

“opinionway

pour

 CCI FRANCE

 LA
TRIBUNE

 LCI

La grande consultation des entrepreneurs

Les dirigeants d'entreprise et la cybersécurité



Méthodologie & principaux enseignements

“*opinionway*” pour

 CCI FRANCE

LA
TRIBUNE

LCI



Étude réalisée auprès d'un échantillon de **610 dirigeants d'entreprise**.



La **représentativité** de l'échantillon a été assurée par un redressement selon le secteur d'activité et la taille, après stratification par région d'implantation.



L'échantillon a été interrogé **par téléphone**.



Les interviews ont eu lieu **du 20 au 28 octobre 2021**.



OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la **norme ISO 20252**.

La cybersécurité préoccupe une part croissante des dirigeants



610

CHEFS D'ENTREPRISE

- ▶ Alors que les entreprises ont amorcé en 2021 le retour progressif du travail en présentiel, les risques liés à la cybersécurité sont en hausse. 39% des dirigeants d'entreprise déclarent que ces risques les préoccupent, soit 14 points de plus par rapport à 2020. Cet indicateur, s'il est sensiblement plus élevé que les scores enregistrés depuis 2018 (entre +7 points et +15 points), est néanmoins presque identique à celui atteint en 2017 (1 point de moins seulement cette année vs 2017 ; 40% de dirigeants préoccupés il y a quatre ans).
 - Les dirigeants d'entreprises comptant 10 salariés voire plus, davantage susceptibles d'avoir un nombre croissant de point d'entrée des cyberattaques, se montrent plus préoccupés : 58% contre 37% des dirigeants d'entreprises moins grandes.
 - Le principal facteur d'inquiétude semble toutefois être le vécu d'une cyberattaque au cours de l'année passée. 77% des dirigeants dont l'entreprise a subi un tel évènement craignent les risques liés à la cybersécurité, contre 36% de ceux dont l'entreprise a été épargnée.
- ▶ Si plus d'un tiers des dirigeants s'inquiète des risques liés à la cybersécurité, peu d'entre eux jugent que leur entreprise fait face au risque imminent d'une cyberattaque. 17% indiquent que le niveau de probabilité est élevé, dont seulement 3% *très élevé*. Plus de 4 dirigeants sur 5 estiment au contraire que ce risque est faible (81%), dont 42% *très faible*.
 - Une nouvelle fois, les dirigeants d'entreprises comptant au moins 10 salariés se sentent davantage exposés : 39% jugent la probabilité d'une attaque élevée, contre 14% des dirigeants d'entreprises plus petites.
 - L'expérience récente d'une cyberattaque nourrit la crainte de devoir à nouveau affronter cette épreuve : 58% des dirigeants ayant subi une cyberattaque jugent le risque d'une nouvelle agression élevée, contre seulement 13% des autres dirigeants.
- ▶ Dans les faits, près de 10% des entreprises ont subi une cyberattaque dans les 12 derniers mois (8%). Cette menace ne pèse pas uniquement sur les entreprises de 10 salariés ou plus. Ces dernières sont certes plus nombreuses à déplorer une attaque (12%), mais les entreprises plus petites ne sont pas épargnées : 7% de leurs dirigeants font état d'une attaque dans les 12 mois écoulés.

La moitié des dirigeants se jugent prêts à gérer une cyberattaque



- ▶ Les attaques recensées par les dirigeants d'entreprise concernés sont variées. 30% témoignent d'une attaque *phishing*, 22% d'un virus informatique, 19% d'un vol de données présentes sur leurs serveurs. 17% déplorent un piratage de leur site, 15% une attaque aux faux ordres de virement, et encore 12% une usurpation d'identité. Dans plus d'un tiers des cas, les dirigeants déclarent que cela a mis en leur activité en difficulté (37%). Cela a duré plusieurs jours le plus souvent (23%), mais a parfois pu se compter en semaines (6%) voire en mois (8%).

