beazley

Rapport de situation en France

Risques et résilience en période de changement

Résumé

Bienvenue dans ce tout premier rapport de situation en France sur les risques et la résilience en période de changement. Alors que les conseils d'administration français sont confrontés à l'impact du changement climatique, aux nouvelles réglementations et à la menace cyber croissante, nous explorons les risques pour lesquels de nombreuses entreprises se sentent de plus en plus mal préparées.

Malgré un fort rebond après la crise de la COVID, l'économie française a été mise à mal par les perturbations de la chaîne d'approvisionnement, la hausse des prix de l'énergie et l'impasse de la guerre entre la Russie et l'Ukraine. L'inflation devrait se maintenir à 6,1 % en 2023 et diminuer de moitié en 2024, mais la faible confiance des entreprises pourrait freiner cet élan.[1] Les chefs d'entreprise français sont confrontés à un certain nombre de défis et de nouveaux risques peuvent pénaliser ceux qui ne sont pas prêts à s'adapter à l'évolution constante du paysage des menaces.

Ce rapport est basé sur une enquête menée auprès de 250 chefs d'entreprise français responsables de l'achat d'assurances dans 9 grands secteurs d'activité et dans des entreprises de différentes tailles. Il reprend également des réflexions d'experts en matière de risques et vise à fournir une analyse opportune de l'attitude des entreprises. Beazley a interrogé des dirigeants d'entreprise sur une série de risques actuels et à venir, dans six mois et dans un an, et sur leur degré de résilience par rapport à ces risques.

Les participants à l'enquête ont été interrogés sur leur opinion concernant les assureurs et l'assurance, ainsi que sur les catégories de risques, notamment:

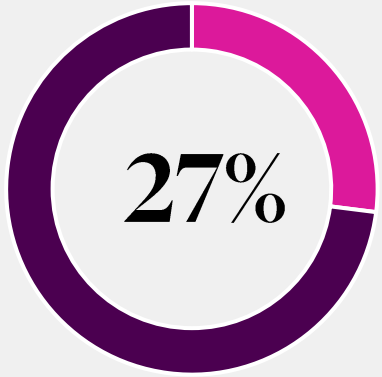
- **Cyber et technologie –** y compris la menace de bouleversements, l'incapacité à suivre le rythme de l'évolution technologique, le risque cyber et le risque de propriété intellectuelle.

- **Entreprises –** y compris l'instabilité de la chaîne d'approvisionnement, l'interruption des activités, les risques liés aux conseils d'administration, la criminalité, les risques liés à la réputation et à l'employeur, et le non-respect des réglementations ESG (environnement, social et gouvernance) et des exigences en matière d'information.

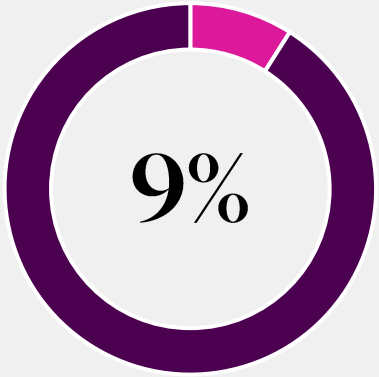
Nous avons entrepris cette étude en janvier et février 2023 aux côtés d'entreprises en Allemagne et en Espagne.

[1] https://www.oecd.org/fr/economie/france-en-un-coup-d-oeil/

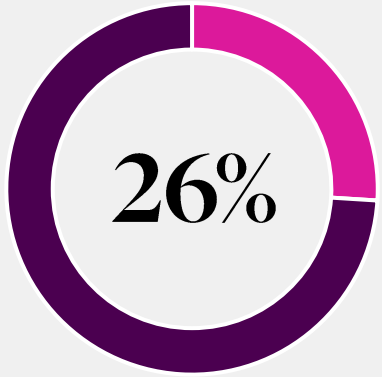
Parmi les chefs d'entreprise français...



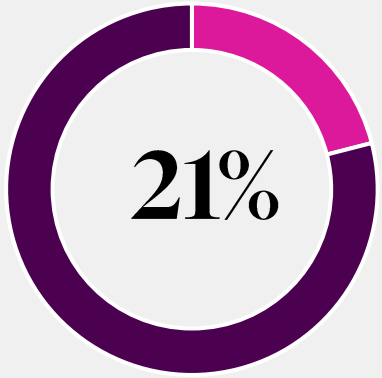
Estiment qu'ils opèrent actuellement dans un environnement à haut risque



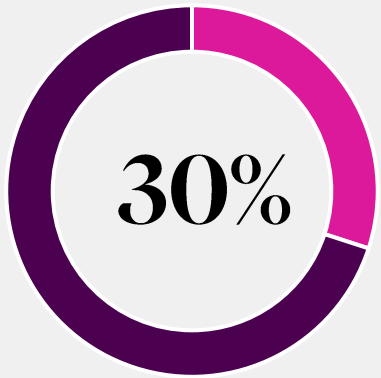
Ont le sentiment d'être moins résilients qu'il y a un an face aux risques qui pèsent sur leur entreprise



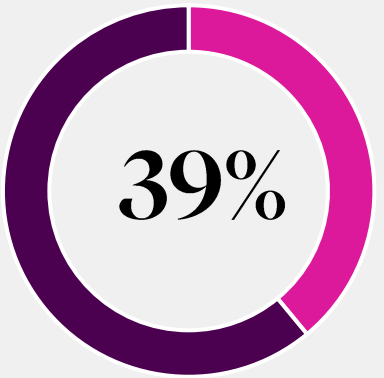
Se déclarent mal préparés à faire face aux risques de disruption technologique tels que l'IA et les nouvelles technologies



