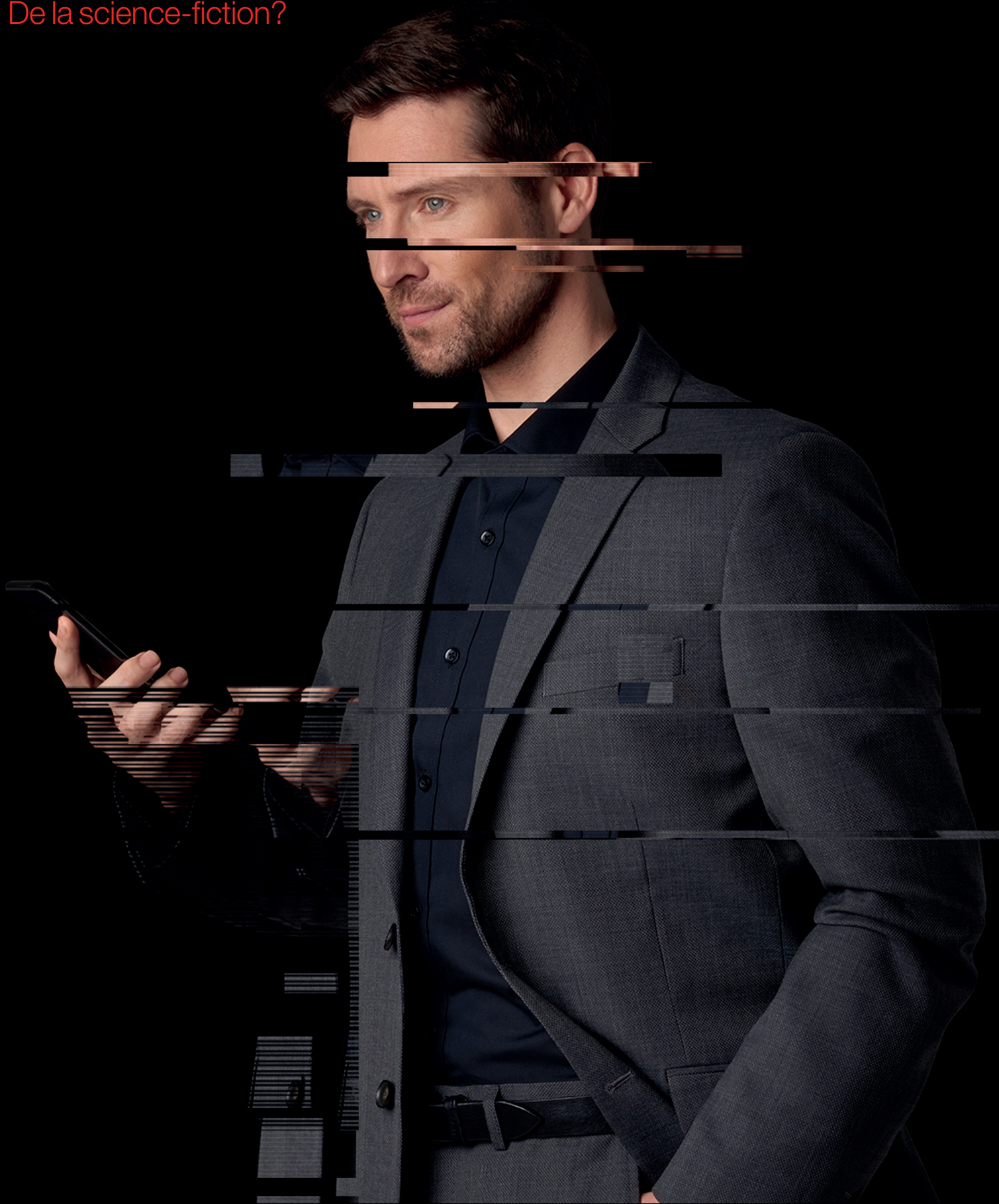
HISCOX
ASSURANCES

Penser à tout, et surtout à vous

Petites entreprises et risques Cyber

De la science-fiction?



Les petites entreprises sont vulnérables

La cyber-menace s'intensifie pour les petites entreprises. Quelles ressources sont-elles disposées à consacrer à ce problème et quelles sont leurs capacités?