- ▶ Plus de la moitié des dirigeants déclare que leur entreprise pourrait gérer une cyberattaque (52%). Toutefois, si 18% considèrent que leur entreprise pourrait faire face à cette agression sans problème, 34% concèdent qu'elle rencontrerait tout de même des difficultés à la surmonter. 41% des dirigeants déclarent enfin que leur entreprise se trouverait démunie en cas de cyberattaque.
 - Dotées de davantage de ressources humaines et matérielles, les entreprises comptant 10 salariés ou plus se montrent plus préparées à gérer une cyberattaque : 77% pourraient le faire contre 49% des entreprises plus petites.
 - Une majorité des dirigeants dont l'entreprise a récemment subi une attaque déclare qu'elle pourrait en affronter une nouvelle (58%). Les dirigeants épargnés par des cyberattaques au cours de l'année écoulée sont à peine moins confiants (52%).

- ▶ 44% des dirigeants déclarent que leur entreprise a déployé des mesures de défense contre les cyberattaques au cours des 12 derniers mois. Pour l'essentiel, il s'agit de la mise en place ou d'un renforcement de systèmes de sécurité comme des antivirus, pare-feu, etc.). Avec 37%, cette action rassemble plus d'entreprises que toutes les autres actions combinées.
 - Une large majorité des entreprises ayant subi cette année une cyberattaque ont mené des actions pour se renforcer face à ces risques (71%). Au contraire, moins de la moitié des entreprises non concernées par ces attaques ont pris des mesures pour se protéger (42%).

Les petites entreprises se désintéressent davantage des risques cyber



- ▶ Le sentiment que leur entreprise n'est pas concernée par les risques cyber est le premier frein évoqué par les dirigeants concernant la mise en place d'une politique de cybersécurité (30%). Dans une moindre mesure, les dirigeants citent le manque de connaissance en interne sur le sujet (16%), le manque de ressources financières (13%) et la complexité technique du sujet (11%). Près d'un tiers des dirigeants déclare toutefois qu'aucun frein ne s'oppose à la mise en place d'une politique de cybersécurité (35%).
- Les entreprises comptant au moins 10 salariés semblent avoir à surmonter moins de freins : 57% de leurs dirigeants déclarent qu'il n'y en a aucun. De leur côté, les dirigeants d'entreprises de moins de 10 salariés sont nettement plus nombreux à ne pas se sentir concernés par les risques cyber (33% contre 5% des dirigeants d'entreprises plus grandes).