Ne sont pas préparés à faire face aux risques liés à l'ESG



Déclarent que la menace cyber est la plus grande menace technologique actuelle pour leur entreprise



Prévoient d'explorer les options d'assurance qui incluent la gestion des risques et des crises

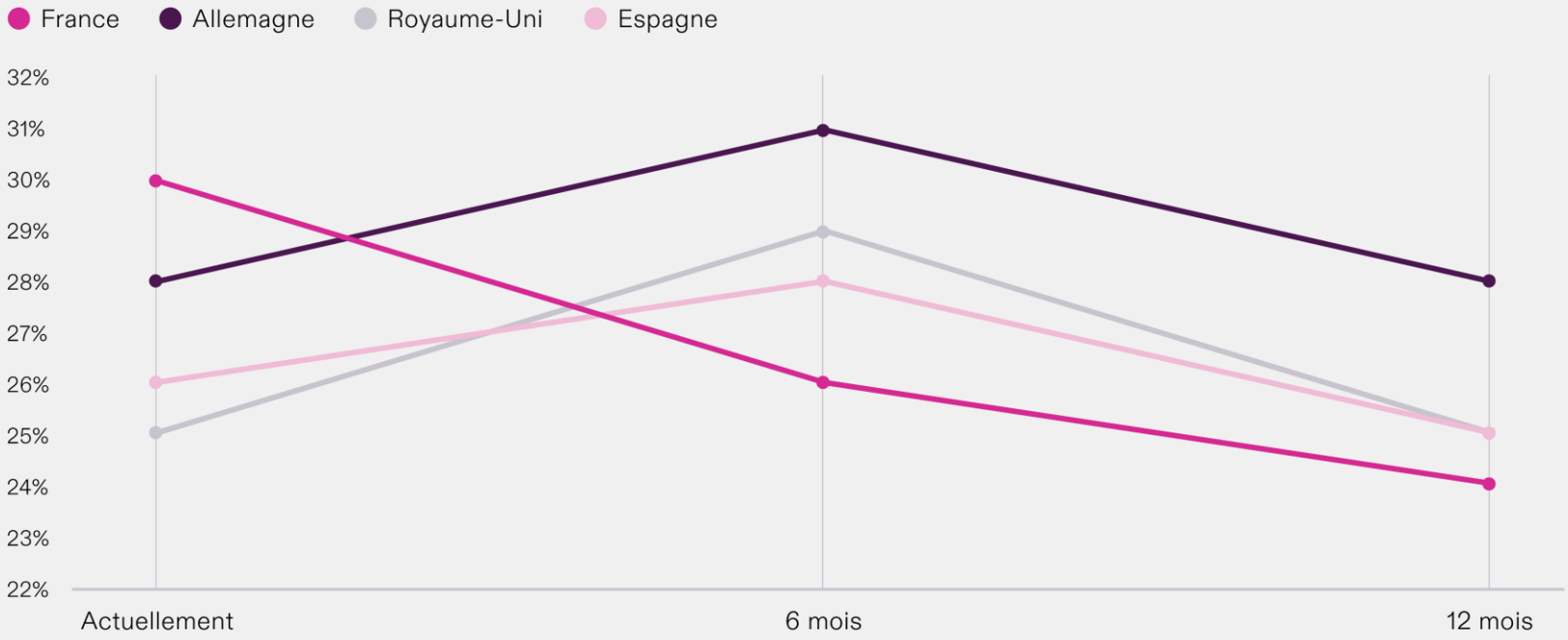
Résumé

Risques cyber : imperméables au danger ?

À la suite de l'invasion de l'Ukraine par la Russie, les conseils d'administration français ont fait l'objet de plusieurs attaques très médiatisées de la part de groupes de pirates informatiques. Ces groupes ont ciblé des entreprises de tous les pans de l'économie française, les exposant à des rançons coûteuses et à des atteintes importantes à leur réputation.

Les entreprises françaises pensent que l'impact du risque cyber va décroître sur le long terme

Pourcentage de dirigeants d'entreprise qui considèrent la cybercriminalité comme leur principal risque à terme