Le Rapport Hiscox 2019 sur la gestion des cyber-risques se base sur une étude réalisée auprès de plus de 2 000 petites entreprises (moins de 50 salariés) au Royaume-Uni, en Europe et aux États-Unis. Il révèle que le nombre de petites entreprises ayant signalé au moins un cyber-incident dans l'année a progressé, passant de 33% à 47%.

Des coûts en hausse

Comment cela se traduit-il en terme de coûts ? Le coût moyen de l'ensemble des cyber-incidents subis par les petites entreprises s'élevait à 14 000 €, et le coût moyen du pire incident subi était de 9 000 € (contre 3 000 € l'année précédente).

Un nombre limité de cyber ressources disponibles

Lorsqu'il s'agit de s'attaquer au problème, quelles ressources les petites entreprises sont-elles disposées à déployer et quelles sont leurs capacités ? En moyenne, les petites entreprises que nous avons interrogées ont consacré une plus faible proportion de leurs budgets informatiques à la gestion des cyber-risques que les grandes entreprises (8,3% contre 9,5%).

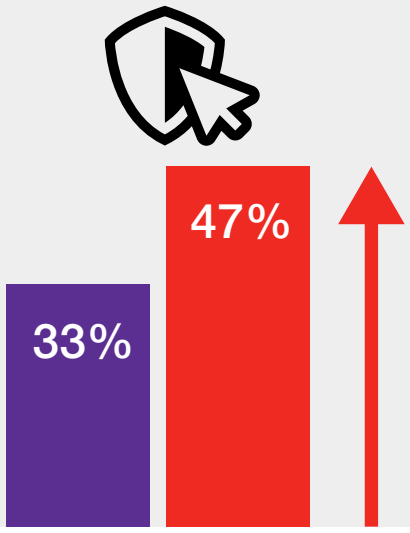
Réduction des dépenses

21% des petites entreprises ont indiqué vouloir réduire leurs dépenses consacrées aux cyber-risques de 5% ou plus au cours de l'année à venir. Interrogées sur le nombre de salariés à temps plein au sein de leur équipe de gestion de la cybersécurité (comprenant les équivalents temps plein de leurs consultants externes), près de trois-quarts des petites entreprises ont répondu « aucun » (23%), ou moins de cinq (53%).

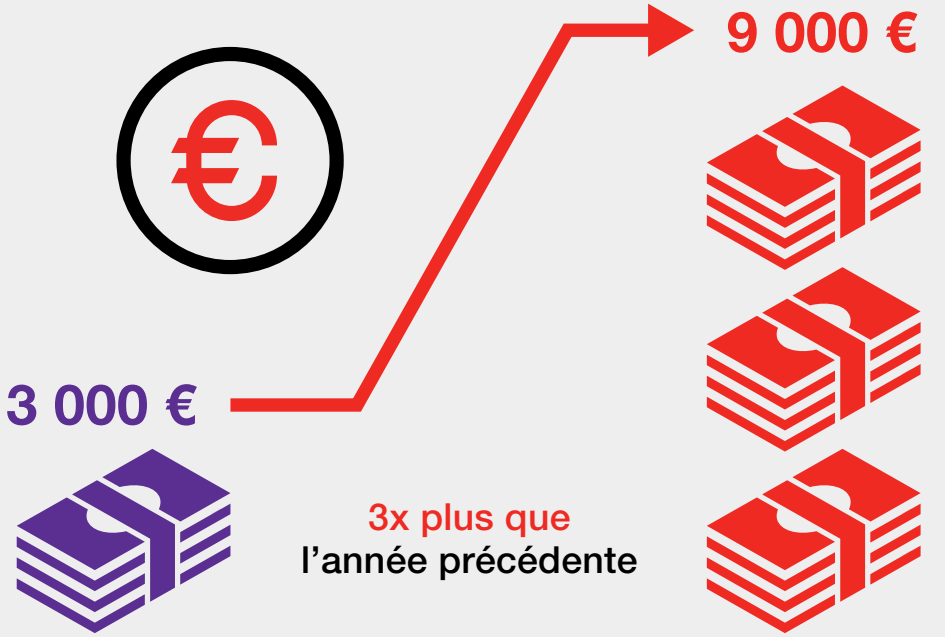
Les petites entreprises identifient moins rapidement une faille