Les résultats

“*opinionway* pour

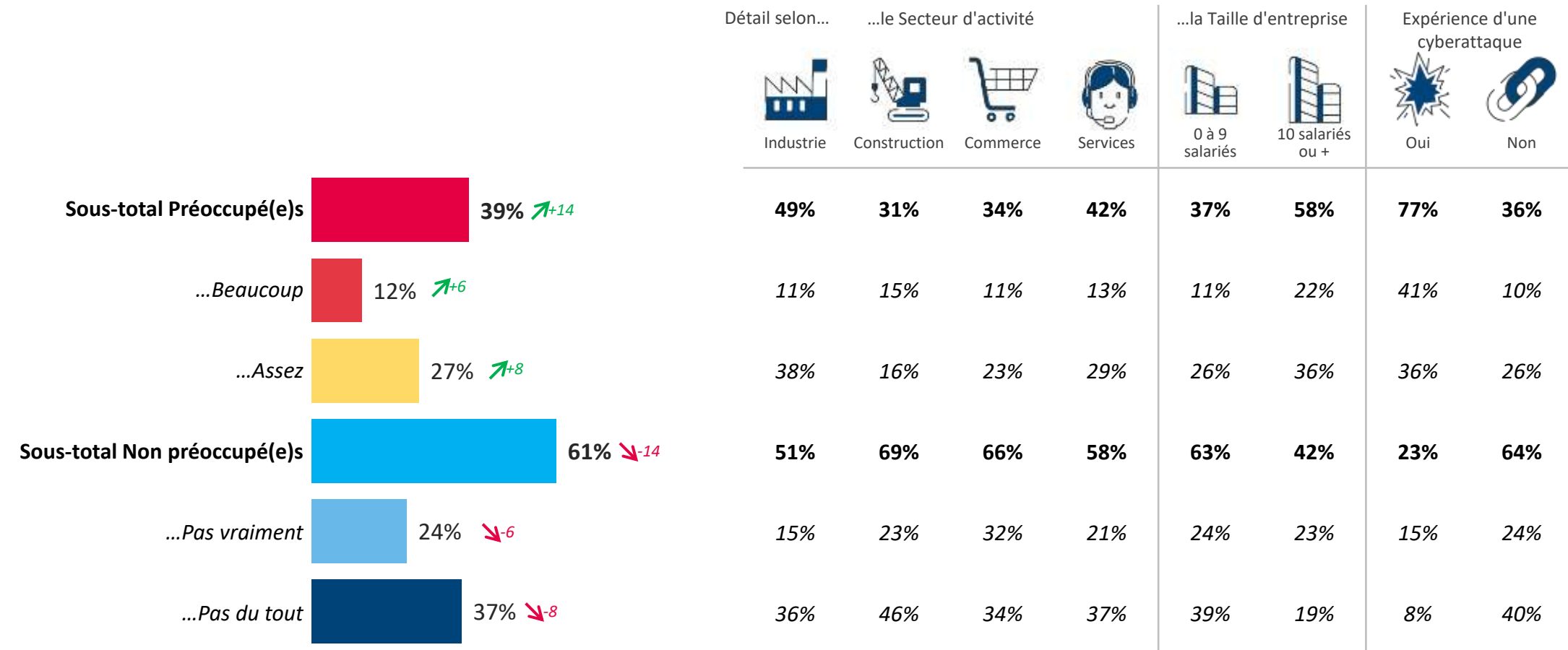


Les préoccupations concernant les risques liés à la cyber sécurité



Q : Diriez-vous que les risques liés à la cyber sécurité (vol de données, *e-reputation*, perte d'information, etc..) de votre entreprise vous préoccupent ?

BASE : Ensemble



Evolution depuis octobre 2020

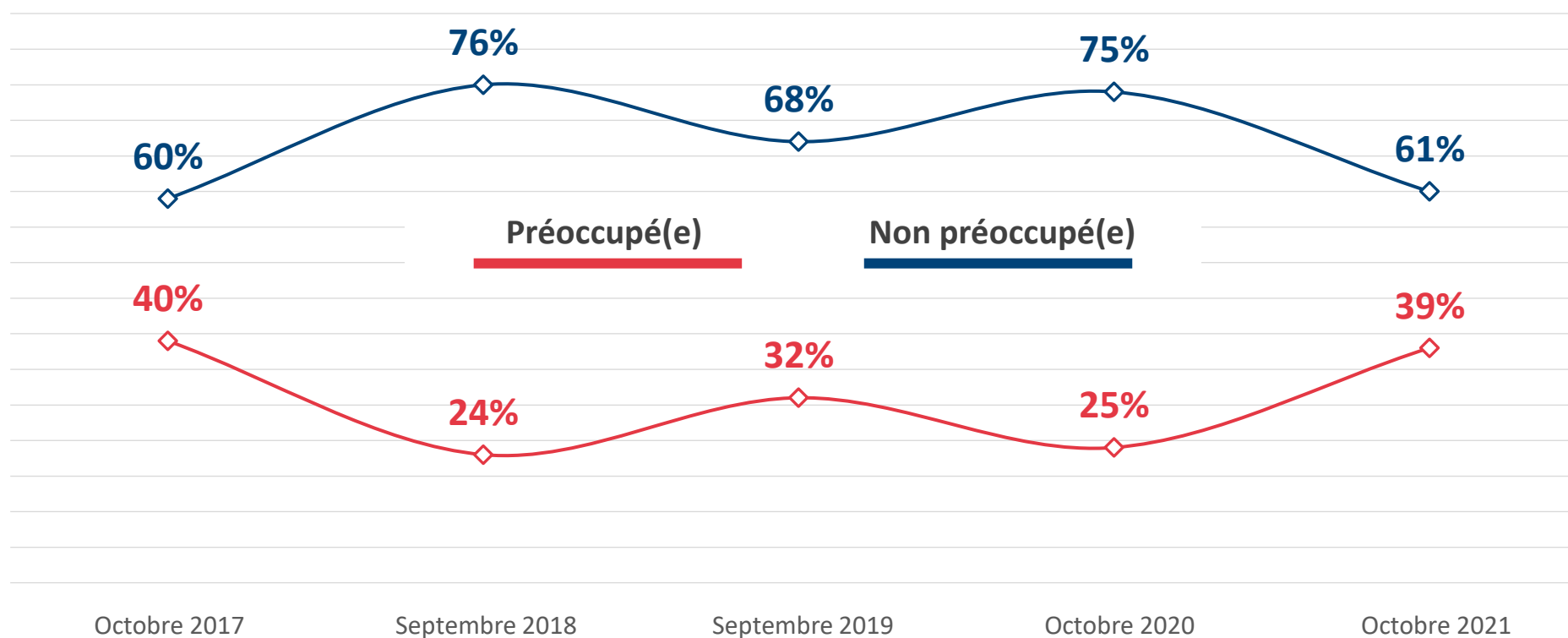
Les préoccupations concernant les risques liés à la cyber sécurité



