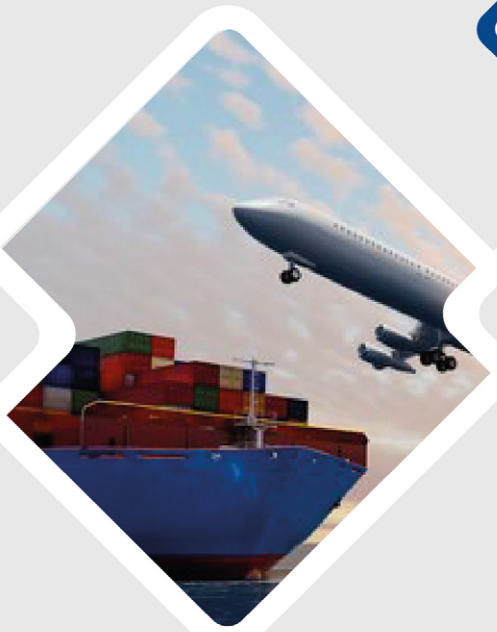
Tunis Re
...à la hauteur de vos risques

2ème Édition

Les Risques Émergents



Février 2024

Les Risques Émergents

Dossier élaboré par :

Aymen Boulares
Les Changements Climatiques

Imen Ksouma
Les Risques Cyber

Samia Guinoubi
Les Risques Politiques

Nahla Haouel
L'instabilité Economique

Sonia Chayada
Les Risques Réglementaires

Sommaire

Introduction P.6

Les Changements Climatiques P.8

Les Risques Cyber P.22

Les Risques Politiques P.42

L 'Instabilité Economique P.54

Les Risques Réglementaires P.63

Conclusion P.75

Introduction

L'industrie de l'assurance, en constante adaptation aux évolutions économiques et sociétales, se trouve aujourd'hui confrontée à un paysage complexe de risques émergents.

À l'aube de l'année 2023, le monde a été confronté à une série de risques qui semblent à la fois totalement nouveaux et étrangement familiers. Nous avons assisté à un retour des "anciens" risques - inflation, crise du coût de la vie, guerres commerciales, fuite des capitaux des pays émergents, troubles sociaux généralisés, affrontements géopolitiques, etc.

Ces phénomèmenes sont amplifiés par des développements relativement nouveaux dans le paysage mondial des risques, notamment des niveaux d'endettement insoutenables, une nouvelle ère de faible croissance, d'investissements et de démondialisation, un déclin du développement après des décennies de progrès, le développement rapide et illimité des technologies à double usage (civil et militaire) et la pression croissante des impacts liés au changement climatique.

Tous ces éléments convergent pour façonner une décennie unique, incertaine et turbulente.

L'instabilité géopolitique est perçue comme une préoccupation majeure. Plus d'un an après le début de l'invasion de l'Ukraine par la Russie, les effets étendus du conflit jettent une ombre sur un monde déjà affecté par les adversités de la pandémie de Covid-19.

L'année 2024 s'ouvre sur un horizon complexe et dynamique où les contours des risques émergents tracent de nouvelles lignes dans le paysage mondial. Alors que la société évolue, façonnée par des avancées technologiques, des changements environnementaux et des dynamiques géopolitiques en constante mutation, l'identification et la compréhension des risques émergents deviennent impératives.

Les défis auxquels le monde est confronté sont de plus en plus interconnectés et transcendent les frontières traditionnelles. Que ce soit dans le domaine de la santé, de la finance, de la technologie, de l'environnement, ou des relations internationales, de nouveaux risques émergent, souvent imprévisibles et potentiellement transformateurs.

Les Changements Climatiques

LE CHANGEMENT CLIMATIQUE : UN RISQUE ÉMERGENT À GRANDE AMPLEUR

Les risques liés au changement climatique inquiètent de plus en plus la communauté internationale et ce phénomène se classe en tête des risques émergents selon les études faites par les différents experts et spécialistes de la gestion des risques qui mesurent et classent chaque année leur perception de l'évolution et de l'émergence des risques. En effet, le changement climatique affecte déjà toutes les régions de la planète. La modification du régime des précipitations, l'élévation du niveau des mers, la fonte des glaciers, le réchauffement des océans et l'augmentation de la fréquence et de l'intensité des phénomènes météorologiques extrêmes ne sont que quelques-uns des changements qui affectent déjà des millions de personnes. Le changement climatique peut affecter notre santé, notre nourriture, notre logement, notre sécurité et nos conditions de travail. Les changements climatiques sont généralisés, rapides et s'intensifient, et certains d'entre eux, tels que l'élévation du niveau de la mer ou la fonte des nappes glaciaires, sont irréversibles sur des centaines, voire des milliers d'années.

I. Définition du changement climatique

1. Définition

Le changement climatique est défini par les Nations unies comme une évolution à long terme des températures et des conditions météorologiques. Il convient de noter que si les termes «changement climatique» et «réchauffement planétaire» sont souvent utilisés de manière interchangeable, le réchauffement planétaire - l'augmentation récente de la température moyenne mondiale près de la surface de la terre - n'est qu'un aspect du changement climatique.

2. Effets déclencheurs

Certes, la Terre a connu des phases de réchauffement et de refroidissement dans le passé, bien avant l'apparition de l'homme. L'intensité du soleil, les éruptions volcaniques et les variations des concentrations de gaz à effet de serre d'origine naturelle sont autant de facteurs qui peuvent contribuer au changement climatique. Toutefois, les relevés indiquent que le réchauffement climatique actuel - en particulier celui qui s'est produit depuis le milieu du 20ème siècle - se produit à un rythme beaucoup plus rapide que jamais auparavant, et qu'il ne peut s'expliquer uniquement par des causes naturelles.

- L'activité humaine

En effet, la principale cause de ce changement climatique qui évolue depuis le 19ème siècle est l'activité humaine, en particulier l'utilisation des combustibles fossiles tels que le charbon,

le pétrole et le gaz utilisés notamment pour produire de l'électricité, pour le chauffage et pour le transport.

- La déforestation

La deuxième source majeure est la déforestation, qui libère dans l'air le carbone séquestré (ou stocké). On estime que l'exploitation forestière, les incendies et d'autres formes de dégradation des forêts libèrent en moyenne 8,1 milliards de tonnes de dioxyde de carbone par an, ce qui représente plus de 20 % de l'ensemble des émissions mondiales de CO2.

Parmi les autres activités humaines génératrices de pollution atmosphérique figurent l'utilisation d'engrais (source principale d'émissions d'oxyde nitreux), l'élevage (les bovins, les buffles, les moutons et les chèvres sont d'importants émetteurs de méthane) et certains procédés industriels qui libèrent des gaz fluorés. Des activités telles que l'agriculture et la construction de routes peuvent également modifier la réflectivité de la surface de la terre, entraînant un réchauffement ou un refroidissement local.

- Les gaz à effet de serre

Bien que les forêts et les océans de notre planète absorbent les gaz à effet de serre présents dans l'atmosphère grâce à la photosynthèse et à d'autres processus, ils ne parviennent pas à suivre l'augmentation de nos émissions. L'accumulation de gaz à effet de serre qui en résulte est à l'origine d'un réchauffement mondial d'une rapidité alarmante. Ces gaz à effet de serre agissent comme une couverture autour de la terre, piégeant la chaleur du soleil et augmentant les températures. Un grand nombre de ces gaz à effet de serre sont présents à l'état naturel, mais les activités humaines augmentent les concentrations de certains d'entre eux dans l'atmosphère, en particulier le dioxyde de carbone (CO2) principal responsable du réchauffement de la planète, le méthane, l'oxyde nitreux et les gaz fluorés. Le méthane est un gaz à effet de serre plus puissant que le CO2, mais sa durée de vie dans l'atmosphère est plus courte. L'oxyde nitreux, comme le CO2, est un gaz à effet de serre à longue durée de vie qui s'accumule dans l'atmosphère pendant des décennies, voire des siècles.

En 2020, la concentration du CO2 dans l'atmosphère avait augmenté de 48% par rapport à son niveau préindustriel (avant 1750).

- Les vagues de chaleurs

La décennie 2011-2020 a été la plus chaude jamais enregistrée, la température moyenne mondiale a atteint 1,1°C au-dessus des niveaux préindustriels. Une augmentation de 2°C par rapport à la température de l'ère préindustrielle sera associée à de graves incidences négatives sur l'environnement naturel, la santé et le bien-être de l'homme.

En effet, les conséquences du changement climatique sont multiples et malheureusement néfastes pour l'homme et pour tous les êtres vivants sur terre : sécheresses intenses, pénurie d'eau, incendies graves, élévation du niveau de la mer, inondations, fonte des glaces polaires, tempêtes catastrophiques, déclin de la biodiversité, manque de nourriture et augmentation des risques pour la santé.

Consciente de ces effets graves, la communauté internationale a reconnu la nécessité de maintenir le niveau du réchauffement bien en deçà de 1,5°C.

II. Impact du changement climatique :

La gravité des effets du changement climatique dépendra de l'évolution de l'activité humaine. L'augmentation des émissions de gaz à effet de serre entraînera une augmentation des conditions climatiques extrêmes et des effets néfastes généralisés sur notre planète.

Les preuves scientifiques sont sans équivoque: le changement climatique constitue une menace pour le bien-être de l'homme et la santé de la planète. Tout retard supplémentaire dans la mise en œuvre d'une action concertée au niveau mondial nous fera manquer une occasion à ne pas rater pour garantir un avenir vivable.

Il est à noter que l'été 2023 a été le plus chaud jamais enregistré sur Terre, avec 0,23 degré Celsius (C) de plus que tout autre été enregistré par la NASA et 1,2 C de plus que l'été moyen entre 1951 et 1980. Ce nouveau record intervient alors qu'une chaleur exceptionnelle a balayé une grande partie du monde, exacerbant les incendies de forêt meurtriers au Canada et à Hawaï, et les vagues de chaleur torride en Amérique du Sud, au Japon, en Europe et aux États-Unis, tout en contribuant probablement aux fortes précipitations en Italie, en Grèce et en Europe centrale. Dans l'ensemble, les chaleurs extrêmes de cet été ont placé des

dizaines de millions de personnes sous alerte canicule et ont été à l'origine de centaines de maladies et de décès liés à la chaleur.

Selon un rapport sur les risques mondiaux du Forum économique mondial, l'incapacité à atténuer le changement climatique et à s'y adapter est le risque le plus important auquel sont confrontées les communautés du monde entier, avant même les armes de destruction massive et les crises de l'eau.