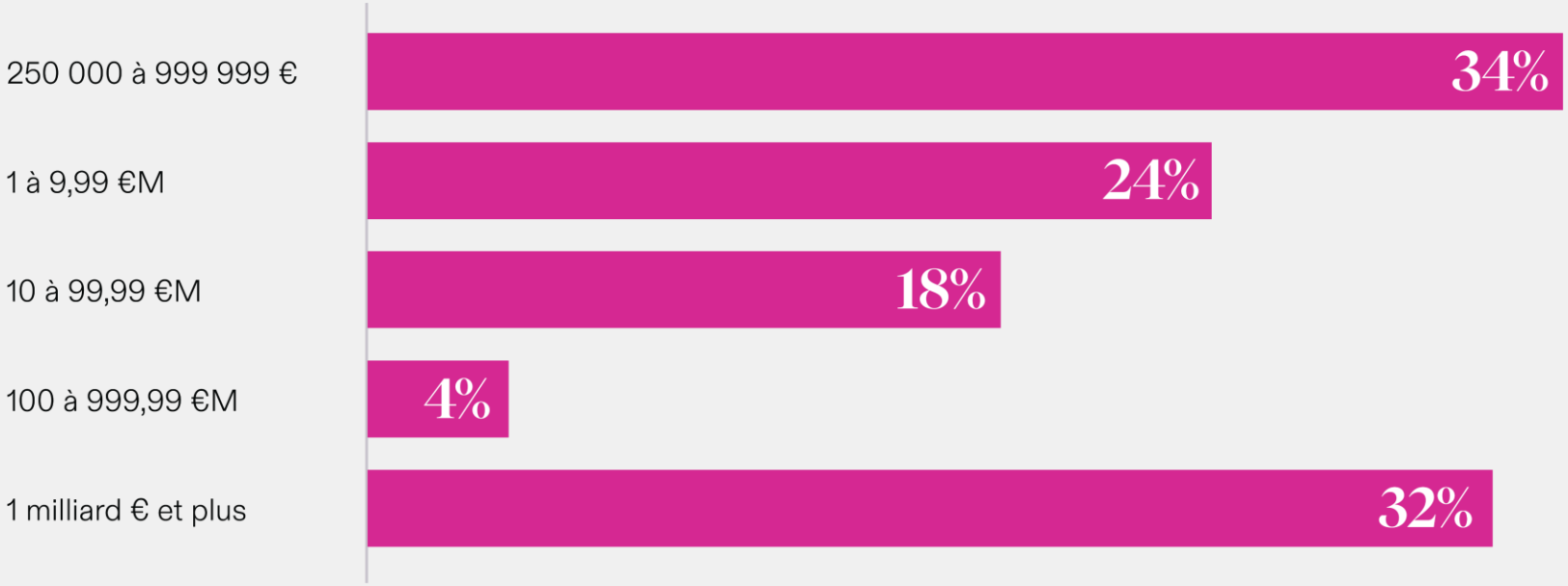


En mars 2023, le site web de l'Assemblée nationale française a été mis hors service par le groupe cybercriminel prorusse NoName057(16), dernière attaque à visée politique contre un organisme français.[2] Bien que l'impact ait été de courte durée, cette attaque reflète la menace de la cybercriminalité qui pèse de plus en plus sur les organisations en France. L'année dernière, la France a été l'un des cinq pays les plus attaqués par les ransomwares dans le monde, alors qu'un certain nombre de nouveaux groupes d'attaque ciblant les entreprises européennes sont apparus.[3]

De tous les risques auxquels les conseils d'administration français sont actuellement confrontés, la menace cyber est considérée comme le plus important – 30 % des interrogés la citent comme leur principale préoccupation. Il s'agit du taux le plus élevé d'Europe, devant l'Allemagne, l'Espagne et le Royaume-Uni. Toutefois, alors que les entreprises allemandes s'attendent à une augmentation de la menace cyber, les entreprises françaises estiment qu'elles y seront moins exposées à long terme.

En France, ce sont les TPE et les très grandes entreprises qui se sentent les plus vulnérables aux attaques cyber

Pourcentage de dirigeants français qui se sentent les plus vulnérables aux attaques cyber en fonction du chiffre d'affaires annuel de l'entreprise



[2] https://www.politico.eu/article/french-national-assembly-website-russian-cyberattack-hack-kremlin-emmanuel-macron/
[3] https://www.strategic-risk-europe.com/home/ransomware-uk-germany-and-france-among-most-attacked-nations/1443729.article

Si nos données montrent que la menace perçue des risques cyber est appelée à diminuer, il est préoccupant de constater que plus d'une entreprise française sur cinq (22 %) ne se sent pas prête à faire face aux risques cyber à l'heure actuelle. Ce chiffre s'élève à 32 % chez les entreprises dont le chiffre d'affaires est supérieur à 1 milliard d'euros et à 34 % chez les petites et moyennes entreprises (PME) françaises dont le chiffre d'affaires est compris entre 250 000 et 999 999 euros. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) rappelle dans un récent rapport que les entreprises françaises doivent rester vigilantes face aux risques relevés : « L'espionnage, le sabotage informatique et les ransomwares sont des menaces auxquelles, chaque jour, en France, les entreprises et les institutions publiques sont soumises. »[4]

Contrairement à la perception de la menace cyber, la fréquence des incidents, les perturbations qu'ils entraînent et leur coût économique augmentent en France – comme dans le monde. Une étude de CyberSecurity Ventures a montré que le coût annuel mondial de la cybercriminalité devrait atteindre 8 000 milliards $ en 2023, soit les PIB cumulés de la France, de l'Espagne et de l'Allemagne. Ce chiffre devrait atteindre 10 500 milliards $ d'ici à 2025 – contre 3 000 milliards $ au début de l'étude en 2015.[5]

« Alors que les cas de ransomware et d'attaques par hameçonnage par des groupes de cybercriminels russes et ukrainiens ont diminué lorsque le conflit a éclaté entre les deux pays l'année dernière, des signes indiquent que les groupes commencent à se réconcilier. Du point de vue des sinistres, les attaques cyber ont un impact particulier sur les interruptions d'activité, ce qui constituera une menace majeure pour les chefs d'entreprise français à l'avenir. Ces derniers doivent continuer à investir dans les défenses de cybersécurité, car les cybercriminels ciblent souvent les entreprises dont les systèmes offrent le moins de résistance. »

Charlotte Jephos
Responsable indemnisation
France chez Beazley

[4] https://www.ssi.gouv.fr/uploads/anssi-annual-review-2022.pdf
[5] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

