beazley

Lumière sur
La transformation technologique et les risques cyber 2025

France

Notre recherche

L'enquête de cette année a été réalisée entre le 06.01.25 et le 17.01.25.En 2021, l'enquête a été réalisée auprès de répondants basés au Royaume-Uni et aux États-Unis. En 2022 et 2023, la base d'échantillonnage comprenait également des répondants basés au Canada et à Singapour, et en 2024, la base d'échantillonnage a été élargie pour inclure des répondants en France, en Allemagne et en Espagne.

beazley

Nous avons interrogé 3 500 chefs d'entreprise sur...

leurs plus grandes préoccupations en matière de risques d'entreprise et leur degré de résilience face aux risques suivants :

- Risques cyber
- Risques de perturbations technologiques
- Risques d’obsolescence technologiques
- Risques de propriété intellectuelle

Nous avons entrepris cette étude en janvier 2025 auprès de chefs d'entreprise internationaux (acheteurs d'assurance), issus de ces différents secteurs d'activité :

- Santé et sciences de la vie
- Industrie, commerce de détail, commerce de gros et alimentation et boissons
- Immobilier et construction
- L'hôtellerie, le divertissement et les loisirs
- Institutions financières et services professionnels
- Énergie et services publics (y compris l'exploitation minière), marine et entreposage
- Secteur public et éducation
- Technologie, médias et télécommunications
- Transport, logistique, fret et aviation

Perception

Les préoccupations liées aux risques cyber et technologiques augmentent, mais les dirigeants se sentent mieux préparés à y faire face.

Réalité

De nombreuses entreprises sont exposées et mal préparées aux menaces numériques en constante évolution.

Les entreprises françaises sont confrontées à une **« lutte sans fin »** contre les risques cyber et technologiques qui exigent une gestion vigilante et continue des risques.

Les entreprises ont besoin d'aide pour mettre en place des **stratégies de défense** en profondeur afin de renforcer leur résilience.

27%

Les risques cyber ont été désignés comme la plus grande menace de cette année, contre 26 % en 2024. Malgré cela, 76 % des personnes interrogées se sentent prêtes* à faire face à ces risques, contre 70 % en 2024

32%

Prévoient d'investir dans l'amélioration de la cybersécurité cette année, contre 22 % en 2024.

25%

ont classé le risque d'obsolescence technologique comme leur principale menace cyber et technologique cette année, contre 29 % en 2024.

72%

ont convenu que leur entreprise prévoyait d'améliorer leur cybersécurité avec ses fournisseurs tiers à la suite d'incidents cyber systémiques très médiatisés.

73%

S'accordent à dire que l'IA aura un impact positif sur les perspectives économiques de leur entreprise cette année, et 54 % ont convenu que l'IA remplacera des emplois dans leur entreprise au cours des 18 prochains mois.

25%

ont classé le risque lié à la propriété intellectuelle comme leur principale menace cette année, contre 19 % en 2024. Dans le même temps, leur sentiment de résilience face à ce risque a augmenté, dont 26 % d'entre eux se sentant mal préparés**, contre 30 % en 2024.

* Réponses très bien préparées et moyennement bien préparées combinées.
** Réponses pas très bien préparées et pas du tout préparées combinées.

beazley

Ce que les chiffres révèlent

- De nombreuses entreprises surestiment leur résilience face aux risques cyber et technologiques.
- De nombreuses organisations sont mal préparées à faire face à une cyberattaque ou à une violation de données.
- Les entreprises cherchent à améliorer leur cybersécurité.
- L'optimisme quant aux avantages commerciaux de l'IA est en hausse.
- Les inquiétudes concernant le risque d'obsolescence technologique sont en baisse.

A retenir

Pour les courtiers

1. **La cyber-résilience va au-delà d'une simple couverture d'assurance.** Les entreprises ont besoin d'une cybersécurité multicouche et d'un soutien préventif, réactif et adaptatif pour les aider avant, pendant et après un incident cyber, en plus de simplement souscrire une assurance cybersécurité.

2. **La responsabilité civile envers des tiers.** L'interconnectivité technologique actuelle crée des vulnérabilités chez les fournisseurs, entraînant une responsabilité civile envers des tiers : allant des risques cyber et des interruptions d'activité, aux réclamations D&O et à la perte de réputation.

3. **Les tensions politiques augmentent les risques cyber**
À mesure que les tensions géopolitiques s'intensifient et que les relations évoluent, les risques cyber augmentent également, car les acteurs malveillants des États-nations créent de nouvelles vulnérabilités que les cybercriminels peuvent exploiter.

Pour les entreprises

1. **Une préoccupation croissante pour les actionnaires**
À mesure que les risques cyber augmentent, le risque de perturbation et d'atteinte à la réputation s'accroît également. Les mauvaises décisions en matière de cybersécurité font désormais l'objet d'une plus grande surveillance, exposant les entreprises à des conséquences juridiques, financières et opérationnelles.