1. Conditions météorologiques extrême

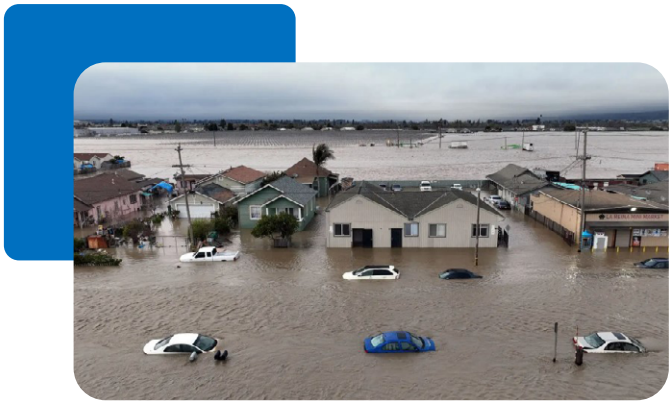
En se réchauffant, l'atmosphère terrestre recueille, retient et laisse tomber davantage d'eau, ce qui modifie les conditions météorologiques et rend les zones humides plus humides et les zones sèches plus arides. Les températures plus élevées aggravent et augmentent la fréquence de nombreux types de catastrophes, notamment les tempêtes, les inondations, les vagues de chaleur et les sécheresses.

En fait, Il existe des preuves scientifiques de l'influence du changement climatique sur les orages violents accompagnés de grêle, les incendies de forêt, les vagues de chaleur et les sécheresses.

Par ailleurs, les tempêtes tropicales (appelées ouragans, typhons ou cyclones selon la région où elles se produisent) ont été accompagnées de précipitations de plus en plus extrêmes.

Ces événements peuvent avoir des conséquences dévastatrices et coûteuses, compromettant l'accès à l'eau potable, alimentant des incendies de forêt hors de contrôle, endommageant les biens, provoquant des déversements de matières dangereuses, polluant l'air et entraînant des pertes de vies humaines.

- Les risques d'inondation augmentent



Chaque année, les inondations détruisent des biens d'une valeur de plusieurs milliards de dollars. Rien qu'au cours des cinq dernières années, les pertes dues aux inondations dans le monde se sont élevées à 300 milliards de dollars, dont environ 45 milliards ont été assurés, ce qui ne représente que 15 %.

La part relativement faible des pertes assurées liées aux inondations même dans les pays industrialisés est en partie due à la gamme limitée de couvertures d'assurance et le manque de demande même dans les régions connues pour être sujettes aux inondations.

En outre, de nombreux sinistres concernent des infrastructures publiques (routes, voies ferrées, digues et ponts) qui ne sont généralement pas assurées.

L'inondation la plus coûteuse de l'histoire s'est produite en juillet 2021 en Europe centrale, lorsque des crues éclairs dévastateurs en Allemagne occidentale et dans les pays voisins ont entraîné des pertes globales de 54 milliards de dollars (46 milliards d'euros).

Des digues, des murs anti-inondations et des bassins de rétention sont souvent construits le long des rivières pour les protéger contre les inondations. La prévention des sinistres au niveau individuel consiste à prendre des mesures appropriées pour améliorer la résistance des bâtiments aux inondations. Par ailleurs, une police d'assurance contre les risques naturels est le moyen idéal pour indemniser les pertes liées au risque d'inondation.

- Ouragans, typhons, cyclones : le risque naturel avec les pertes les plus élevées

Les cyclones tropicaux deviendront plus puissants et plus aptes à s'intensifier rapidement. Dans le dernier rapport du Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC), les scientifiques ont constaté que les précipitations quotidiennes lors d'événements extrêmes augmenteraient d'environ 7 % pour chaque degré Celsius de réchauffement de la planète, ce qui accroîtrait les risques d'inondation. La fréquence des ouragans violents de catégorie 4 et 5 devrait également augmenter.

Les cyclones tropicaux ont un énorme potentiel de destruction. Ces tempêtes sont à l'origine des pertes les plus élevées de tous les risques naturels au fil du temps. L'ouragan Katrina, qui a frappé la Nouvelle-Orléans en 2005 avec une onde de tempête dévastatrice, reste l'une des catastrophes naturelles les plus coûteuses de l'histoire, dépassée seulement par le tremblement de terre de 2011 au Japon qui a déclenché un tsunami dévastateur et la catastrophe nucléaire de Fukushima.

Lors de la saison des ouragans 2022, l'ouragan Ian a presque battu le record des pertes : l'un des ouragans les plus puissants à avoir jamais frappé le continent américain, il a détruit des biens d'une valeur de 100 milliards d'USD, dont près de la moitié était assurée.

Image satellitaire de Dorian le 1er septembre 2019 au large des Bahamas, après son passage en catégorie 5 et son pic d'intensité.

- Les tempêtes hivernales et les blizzards

Les grandes tempêtes hivernales peuvent causer autant de dégâts que les ouragans. Bien que la vitesse des vents de ces tempêtes hivernales n'atteigne pas celle des cyclones, les fronts de tempête peuvent balayer des surfaces énormes ou recouvrir de neige et de glace une zone étendue.

Les pertes causées par les tempêtes hivernales proviennent principalement des dommages causés aux bâtiments, aux véhicules et aux infrastructures. Les pertes liées aux interruptions d'activité augmentent également notamment lorsque les dommages causés par les tempêtes ou les grandes quantités de neige et de glace paralysent les infrastructures.

En février 2021, un puissant front de tempête hivernale (nommée tempête hivernale Uri) a apporté des températures glaciales exceptionnelles jusque dans le sud des États-Unis. Des millions de personnes ont été privées d'électricité pendant de longues périodes, ce qui a entraîné le gel et l'éclatement des canalisations d'eau dans de nombreux bâtiments. Avec des pertes globales d'environ 30 milliards de dollars, il s'agit de la tempête hivernale la plus coûteuse au monde à ce jour. Près de la moitié des pertes ont été assurées.

- Orages : Grêle, tornades et crues soudaines

Les orages sont rarement isolés : la grêle, les coups de vent, les tornades et les fortes précipitations sont des risques courants. Il peut en résulter des crues soudaines, des glissements de terrain, des dégâts causés par la grêle et des inondations. Les pertes se chiffrent souvent en milliards.

Après les ouragans, les orages constituent le risque météorologique le plus important pour le secteur de l'assurance aux États-Unis. Une tornade ou une violente tempête de grêle survenant dans le centre d'une grande ville peut entraîner des pertes individuelles extrêmement élevées et des pertes totales qui se chiffrent en milliards de dollars par an. Rien qu'en 2022, les orages aux États-Unis ont été responsables de 32 milliards de dollars de pertes, dont les deux tiers étaient assurés.

Des études basées sur des modèles climatiques ont conclu que l'augmentation de l'humidité atmosphérique est le moteur de ce changement. À son tour, l'humidité est due à la hausse des températures océaniques et à l'augmentation de l'évaporation, ce qui met en évidence les effets du changement climatique.

L'intensité des orages dans certaines régions d'Europe a également augmenté ces dernières années. En effet, l'été 2022 a été caractérisé par des températures extrêmes, entrecoupées d'orages violents et de grêle.

Les bâtiments et les infrastructures sont particulièrement exposés aux pertes causées par les violentes tempêtes de grêle. Les panneaux photovoltaïques, l'isolation des bâtiments et les stores extérieurs contribuent à l'augmentation des sinistres, d'où l'importance des mesures de prévention.

- Incendies de forêt et feux de brousse : le changement climatique accroît le risque d'incendie de forêt

Chaque année, les incendies de forêt causent des milliards de dollars de pertes. Le changement climatique influe également sur le risque, avec des températures en hausse et des sécheresses plus fréquentes. 69 milliards USD de pertes mondiales dues aux incendies de forêt sur la période 2018-2022 ont été enregistrées, les assureurs versant un total de 39 milliards USD.

En Californie, le changement climatique est manifestement un facteur important dans l'augmentation du risque d'incendies de forêt entraînant de lourdes pertes. Par ailleurs, la région méditerranéenne et certaines parties de l'Australie connaissent également plus fréquemment les conditions nécessaires à l'apparition d'incendies de forêt (des incendies de forêt ont ravagé la Grèce, L'Italie, l'Algérie et la France au mois de Juillet 2023 causant des dégâts énormes et des pertes humaines).

Cependant, l'interaction de facteurs naturels et humains a fait des incendies de forêt et des feux de brousse un risque difficile à quantifier dont la modélisation est complexe.

- Sécheresses et vagues de chaleur

Le Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC) s'attend à ce que les vagues de chaleur et les sécheresses augmentent en gravité, en fréquence et en durée dans de nombreuses régions en raison du changement climatique. Les sécheresses, en particulier, deviendront un risque naturel extrêmement coûteux au cours des prochaines décennies, car elles mettent en péril l'approvisionnement alimentaire mondial en raison des mauvaises récoltes et de l'incidence accrue des maladies végétales.

Par ailleurs, dans les régions où les bâtiments sont construits sur de l'argile gonflante, le sol peut se rétracter en cas de sécheresse, ce qui entraîne un affaissement. Les bâtiments peuvent alors être endommagés, par exemple en se fissurant ou en s'inclinant.

La réduction de la disponibilité de l'eau et l'augmentation de la température de l'eau ont également des effets indirects. Les centrales hydroélectriques et thermiques sont obligées de réduire leur production s'il n'y a pas assez d'eau pour assurer la production d'électricité ou s'il n'y a pas assez d'eau de refroidissement pour maintenir les températures de rejet autorisées.

Si la sécheresse et les chaleurs extrêmes représentent des risques importants, des solutions innovantes, par exemple celles basées sur des déclencheurs paramétriques, offrent une protection flexible. Ainsi, la numérisation et l'intelligence artificielle ouvrent la voie à de nouvelles solutions d'assurance.

- La montée des eaux

L'Arctique se réchauffe deux fois plus vite que n'importe quel autre endroit de la planète. Avec la fonte des calottes glaciaires, nos océans sont en passe de s'élever de 0,95 à 3,61 pieds d'ici la fin du siècle, menaçant les écosystèmes côtiers et les zones de faible altitude. Les nations insulaires sont particulièrement menacées, tout comme certaines des plus grandes villes du monde, notamment New York City, Miami, Mumbai en Inde et Sydney en Australie.

