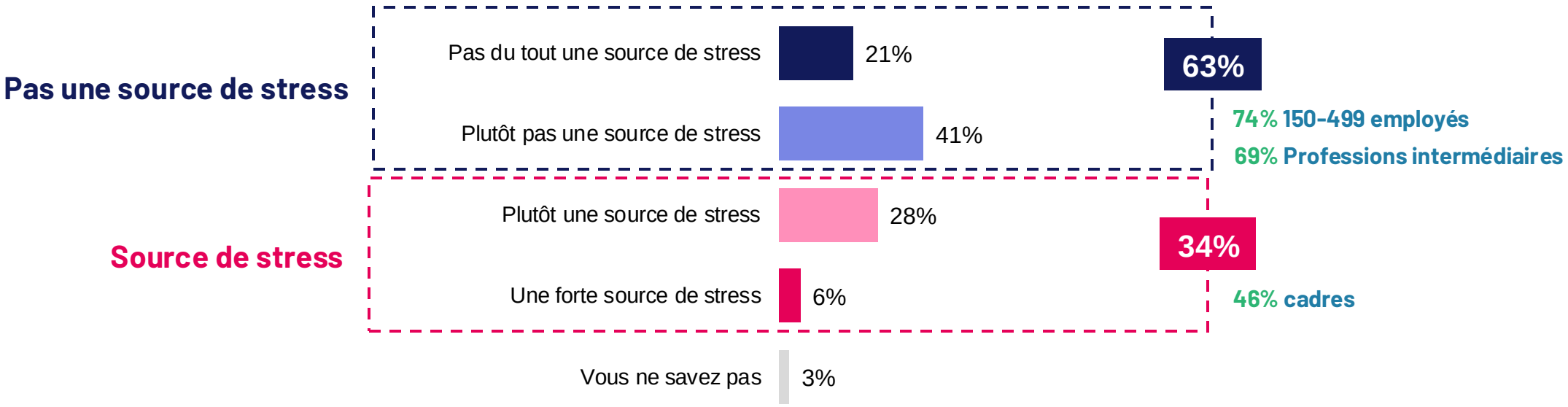


Base: 206 personnes - A bénéficié d'une formation au cours des 24 derniers mois

B9. Dans quelle mesure étiez-vous satisfait de cette formation sur la cybersécurité ?B6. Est-ce que cette formation était adaptée à votre fonction et aux enjeux spécifiques de votre métier ?
B7. Quels thèmes ont été abordés lors de cette formation sur la cybersécurité ?

La cybercriminalité, une source de stress

Pour près de 2 salariés sur 3, les cyberattaques ne sont pas une source de stress.
Les cadres se disent davantage stressés ou inquiets à ce sujet (46%).



Base: 500 personnes - Ensemble

B10. Dans quelle mesure la cybercriminalité est-elle une source de stress ou d'inquiétude pour vous dans le cadre de votre travail ?