2. **Regards sur la propriété intellectuelle et la confidentialité des données.** Les réglementations nationales en matière de propriété intellectuelle et de confidentialité des données sont fragmentées et créent des risques pour les entreprises opérant à l'international qui pourraient enfreindre involontairement la nouvelle législation. Pourtant, les préoccupations relatives aux risques liés à la propriété intellectuelle sont en baisse.

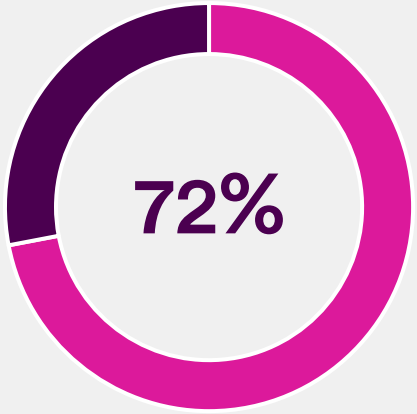
3. **Exploiter la puissance de l'IA.** Avec **30 %** des dirigeants français prévoyant d'investir dans les nouvelles technologies cette année et **54 %** anticipant des pertes d'emplois induites par l'IA dans les 18 prochains mois, les entreprises doivent rester vigilantes quant aux meilleures pratiques et aux risques liés à l'IA.

Le mirage de la cybersécurité

Les entreprises mondiales sont confrontées à une multitude de risques cyber et technologiques.

Connexions vulnérables

- Le risque cyber lié aux fournisseurs tiers s'intensifie, à mesure que les chaînes d'approvisionnement deviennent interconnectées et de plus en plus vulnérables aux cyberattaques.
- Les cybercriminels ciblent les grandes entreprises par l'intermédiaire de petits fournisseurs qui peuvent ne pas disposer des ressources nécessaires pour maintenir une cybersécurité robuste.
- L'externalisation de la cybersécurité peut créer un faux sentiment de sécurité et ne remplace pas :
  - La formation continue des employés
  - La planification de la continuité des activités
  - Le maintien des meilleures pratiques internes
  - La cybersécurité à plusieurs niveaux
  - Les connexions vulnérables



des dirigeants français ont déclaré prévoir d'améliorer leur cybersécurité avec ses fournisseurs tiers à la suite de récents incidents cyber systémiques très médiatisés.

beazley

Le mirage de la cybersécurité

Les Etats utilisent le cyberespace comme une forme de cyberguerre, et l'IA rend les cybercriminels plus efficaces.

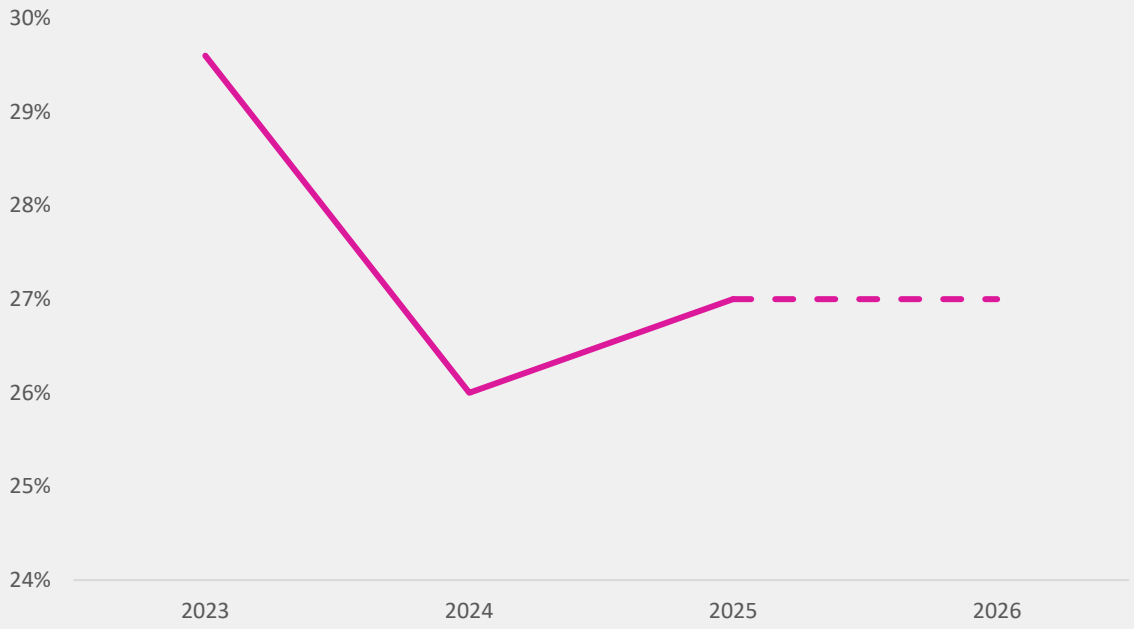
L'intersection entre politique et cybersécurité

- Les cyberattaques sont désormais des outils de guerre hybride, utilisés pour semer le chaos et exercer une pression politique.
- Les hacktivistes utilisent les cyberattaques pour faire avancer leurs agendas, souvent en restant dans les systèmes et en représentant une menace à long terme.