L'Assurance cyber : la prévention fait partie du remède

La valeur de l'assurance cyber est désormais incontestable. Le secteur mondial de l'assurance a été appelé à répondre à une avalanche d'incidents et a versé des milliards de dollars en indemnités pour les seuls sinistres liés aux ransomwares. Cela a permis à des entreprises d'Amérique du Nord, du Royaume-Uni et d'Asie de rebondir, en les protégeant de l'impact financier important qu'elles auraient subi et en les aidant à reprendre leur activité après l'incident. Les entreprises françaises, tout comme leurs homologues européennes, ont tardé à reconnaître la nécessité de se protéger contre cette menace bien réelle. Il incombe à tous ceux qui reconnaissent le danger de mettre en avant l'assurance cyber comme un outil déterminant pour limiter le risque. Nos données montrent que 41 % des entreprises françaises prévoient d'investir dans la cybersécurité cette année.

Pour le secteur de l'assurance, la collaboration avec les clients pour les aider à relever ces défis, à saisir ces opportunités et à faire face à ces risques est capitale pour garantir aux entreprises d'opérer dans un environnement aussi sûr que possible. Le secteur de l'assurance doit être vigilant et continuer à expliquer à quel point il est important de rester attentif et de continuer à investir et à appliquer une stratégie de défense en profondeur contre les risques cyber.

Le paysage des risques cyber est en constante évolution et l'augmentation spectaculaire des attaques par ransomware contre des entreprises de toutes tailles signifie que les mesures de cybersécurité fondées sur les bonnes pratiques sont plus importantes que jamais. Les chefs d'entreprise doivent également être convaincus que leurs outils de gestion des risques sont à la hauteur, afin de réduire davantage le risque d'être victime d'une attaque. Fournir aux clients les outils dont ils ont besoin pour garder une longueur d'avance dans le cyber reste un objectif clé. Nous reconnaissons que la prévention, la préparation et la réponse sont trois techniques essentielles et indissociables de l'assurance contre les pertes liées à un sinistre cyber.

« Il est essentiel que les entreprises soient conscientes des menaces qui pèsent sur elles et qu'elles s'efforcent constamment de comprendre comment elles peuvent se protéger dans un environnement cyber en constante évolution. Nous constatons que les entreprises françaises, grandes ou petites, sont de plus en plus conscientes de la menace cyber, mais les chefs d'entreprise doivent constamment évoluer pour se prémunir contre les nouvelles techniques d'attaque. »

Luc Vignancour
Responsable souscription cyber France chez Beazley

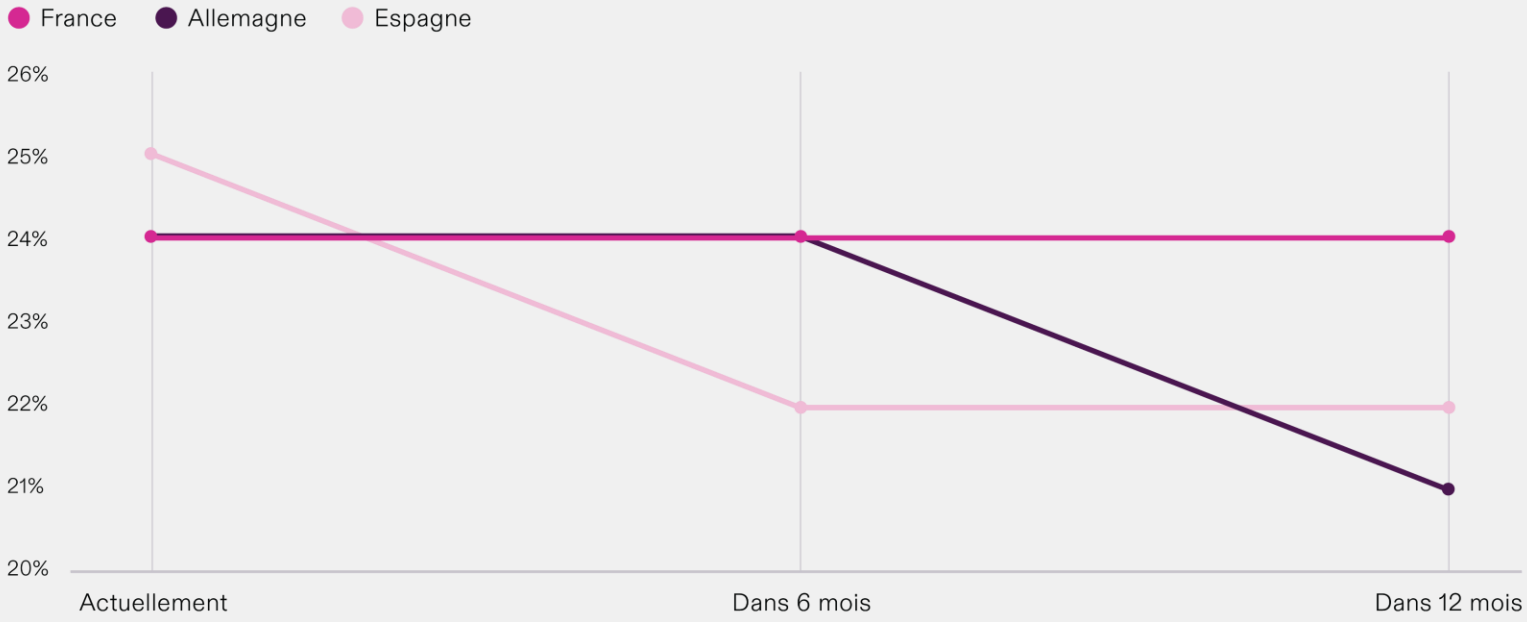
L’imminence d’une réglementation ESG est un risque croissant pour les entreprises françaises

Chaque année, le cadre réglementaire des rapports ESG en Europe s’approfondit et s’étend à toujours plus d’entreprises. Les entreprises françaises doivent aujourd’hui suivre le rythme de l’introduction rapide de nouvelles réglementations.