Sans surprise, étant donné leurs ressources plus limitées, les petites entreprises identifient moins rapidement une faille de cybersécurité. A la question de savoir combien de temps elles ont mis à découvrir l'incident le plus grave subi au cours des 12 derniers mois, les petites

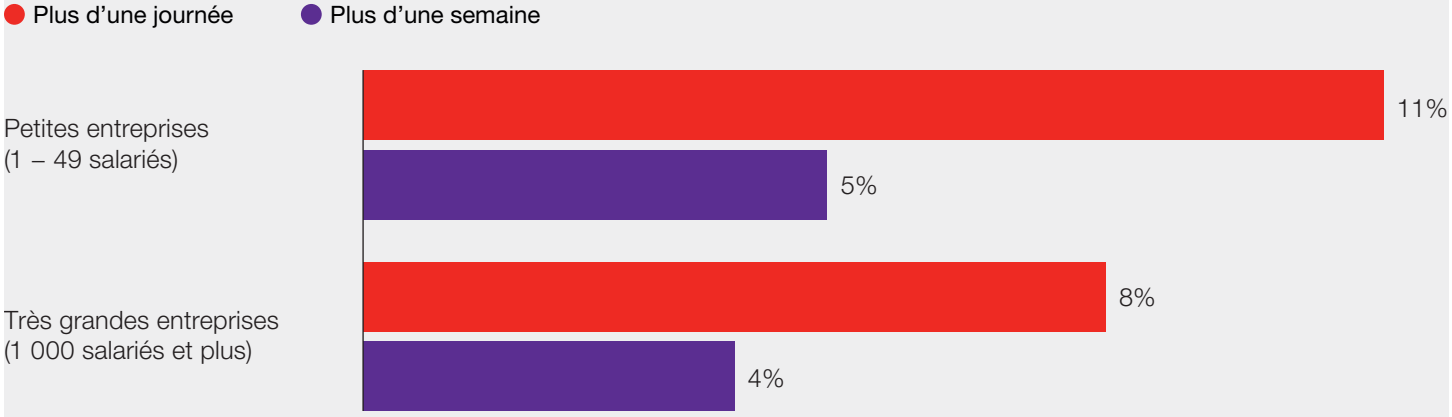
Augmentation des cyber-incidents déclarés au cours de l'année passée



Augmentation du coût moyen du pire incident déclaré



Temps nécessaire à la découverte de la faille la plus importante



Les dirigeants voient la cybersécurité comme une problématique sérieuse, mais...

Au vu des meilleures pratiques, les petites entreprises demeurent insuffisamment préparées face aux cyber-risques.

entreprises ont généralement rapporté des délais plus longs (voir ci-dessous). Les chiffres ne tiennent pas compte de la nature de l'incident en question et celui-ci a vraisemblablement été plus grave pour les grandes entreprises.

Plus de la moitié (56%) des petites entreprises ont indiqué que la cybersécurité constituait une « priorité majeure » aux yeux des dirigeants ou du conseil 'administration. Seule une minorité de petites entreprises ont déclaré qu'elles avaient un responsable de la cybersécurité (28%) ou une équipe dédiée à la cybersécurité (22%), un nombre équivalent ayant indiqué recourir aux services d'un prestataire externe (23%).

Près d'un tiers des petites entreprises (31%) ont répondu qu'elles n'avaient aucun employé en charge de la cybersécurité.