Évolution des ransomwares

- L'essor des appareils Edge et de l'IoT offre aux cybercriminels de nouveaux points d'entrée dans les systèmes.
- L'IA aide les cybercriminels à automatiser leurs attaques, à améliorer le phishing et à créer des deepfakes plus convaincants.

Préoccupations relatives aux risques cyber au fil du temps



Pourcentage de dirigeants basés en France qui ont classé le risque cyber (incapacité de l'entreprise à garantir la confidentialité des données ou menace criminelle externe, y compris les ransomwares ou les menaces systémiques plus larges entraînant une interruption grave de l'activité) comme leur principal risque cyber et technologique au fil du temps. Les chiffres pour 2026 sont une prévision du principal risque dans 12 mois.

beazley

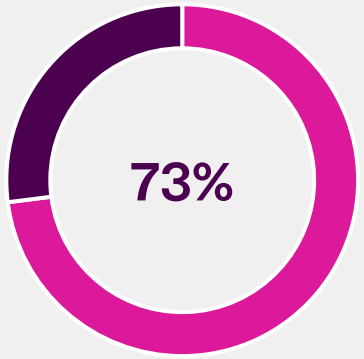
Transformation technologique – du code à la cognition

L'IA oblige les entreprises à trouver un équilibre entre ses avantages et la nécessité de mettre en place des mesures de protection solides contre les risques émergents.

Risques et avantages

- L'optimisme envers l'IA est en plein essor. Aujourd'hui, le risque de sous-investir dans l'IA l'emporte sur celui de surinvestir.

- La supervision humaine est essentielle pour atténuer les risques tels que la violation du droit d'auteur, la violation de la propriété intellectuelle, les préjugés et la diffamation.

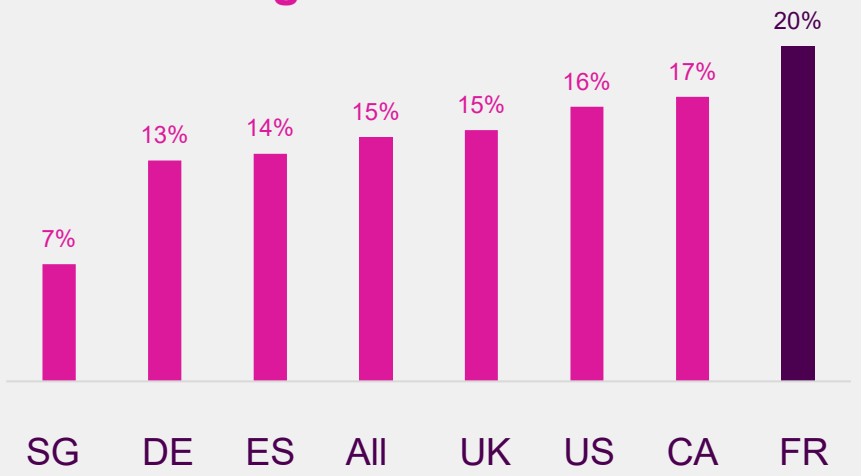


des dirigeants basés en France s'accordent à dire que l'IA aura un impact positif sur les perspectives économiques de leur entreprise cette année.

Technologies obsolètes

- L'IA soulève des inquiétudes quant à l'obsolescence technologique, aux perturbations et au déclin de la compétitivité.

La préparation à l'obsolescence technologique varie selon les régions.



Pourcentage de dirigeants qui se sentent mal préparés (réponses « pas très bien » et « pas du tout » combinées) pour anticiper et répondre au risque d'obsolescence technologique – l'incapacité à suivre le rythme des évolutions technologiques et des opportunités (par exemple, l'IA générative, l'IoT et l'automatisation) ; l'incapacité à mettre à jour les systèmes – comme leur principal risque cyber et technologique par région.

beazley

Sécurisé ou exposé – Confidentialité des données et de la propriété intellectuelle

La protection des données et la sécurité de la propriété intellectuelle sont devenues de plus en plus importantes.

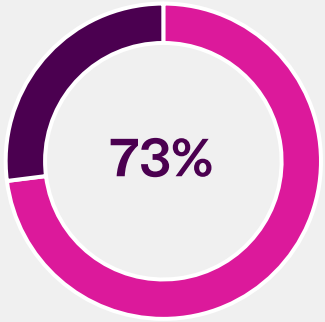
Risques latents

- Les règles relatives à l'IA et aux droits d'auteur restent floues, et le risque de vol de propriété intellectuelle existante est important.