610
CHEFS D'ENTREPRISE

Q : Diriez-vous que les risques liés à la cyber sécurité (vol de données, *e-reputation*, perte d'information, etc..) de votre entreprise vous préoccupent ?

BASE : Ensemble

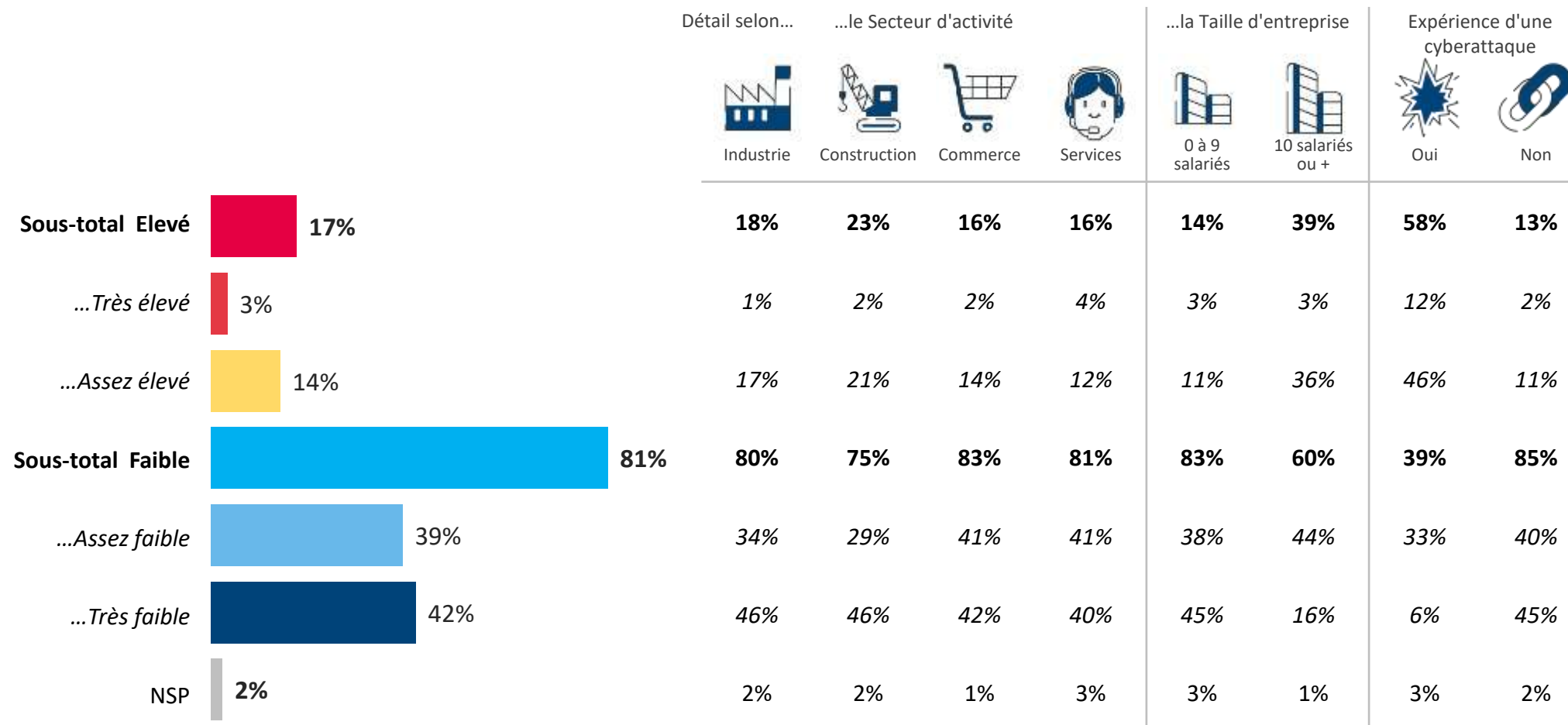


Le niveau de probabilité d'une cyberattaque à l'encontre des entreprises



Q : Aujourd'hui, selon vous, quel est le niveau de probabilité d'une cyberattaque à l'encontre de votre entreprise ?