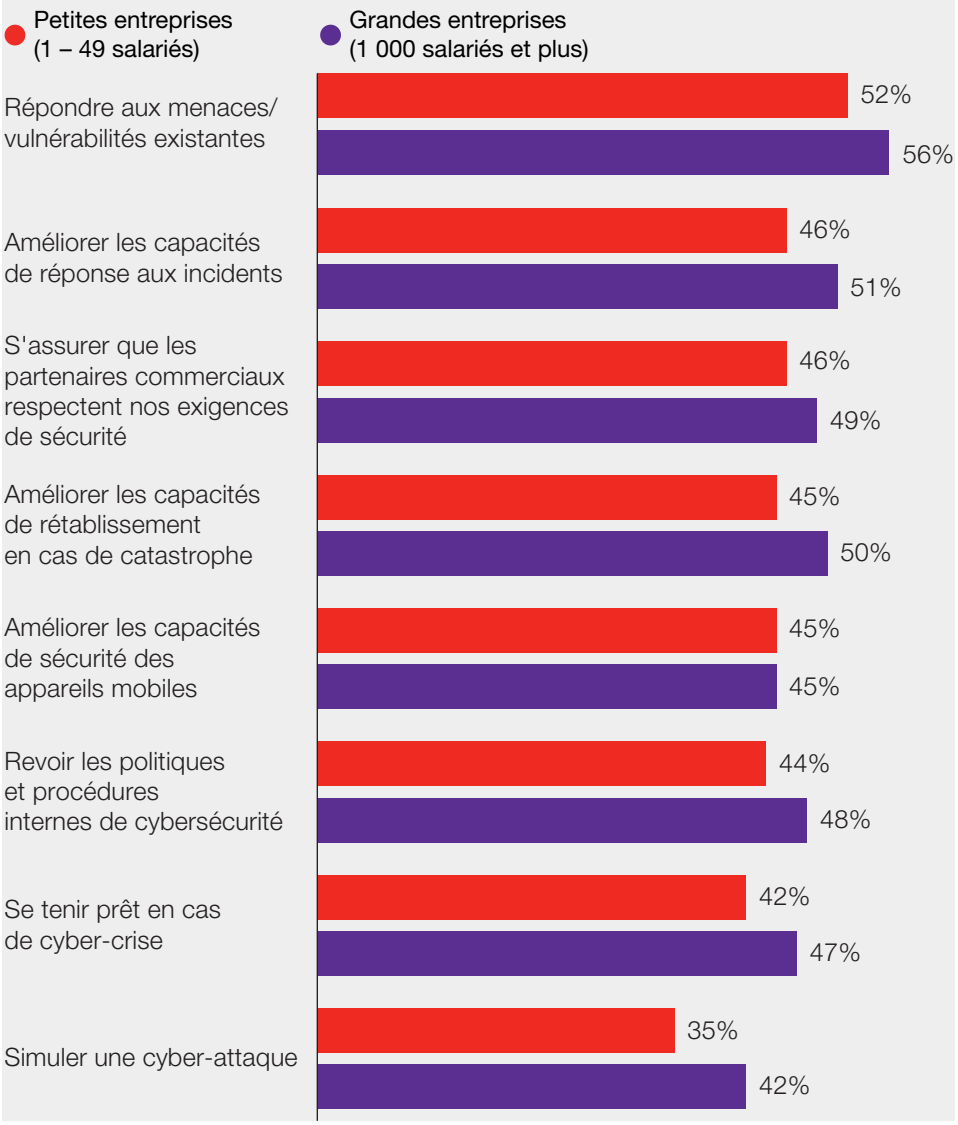
Concernant la définition de leurs priorités pour l'année à venir, les petites entreprises sont très en retard par rapport aux grandes entreprises dans de nombreux domaines clés.

Capacités de gestion des cyber-risques

La modélisation des capacités de gestion des cyber-risques mesure précisément l'écart entre les pratiques d'une société et ce qu'on peut considérer comme les meilleures pratiques. Les personnes interrogées doivent répondre à une série de questions couvrant leur approche dans deux domaines: stratégie et ressources d'une part et technologie et procédures de l'autre. Elles sont invitées à nous dire à quel point leurs pratiques relèvent d'une approche bien structurée, rigoureuse et efficace.

Les petites entreprises se sont en moyenne classées dans la tranche basse du panel de l'étude, seuls 7% des répondants rentrant dans la catégorie expert (pour une moyenne de 10%). 76% des petites entreprises sont classées en tant que novices, les 17% restant se classant intermédiaires.

Priorité élevée ou critique pour l'année à venir=



Quelles solutions pour les petites entreprises?

Comment les petites entreprises peuvent-elles améliorer leur cybersécurité et s'assurer que leurs défenses sont aussi solides que possible?

Voici une brève liste de quelques bonnes pratiques recommandées aux petites entreprises.

1. **Désigner un responsable de la cybersécurité**
   Seule une minorité de petites entreprises ont un préposé à la cybersécurité. Cela complexifie l'identification, le suivi et la documentation des cyber-incidents et réduit également la possibilité d'une planification stratégique de long-terme dans ce domaine.