xx% / xx% = différence significativement supérieure / inférieure au total

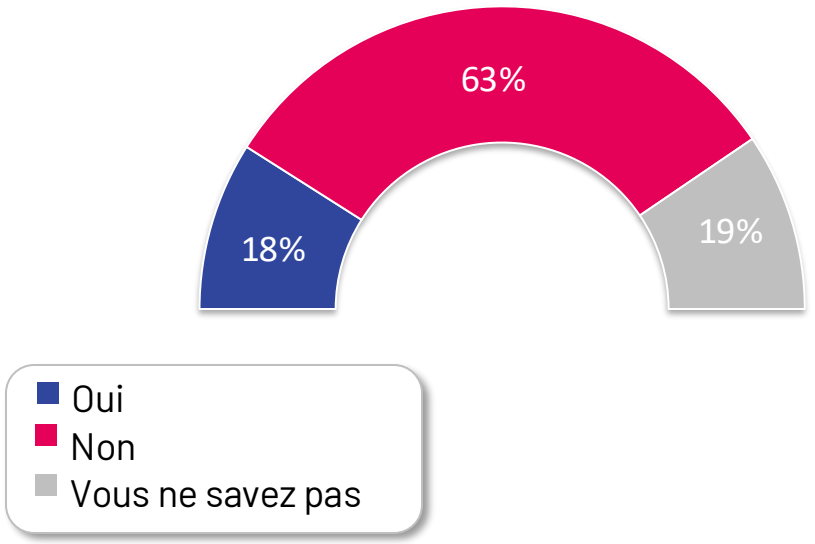
RÉSULTATS DÉTAILLÉS

CYBERATTAQUE

Cyberattaque & raison des cyberattaques

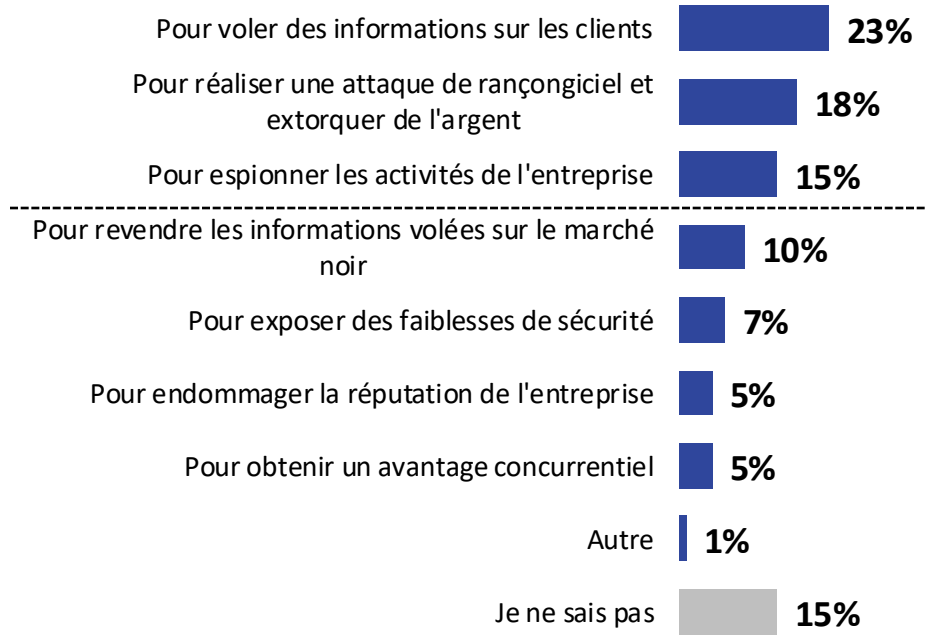
18% des salariés ont eu connaissance d'une cyberattaque dans leur entreprise au cours des 12 derniers mois. Des cyberattaques diverses :

Cyberattaque



Base: 500 personnes - Ensemble

Raison des cyberattaques



Base: 90 personnes - Entreprise cyberattaquée

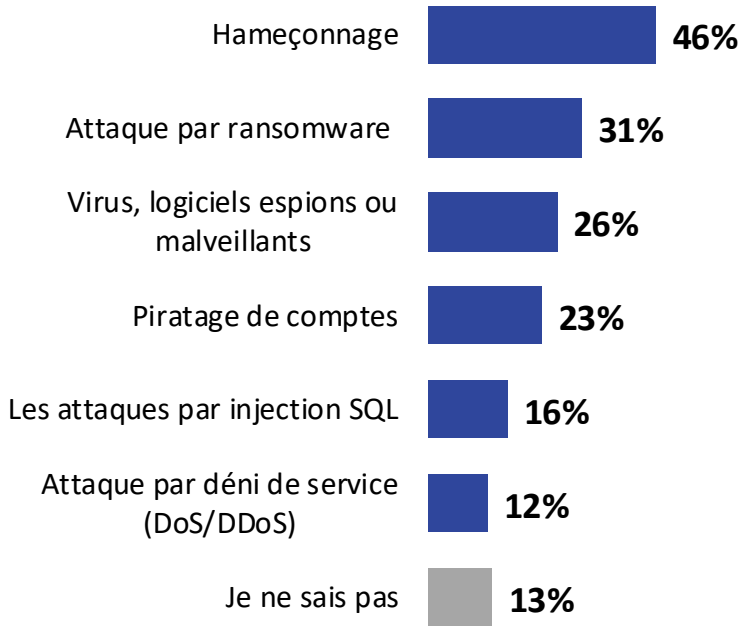
C1. Votre entreprise a-t-elle subi au cours des 12 derniers mois une cyberattaque ?
C2. Pour quelle raison l'entreprise a-t-elle été ciblée par cette cyberattaque ?