La réglementation ESG est un phénomène mondial. Les pays cherchent à encourager leurs industries vers des objectifs « zéro net », des pratiques plus durables et la réduction du « greenwashing » grâce à des rapports plus transparents. S’adapter à ces réglementations est de plus en plus difficile, en particulier dans l’UE où les lois ont tendance à se multiplier.

Les sujets ESG considérés comme importants à plus long terme en France qu’en Allemagne et en Espagne

Pourcentage de dirigeants d’entreprise qui considèrent l’ESG comme leur principal risque à terme



Les premières échéances pour un certain nombre de réglementations – de la directive sur la publication d'informations en matière de durabilité (CSRD) à la directive sur le devoir de vigilance des entreprises en matière de durabilité (CSDDD), en passant par la norme européenne de rapport sur le développement durable numéro 5 (ESRS5) – seront applicables dès 2024.

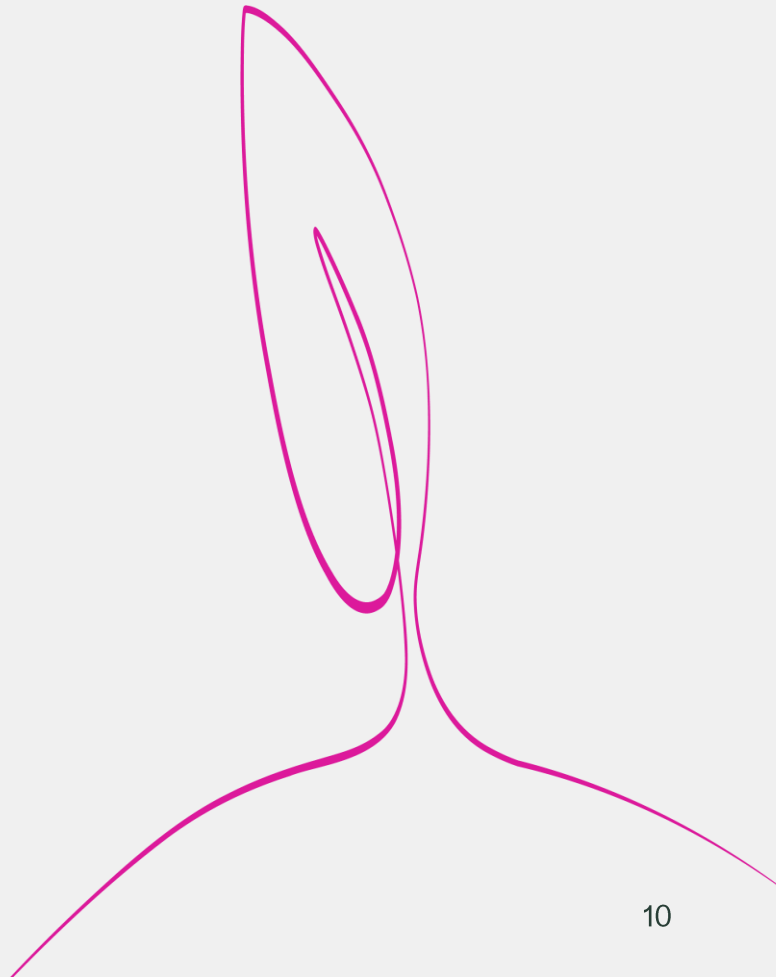
Le non-respect de ces règles pourrait entraîner de lourdes sanctions – de la dénonciation publique à des amendes non encore plafonnées. Il est clair que la non-conformité n'est pas une option. Si les chefs d'entreprise n'agissent pas par devoir envers l'environnement, ils le feront au moins pour protéger leur bilan et leur réputation. L'imminence des échéances est source de préoccupations en France, les conseils d'administration ressentant de plus en plus la. pression de répondre aux exigences de ces nouvelles réglementations.

Un quart (24 %) des chefs d'entreprise français ont déclaré que l'incapacité à se conformer aux exigences liées à l'ESG, y compris la législation, la réglementation ou le reporting, constituait le principal risque auquel leur entreprise était confrontée. Cette proportion atteint 43 % dans les entreprises du secteur des technologies, des médias et des télécommunications. Le niveau de menace devrait rester élevé au cours des 12 prochains mois, 24 % des entreprises s'attendant à ce que l'ESG soit leur principal risque en 2024.

Les entreprises, quelle que soit leur taille, sont confrontées à différentes pressions liées aux réglementations ESG existantes et à venir. Les entreprises de plus grande taille et plus complexes, qui ont un chiffre d'affaires plus élevé et des budgets plus importants, disposeront d'équipes entières pour mettre en œuvre des plans de conformité ESG, sous la pression d'une échéance imminente. La directive CSRD, par exemple, entrera progressivement en vigueur, par paliers : les entreprises cotées en bourse de plus de 500 salariés seront tenues de présenter un rapport dès 2024, suivies par les grandes entreprises non cotées en bourse en 2025 et les PME à partir de 2026. Les petites entreprises auront également moins de ressources et ne seront pas immédiatement soumises au changement, mais elles seront probablement moins préparées, même à l'impact par ricochet de la réglementation ESG sur les grandes entreprises.