2. **Mettre en place des processus et une planification**
   Les petites entreprises ne sont pas nécessairement moins enclines que les grandes à installer des technologies antivirus, anti spyware ou anti malware. Là où elles sont en revanche en retard, c'est dans la mise en place de processus fiables - collecte des données de cybersécurité, intégration de la cybersécurité dans la planification, les opérations commerciales et les procédures d'audit interne, suivi et documentation.

3. **Mieux former le personnel**
   Moins de la moitié des petites entreprises (43%) ont déclaré que l'affirmation « l'organisation dispense des formations de sécurité et de sensibilisation à l'ensemble du personnel » était juste en tout ou partie. Seules 29% des petites entreprises ont indiqué qu'elles prévoyaient d'augmenter de 5% ou plus leurs dépenses de formation à la sensibilisation des salariés dans l'année à venir. On déplore néanmoins qu'un tiers des petites entreprises (33%) prévoient de réduire leur budget de formation à la cybersécurité dans l'année à venir.

4. **Répondre aux failles par des mesures concrètes**
   Près de la moitié (45%) des petites entreprises ont déclaré qu'elles n'avaient apporté aucun changement à la suite d'un incident ou d'une série d'incidents. Ce chiffre est inférieur à celui de 58% relevé l'année précédente, et il est clair que les petites entreprises doivent davantage apprendre de leurs failles de cybersécurité passées pour s'assurer de ne pas être de nouveau victimes d'un incident semblable.

5. **Prendre en compte les risques liés à la chaine logistique**
   Les petites entreprises identifient mal les menaces de cybersécurité qui pèsent sur leur chaîne logistique. La plupart d'entre elles (60%) se disent confiantes dans les mesures de protection des données de leurs fournisseurs, et à peine plus de la moitié (51%) rapportent avoir subi un incident lié à la chaine logistique. Mais seule une minorité de petites entreprises incluent des indicateurs clés de performance de la cybersécurité dans les contrats avec les fournisseurs et imposent à leurs fournisseurs de rendre des comptes au regard de ces indicateurs (39% dans chacun des cas). En comparaison, dans les grandes entreprises ces chiffres atteignent respectivement 65% et 61%.

   Cela peut s'expliquer par le fait que les petites entreprises n'ont pas le poids des grandes pour imposer des conditions à leurs fournisseurs. Mais un nombre relativement faible d'entre elles associent leur équipe d'achats dans la définition de la cyberstratégie (9% contre 14% dans les grandes entreprises).

6. **Simuler une cyber-attaque/Faire des tests de phishing en interne**
   Seules 26% des petites entreprises ont indiqué que simuler une cyber-attaque constituait une priorité élevée ou critique pour l'année à venir, et 35% ont indiqué qu'elles avaient mené leurs propres tests de phishing pour comprendre le comportement des salariés et leur capacité de réaction en cas d'attaque.

7. **Souscrire une cyber-assurance**
   Les petites entreprises sont moitié moins nombreuses que les grandes entreprises à avoir souscrit une police d'assurance cyber (27% contre 51%) et seules 32% d'entre elles considéraient que « souscrire une police cyber ou améliorer les garanties de la police cyber en place » constituaient une priorité critique ou élevée pour l'année à venir.

HISCOX
ASSURANCES

Penser à tout, et surtout à vous

Méthodologie

Toutes les statistiques de ce rapport proviennent du Rapport Hiscox 2019 sur la gestion des cyber-risques. Hiscox, assureur spécialisé, a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5 392 professionnels impliqués dans la stratégie de cybersécurité de leur entreprise ont été contactés (plus de 1 000 personnes par pays pour le Royaume-Uni, les États-Unis et l'Allemagne et 500 pour la Belgique, la France, l'Espagne et les Pays-Bas). 39% des répondants représentaient des entreprises de moins de 50 salariés (petites entreprises), 16% des entreprises de taille moyenne (entre 50 et 250 salariés), 16% des grandes entreprises (entre 250 et 999 salariés) et les 28% restants, des très grandes entreprises (1 000 salariés ou plus). Les répondants ont rempli le questionnaire en ligne entre le 22 octobre et le 7 décembre 2018.

Hiscox SA

38 Avenue de l'Opéra
75002 Paris

T +33(0) 15 321 8282
F +33(0) 15 320 0720
E info.france@hiscox.com
www.hiscox.fr

20364 11/19