Labyrinthe réglementaire

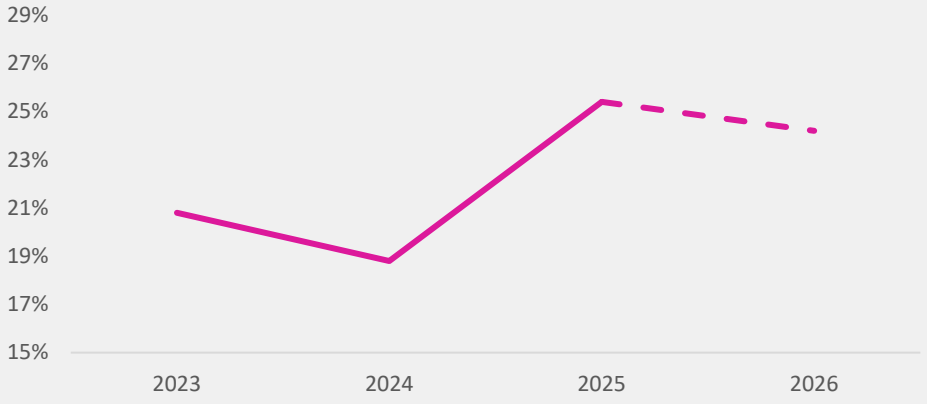
- Les nouvelles réglementations nationales visant à contrer les risques liés à la confidentialité des données et à la propriété intellectuelle compliquent encore davantage la tâche des entreprises internationales.

- Alors que les tensions géopolitiques persistent, les organisations sont exposées au risque de vol de propriété intellectuelle et de violation des données par des gouvernements hostiles.



des dirigeants français continuent de négliger les risques liés à la propriété intellectuelle, alors même que les préoccupations sur ce sujet ne cessent de croître, et la perception de préparation est en hausse de 67 % depuis 2004.

Les préoccupations relatives aux risques liés à la propriété intellectuelle en France atteignent un pic en 2025



Pourcentage de cadres dirigeants basés en France qui ont classé le risque lié à la propriété intellectuelle (incapacité à reconnaître et à protéger la valeur des actifs de propriété intellectuelle tels que le savoir-faire, les brevets ou les actifs incorporels) comme leur principal risque cyber et technologique au fil du temps. Les chiffres pour 2026 correspondent à une prévision de leur principale préoccupation en matière de risques dans les 12 prochains mois.

beazley

Renforcer la résilience

La nécessité d'une approche de sécurité multicouche et approfondie de la cybersécurité n'a jamais été aussi grande.

Murs à l'intérieur des murs

- Il est essentiel de mettre en place plusieurs niveaux de défense pour restreindre l'accès aux systèmes et aux données.

- Les organisations ont besoin d'une stratégie de défense en profondeur sur mesure qui reflète leur chaîne d'approvisionnement et leur propre profil de risque.

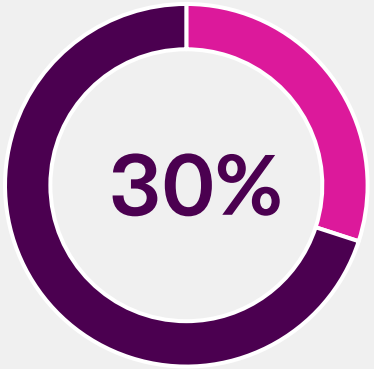
Menace provenant d'un tiers

- Les contrats avec les fournisseurs peuvent limiter la responsabilité, laissant aux entreprises le soin d'assumer les conséquences juridiques et financières des attaques et des perturbations causées par des tiers.

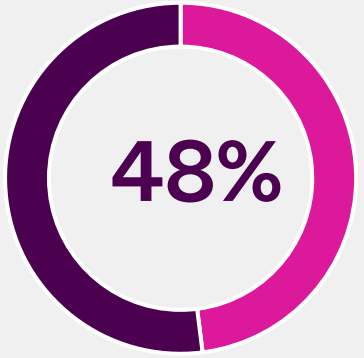
Améliorer la cyber-hygiène

- Une bonne cybersécurité comprend une approche préventive, réactive et adaptative de l'atténuation des risques cyber.

- Investir dans la cybersécurité peut contribuer à réduire la probabilité d'un incident, car la plupart des cybercriminels recherchent la voie la plus facile.



des dirigeants français prévoient d'étudier cette année différentes options d'assurance, notamment en matière de gestion des risques et des crises.