xx% / xx% = différence significativement supérieure / inférieure au total

Incidents rencontrés & impact

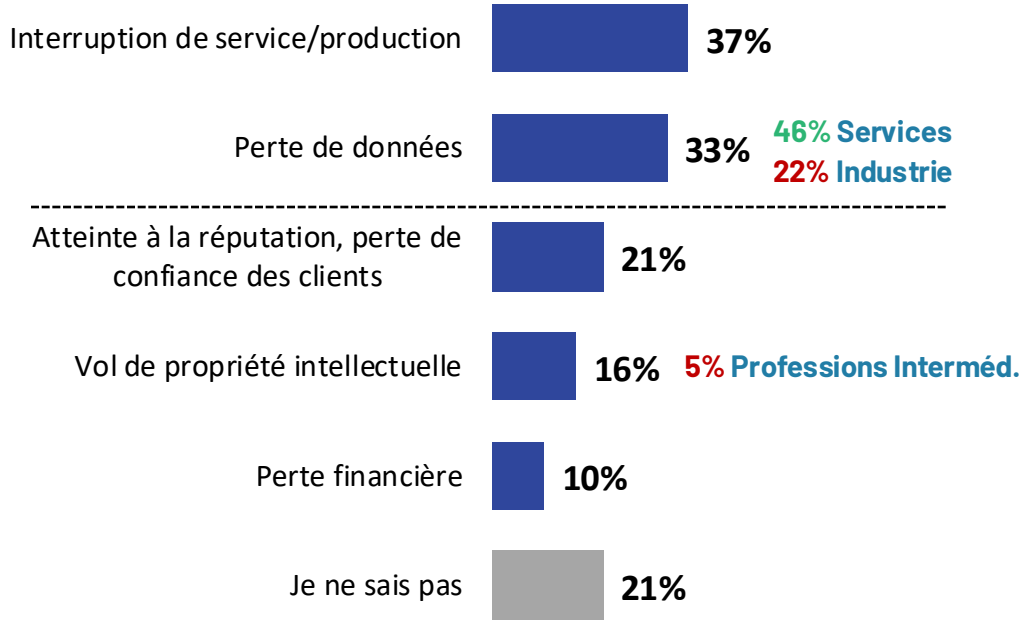
Les répondants concernés relatent divers types de cyberattaque, notamment l'hameçonnage, des ransomwares et des virus. L'interruption de l'activité et la perte de données en sont les principales conséquences. Les services sont davantage touchés par la perte de données que le secteur de l'industrie.

Incidents rencontrés



Base: 90 personnes - Entreprise cyberattaquée

Impact cyberattaque



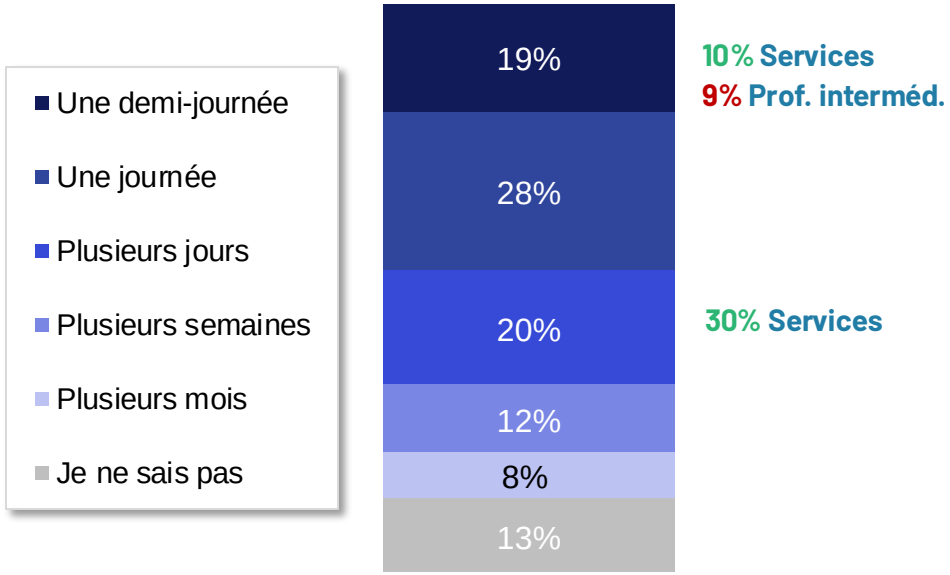
xx% / xx% = différence significativement supérieure / inférieure au total

C3. Quel(s) incident(s) votre entreprise a-t-elle subi au cours des 12 derniers mois ?
C4. Quel a été l'impact de cette cyberattaque sur l'entreprise ?

Durée cyberattaque & actions mises en place

Si près de la moitié des répondants estime la durée de l'incident à une journée tout au plus, 40% mentionnent des impacts allant de plusieurs jours à plusieurs mois. Le renforcement des protocoles d'authentification et les mises à jour régulières des systèmes et logiciels sont les principales réponses apportées par les entreprises.