Notre étude montre qu'une entreprise sur cinq (21 %)* en France estime ne pas être préparée à faire face aux risques liés à l'ESG. C'est parmi les PME que les risques se font le plus sentir : plus d'un tiers (36 %)* des entreprises de taille moyenne (chiffre d'affaires compris entre 1 et 9,99 millions d'euros) déclarent ne pas être préparées aux nouvelles réglementations.

Près d'un quart (24 %)* des dirigeants de grandes entreprises (chiffre d'affaires de 1 milliard d'euros ou plus) en France ont déclaré qu'ils n'étaient pas non plus préparés aux risques de l'ESG.

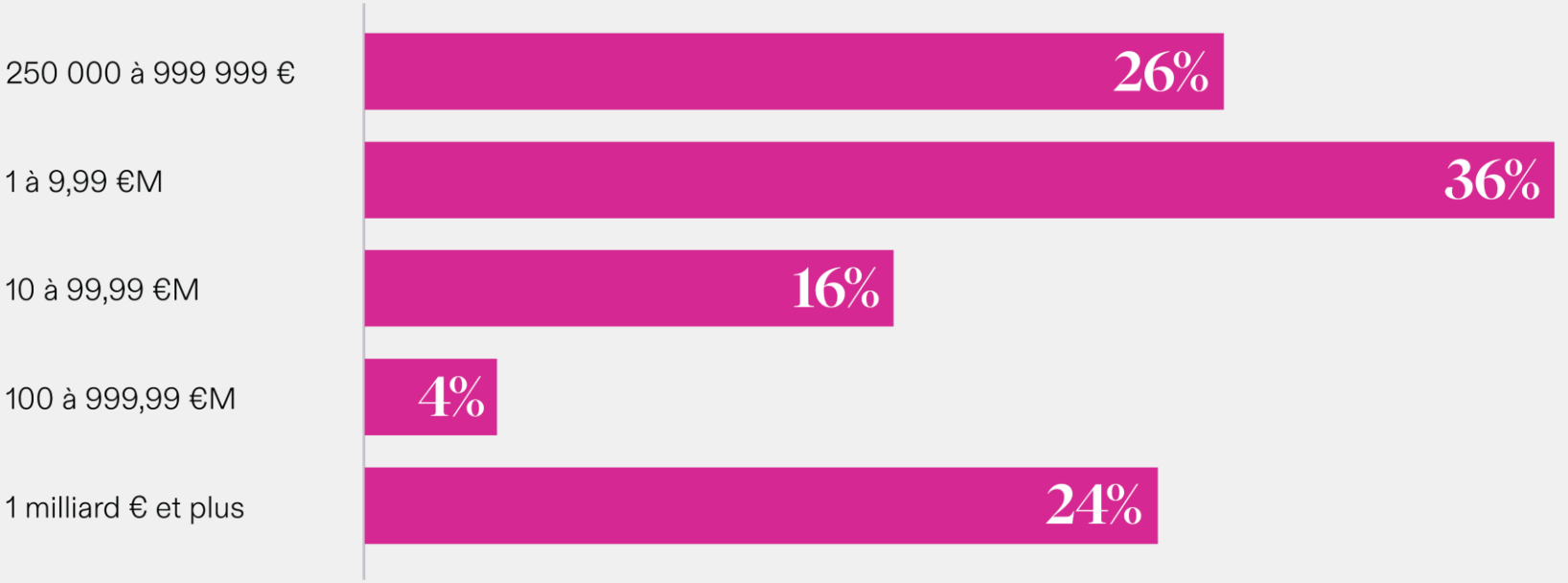


La menace d'accusations de « greenwashing » est particulièrement difficile à gérer pour les entreprises françaises, car nombre d'entre elles se sont engagées à atteindre des objectifs d'émissions nettes nulles dans les années à venir. L'Oréal, Engie, Fnac Darty, Icade, Ipsen, General Electric, Sanofi se sont toutes engagées à limiter leurs émissions de gaz à effet de serre dans les années à venir.[6]

Début 2023, de nouvelles règles publicitaires sont également entrées en vigueur en France : toutes les entreprises qui mettent en avant la neutralité carbone d'un produit ou d'un service doivent fournir un rapport sur l'ensemble des émissions de gaz à effet de serre de ce travail.[7] Les institutions financières, en particulier, doivent se conformer à des règles particulièrement strictes en matière de transparence et de rapports ESG. Nos données montrent qu'un quart des institutions financières françaises considèrent les risques ESG comme la principale menace pesant sur leur activité.

Les PME et grandes entreprises les plus impactées par la réglementation ESG en France

Pourcentage d'entreprises françaises non préparées face aux risques liés à l'ESG (en fonction des revenus annuels)



[6] https://www.euractiv.com/section/energy/news/top-french-firms-commit-to-climate-change-fight/
[7] https://www.thedrum.com/news/2023/02/09/france-s-leading-greenwashing-laws-could-go-wider-brands-should-be-anxious

Naviguer dans un paysage ESG de plus en plus complexe

Alors que les réglementations se multiplient et que l'impact du changement climatique s'intensifie, les entreprises doivent se préparer aux risques ESG et réfléchir à la manière de garder une longueur d'avance dans un paysage réglementaire de plus en plus complexe.