BASE : Ensemble

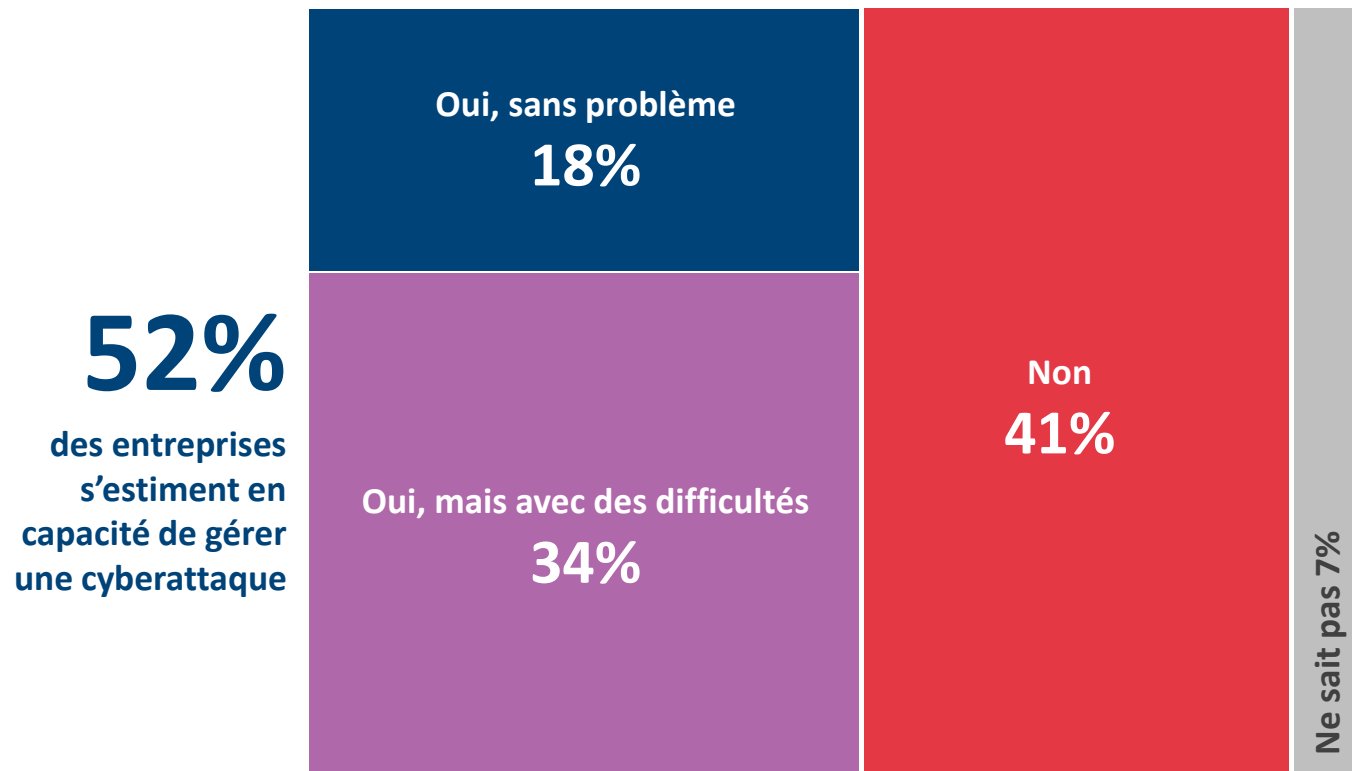


La capacité des entreprises à gérer une cyberattaque



Q : Selon vous, votre entreprise est-elle capable de gérer une cyberattaque?