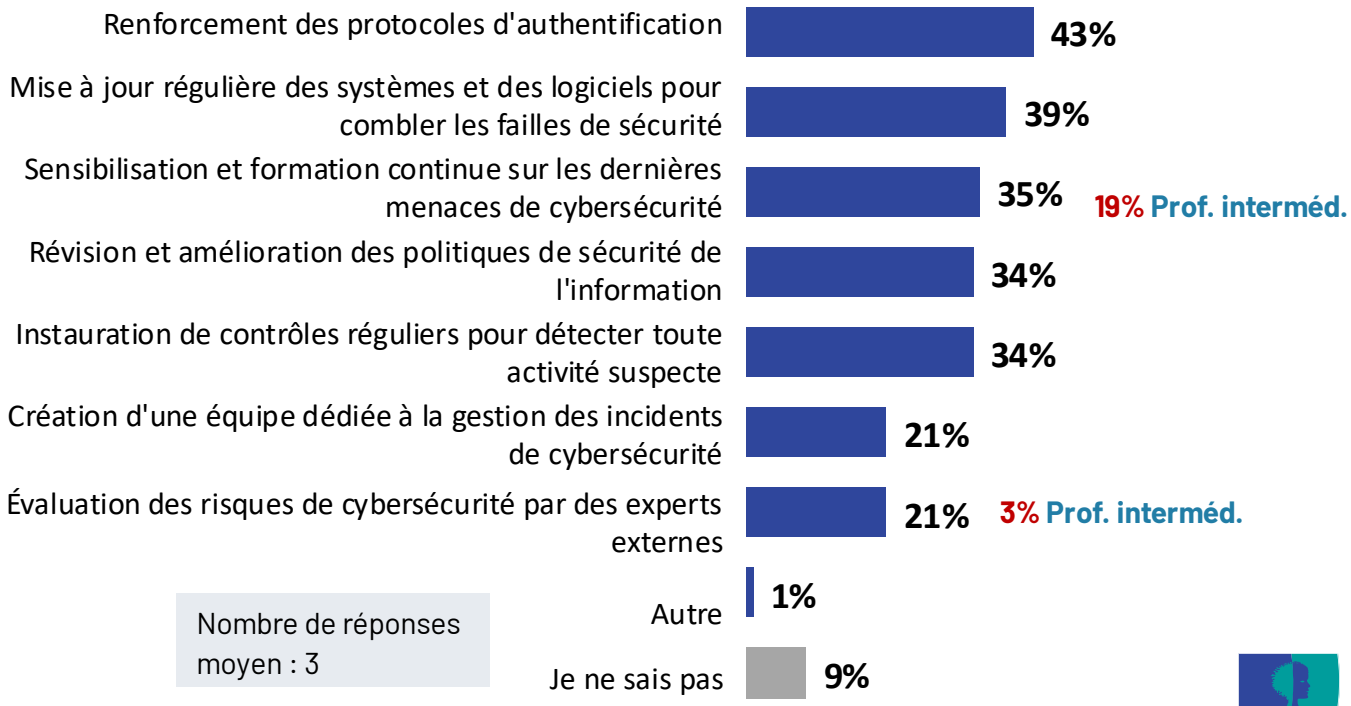
Durée des effets de l'incident



Base: 90 personnes - Entreprise cyberattaquée

C5. Pendant combien de temps cela a impacté l'entreprise ?