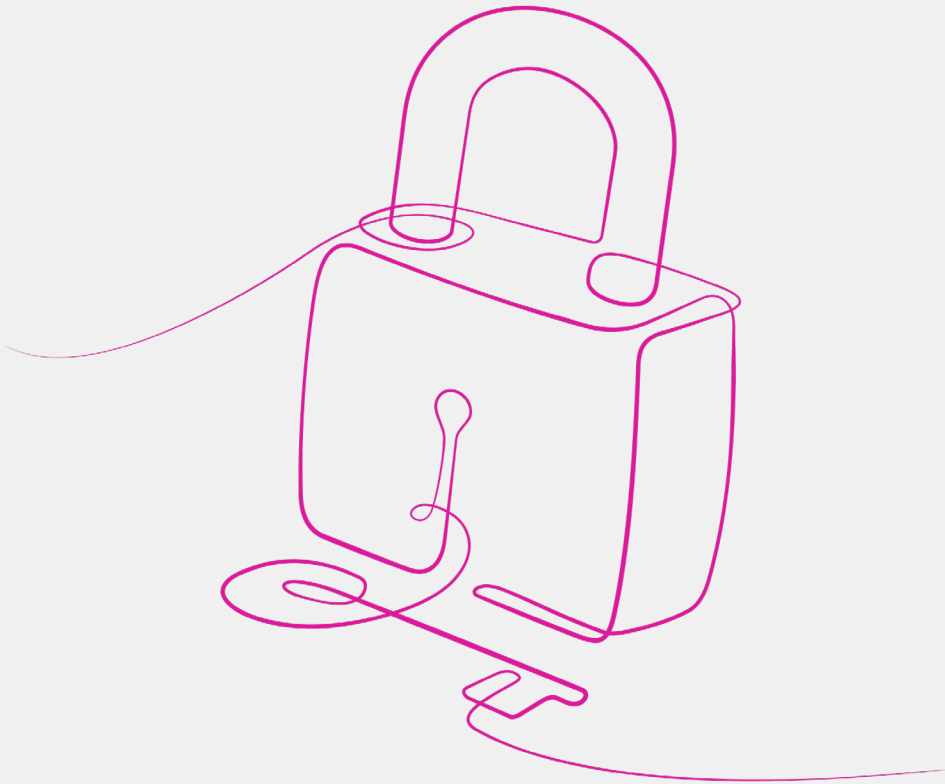


des dirigeants basés en français déclarent que leur confiance dans la valeur de l'assurance a augmenté.