2. Facteurs de stress des écosystèmes

Le changement climatique semble déclencher une série de changements écologiques en cascade que nous ne pouvons ni prévoir complètement, ni arrêter complètement une fois qu'ils ont pris suffisamment d'ampleur. Cette déstabilisation des écosystèmes peut être plus évidente lorsqu'il s'agit d'espèces clés qui jouent un rôle majeur dans le maintien de la structure d'un écosystème.

Le changement climatique est susceptible d'accroître les épidémies. Il modifie les types de végétation qui peuvent prospérer dans une région donnée et perturbe les cycles de vie de la faune, ce qui modifie la composition des écosystèmes et les rend moins résistants aux facteurs de stress. Si les écosystèmes ont la capacité de s'adapter, nombre d'entre eux atteignent les limites de cette capacité naturelle.

- Dégradation de la santé du sol

Un sol sain a une bonne teneur en eau et en minéraux et regorge d'insectes, de bactéries, de champignons et de microbes qui, à leur tour, contribuent à la bonne santé des cultures. Mais le changement climatique, en particulier les chaleurs extrêmes et les changements dans les précipitations, peut dégrader la qualité des sols. Ces effets sont exacerbés dans les régions où la monoculture industrielle, dépendante des produits chimiques, a rendu le sol et les cultures moins aptes à résister aux changements environnementaux.

- Effets sur l'agriculture et pénuries alimentaires

Dans un monde qui se réchauffe, l'agriculture est plus imprévisible et le bétail, qui est sensible aux conditions météorologiques extrêmes, devient plus difficile à élever. Le changement climatique modifie les régimes de précipitations, provoquant des inondations imprévisibles et des sécheresses plus longues. Des ouragans plus fréquents et plus violents peuvent dévaster une saison entière de récoltes. Par ailleurs, la dynamique des agents pathogènes et des espèces envahissantes, dont la gestion est coûteuse pour les agriculteurs, devrait également devenir plus difficile à prévoir. Une mauvaise sécheresse ou une inondation peut décimer une récolte ou un troupeau pendant toute une saison. Nous prenons à titre d'exemple, les Plants de café détruits par le gel dû à des températures extrêmement basses près de Caconde, dans l'État de São Paulo, au Brésil, le 25 août 2021.

Il en résulte que les changements climatiques et l'augmentation des phénomènes météorologiques extrêmes sont l'une des raisons de l'augmentation mondiale de la faim et de la malnutrition. Les pêcheries, les cultures et le bétail peuvent être détruits ou devenir moins productifs. L'océan devenant plus acide, les ressources marines qui nourrissent des milliards de personnes sont menacées. Les changements dans la couverture de neige et de glace dans de nombreuses régions arctiques ont perturbé l'approvisionnement en nourriture provenant de l'élevage, de la chasse et de la pêche. Le stress thermique peut réduire l'eau et les prairies pour le pâturage, entraînant une baisse des rendements agricoles et affectant le bétail.

Par ailleurs, les pénuries alimentaires et les hausses de prix provoquées par le changement climatique ne toucheront pas tout le monde de la même manière : Les plus riches continueront d'avoir plus d'options pour accéder à la nourriture, tandis que des milliards d'autres seront potentiellement plongés dans l'insécurité alimentaire s'ajoutant aux milliards de personnes qui ont déjà des difficultés modérées ou sévères à se nourrir.

- Des océans plus chauds et plus acides

L'océan absorbe la majeure partie de la chaleur due au réchauffement climatique. La vitesse à laquelle l'océan se réchauffe a fortement augmenté au cours des deux dernières décennies, à toutes les profondeurs de l'océan. À mesure que l'océan se réchauffe, son volume augmente, car l'eau se dilate à mesure qu'elle se réchauffe. En outre, l'océan absorbe le dioxyde de carbone et l'empêche de pénétrer dans l'atmosphère. Mais plus de dioxyde de carbone rend l'océan plus acide,

ce qui met en danger la vie marine et les récifs coralliens.

Les océans absorbent entre un quart et un tiers de nos émissions de combustibles fossiles et sont aujourd'hui 30 % plus acides qu'ils ne l'étaient à l'époque préindustrielle. Cette acidification constitue une menace sérieuse pour la vie sous-marine, en particulier pour les créatures dont la coquille ou le squelette est calcifié, comme les huîtres, les palourdes et les coraux. Elle peut avoir un impact dévastateur sur les pêcheries de coquillages, ainsi que sur les poissons, les oiseaux et les mammifères qui dépendent des coquillages pour leur subsistance. Dans les communautés côtières où la pêche et la production de fruits de mer soutiennent l'économie locale, cet impact s'étend également aux populations humaines, détruisant les moyens de subsistance et ouvrant la porte à la ruine économique. L'augmentation de la température des océans modifie également l'aire de répartition et la population des espèces sous-marines et contribue au blanchiment des coraux, capable de tuer des récifs entiers.

- Perte d'espèces

Le changement climatique met en péril la survie des espèces sur terre et dans les océans. Ces risques augmentent avec la hausse des températures. Exacerbé par le changement climatique, le monde perd des espèces à un rythme 1 000 fois plus élevé qu'à n'importe quelle autre période de l'histoire de l'humanité. Un million d'espèces risquent de disparaître au cours des prochaines décennies. Les incendies de forêt, les conditions météorologiques extrêmes, les ravageurs et les maladies envahissantes font partie des nombreuses menaces liées au changement climatique. Certaines espèces pourront se déplacer et survivre, d'autres non.

3. Risques pour la santé

Selon l'Organisation mondiale de la santé, «le changement climatique devrait entraîner environ 250 000 décès supplémentaires par an» entre 2030 et 2050. L'augmentation des températures mondiales s'accompagne d'un accroissement du nombre de décès et de maladies dus au stress thermique, aux coups de chaleur et aux maladies cardiovasculaires et rénales. L'aggravation de la pollution atmosphérique a des répercussions sur la santé respiratoire, en particulier pour les 300 millions de personnes souffrant d'asthme dans le monde ; les pollens et les moisissures en suspension dans l'air sont également plus nombreux à tourmenter les personnes souffrant de rhume des foins et d'allergies.

Les phénomènes météorologiques extrêmes, tels que les tempêtes violentes et les inondations, peuvent entraîner des blessures, la contamination de l'eau potable et des dégâts dus aux tempêtes qui peuvent compromettre les infrastructures de base ou entraîner le déplacement de communautés.

4. Pauvreté et déplacements

Le changement climatique accroît les facteurs qui plongent les gens dans la pauvreté et les y maintiennent. Les inondations peuvent balayer les bidonvilles urbains, détruisant les habitations et les moyens de subsistance. La chaleur peut rendre difficile le travail en extérieur. La pénurie d'eau peut affecter les cultures. Au cours de la dernière décennie (2010-2019), les événements météorologiques ont provoqué le déplacement d'environ

23,1millions de personnes en moyenne chaque année, ce qui a rendu de nombreuses personnes encore plus vulnérables à la pauvreté.

La plupart des réfugiés viennent des pays les plus vulnérables et les moins prêts à s'adapter aux effets du changement climatique. En effet, les modèles historiques suggèrent que la probabilité d'être déplacé à la suite d'une catastrophe est aujourd'hui 60% plus élevée qu'il y a quarante ans - et les plus fortes augmentations de déplacements sont dues à des événements météorologiques et climatiques.

III. Comment faire face au changement climatique

1. Actions de lutte contre le changement climatique

Pour limiter le réchauffement de la planète, des transitions majeures seront nécessaires dans le secteur de l'énergie, ce qui implique une forte réduction de l'utilisation des combustibles fossiles, une électrification généralisée, une amélioration de l'efficacité énergétique et l'utilisation de combustibles alternatifs (tels que l'hydrogène). En ce sens, le passage des systèmes énergétiques des combustibles fossiles aux énergies renouvelables, telles que le solaire ou l'éolien, est essentiel pour réduire les émissions. De nombreux pays s'efforcent déjà d'atteindre l'objectif de zéro émission d'ici 2050, mais les experts estiment que la moitié des réductions d'émissions doivent être réalisées avant 2030 pour maintenir le réchauffement en dessous de 1,5°C.

2. L'effort mondial pour atteindre l'objectif «zéro émission»

Effectivement, une coalition croissante de pays, d'entreprises et d'autres institutions s'engage à parvenir à des émissions de gaz à effet de serre nettes nulles. Plus de 70 pays, dont les plus gros pollueurs se sont fixés un objectif de zéro émission, ce qui réduira considérablement les émissions mondiales. Les sept principaux émetteurs de gaz à effet de serre (la Chine, les États-Unis d'Amérique, l'Inde, l'Union européenne, l'Indonésie, la Fédération de Russie et le Brésil) représentaient environ la moitié des émissions mondiales de gaz à effet de serre en 2020.

Le Groupe des 20 (Argentine, Australie, Brésil, Canada, Chine, France, Allemagne, Inde, Indonésie, Italie, Japon, République de Corée, Mexique, Russie, Arabie Saoudite, Afrique du Sud, Turquie, Royaume-Uni, États-Unis et Union européenne) est responsable d'environ 75 % des émissions mondiales de gaz à effet de serre.

3. Les instruments juridiques des Nations Unies

- La Convention-cadre des Nations Unies sur les Changements Climatiques (CCNUCC)

En 1992, 197 pays ont joint un traité international, la Convention-cadre des Nations Unies sur les changements climatiques (CCNUCC), en vue de considérer ce qui pouvait être fait pour réduire le réchauffement global et faire face au défi posé par les changements climatiques.

- Le Protocole de Kyoto

En 1995, dans une décision connue sous le nom de Mandat de Berlin, les Parties à la Convention CCNUCC entamèrent un cycle de négociations en vue de décider des engagements plus solides et plus détaillés pour les pays industrialisés. Après deux années et demie d'intenses négociations, le Protocole de Kyoto fut adopté au Japon, le 11 décembre 1997. Le Protocole de Kyoto pose une limite aux grandes économies mondiales sur le rejet total des émissions de gaz à effet de serre (GES). Une première période d'engagements allait de 2008 à 2012. La seconde période d'engagement a démarré le 1er janvier 2013 et s'est terminé en 2020. Le Protocole compte 192 Parties.

- L'Accord de Paris

L'Accord de Paris est entré en vigueur le 4 novembre 2016. Cet accord universel s'appuie sur la Convention et rassemble toutes les nations autour d'une cause commune qui vise à accélérer et intensifier les actions et les investissements nécessaires avec pour objectif de limiter la hausse de la température à 1,5 °C au-dessus des niveaux de l'ère préindustrielle.