Actions mises en place par les entreprises



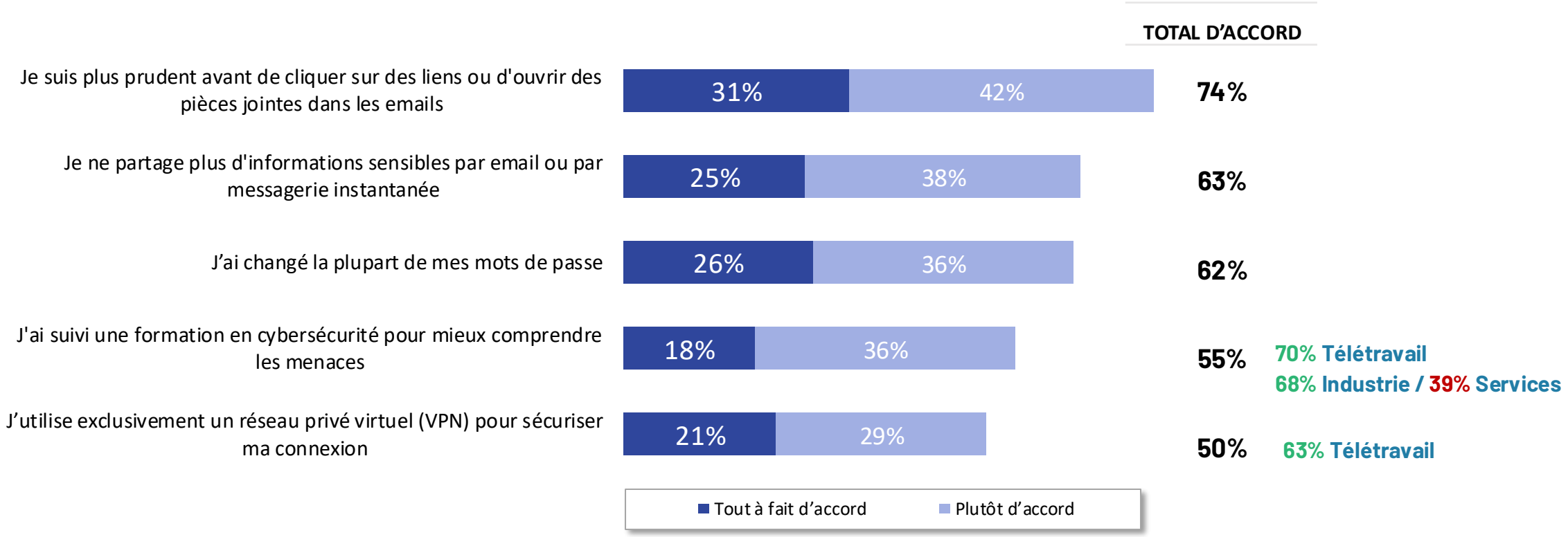
Nombre de réponses moyen : 3

C6. Quelles actions ont été mises en place à la suite de cette cyberattaque ?

xx% / xx% = différence significativement supérieure / inférieure au total

Des salariés plus prudents suite aux cyberattaques...

75% des personnes ayant vécu une cyberattaque affirment être plus attentifs aux liens et aux pièces jointes présents dans les emails. Environ 2/3 ont changé leurs mots de passe et ne partagent plus de contenu confidentiel via des canaux non sécurisés.



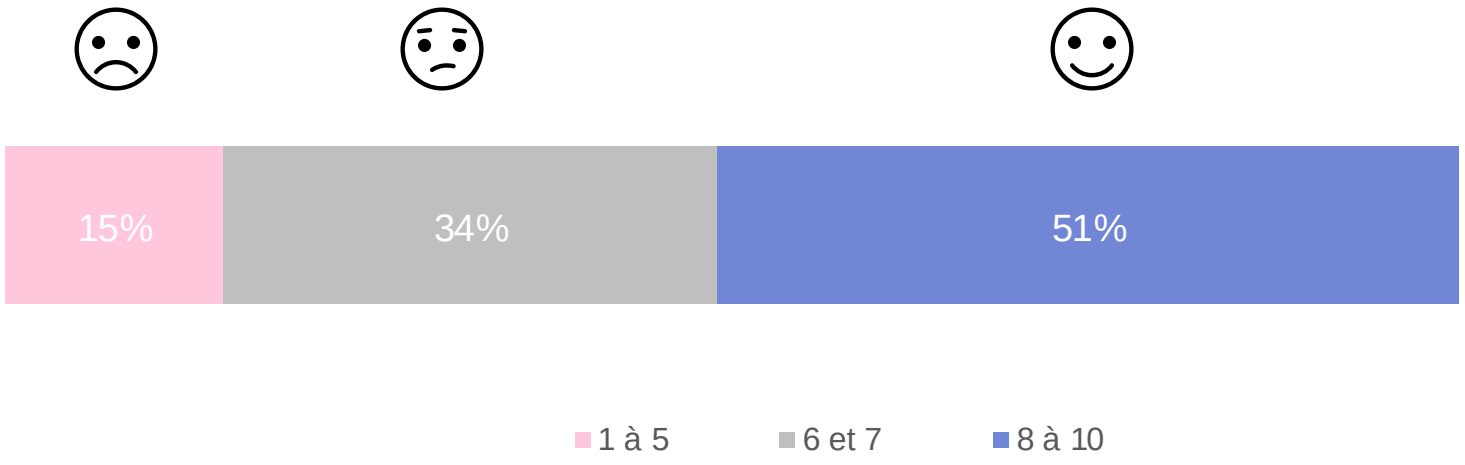
Base: 90 personnes - Entreprise cyberattaquée

xx% / xx% = différence significativement supérieure / inférieure au total

C6bis. La cyberattaque a pu avoir des conséquences sur votre comportement.
Pour chacune des phrases suivantes, veuillez indiquer dans quelle mesure vous êtes d'accord ou non avec ce qui est dit.

Capacité de l'entreprise à se protéger contre les cyberattaques

1 salarié sur 2 estime que son entreprise est tout à fait capable de se protéger d'une cyberattaque.
Parmi les plus convaincus, on retrouve les employés issus d'une grande entreprise et les personnes n'ayant pas fait face à une cyberattaque.



Moyenne

7,2 / 10

7,5/10 500-4999 employés (vs.
6,9/10 20-149 employés)
7,4/10 n'a pas subi de cyberattaque

Base: 500 personnes - Ensemble

C7. Dans quelle mesure êtes-vous confiant(e) dans la capacité de votre entreprise à se protéger contre les cyberattaques ? Veuillez utiliser une échelle de 1 à 10 où « 1 » signifie Pas du tout confiant et « 10 » signifie Tout à fait confiant.

xx% / xx% = différence significativement supérieure / inférieure au total

Actions à mettre en place

QUESTION OUVERTE

Un réel besoin d'être formé et informé émerge chez les répondants.
Les solutions concrètes proposées résident dans la sélection de logiciels efficaces et le renouvellement régulier des mots de passe.