beazley

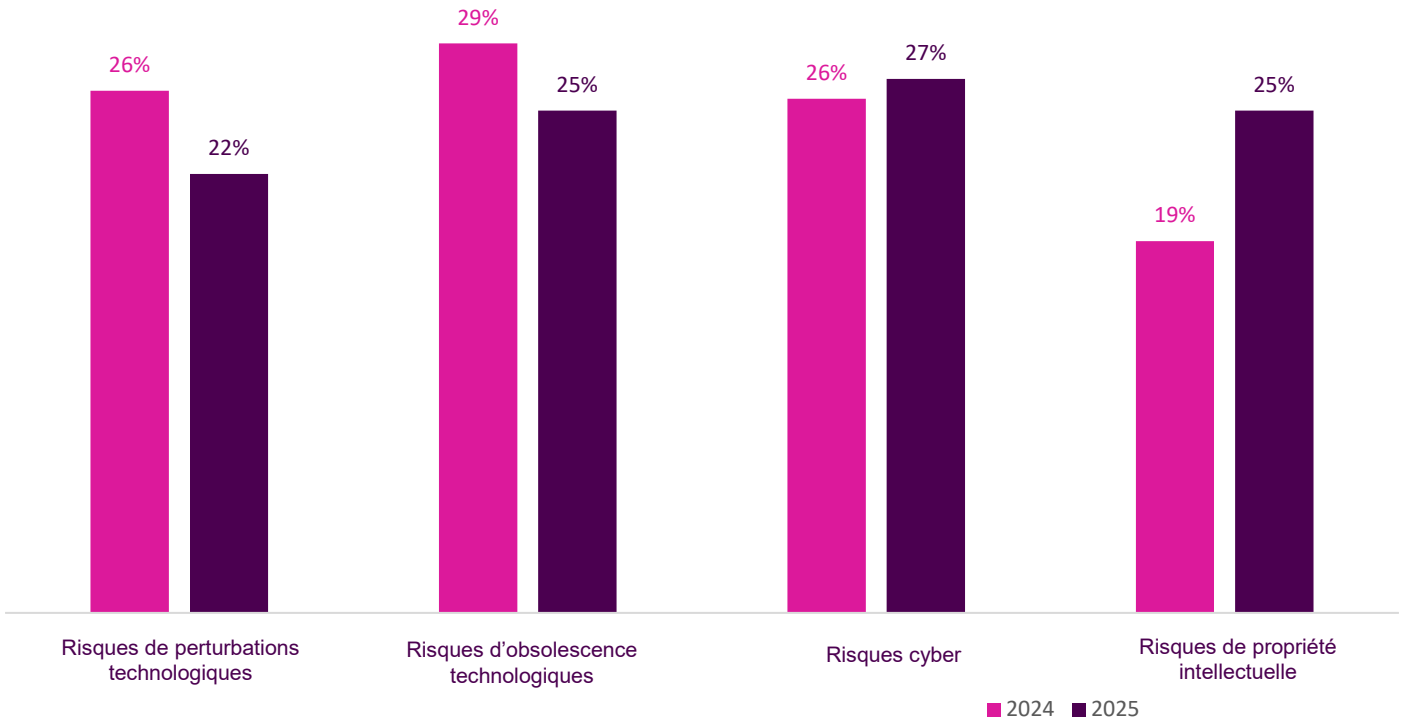
Risk & Resilience 2025

Plongez au cœur des données



beazley

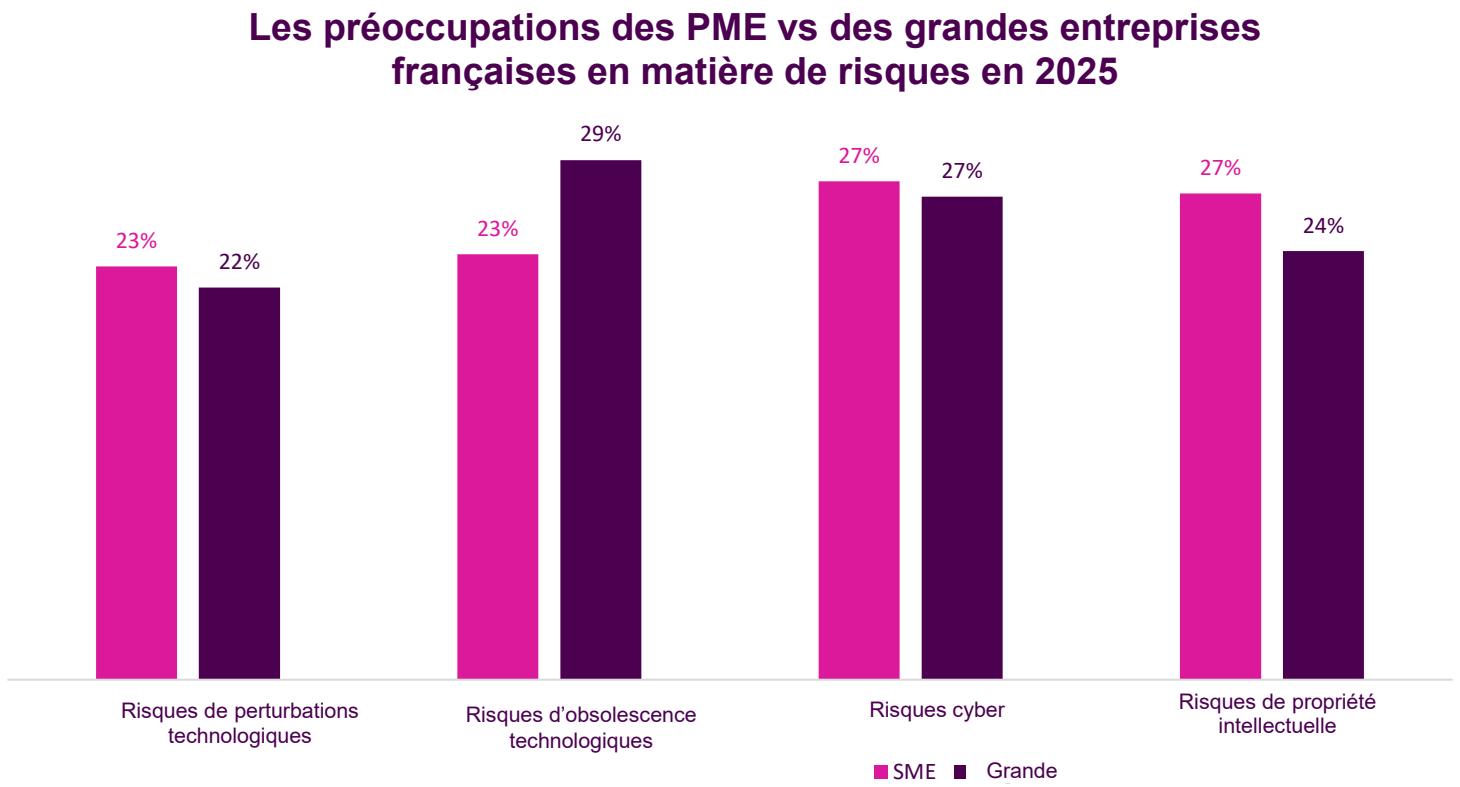
Classement des risques liés à la cybersécurité et aux technologies en France



Pourcentage de dirigeants basés en France qui ont classé ces risques liés à la cybersécurité et aux technologies parmi leurs principales préoccupations pour 2024 et 2025.