BASE : Ensemble



	...le Secteur d'activité				...la Taille d'entreprise		Expérience d'une cyberattaque	
	Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +	Oui	Non
Total Oui	54%	45%	49%	55%	49%	77%	58%	52%
●	24%	12%	15%	20%	17%	25%	27%	17%
●	30%	33%	34%	35%	32%	52%	31%	35%
●	46%	48%	46%	37%	43%	20%	36%	42%
●	-	7%	5%	8%	8%	3%	6%	6%

Les actions déployées en matière de cybersécurité



610
CHEFS D'ENTREPRISE

Q : Dans les 12 derniers mois, quelles sont les actions que vous avez déployées en matière de cybersécurité au sein de votre entreprise ?

BASE : Ensemble / Plusieurs réponses possibles, total supérieur à 100%

Détail selon...

...le Secteur d'activité

...la Taille d'entreprise

Expérience d'une cyberattaque



Industrie



Construction



Commerce



Services



0 à 9 salariés



10 salariés ou +



Oui



Non

Sous-total Au moins une mesure 44%

Mise en place ou renforcement de systèmes de sécurité (achat d'anti-virus, déploiement de pare-feu, mise à jour des logiciels ...) 37%

Sensibilisation/Formation des collaborateurs aux risques 9%

Souscription à une assurance couvrant les risques de cybersécurité 5%

Collaboration avec des labels certifiés 4%

Mise en place d'un audit des systèmes d'information 4%

Création d'un ou plusieurs postes dédiés à la cybersécurité 1%

Autre 4%

Aucune mesure 54%

NSP 2%

	Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +	Oui	Non
Sous-total Au moins une mesure	53%	50%	40%	44%	41%	69%	71%	42%
Mise en place ou renforcement de systèmes de sécurité (achat d'anti-virus, déploiement de pare-feu, mise à jour des logiciels ...)	47%	46%	34%	36%	35%	62%	60%	36%
Sensibilisation/Formation des collaborateurs aux risques	11%	5%	9%	9%	6%	31%	17%	8%
Souscription à une assurance couvrant les risques de cybersécurité	2%	2%	3%	6%	5%	7%	9%	4%
Collaboration avec des labels certifiés	7%	2%	2%	6%	4%	6%	11%	4%
Mise en place d'un audit des systèmes d'information	6%	1%	2%	6%	3%	14%	5%	4%
Création d'un ou plusieurs postes dédiés à la cybersécurité	2%	2%	1%	1%	-	7%	2%	1%
Autre	4%	8%	4%	4%	4%	6%	9%	4%
Aucune mesure	47%	47%	60%	54%	58%	26%	29%	57%
NSP	-	3%	-	2%	1%	4%	-	1%

Les freins à la mise en place d'une politique de cybersécurité



610
CHEFS D'ENTREPRISE

Q : Quels sont les principaux freins à la mise en place d'une politique de cybersécurité au sein de votre entreprise ?

BASE : Ensemble / Plusieurs réponses possibles, total supérieur à 100%

	Détail selon...	...le Secteur d'activité				...la Taille d'entreprise		Expérience d'une cyberattaque	
		Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +	Oui	Non
Sous-total Au moins un frein	63%	66%	77%	65%	59%	66%	42%	72%	63%
Votre entreprise n'est pas concernée par les risques cyber	30%	28%	37%	35%	26%	33%	5%	6%	32%
Manque de connaissances et de compétences en interne	16%	26%	29%	13%	14%	16%	19%	32%	15%
Manque de ressources financières	13%	10%	10%	9%	16%	14%	9%	20%	13%
Complexité technique du sujet (organisation, déploiement, maintenance, ...)	11%	10%	23%	10%	9%	11%	8%	7%	11%
Difficultés à identifier et/ou à choisir des éditeurs spécialisés en cybersécurité	2%	4%	5%	1%	1%	2%	3%	2%	2%
Difficultés à sensibiliser et former les collaborateurs en interne	1%	1%	2%	1%	1%	1%	4%	-	1%
Autre	3%	3%	-	5%	3%	3%	4%	19%	2%
Aucun frein	35%	32%	20%	35%	38%	32%	57%	28%	35%
NSP	2%	2%	3%	-	3%	2%	2%	-	2%

L'expérience récente d'une cyberattaque au sein de l'entreprise



Q : Votre entreprise a-t-elle été victime d'une ou plusieurs cyberattaque(s) ces 12 derniers mois ?