Informations 36%

Formations (28%) :
« faire davantage de préventions avec des formations courtes mais régulières » ; « formation régulière du personnel » ; « Faire de la formation sur les risques et quoi faire en cas d'attaque » ; « une formation en interne pour tous les nouveaux collaborateurs serait un + »; « Des formations individuelles adaptées à chaque poste » ; « formation tous les 3 mois » ; « Une formation et une information régulièrement mise à jour dans ce domaine qui évolue constamment. »

Informations en général (13%)
« Meilleure communication sur les risques» ; « informer le personnel des menaces extérieurs» ; « informer les équipes sur les bons et mauvais gestes» ; « charte des bonnes pratiques informatiques » ;

Technologie 24%

Logiciel (11%)
« choisir les bons logiciels de protection » ; « utiliser les logiciels plus sécurisés » ; «installer un logiciel antivirus» ; « logiciel de blocage » ; « logiciel de surveillance en temps réel » ; « investir dans les logiciels plus performants »

Authentification (7%)
« renouveler les mots de passe plus souvent » ; « trois antivirus obligations d'un mot de passe compliqué et plusieurs mots de passe suivant les sites » ;
« changement de mot de passe obligatoire »

Technologie en général (6%)
« protections des systèmes et des réseaux» ;
« protection des données» ; « MAJ plus régulières »

Prévention 8%

«Sensibilisation des usagers aux bonnes pratiques » ; «Prévention des gestes dangereux» ; «Plus de prévention» ; « Sensibiliser ses employés plus fréquemment et de manière plus ludique en proposant par exemple des challenges ou concours récompensés autour de cette problématique »

Personnel 5%

« Engager un responsable de la sécurité informatique» ; « prendre une équipe pour surveiller » ; «Renforcement de l'équipe de protection» ; «Avoir un service informatique dédiée spécialement à ça»

Restrictions 5%

«Interdire totalement l'utilisation d'outils personnels sous peine de sanctions» ; « interdire certains accès internet» ; «Interdiction des clefs USB et des téléphones sur les locaux informatiques»

Ne sait pas / Rien : 27%

Base: 500 personnes - Ensemble

C8. Quelles sont, selon vous, les principales mesures que votre entreprise pourrait prendre pour améliorer sa sécurité informatique (prévention, formations, etc...) ?

SYNTHÈSE & CONCLUSIONS

05

SYNTHESE (1/4) :

1 Les salariés face aux risques cyber : un engagement globalement positif, mais des vulnérabilités persistent

- Des **employés très connectés**, en contacts avec une multitude de sites et outils au quotidien (messageries instantanées, moteurs de recherche, logiciels métier…) et donc **logiquement sujets aux risques de cybercriminalité**.
- La plupart ont cependant intégré les **bonnes pratiques**. Néanmoins des **risques persistent**, comme l'utilisation fréquente des appareils personnels.
- Pourtant, les salariés admettent sans mal leur sentiment de **responsabilité** dans la sécurité des données.
- Ainsi, ils se sentent pour la plupart **préoccupés** par les différents risques d'attaque.
- Plus de la moitié a d'ailleurs déjà remonté **un risque potentiel** à sa hiérarchie ou au service informatique.

- **87%** des salariés utilisent leurs messageries et outils collaboratifs dans le cadre de leur travail et 78% d'entre eux utilisent des moteurs de recherche
- **85%** d'entre eux sont par exemple vigilants lorsqu'ils ouvrent des pièces jointes ou cliquent sur des liens dans les emails
- **60%** utilisent leurs appareils personnels au moins une fois par mois pour effectuer une tâche professionnelle, et même 75% des 18-34 ans déclarent le faire.
- **Près de 8 salariés sur 10** pensent avoir leur part de responsabilité dans la sécurité des données de leur entreprise.
- **66%** des salariés sont préoccupés par les risques de phishing, **58%** préoccupés par le risque d'installer involontairement un logiciel malveillant sur le matériel de l'entreprise.
- **54%** des salariés ont déjà signalé un risque potentiel

SYNTHESE (2/4) :

2 Des salariés majoritairement conscients des risques de cyberattaques, mais un réel besoin d'information et surtout de formation persiste.

55% des salariés estiment que leur entreprise serait exposée aux risques de cyberattaque.

Mais ils se sentent pour la plupart aptes à y faire face :

- Pour près de 2 salariés sur 3, les cyberattaques ne sont pas une source de stress.
- 65% se disent bien informés sur les risques et bonnes pratiques
- Près de 60% ont connaissance des politiques de sécurité informatique de leur entreprise
- 41% ont été formés et sont globalement satisfaits de leur formation qu'ils jugent utile et adaptée à leur profession
- 1 salarié sur 2 estime que son entreprise est tout à fait capable de se protéger d'une cyberattaque.