beazley

Préoccupations en matière de risques liés à la cybersécurité et aux technologies

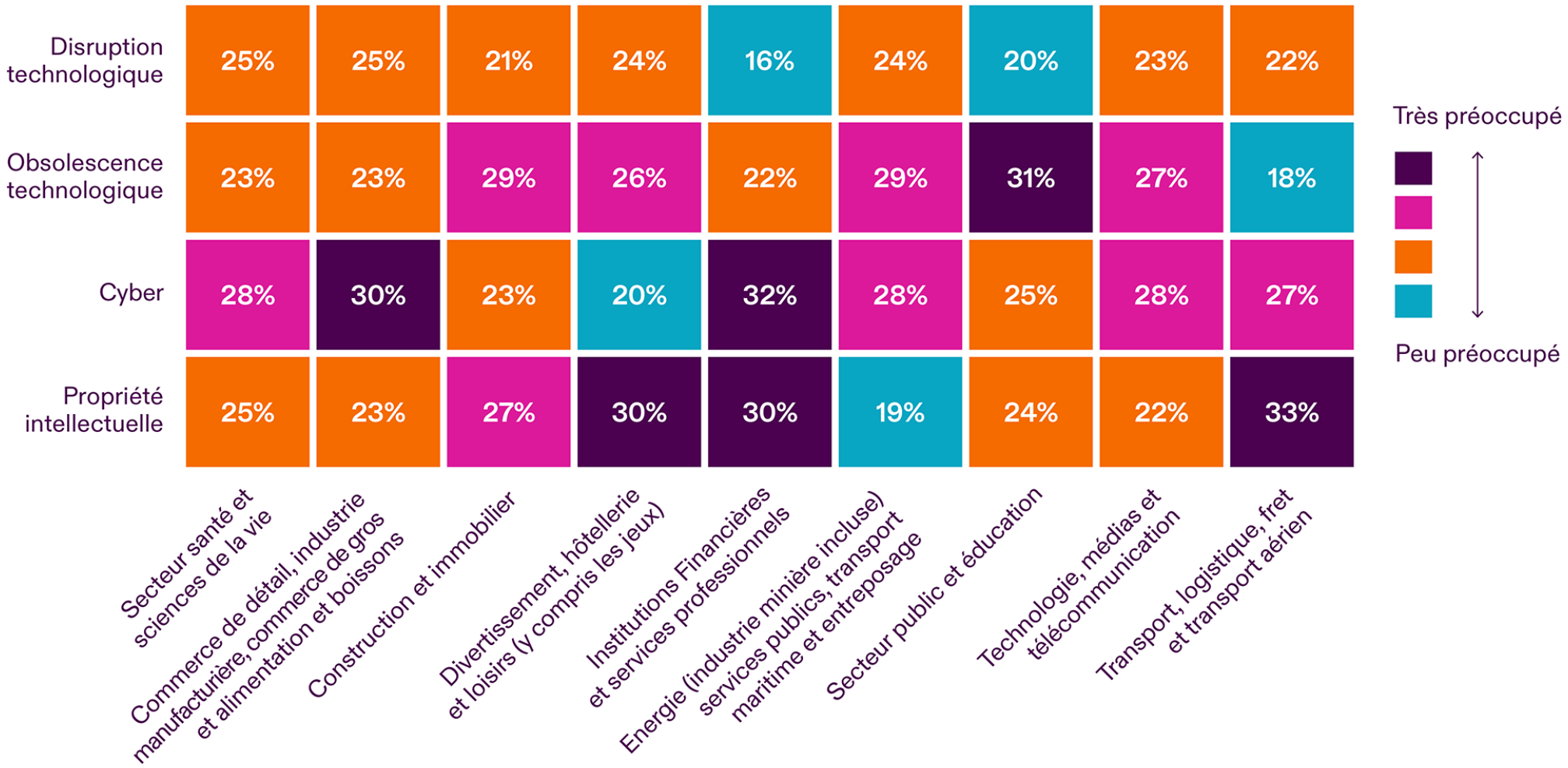


Pourcentage des dirigeants français issus de PME (chiffre d'affaires annuel compris entre 250 000 et 99,99 millions d'euros) et de grandes entreprises (chiffre d'affaires annuel supérieur à 100 millions d'euros) citant ces risques comme leurs principales préoccupations.