- Conférence des Nations unies sur les changements climatiques COP 28

La COP 28, conférence des Nations unies sur les changements climatiques s'est achevée le 12 Décembre 2023 sur un accord qui marque le « début de la fin » de l'ère des combustibles fossiles, en jetant les bases d'une transition rapide, juste et équitable, étayée par de fortes réductions des émissions et un financement accru.

Dans une démonstration de solidarité mondiale, les négociateurs de près de 200 parties se sont réunis à Dubaï avec une décision sur le premier « bilan mondial » visant à intensifier l'action climatique avant la fin de la décennie, avec pour objectif principal de réduire les émissions de gaz à effet de serre et d'améliorer la qualité de l'air.

L'objectif principal est de maintenir la limite de haussement de température de 1,5 °C à portée de main.

Le bilan mondial reconnaît les données scientifiques qui indiquent que les émissions mondiales de gaz à effet de serre doivent être réduites de 43% d'ici à 2030, par rapport aux niveaux de 2019, pour limiter le réchauffement de la planète à 1,5°C. Mais il note que les parties ne sont pas sur la bonne voie pour atteindre les objectifs de l'Accord de Paris.

Le bilan mondial invite les parties à prendre des mesures pour tripler, à l'échelle mondiale, les capacités en matière d'énergies renouvelables et doubler les améliorations en matière d'efficacité énergétique d'ici à 2030. La liste comprend également l'accélération des efforts en vue de la réduction progressive de la production d'électricité à base de charbon, l'élimination des subventions aux combustibles fossiles, et d'autres mesures qui favorisent la transition vers l'abandon des combustibles fossiles dans les systèmes énergétiques, de manière juste, ordonnée et équitable, les pays développés continuant à jouer un rôle de chef de file.

Le financement de la lutte contre les changements climatiques a occupé le devant de la scène lors de la conférence et a été qualifié à plusieurs reprises de « grand catalyseur de l'action climatique ».

Toutefois, les engagements financiers doivent faire face aux milliers de milliards d'euros nécessaires pour soutenir les pays en développement dans leur lutte contre les changements climatiques, dans leur transition vers des énergies propres, dans la mise en œuvre de leurs plans nationaux et dans leurs efforts d'adaptation.

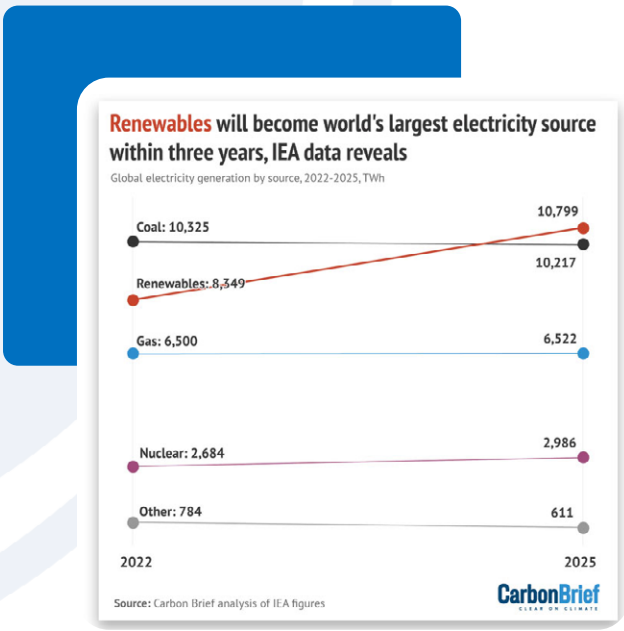
4. Les avantages des technologies d'énergie propre :

- Les énergies renouvelables seront bientôt la première source d'électricité au monde

Les sources d'énergie renouvelables - telles que l'eau, la géothermie, le vent et le soleil sont disponibles dans tous les pays et leur potentiel n'est pas encore pleinement exploité. Cependant, près de 30% de l'électricité mondiale provient aujourd'hui des énergies renouvelables. D'ici 2050, 90 % de l'électricité mondiale peut et doit provenir des énergies renouvelables.

Les énergies renouvelables devraient devenir la principale source de production d'électricité dans le monde d'ici le début de 2025, dépassant le charbon.

Comme le montre le graphique ci-dessous, les énergies renouvelables sont la source d'énergie qui connaît la croissance la plus rapide.



- Les énergies renouvelables sont moins chères que les combustibles fossiles

Dans la plupart des régions du monde, l'électricité produite par les nouvelles centrales d'énergie renouvelable, telles que l'énergie éolienne ou solaire, est aujourd'hui moins chère que l'électricité produite par les nouvelles centrales à combustibles fossiles. Les nouveaux projets éoliens et solaires terrestres coûtent environ 40 % de moins que

les centrales au charbon ou au gaz et l'écart se creuse.

Depuis 2010, le monde a été témoin d'un changement radical dans la compétitivité des options d'énergie renouvelable : L'énergie solaire a connu les réductions de coûts les plus rapides, les coûts des projets à grande échelle nouvellement mis en service ayant chuté de 88 % au niveau mondial entre 2010 et 2021, principalement grâce aux améliorations technologiques continues, aux économies d'échelle plus importantes et à la réduction des coûts de financement pour les centrales éoliennes et solaires. Le coût de l'éolien terrestre a baissé de 68 % et celui de l'éolien en mer de 60 % depuis 2010.

- Les panneaux solaires et les éoliennes font bon usage du sol

Toutes les sources d'énergie nécessitent des terres : du terrain utilisé pour l'extraction du charbon à celui occupé par une centrale électrique.

Les parcs éoliens nécessitent beaucoup de terrain, mais alors qu'une mine de charbon n'est utilisée qu'une seule fois, un parc éolien continue à produire de l'énergie, année après année. Au fil du temps, un hectare de parc éolien ou solaire peut produire plus d'électricité qu'un hectare de mine de charbon ou d'uranium.

Les terres utilisées pour les parcs solaires et éoliens peuvent être «à double usage», c'est-à-dire utilisées à la fois pour la production d'énergie et l'agriculture. Une fois construit, un parc solaire ou éolien a si peu d'impact sur ses terres qu'il est de plus en plus courant d'autoriser le pâturage et l'agriculture sur les mêmes acres en même temps.

Les panneaux solaires n'ont pas besoin d'être installés directement sur le sol, ils peuvent être placés sur des structures existantes telles que des toits, des routes ou des auvents de parking, au-dessus de canaux et sur des terres agricoles, et même flotter sur des lacs et des étangs.

Les fermes solaires peuvent également être installées sur des terrains qui ne se prêtent pas à d'autres utilisations : déserts, décharges, anciennes mines de charbon ou territoires contaminés (Tchernobyl accueille aujourd'hui une centrale solaire).

Les panneaux solaires peuvent être installés n'importe où sur Terre, car le soleil brille partout. Aucun autre type de production d'électricité ne peut rivaliser avec cette flexibilité.

- Les technologies d'énergie propre produisent beaucoup moins de pollution par le carbone que les combustibles fossiles.

Les technologies d'énergie propre - des éoliennes aux panneaux solaires en passant par les véhicules électriques et le stockage des batteries - nécessitent un large éventail de minéraux et de métaux et produisent donc des émissions, mais bien moins que les combustibles fossiles.

Les panneaux solaires produits aujourd'hui n'ont besoin de fonctionner que pendant 4 à 8 mois pour compenser leurs émissions de fabrication (et le panneau solaire moyen a une durée de vie d'environ 25 à 30 ans). De même, les éoliennes ne nécessitent qu'environ 7 mois pour produire suffisamment d'électricité propre pour compenser la pollution par le carbone générée lors de leur fabrication (et leur durée de vie moyenne est de 20 à 25 ans).

Les véhicules électriques, sur l'ensemble de leur cycle de vie, de la fabrication à la mise au rebut, produisent environ la moitié des émissions de carbone d'une voiture moyenne à moteur à combustion interne, avec un potentiel de réduction supplémentaire de 25 % grâce à une électricité à faible teneur en carbone.

- Les énergies renouvelables résistent mieux aux phénomènes météorologiques extrêmes

Les centrales à gaz n'ont pas pu répondre à la demande d'électricité pendant le froid exceptionnel qui a sévi au Texas, aux États-Unis, en février 2021, privant d'électricité jusqu'à 5 millions de clients pendant quatre jours, principalement en raison du gel des puits de gaz et des pannes d'électricité des

générateurs de gaz. Les centrales au charbon et les centrales nucléaires ont également connu des pannes.

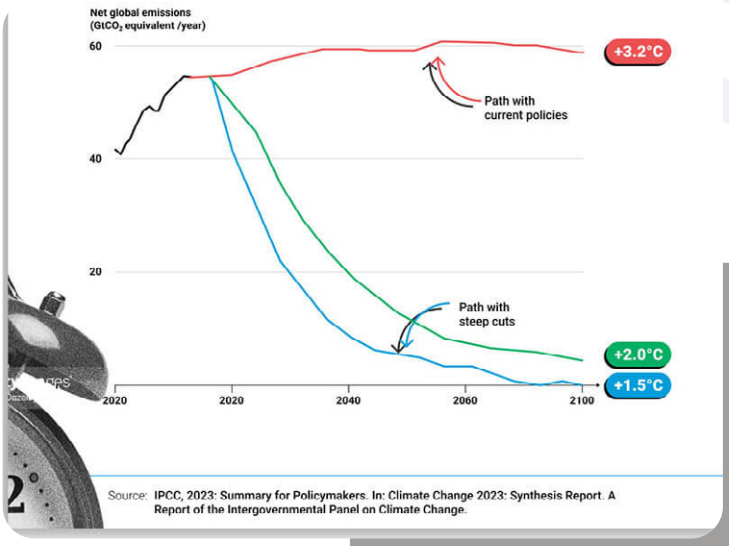
- Les alternatives aux produits à base de pétrole

De nombreux produits d'usage courant sont encore fabriqués à partir de pétrole ou d'autres combustibles fossiles. Le processus d'extraction et de transport de ces combustibles, puis la fabrication des produits génère beaucoup d'émissions de carbone. La plupart des plastiques, des vêtements, des pneus, des appareils numériques, des engrais, des détergents et d'innombrables autres produits de la vie courante sont fabriqués à partir de produits pétrochimiques.

La production de plastique est l'un des processus de fabrication les plus énergivores au monde. Le matériau est fabriqué à partir de combustibles fossiles tels que le pétrole brut, qui sont transformés en polymère par la chaleur et d'autres additifs. En 2019, les plastiques ont généré 1,8 milliard de tonnes métriques d'émissions de carbone, soit 3,4 % du total mondial.