Pour mieux naviguer dans la mosaïque mondiale des réglementations ESG, les multinationales semblent adhérer aux réglementations établies par un régime législatif particulier et appliquer cette approche à toutes les autres juridictions dans lesquelles elles opèrent. Pour ce faire, elles doivent décider quelles réglementations correspondent le mieux à leurs propres valeurs, ce qui montre que les entreprises sont désormais contraintes de prendre une position politique comme jamais auparavant.

Ignorer ou contester la législation n'est en aucun cas une solution viable pour les entreprises. Les petites entreprises, par exemple, n'ont tout simplement pas la puissance financière et juridique nécessaire pour le faire, ce qui signifie qu'elles peuvent être contraintes de se conformer à des réglementations qui ne correspondent pas nécessairement à leurs valeurs, simplement pour maintenir leur croissance.

Nos données montrent que les entreprises se sentent de plus en plus mal préparées à anticiper les risques ESG et à y répondre, et si les défis posés par la mosaïque mondiale de réglementations sont particulièrement prégnants chez les multinationales, les entreprises de toutes tailles sont finalement touchées. L'assurance peut sans aucun doute apporter de la tranquillité d'esprit aux entreprises qui évoluent sur le terrain miné des risques ESG.

« Alors que les entreprises françaises ont commencé à se préparer très tôt aux réglementations ESG, l'accumulation de nouvelles règles et lignes directrices constitue un défi pour les chefs d'entreprise. Les entreprises doivent s'assurer que les objectifs de zéro net qu'elles se fixent pour les années à venir sont réalisables et qu'elles ont mis en place les structures d'information nécessaires pour ne pas être accusées de greenwashing ou de manque de transparence. »

Paul Sterckx
Responsable souscription des lignes financières France chez Beazley

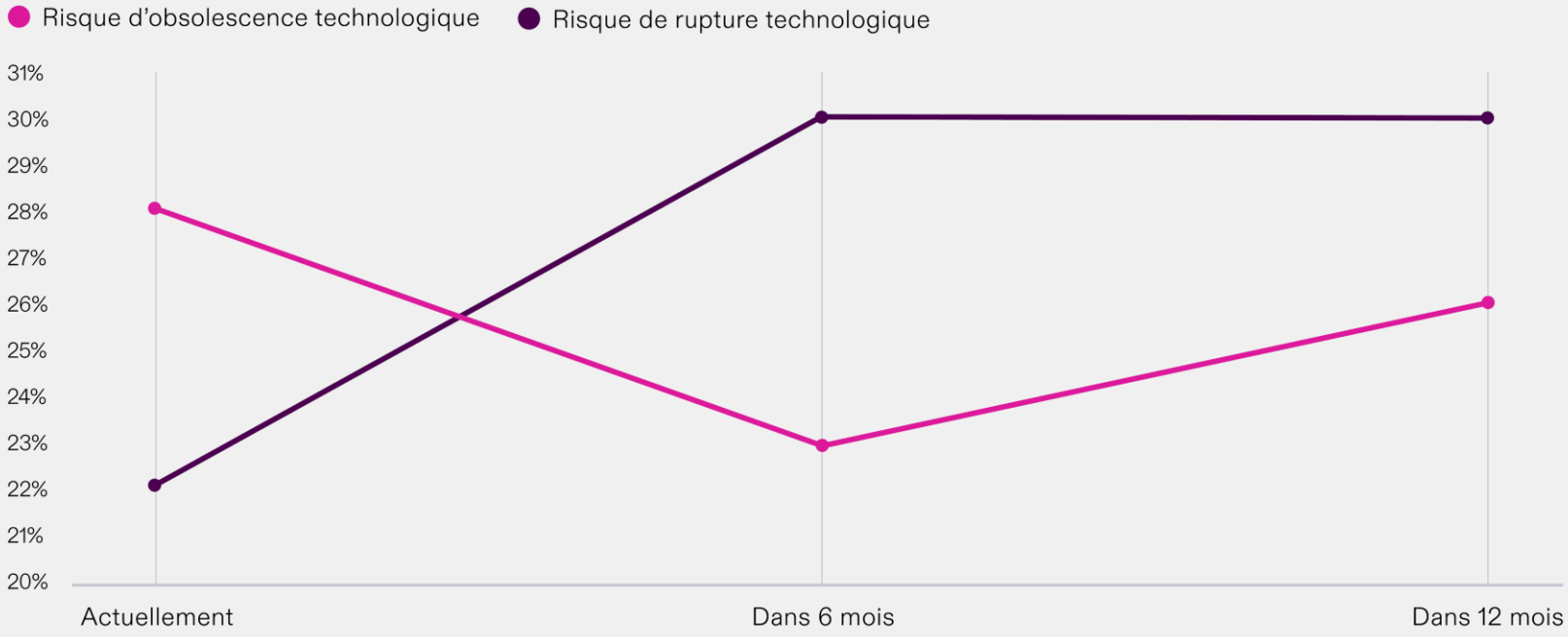
Les entreprises françaises s'efforcent de suivre les progrès technologiques

Les entreprises sont constamment en danger si elles ne parviennent pas à suivre le rythme effréné de l'évolution technologique et à s'adapter aux innovations telles que l'intelligence artificielle (IA). Pour les conseils d'administration français, cette menace est appelée à se renforcer dans les années à venir.