Néanmoins, une marge de progression subsiste : **55% des salariés n'ont pas été formés**, alors que la majorité d'entre eux jugerait cette formation utile.

« faire davantage de préventions avec des formations courtes mais régulières »

« une formation en interne pour tous les nouveaux collaborateurs serait un plus »

« Sensibiliser ses employés plus fréquemment et de manière plus ludique en proposant par exemple des challenges ou concours récompensés autour de cette problématique »

SYNTHESE (3/4) :

3 Impact des cyberattaques : face à des pertes financières importantes, entreprises et salariés se montrent réactifs

18% des salariés ont eu connaissance d'une cyberattaque au sein de leur entreprise au cours des 12 derniers mois. Il en a résulté principalement des interruptions de service (37%) ou des pertes de données (33%). L'impact de ces incidents est variable, si près de la moitié estime la durée de l'incident a une journée, 40% mentionnent des incidents pouvant durer plusieurs jours, voire plusieurs mois.

En conséquence, les entreprises mettent en place différentes actions :

- 43% des salariés témoins d'une cyberattaque ont noté un renforcement des protocoles d'authentification, près de 40% une mise à jour régulière des systèmes et logiciels et 35% une sensibilisation et formation continue sur les dernières menaces.

et les salariés se montrent plus prudents :

- 74% des personnes ayant vécu une cyberattaque affirment être plus attentifs aux liens et aux pièces jointes présents dans les emails.
- Environ 2/3 ont changé leurs mots de passe et ne partagent plus de contenu confidentiel via des canaux non sécurisés.

SYNTHESE (4/4) :

4 Les entreprises de plus de 500 salariés sont plus exposées et mieux organisées, mais les PME ne sont pas en reste en matière de cybersécurité

- Les grandes entreprises sont plus exposées aux risques mais aussi mieux armées face aux attaques de cybercriminalité.
- Elles offrent davantage de formations à leurs salariés et sont perçues comme plus à même de se protéger contre les cyberattaques.
- Les employés issus d'une grande entreprise estiment que leur entreprise est tout à fait capable de se protéger d'une cyberattaque.
- Mais les scores dans les plus petites entreprises sont certes en-dessous, mais restent satisfaisants.

- **Pour 55% des salariés,** leur entreprise peut être exposée à un risque potentiel de cybercriminalité **vs 66% des salariés des entreprises de + de 500 salariés vs 47% des salariés des entreprises entre 20 et 149 salariés.**
- **1 salarié sur 2** dans les entreprises de + de 500 salariés a bénéficié d'une formation au cours des 24 derniers mois vs **41% en moyenne**.
- Une note de confiance de **7,5/10** pour les entreprises entre 500-4999 employés vs **6,9/10** pour les employés des entreprises de 20 à 149 employés)

- 59% des salariés des entreprises de 20-149 employés se sentent bien informés sur les risques de cybercriminalité et bonnes pratiques
- 49% d'entre eux ont connaissance des politiques de sécurité informatique.
- 33% des salariés des entreprises de 20-149 employés ont suivi une formation au cours des 24 derniers mois.

ANNEXES

NOS ENGAGEMENTS

CODES PROFESSIONNELS, CERTIFICATION QUALITÉ CONSERVATION ET PROTECTION DES DONNÉES

Ipsos est membre des organismes professionnels français et européens des études de marché et d'opinion suivants :

- **SYNTEC** (syndicat professionnel des sociétés d'études de marché en france ; www.Syntec-etudes.Com)
- **ESOMAR** (European Society for Opinion and Market Research, www.Esomar.Org)

Ipsos France est certifiée ISO 20252 : Market Research - version 2019 par AFNOR CERTIFICATION

Ce document est élaboré dans le respect de ces codes et normes internationales.

Ipsos France s'engage à appliquer le **code ICC/Esomar** des études de marché et d'opinion. Ce code définit les règles déontologiques des professionnels des études de marché et établit les mesures de protection dont bénéficient les personnes interrogées.

Ipsos s'engage à respecter les lois applicables. Ipsos a désigné un Data Protection Officer et a mis place un plan de conformité au Règlement Général sur la Protection des Données (Règlement (UE) 2016/679). Pour plus d'informations sur notre politique en matière de protection des données personnelles : https://www.ipsos.com/fr-fr/confidentialite-et-protection-des-donnees-personnelles

A ce titre, la durée de conservation des données personnelles des personnes interviewées dans le cadre d'une étude est, à moins d'un engagement contractuel spécifique :

de 12 mois suivant la date de fin d'une étude Ad Hoc .

de 36 mois suivant la date de fin de chaque vague d'une étude récurrente.