Mais il existe des alternatives. Il est possible de remplacer les combustibles fossiles utilisés pour fabriquer des plastiques ou des engrais par de la biomasse (matière organique provenant de plantes et d'animaux).

Nous pouvons encore limiter le changement climatique si nous agissons maintenant.



Source: IPCC, 2023: Summary for Policymakers. In: Climate Change 2023: Synthesis Report. A Report of the Intergovernmental Panel on Climate Change.

Cas de la Tunisie :

La Tunisie est un pays fortement vulnérable aux changements climatiques. En effet, le changement climatique et l'aggravation des sinistres liés aux catastrophes naturelles est désormais considéré comme l'un des risques environnementaux les plus importants et les plus préoccupants pour les assureurs et réassureurs tunisiens.

Les catastrophes naturelles auxquelles est exposée la Tunisie

Le ministère des Finances tunisien a publié en 2022 un rapport intitulé « Rapport de synthèse sur la Base de données des Expositions financières de la Tunisie aux Catastrophes naturelles ». L'objectif principal de ce rapport est d'améliorer la connaissance des risques auxquels la Tunisie est confrontée en matière de catastrophes naturelles et présente des statistiques descriptives détaillant l'état de l'exposition financière des actifs immobiliers tant publics que privés.

- Les inondations : un risque accru

L'inondation est la catastrophe naturelle qui a le plus touché, à différents degrés, les diverses régions du pays. Les inondations qui ont plus marqué le pays à travers les dégâts qu'ils ont causé sont celles de l'automne 1969 avec plus de 900 mm de précipitations en plusieurs séries orageuses. Cet évènement a frappé les régions centrales et méridionales de la Tunisie et a engendré 542 morts, laissant 340 000 personnes sans abri et générant entre 30 et 35 millions de dinars de pertes à cette époque selon le rapport évoqué ci-dessus. La crue de mars 1973 dans le bassin de la Medjerda survenue au nord de la Tunisie a engendré 100 décès. Par ailleurs, les crues soudaines catastrophiques de septembre 2018 qui ont eu lieu dans la région du Cap Bon avec près de 200 mm de précipitations sur la ville de Nabeul en quelques heures ont engendré 6 morts et des dégâts importants dans la ville (plus de 2500 maisons et 57 écoles ont été endommagées et 1791 agriculteurs ont été sinistrés). Les inondations de Nabeul de 2018 ont coûté 19,1 millions de dinars aux assureurs. Celles d'octobre 2018 ont aussi mobilisé 14,1 millions de dinars d'indemnisations.

- Le risque de tremblement de terre

D'un autre côté, la Tunisie a également été touchée par les tremblements de terre, bien que leurs dégâts aient été beaucoup moins désastreux que ceux des inondations. Selon le même rapport du ministère des finances tunisien, trois évènements majeurs ont été enregistrés au cours de l'histoire contemporaine du pays : le tremblement de terre de 1856 qui a détruit près de 13 villages aux environs du gouvernorat de Kairouan, celui de 1957 qui est le plus dévastateur de tout le 20ème siècle en Tunisie et qui s'est produit à Jendouba, avec une magnitude de 5,6 sur l'échelle Richter, causant 13 morts et l'effondrement de plusieurs bâtiments. Enfin, un séisme de magnitude 5,1 a été enregistré dans le centre de la Tunisie en 2018. L'épicentre a été localisé à une soixantaine de kilomètres au nord-ouest de la ville de Gabès où vivent environ 110 000 habitants et à seulement 10 kilomètres de profondeur, aucun dégât particulier n'a été noté.

- Des sécheresses plus fréquentes et plus intenses

En Tunisie, environ deux tiers du territoire sont constitués de régions semi-arides à arides, ce qui les rend vulnérables aux sécheresses fréquentes et intenses. Au cours du 20ème siècle, le pays a déjà connu une augmentation marquée du nombre de jours de fortes chaleurs, principalement entre juillet et septembre. D'ici 2050, les projections indiquent que la pluviométrie en Tunisie devrait diminuer de manière significative. Cependant, on s'attend à une augmentation de la fréquence des pluies torrentielles, ce qui accentuera le risque d'inondations à fort impact.

Conclusion

L'atténuation du changement climatique et notre capacité à en annuler les effets dépend de la mise en œuvre réussie de politiques qui réduisent considérablement ses effets générateurs et mettent fin à notre dépendance à l'égard des combustibles fossiles dangereux. Ces mesures doivent être prises rapidement afin de garantir un présent et un avenir plus sains.

En suivant les avertissements urgents et en limitant le réchauffement, nous pourrons peut-être éviter de franchir certains des seuils critiques qui, une fois franchis, peuvent avoir des conséquences catastrophiques et potentiellement irréversibles pour la planète, y compris un réchauffement plus important.

Ainsi, les choix que nous faisons aujourd'hui détermineront les changements climatiques que nous connaîtrons à l'avenir. En effet, des réductions importantes et durables des émissions de dioxyde de carbone et d'autres gaz à effet de serre permettraient de limiter le changement climatique.

Si nous agissons maintenant, nous pouvons limiter le changement climatique et préserver une planète vivable. Nous disposons des connaissances, des outils et des ressources nécessaires pour garantir un avenir vivable et durable pour tous.

Mais la mesure dans laquelle la crise climatique bouleverse nos vies dépend de la décision des dirigeants mondiaux de tracer une voie différente. Si nous ne parvenons pas à réduire les émissions de gaz à effet de serre, les scientifiques prévoient un réchauffement catastrophique de 4,3 degrés Celsius d'ici la fin du siècle. On s'attendra alors à des guerres pour l'eau, des hôpitaux bondés pour faire face à la propagation des maladies, des pêcheries effondrées, des récifs coralliens morts, des vagues de chaleur encore plus meurtrières… Ce ne sont là que quelques-unes des conséquences prévues par les climatologues.

Les Risques Cyber

CYBER RISQUES

L'avènement de l'ère numérique et son expansion rapide ont engendré une transformation profonde, laissant une empreinte sur tous les aspects de notre quotidien. Les avancées technologiques ont ouvert des horizons innovants, mais ont également posé des défis complexes en matière de sécurité des données. La protection des données est désormais une priorité absolue pour prévenir les atteintes à la vie privée, le vol d'identité et l'accès non autorisé à des informations confidentielles.

La vie moderne repose entièrement sur le bon fonctionnement de la technologie. Quelques heures sans accès à l'e-mail ou à Internet peuvent générer de l'inquiétude dans n'importe quel environnement professionnel. La nécessité de maintenir une hygiène cybernétique devient aussi cruciale qu'une routine quotidienne. Bien que le marché de l'assurance cyber ne soit pas encore pleinement développé, les clients manifestent un intérêt croissant pour des produits d'assurance mitigeant les risques liés à la cybernétique.

Dans ce contexte, toutes les entités, qu'elles soient du secteur public ou privé, grandes ou petites, font face à une menace constante d'attaques cybernétiques. Les particuliers ne sont pas exempts de ces risques. Cependant, évaluer précisément l'ampleur quotidienne des attaques contre les entreprises demeure complexe, en raison du sous-signalement et de la détection initiale limitée. La cybersécurité s'érige en rempart essentiel, visant à protéger entreprises et individus contre fraudes, escroqueries, intrusions, et fuites de données en ligne, garantissant ainsi l'intégrité, la disponibilité et la confidentialité des informations sensibles.

I. Qu'est-ce qu'une cyberattaque

1. Définition

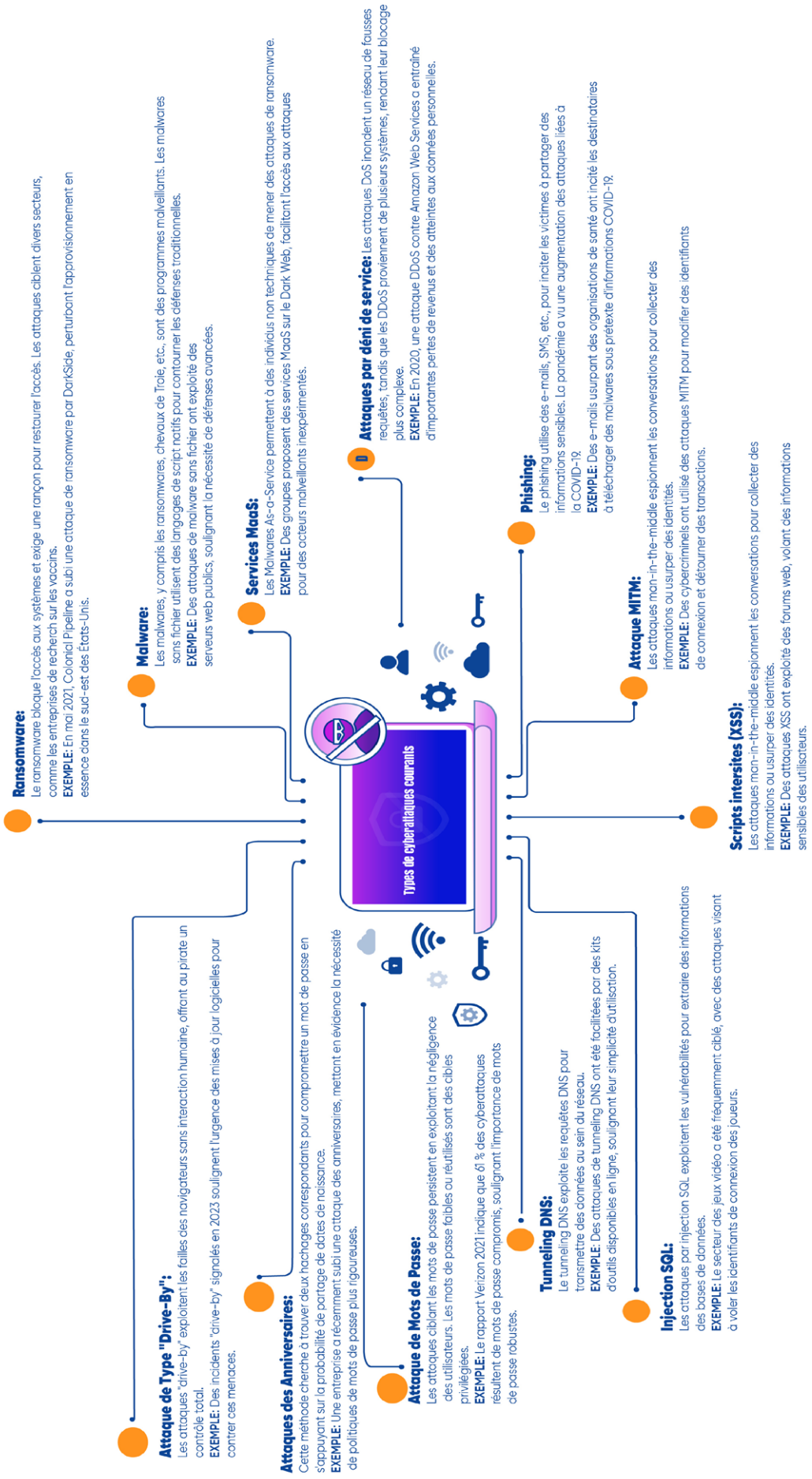
Une cyberattaque est une tentative d'accès non autorisé à un réseau ou système informatique ou un appareil numérique menée par des cybercriminels, des cyberattaquants ou des cybers adversaires,

C'est une intention visant à voler, exposer, modifier, désactiver ou détruire des données, des applications ou d'autres actifs.