BASE : Ensemble

8%

des entreprises déclarent avoir été victimes d'une cyberattaque



Détail selon...

...le Secteur d'activité

...la Taille d'entreprise



Industrie



Construction



Commerce



Services



0 à 9 salariés



10 salariés ou +

	Industrie	Construction	Commerce	Services	0 à 9 salariés	10 salariés ou +
Total Oui	5%	9%	7%	9%	7%	12%
●	5%	-	2%	3%	2%	3%
●	-	9%	5%	6%	5%	9%
●	95%	91%	93%	90%	92%	87%
●	-	-	-	1%	1%	1%

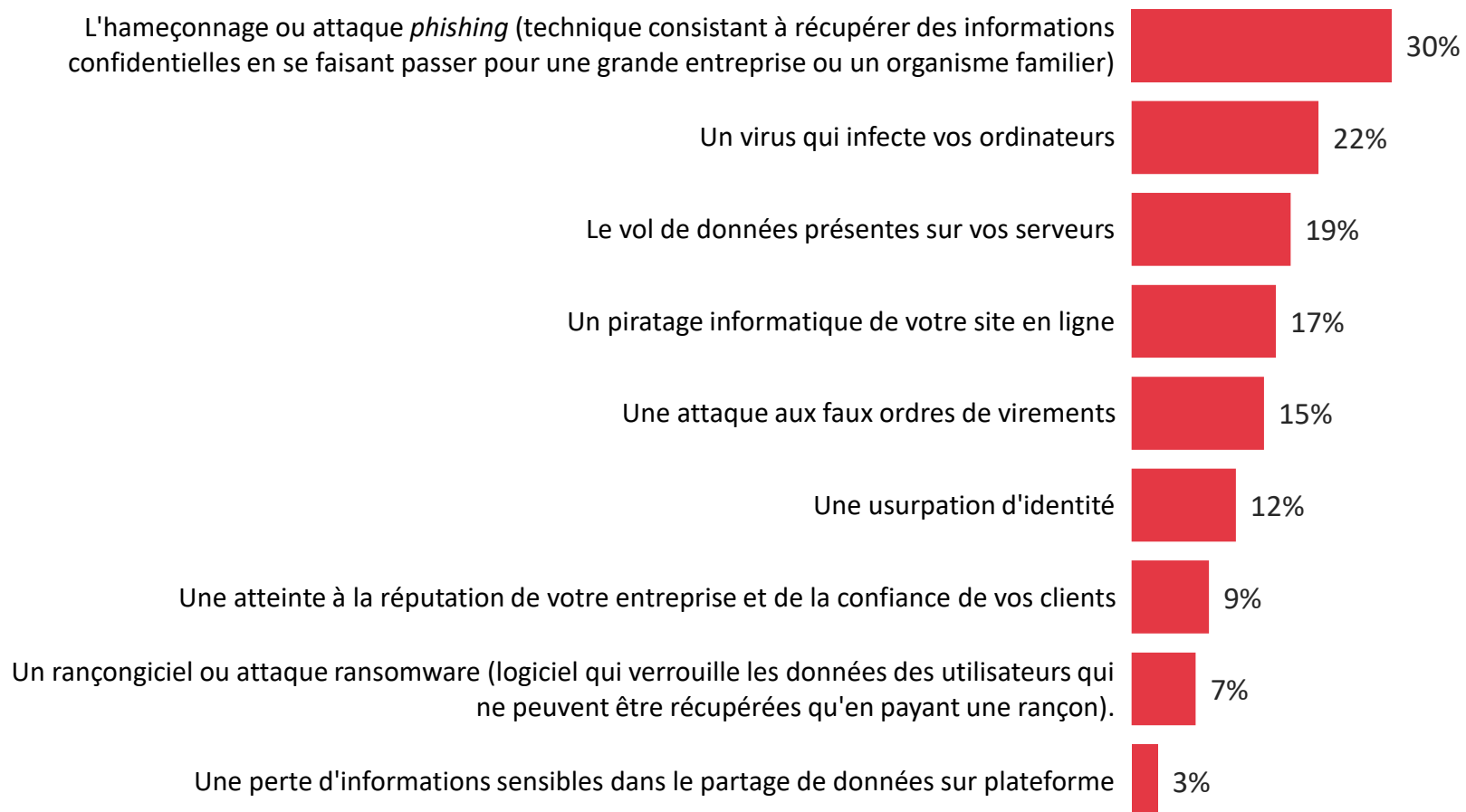
NSP 1%

La nature des cyberattaques subies



Q : Merci de préciser le(s) type(s) de cyberattaque(s) :