En juin, le président Macron s'est exprimé lors du plus grand salon technologique de France, VivaTech. Il a annoncé un nouveau plan de 500 millions d'euros pour financer les développements dans le domaine de l'IA.[8] Il a également exhorté les entreprises françaises à devenir une force motrice dans l'émergence de l'IA et son déploiement, en vue de positionner stratégiquement le pays dans le domaine disruptif de cette technologie.

Les nouvelles technologies considérées comme un risque restant élevé sur le long terme

Pourcentage de dirigeants d'entreprises françaises qui placent les risques technologiques en tête



[8] https://www.euronews.com/next/2023/06/14/macron-unveils-ambitious-plan-to-boost-french-ai-and-tech-start-ups-at-vivatech

Environ 63 % des employeurs utilisant des outils d'IA ont déclaré qu'ils réduisaient les tâches fastidieuses, mais seulement un cinquième d'entre eux (22 %) ont été formés à cette technologie.[9] Une majorité (57 %) a déclaré qu'elle n'utilisait pas l'IA et ne prévoyait pas de le faire à l'avenir, ce qui met en évidence les craintes croissantes que suscite cette technologie.

Nos données montrent que plus d'un quart (28 %) des chefs d'entreprise français déclarent que l'incapacité à suivre le rythme de l'évolution des technologies et des opportunités est le plus grand défi auquel ils sont confrontés actuellement. En outre, la menace de technologies disruptives telles que l'IA devrait augmenter considérablement à l'avenir, passant de 22 % aujourd'hui à 30 % d'ici 2024. Malgré ce risque croissant, plus d'un quart (26 %)* des entreprises ont déclaré ne pas être préparées à faire face à ce type de risque. Cette proportion atteint 36 %* chez les entreprises dont le chiffre d'affaires est supérieur à 1 milliard d'euros.

Le fait que les entreprises se sentent mal équipées et envisagent de procéder à des changements radicaux est compréhensible si l'on considère les événements de l'année écoulée.

L'avènement de l'IA représente le dernier sommet du progrès technologique et les entreprises du monde entier s'efforcent de comprendre comment elles peuvent en tirer profit et dans quelle mesure elles pourraient être exposées à des risques.

Si l'IA suscite l'enthousiasme, elle ne doit pas détourner l'attention de la mise à jour régulière des technologies et des systèmes existants dans l'entreprise. En ne mettant pas régulièrement à jour les systèmes actuels, les entreprises se retrouveront avec des systèmes obsolètes, vulnérables aux attaques cyber ou aux pannes. L'IA est peut-être au cœur de l'actualité, mais les entreprises seront davantage exposées aux aléas technologiques si elles ne mettent pas régulièrement à jour leur infrastructure existante.

« La technologie de l'IA se développe plus rapidement qu'on ne l'aurait imaginé. Les entreprises sont encore en train d'apprendre à utiliser cette nouvelle technologie et les risques qu'elle présente. Nous en sommes encore aux prémices de l'adoption de l'IA et les possibilités sont infinies et inconnues. Les entreprises doivent manipuler cette technologie avec précaution et s'assurer qu'elles prennent des mesures pour limiter les risques. »

Luc Vignancour
responsable souscription cyber France chez Beazley

[9] https://www.euronews.com/next/2023/06/16/more-than-half-of-french-employers-do-not-plan-on-using-artificial-intelligence

Méthodologie

À propos de la recherche sur les risques et la résilience

En février 2023, nous avons demandé à la société d'études Opinion Matters de sonder l'opinion de plus de 750 chefs d'entreprise et acheteurs d'assurances professionnelles basés en France, en Allemagne et en Espagne (250 dans chaque pays) et opérant à l'internationale. Opinion Matters respecte et emploie des membres de la Market Research Society qui est basée sur les principes d'ESOMAR. Les participants à l'enquête ont été interrogés sur leur opinion concernant les assureurs et l'assurance, ainsi que sur deux catégories de risques :

- **Cyber et technologie –** y compris la menace de bouleversements, l'incapacité à suivre le rythme de l'évolution technologique, le risque cybernétique et le risque de propriété intellectuelle.
- **Entreprises –** y compris l'instabilité de la chaîne d'approvisionnement, l'interruption des activités, les risques liés aux conseils d'administration, la criminalité, les risques liés à la réputation et à l'employeur, et le non-respect des réglementations ESG et des exigences en matière d'information.

Parmi les entreprises interrogées, les répondants se répartissent équitablement entre les différentes tailles d'entreprises : 250 000 à 999 999 euros, 1 million à 9,99 millions d'euros, 10 millions à 99,99 millions d'euros, 100 millions à 999,99 millions d'euros et plus de 1 milliard d'euros.

Voici les secteurs d'activité représentés avec un minimum de 25 répondants par pays et par secteur :

- Soins de santé et sciences de la vie
- Industrie manufacturière, commerce de détail, commerce de gros et alimentation et boissons
- Propriété commerciale, immobilier et construction
- Accueil, divertissement et loisirs (y compris les jeux)
- 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

Les contributeurs

Luc Vignancour
Responsable souscription - cyber chez Beazley France

Paul Sterckx
Responsable souscription – lignes financières chez Beazley France

Charlotte Jephos
Responsable indemnisation chez Beazley France

Discover more

Beazley.com

beazley