Les cyberattaques peuvent cibler un large éventail de victimes, qu'il s'agisse de particuliers, d'entreprises ou encore d'administrations publiques.

Lorsqu'il s'attaque à des entreprises ou d'autres organisations, l'objectif du cyberattaquant est généralement d'accéder à des ressources sensibles et précieuses de l'entreprise, telles que les éléments de propriété intellectuelle (PI), les données des clients ou les informations de paiement.

2. Types de cyberattaques courants



II. L'assurance cyber

1. Définition de l'assurance cyber

L'assurance cybersécurité est un produit qui aide les entreprises à gérer le risque d'activités cybercriminelles telles que les cyberattaques et les violations de données. Les menaces basées sur Internet qui affectent l'infrastructure informatique d'une organisation ont un coût élevé, qui n'est généralement pas couvert par les polices ordinaires de responsabilité civile des entreprises ou par les produits d'assurance traditionnels. La cyber-assurance peut aider à protéger les organisations contre ce coût.

Avec le risque croissant de cyber-attaques sur les applications, les appareils, les réseaux et les utilisateurs, la cyber-assurance devient de plus en plus importante pour les entreprises. Les violations de données peuvent avoir un impact significatif sur votre entreprise, notamment un impact financier direct, des coûts indirects, une atteinte à la protection des données personnelles et une perte de revenus. Un autre type de dommage est la responsabilité juridique ou les amendes réglementaires, suite à la perte ou au vol de données de tiers.

La cyber assurance est très similaire au processus de souscription d'une assurance contre les risques physiques et les catastrophes naturelles. Elle couvre toutes

les pertes qu'une entreprise peut subir à la suite d'une cyberattaque.

La cyber-assurance protège les entreprises contre les cyber-incidents, y compris le cyber-terrorisme et les cyber-attaques, et donne aux organisations les ressources nécessaires pour se remettre d'incidents de sécurité majeurs.

2. Importance du cyber sécurité pour les entreprises

Au vu du nombre croissant de cyberattaques et des coûts élevés associés aux mesures correctives, la cyber assurance est importante pour la quasi-totalité des entreprises.

L'une des principales cibles des pirates informatiques et des cybercriminels sont les données contenant des informations personnelles identifiables (IPI) telles que les noms, les adresses, les numéros de sécurité sociale, les informations sur les comptes bancaires et les numéros de cartes de crédit. Ces informations peuvent être utilisées pour commettre des fraudes, mener des attaques secondaires et être vendues sur le dark web. Il s'agit d'une préoccupation particulière, car elle expose l'organisation à des risques juridiques et de conformité.

Nombreux sont ceux qui pensent que les petites organisations, ou celles qui sont peu connues du public, sont à l'abri des cyberattaques. En réalité, les cybercriminels peuvent facilement cibler ces organisations. De nombreuses attaques sont automatisées et ne visent pas spécifiquement des organisations bien connues, mais elles peuvent tout de même avoir des conséquences dévastatrices.

D'autre part, les grandes organisations bien connues peuvent être la cible d'attaquants sophistiqués et de groupes de pirates organisés. Ce type de cyberattaque utilise généralement des ransomwares pour attaquer des cibles importantes et de grande valeur. Les victimes sont sélectionnées en fonction de leur capacité à payer la rançon et de la probabilité qu'elles paient la rançon pour rétablir leurs activités ou éviter une enquête publique.

3. Comment fonctionne l'assurance cybersécurité ?

De nombreux assureurs proposent également des polices d'assurance cybersécurité telles que l'assurance erreurs et omissions (E&O), l'assurance responsabilité civile des entreprises et l'assurance des biens commerciaux. La plupart des polices comprennent :

- Une couverture de première ligne visant les pertes subies par l'assuré
- Une couverture des tierces parties pour les pertes subies par autrui à la suite d'un cyber incident ou d'un incident résultant d'une relation d'affaires avec cette entreprise.
- L'assurance responsabilité civile est généralement incluse.

La cyber-assurance permet de couvrir les cyber-accidents et les pertes financières causées par les accidents. La couverture du risque cybernétique permet également de couvrir les coûts liés à la remédiation, y compris l'assistance juridique, les paiements aux enquêteurs, les communications et les médias, ainsi que les remboursements aux clients.

4. Que couvre l'assurance cybernétique

En cas de cyberattaque, la plupart des polices d'assurance cyber couvrent les coûts financiers et la protection des données personnelles si des données ou des systèmes électroniques sont perdus, endommagés, volés ou détruits. Il s'agit à la fois des coûts de première partie (supportés par l'organisation qui souscrit l'assurance) et des coûts de tierce partie (supportés par d'autres organisations ou individus).

L'indemnisation de première partie de perte directe de l'assuré englobe les dépenses et les coûts suivants :

- Des enquêtes sur la cybercriminalité
- Récupération des données et des systèmes informatiques perdus à la suite d'une violation de sécurité,
- Perte de revenus due à la fermeture de l'entreprise
- Atteinte aux données personnelles
- Les demandes d'extorsion de pirates informatiques, y compris les paiements
- Les frais de défense, de notification (dans le cas où la réglementation exige que l'organisation notifie les tiers concernés).

Les coûts pour les tierces parties résultant d'une réclamation contre l'assuré, comprennent :

- Les dommages-intérêts et les règlements
- Le coût des défenses juridiques
- Les réclamations en violation du Règlement général sur la protection des données (GDPR General Data Protection Regulation) de la réglementation en vigueur.

5. Comment souscrire une police d'assurance cybernétique

Pour souscrire une police d'assurance cybernétique, la première étape cruciale consiste à réaliser un audit approfondi de votre infrastructure, tout en documentant rigoureusement les politiques et systèmes de cybersécurité de l'entreprise. Cette démarche permet à l'assureur cybernétique d'évaluer les défenses cybernétiques de l'organisation, un aspect essentiel pour déterminer à la fois la couverture nécessaire et le coût associé.

Il est important de souligner que les compagnies d'assurance cybernétique suivent une approche similaire aux autres assureurs, ne pouvant assurer les organisations qui ne disposent pas d'une stratégie et d'une infrastructure de sécurité robustes. Une fois l'audit de cybersécurité effectué, l'entreprise peut entamer le processus en contactant les compagnies d'assurance pour souscrire à une police adaptée.

Les compagnies d'assurance examineront attentivement les stratégies de cybersécurité existante pour évaluer les niveaux de risque associés à l'entreprise. Sur cette base, elles formuleront une offre d'assurance personnalisée, en ajustant le prix en conséquence. Il est crucial de noter que chaque compagnie d'assurance a ses propres normes, exceptions et coûts.

6. Exigences Prédominantes en Cyber assurance

La souscription à une cyber assurance est devenue essentielle pour les entreprises, mais les assureurs imposent des exigences rigoureuses pour atténuer les risques. Voici les principales exigences :

- **Implémentation de la Détection et Réponse aux Menaces (EDR):** Les assureurs préconisent l'EDR sur tous les postes de travail pour surveiller, détecter, et répondre aux menaces avancées. Les logiciels antivirus traditionnels se révèlent souvent insuffisants face aux attaques modernes.
- **Utilisation de l'Authentification Multifactorielle Multi-Factor Authentication (MFA):** L'AMF est souvent une exigence minimale. Elle utilise divers facteurs d'authentification, tels que les mots de passe à usage unique et la biométrie, pour renforcer la sécurité et prévenir les accès non autorisés.
- **Élaboration d'une Stratégie de Sauvegarde Solide :** Une stratégie de sauvegarde robuste est cruciale pour minimiser les perturbations en cas d'attaque par ransomware. Les assureurs exigent des normes spécifiques, telles que des procédures de sauvegarde et des sauvegardes hors ligne.
- **Mise en Place de la Gestion des Identités et des Accès (Identity and access management (IAM)):** L'IAM est

nécessaire pour appliquer des politiques d'accès, surveiller l'activité réseau, et contrôler les autorisations des utilisateurs. Elle atténue les risques liés aux menaces internes et aux erreurs de configuration.

- **Gestion Rigoureuse des Correctifs :** Une gestion efficace des correctifs, notamment pour les vulnérabilités critiques, est cruciale. Cela englobe des mises à jour régulières, une cartographie de l'inventaire, et des tests pour évaluer la robustesse des défenses.

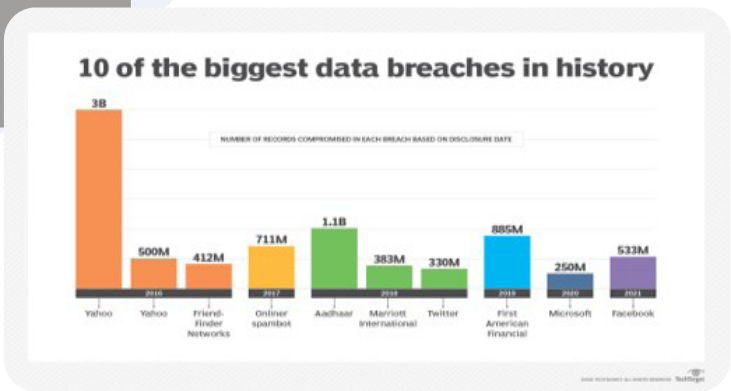
Adopter ces mesures renforce la posture de sécurité des entreprises, réduisant ainsi les risques et faisant en sorte que les assureurs considèrent favorablement leur couverture cyber.