BASE : Question posée uniquement aux entreprises ayant été victimes de cyberattaque, soit 8% des entreprises / Plusieurs réponses possibles, total supérieur à 100%



L'impact des cyberattaques sur la poursuite d'activité des entreprises

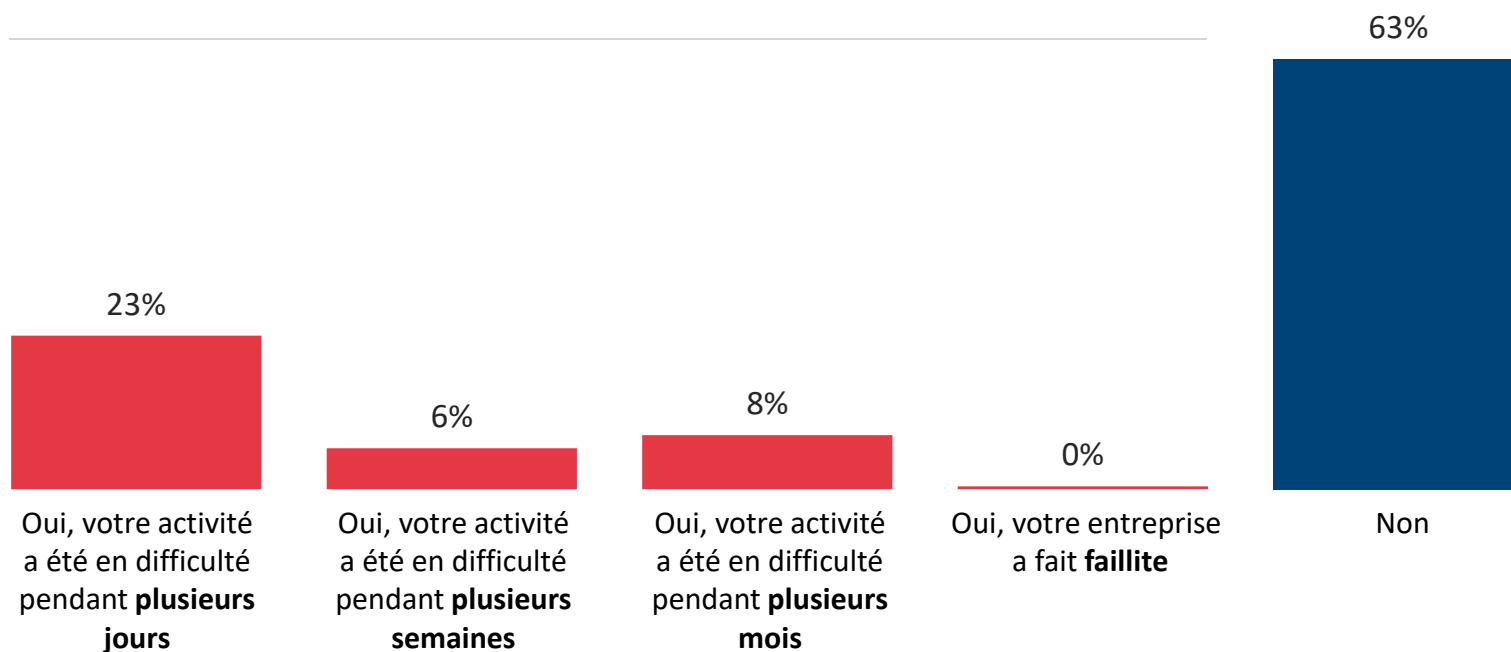


Q : Ces cyberattaques ont-elles mis en danger la poursuite d'activité de votre entreprise ?

BASE : Question posée uniquement aux entreprises ayant été victimes de cyberattaque, soit 8% des entreprises

Un impact de la cyberattaque dans

37% des cas



“opinionway

pour



**LA
TRIBUNE**

LCI

La grande consultation des entrepreneurs