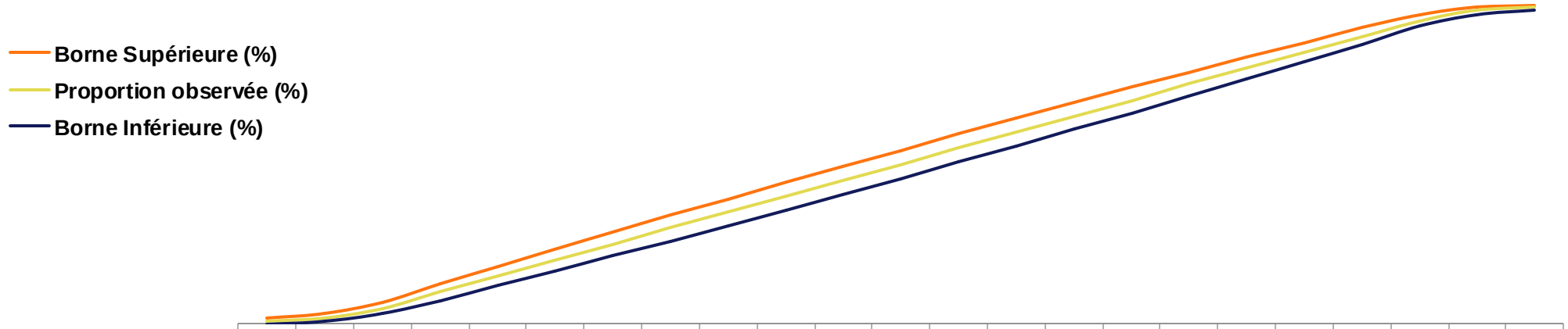
FIABILITÉ DES RÉSULTATS

Feuille de calcul

En l'occurrence s'agissant de cette étude :

- Intervalle de confiance : **95%**
- Taille d'échantillon : **500**

Les proportions observées sont comprises entre :



	1%	2%	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	55%	60%	65%	70%	75%	80%	85%	90%	95%	98%	99%
Borne Supérieure (%)	1.9%	3.2%	6.9%	12.6%	18.1%	23.5%	28.8%	34.0%	39.2%	44.3%	49.4%	54.4%	59.4%	64.3%	69.2%	74.0%	78.8%	83.5%	88.1%	92.6%	96.9%	99.2%	99.9%
Proportion observée (%)	1%	2%	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	55%	60%	65%	70%	75%	80%	85%	90%	95%	98%	99%
Borne Inférieure (%)	0.1%	0.8%	3.1%	7.4%	11.9%	16.5%	21.2%	26.0%	30.8%	35.7%	40.6%	45.6%	50.6%	55.7%	60.8%	66.0%	71.2%	76.5%	81.9%	87.4%	93.1%	96.8%	98.1%

À PROPOS D'IPSOS

Ipsos est l'un des leaders mondiaux des études de marché et des sondages d'opinion, présent dans 90 marchés et comptant près de 20 000 collaborateurs.
Nos chercheurs, analystes et scientifiques sont passionnément curieux et ont développé des capacités multi-spécialistes qui permettent de fournir des informations et des analyses poussées sur les actions, les opinions et les motivations des citoyens, des consommateurs, des patients, des clients et des employés.

Nos 75 solutions s'appuient sur des données primaires provenant de nos enquêtes, de notre suivi des réseaux sociaux et de techniques qualitatives ou observationnelles.

Notre signature « Game Changers » résume bien notre ambition d'aider nos 5 000 clients à évoluer avec confiance dans un monde en rapide évolution.

Créé en France en 1975, Ipsos est coté à l'Euronext Paris depuis le 1er juillet 1999. L'entreprise fait partie des indices SBF 120 et Mid-60 et est éligible au service de règlement différé (SRD).

ISIN code FR0000073298, Reuters ISOS.PA, Bloomberg IPS:FP
www.ipsos.com

GAME CHANGERS

Dans un monde qui évolue rapidement, s'appuyer sur des données fiables pour prendre les bonnes décisions n'a jamais été aussi important.

Chez Ipsos, nous sommes convaincus que nos clients cherchent plus qu'un simple fournisseur de données. Ils ont besoin d'un véritable partenaire qui leur procure des informations précises et pertinentes, et les transforme en connaissances pour leur permettre de passer à l'action.

Voilà pourquoi nos experts, curieux et passionnés, délivrent les mesures les plus exactes pour en extraire l'information qui permettra d'avoir une vraie compréhension de la Société, des Marchés et des Individus.

Nous mêlons notre savoir-faire au meilleur des sciences et de la technologie, et appliquons nos quatre principes de sécurité, simplicité, rapidité et de substance à tout ce que nous produisons.
Pour permettre à nos clients d'agir avec plus de rapidité, d'ingéniosité et d'audace.

La clef du succès se résume par une vérité simple :
You act better when you are sure.