III. L'impact économique des cyber Risk

1. L'impact économique

Actuellement, on estime qu'environ 4000 nouvelles attaques cybernétiques se produisent chaque jour dans le monde. Toutes les 14 secondes, une entreprise devient victime d'une attaque de ransomware, entraînant potentiellement des pertes financières dévastatrices. En 2023, plusieurs tendances significatives ont émergé dans le domaine de la cybersécurité, illustrées par des statistiques clés :

- Le coût moyen d'une fuite de données a atteint 4,45 millions de dollars en 2023, en hausse de 15% en trois ans, soulignant l'importance du chiffrement des données.
- Les ransomwares BlackCat et Black Basta ont représenté 15,5% du volume total des cyberattaques déclarées au deuxième trimestre de 2023 en raison de leur activité soutenue via des plateformes de Ransomware-as-a-Service (RaaS).
- Un rapport d'IBM indique que 47% des victimes de ransomware étudiées ont choisi de payer la rançon, tandis que 37% ont évité d'impliquer les autorités, soulignant les dilemmes auxquels sont confrontées les organisations lors d'une attaque.
- Le groupe de cybercriminels LockBit a exigé un montant record de 80 millions de dollars lors de l'attaque contre l'entreprise CDW en octobre 2023, illustrant la croissance des demandes de rançon.
- Malgré les filtres, 89% des messages indésirables parviennent à contourner les vérifications d'authentification des e-mails, soulignant la nécessité de renforcer la sensibilisation des employés.
- Les attaques de ransomware impliquant une extorsion de données ont augmenté de 112% par rapport à l'année précédente, alimentées par la structuration croissante des collectifs de cybercriminels.
- En 2023, 198 vulnérabilités Zero-Day ont été découvertes, doublant le nombre de l'année précédente, avec 73% de ces vulnérabilités notées comme critiques ou présentant une gravité élevée.
- Depuis le lancement de ChatGPT, les e-mails de phishing ont augmenté de 1 265%, soulignant l'adoption de l'intelligence artificielle pour élaborer des attaques plus sophistiquées et éviter les filtres anti-phishing.
- Un total de 28 902 CVE ont été publiées en 2023, représentant une augmentation de 15% par rapport à 2022, mettant en évidence la persistance des vulnérabilités dans les systèmes informatiques.
- En France, les cyberattaques réussies en 2022 ont coûté 2 milliards d'euros, comprenant des coûts directs, des rançons payées et des pertes de production.
- Selon une étude d'Accenture Security et du Ponemon Institute, le coût moyen d'une cyberattaque pour une entreprise est estimé à 13 millions de dollars, avec une augmentation de 12% en un an



Ces chiffres viennent refléter l'évolution rapide du paysage de la cybersécurité et soulignent la nécessité continue d'innover pour faire face aux menaces émergentes.

2. L'impact sur l'industrie mondiale de l'assurance

L'industrie mondiale de l'assurance cyber est à l'avant-garde de l'expansion, reflétant l'escalade de la sophistication des menaces cybernétiques. Selon la recherche de MarketsandMarkets, une croissance substantielle est prévue, passant de 11,9 milliards de dollars en 2022 à une projection de 29,2 milliards de dollars d'ici 2027. Cette montée en puissance est alimentée par le potentiel accru de pertes financières, l'augmentation des cyberattaques et un labyrinthe de conformité réglementaire. Des secteurs tels que la fabrication, les services financiers et les soins de santé, ainsi que des secteurs fortement réglementés, sont en tête de liste des demandes d'assurance cyber. En 2021, rien que les incidents de ransomwares ont connu une augmentation stupéfiante de 93%.

Swiss Re, met en lumière la hausse sans précédent des cyberattaques signalées, augmentant cinq fois depuis 2016 et entraînant des pertes mondiales d'environ 945 milliards de dollars. Malgré une demande croissante, le secteur de l'assurance cyber se débat avec une capacité limitée, des risques systémiques et des caractéristiques qui défient les normes d'assurabilité conventionnelles.

Reconnaissant le rôle central des assureurs dans la mitigation des risques cybernétiques, Swiss Re souligne la nécessité d'une stratégie complète de résilience cybernétique. La croissance anticipée du marché de l'assurance cyber à 23 milliards de dollars d'ici 2025 souligne la nécessité de redéfinir les procédures de souscription, d'améliorer les exigences et de délimiter de manière transparente les limites de la capacité du marché.

Lloyd's, a publié un scénario de risque systémique qui montre que l'économie mondiale est exposée à des pertes de 3,5 billions de dollars sur une période de cinq ans en cas d'attaque cyber majeure sur les paiements des services financiers.

Le scénario de risque modélise l'impact économique mondial d'une attaque cyber hypothétique mais plausible qui pourrait entraîner des perturbations généralisées dans les affaires mondiales.

Lloyd's a produit le scénario de risque en partenariat avec le Cambridge Centre for Risk Studies. La recherche explore neuf scénarios hypothétiques de risques systémiques pour révéler l'impact économique potentiel de chaque scénario dans 107 pays et à trois niveaux de gravité - majeur, sévère et extrême.

Les États-Unis, la Chine et le Japon sont les trois pays qui connaissent les pertes économiques sur cinq ans les plus élevées à la suite du scénario. Avec des pertes attendues de 1,1 billion de dollars aux États-Unis, suivies de 470 milliards de dollars en Chine et de 200 milliards de dollars au Japon. Le temps de récupération pour chaque pays ou région dépend de la structure de son économie, de ses niveaux d'exposition et de sa résilience.

Utilisant le produit intérieur brut (PIB) comme mesure centrale, Lloyd's et Cambridge calculent que la perte économique mondiale d'une attaque cyber mondiale sur un système de paiement de services financiers majeur serait de 3,5 billions de dollars sur une période de cinq ans (la moyenne pondérée sur les trois niveaux de gravité modélisés).

La perte économique varierait de 2,2 billions de dollars dans le scénario de gravité la plus faible à 16 billions de dollars dans le scénario le plus extrême.

L'étude met en lumière comment les attaques cyber continuent de menacer les entreprises et les gouvernements, avec des coûts annuels liés à la maintenance, à la prévention et à la réponse aux attaques en augmentation. Il s'agit d'un risque ayant le potentiel d'affecter gravement la société, car il s'agit d'un risque complexe et interconnecté ayant des répercussions sur des domaines tels que les chaînes d'approvisionnement et la géopolitique.

L'assurance cyber est un marché en croissance qui devrait atteindre entre 13 et 25 milliards de dollars de primes brutes d'ici 2025. Cependant, cela représente encore une petite partie des pertes économiques potentielles auxquelles les entreprises et la société sont confrontées.

L'assureur Londonien confirme le rôle joué par le secteur quant au renforcement de la résilience face aux risques systémiques, et le soutien et la protection des clients contre la menace potentielle que représente le cyber pour les entreprises et la société. L'interconnexion

mondiale du cyber signifie qu'il s'agit d'un risque trop important pour qu'un seul secteur le supporte seul, et par conséquent il est crucial de continuer à partager les connaissances, l'expertise et les idées innovantes entre le gouvernement, l'industrie et le marché de l'assurance pour nous assurer de renforcer la résilience de la société face à l'ampleur potentielle de ce risque.

La menace croissante de la cybercriminalité est un sujet alarmant. Selon les prévisions de Cyber security Ventures, les coûts associés à la cybercriminalité atteindront 8 billions de dollars d'ici fin 2023, avec une estimation de 10,5 billions de dollars d'ici 2025, comme indiqué dans le rapport officiel 2022 sur la cybercriminalité d'eSentire.

La cybercriminalité se propage à travers tous les secteurs et marchés, impactant quotidiennement les entreprises, comme illustré par l'attaque sophistiquée de ransomware contre l'Agence écossaise de protection de l'environnement (SEPA) en 2021, et la violation des données de santé des employés de Waste Management Services aux États-Unis en janvier 2021.

Le rapport Microsoft Digital Defense souligne que les individus sont désormais le principal vecteur d'attaque, représentant 61 % des violations, avec des attaques basées sur l'identité devenues irrésistibles pour les cybercriminels en raison de leur rapport risque/rendement avantageux. Les attaques par pulvérisation de mot de passe et le phishing restent les formes les plus courantes, avec la compromission des e-mails professionnels (BEC) considérée comme potentiellement la plus coûteuse.

Les ransomwares demeurent la menace prédominante pour les entreprises, avec 76 % d'entre elles ciblées en 2022. Cependant, seulement 50 % ont réussi à récupérer leurs données après avoir payé la rançon, et plus de 66 % ont signalé des infections multiples et isolées.

Les industries des déchets, du recyclage et du transport, avec leurs systèmes ERP centraux, appareils mobiles, capteurs IoT et caméras, présentent des caractéristiques informatiques spécifiques qui ajoutent une complexité accrue à leurs défis de cybersécurité. Cette dépendance croissante à la technologie, souvent à travers des systèmes hérités cloisonnés, rend la détection des menaces et des violations plus difficiles.

Pour surmonter ces défis, les entreprises doivent adopter une approche de cybersécurité intelligente, automatisée et intégrée pour assurer la prévention, la détection et la réponse des utilisateurs finaux grâce à une infrastructure appropriée. Dans le paysage technologique en évolution rapide d'aujourd'hui, les solutions basées sur le cloud, notamment le logiciel en tant que service (SaaS), offrent une sécurité de classe mondiale, renforçant la résilience des entreprises dans divers domaines. Il est impératif que chaque entreprise gère son profil de sécurité, compte tenu de la sophistication croissante des menaces cybernétiques.

Dans le même cadre, le rapport sur la résilience cybernétique d'Aon pour

2023 fournit des informations cruciales sur les conséquences de l'incident cyber majeur. Selon les données recueillies, Bien que les attaques de ransomware aient enregistré une baisse de 16 % du troisième au quatrième trimestre 2022, le premier trimestre 2023 a marqué une augmentation.

Ce rapport propose une approche holistique en couvrant six domaines de risque, à savoir le risque cyber, opérationnel, de la chaîne d'approvisionnement, interne, de protection des données personnelles et systémique.

Les données proviennent de l'évaluation du quotient cybernétique d'Aon (CyQu). Le rapport met en évidence la nécessité croissante pour les entreprises de renforcer leurs mesures de cybersécurité, en particulier contre les attaques de phishing, l'une des principales méthodes d'accès initial au réseau.

Il souligne également que deux entreprises sur cinq signalent un manque de contrôles au sein de leur centre des opérations de sécurité, soulignant ainsi la nécessité d'améliorer les mesures de cybersécurité pour prévenir le phishing, l'un des vecteurs les plus courants pour l'accès initial au réseau.