beazley

Marché français

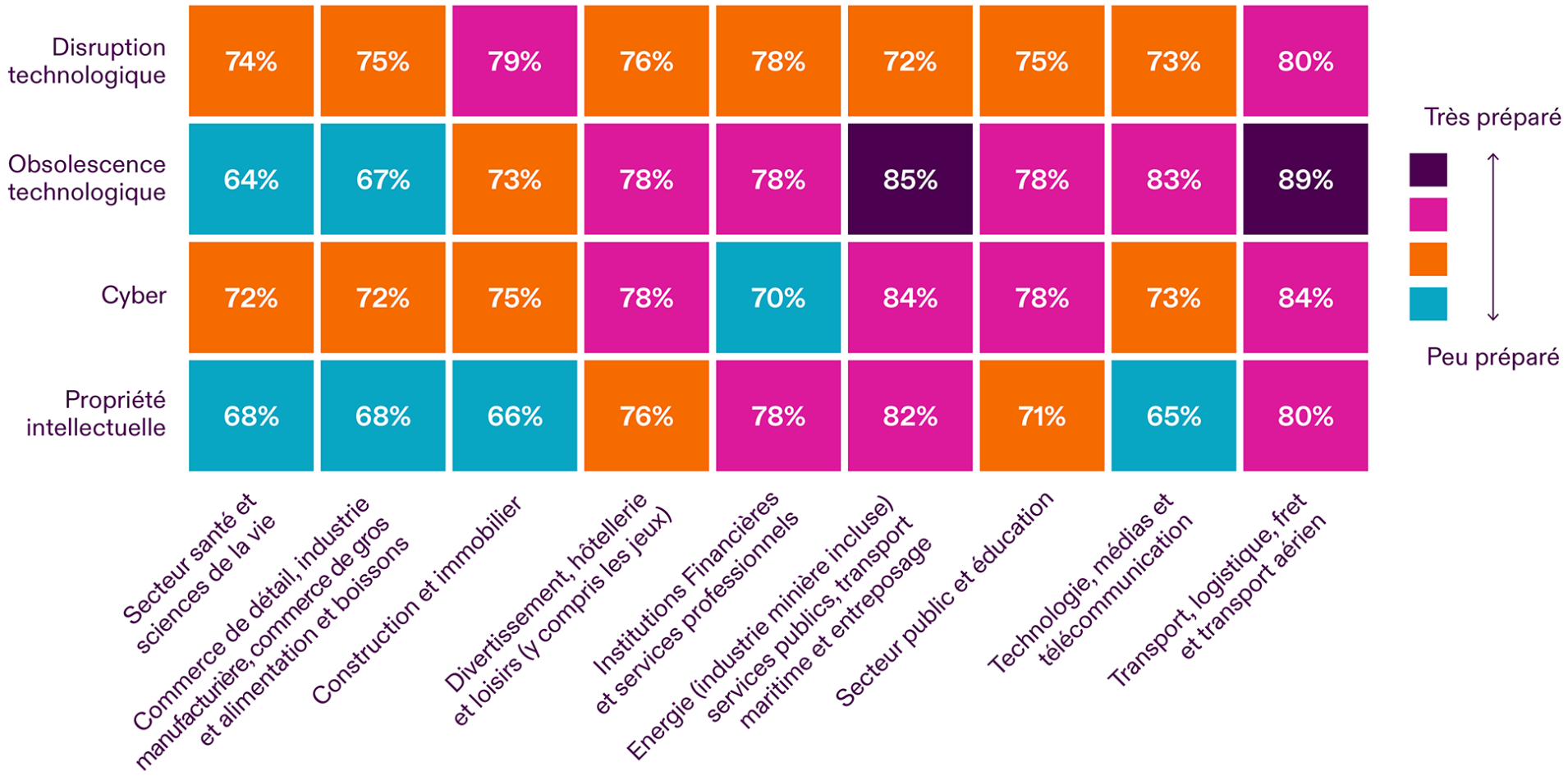
France – Préoccupation du risque cyber par industries



Pourcentage des dirigeants classant ces risques comme leur principale préoccupation en matière de risques cyber et de risques technologiques dans notre enquête Risk & Resilience 2025.

Marché français

France – Comment les industries sont-ils préparés aux risques cyber ?



Pourcentage de dirigeants qui se sentent préparés (réponses « très préparés » et « modérément préparés » combinées) aux risques cyber et technologiques dans notre enquête Risk & Resilience 2025.

beazley

Beazley plc (BEZ.L) est la société mère d'entreprises d'assurance spécialisées présentes en Europe, aux États-Unis, au Canada, en Amérique latine et en Asie. Beazley gère sept syndicats du Lloyd's et, en 2023, souscrira des primes brutes mondiales d'un montant de 5 601,4 millions de dollars. Tous les syndicats du Lloyd's sont notés A par A.M. Best.

Les souscripteurs de Beazley aux États-Unis se concentrent sur la souscription d'une gamme de produits d'assurance spécialisés. Sur le marché admis, la couverture est fournie par Beazley Insurance Company, Inc, un assureur noté A par A.M. Best et autorisé à exercer dans les 50 États. Sur le marché des excédents, la couverture est assurée par Beazley Excess and Surplus Insurance, Inc. et les syndicats de Beazley à Lloyd's. La compagnie d'assurance européenne de Beazley, Beazley Insurance dac, est réglementée par la Banque centrale d'Irlande et est notée A par A.M. Best et A+ par Fitch.

Beazley est présent sur le marché dans un grand nombre de ses branches d'activité, notamment la responsabilité civile professionnelle, la cybercriminalité, les biens, la marine, la réassurance, les accidents et la vie, ainsi que les risques politiques et les activités de contingence.

Pour plus d'informations, veuillez consultez : Beazley.fr

Voir le rapport complet en ligne