IV. Le Marché de la Cyber Assurance: Entre Croissance et Défis Incontournables

Le secteur du cyber assurance se trouve à un carrefour, confronté à des perspectives de croissance prometteuses mais également à des défis persistants. Malgré une meilleure compréhension des risques liés aux menaces cybernétiques et un regain d'intérêt des assureurs, l'instabilité inhérente à ces menaces demeure une menace constante.

Les avertissements émanant d'acteurs clés du secteur, comme Munich Re aux Rendez-Vous de Monte Carlo, soulignent l'impératif pour le marché du cyber assurance de mieux appréhender ces risques pour assurer son essor. Le défi majeur, identifié comme le «Défi N°1», réside dans l'accès aux capacités nécessaires. Les acteurs du secteur, qu'il s'agisse d'assureurs traditionnels ou d'insurtechs, doivent démontrer leur expertise, leur capacité d'analyse fine des risques, et leur aptitude à diversifier leurs approches pour réduire l'exposition. Cependant, équilibrer ces exigences reste délicat, avec de nombreux obstacles sur la voie du succès.

Les limites de cyber-assurance résident dans son aspect complexe et omniprésent. Il pose des défis quant à sa quantification, incitant de nombreuses organisations à transférer une partie du risque financier à une assurance. Cependant, les premières années d'assurabilité ont montré des résultats mitigés, le marché luttant pour se réguler face à la complexité du risque cyber.

L'incertitude entourant l'évaluation financière du risque cyber, en raison de sa nature volatile, rend cette évaluation difficile tant pour les entreprises que pour les assureurs. L'anticipation des coûts d'un sinistre demeure incertaine, incitant souvent les assureurs à surestimer les primes, rendant les contrats d'assurance cyber moins attractifs, surtout pour les TPE/PME et les ETI.

Malgré des signes de maturité, les défis subsistent, liés à l'incertitude, à l'assurabilité et à la complexité des risques cyber. Pour assurer la prospérité continue de ce marché, des solutions sont impératives pour rendre la cyber assurance plus accessible, transparente et adaptée. Il est capital de reconnaître que la cybersécurité demeure la première ligne de défense, la cyber assurance devant être considérée comme un complément essentiel face aux défis croissants du monde numérique.

Les perspectives d'Avenir de la Cyber Assurance

Le marché de l'assurance cyber se trouve à un point crucial, entre des perspectives de croissance encourageantes et des défis persistants. Malgré une meilleure sensibilisation aux risques cyber et un regain d'intérêt des assureurs, la volatilité inhérente à la menace persiste. Des avertissements récents, notamment de Munich Re, mettent en lumière la nécessité d'une meilleure compréhension des risques pour encourager l'engagement des réassureurs. L'accès aux capacités demeure un défi majeur, tandis que les limites des cyber-assurances se manifestent dans la complexité et l'évaluation incertaine des risques.

Les petites entreprises, confrontées à des conditions d'assurabilité strictes et à des primes élevées, renoncent de plus en plus à souscrire une assurance cyber. Les contrats présentent des clauses d'exclusion croissantes, ajoutant à la complexité et à l'incertitude juridique, tandis que des franchises élevées rendent l'assurance cyber moins attrayante. Malgré ces défis, les entreprises reconnaissent l'importance de l'assurance cyber, bien que des clauses d'exclusion croissantes suscitent des inquiétudes quant à l'efficacité future de cette couverture.

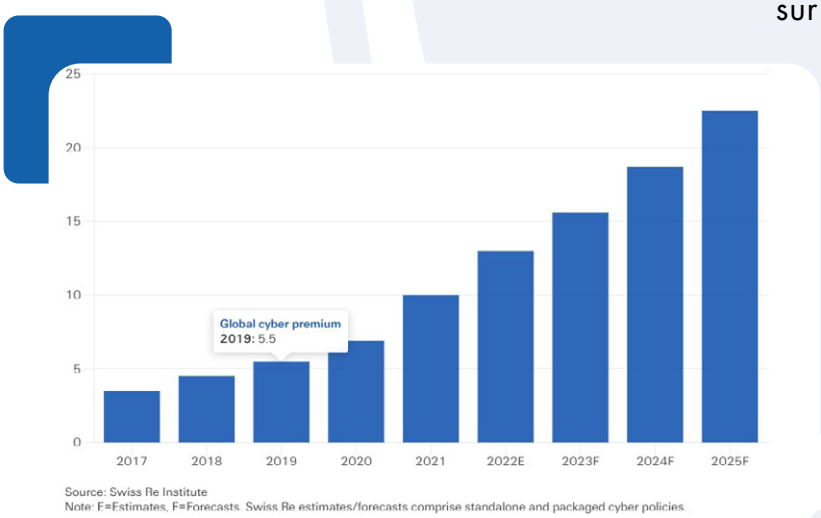
En 2023, le secteur fait face à une montée en intensité des défis, avec environ 67 % des entreprises constatant une augmentation significative des primes, variant de 50 à 100 % lors de la souscription ou du renouvellement. Cependant, 47 % des entreprises ont fait appel à leur cyber assurance à plusieurs reprises, soulignant la reconnaissance de son importance malgré les coûts et délais croissants. Les clauses d'exclusion, telles que l'absence de protocoles de sécurité, les erreurs humaines, les actes de guerre et le non-respect des procédures conformes, présentent un défi préoccupant pour l'efficacité future de la couverture cyber.

V. la croissance de la demande sur Marche mondiale : Une forte demande favorise une croissance rapide

Selon le Swiss Re Institute (SRI), le marché mondial de la cyber assurance a triplé en volume au cours des cinq dernières années, pour atteindre des primes directes brutes d'environ 13 milliards d'USD en 2022.

En l'espace de deux ans seulement, le marché a connu d'importantes augmentations de tarifs et une nouvelle tarification visant à rétablir la rentabilité. Ces mesures ont été prises en réaction à l'intensification de l'activité des ransomwares qui a entraîné une détérioration des ratios de sinistres au cours des années précédentes. En 2023, nous enregistrons une stabilisation des taux avec des hausses et des baisses plus sélectives pour des segments spécifiques du marché.

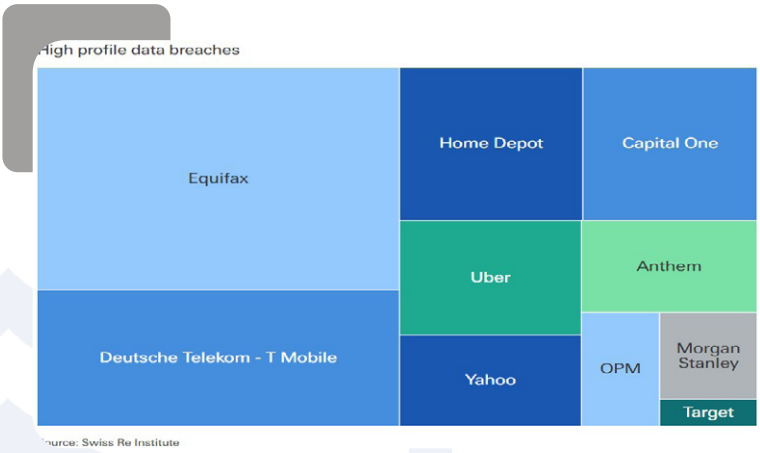
L'Institut Swiss Re s'attend à ce que les primes atteignent 23 milliards d'USD d'ici 2025. Cependant, le marché demeure petit au regard de l'évolution rapide des risques cybernétiques.



La cybercriminalité devrait coûter 8 000 milliards d'USD en 2023. Cyber Security Ventures, une société de recherche et d'édition spécialisée dans la cyberéconomie mondiale, prévoit que le coût des dommages causés par la cybercriminalité augmentera de 15 % par an à court terme, pour atteindre 10 500 milliards de dollars par an d'ici à 2025, contre 3 000 milliards de dollars en 2015.

Les coûts de la cybercriminalité comprennent non seulement les dommages, la destruction et le vol de données et de propriété intellectuelle, mais aussi la perte de productivité, les perturbations et l'atteinte à la protection des données personnelles, ainsi que les coûts des enquêtes médico-légales et de la restauration des actifs piratés.

Les pires violations de données touchent plus d'un milliard de personnes.



- **Analyse de l'évolution des différents types d'attaques**

Les incidents liés aux logiciels malveillants ont augmenté de 2022 pour la première fois depuis 2018, atteignant 5,5 milliards d'attaques, soit une augmentation de 2% d'une année sur l'autre, selon le rapport 2023 SonicWall Cyber Threat Report. Les malwares sont des logiciels malveillants qui infectent un ordinateur et qui sont spécifiquement conçus pour perturber, endommager ou obtenir un accès non autorisé à un système informatique.

Les occurrences de malwares IoT ont augmenté de 87 % en 2022 par rapport à l'année précédente, avec 112,3 millions d'occurrences de malwares IoT enregistrées.

Bien que les attaques aient diminué en 2022, le volume de ransomware est encore beaucoup plus proche des niveaux de montée en flèche que nous avons observés en 2021 que de ce que nous avons vu en 2018, 2019 et 2020. Si l'on exclut l'année 2021 en tant que valeur aberrante, les ransomwares sont toujours en hausse.

En 2022, les analystes des SonicWall Capture Labs ont enregistré 493,3 millions de tentatives de ransomware, soit une baisse de 21 % par rapport aux niveaux enregistrés l'année précédente. Les ransomwares sont des logiciels malveillants conçus pour bloquer l'accès à un système informatique jusqu'au paiement d'une rançon.

Une telle attaque prend la forme d'une intrusion dans un réseau (vol d'informations d'identification, installation de portes dérobées et de logiciels malveillants, déplacement latéral dans le réseau, exfiltration de données, demande de rançon). Les pirates informatiques passent souvent des mois à espionner un réseau compromis pour planifier une attaque et maximiser leurs profits.

Le premier semestre 2023 a vu une augmentation significative des attaques de ransomware, mais les données communiquées par un certain nombre d'assureurs au premier trimestre 2023 suggèrent que cela ne s'est pas encore accompagné d'une augmentation correspondante des demandes d'indemnisation, selon le courtier Howden. Il souligne l'efficacité des contrôles des risques pour rendre les entreprises plus résilientes et soutenir un marché de la cyber-assurance plus stable.

Attaque par déni de service distribué (DDoS) : Dans une attaque DDoS, les pirates tentent de compromettre un réseau cible en l'inondant de trafic provenant de sources multiples (y compris des appels Internet).

En 2022, le monde a connu une activité DDoS sans précédent en termes de volume, de complexité et de fréquence. Cette explosion des attaques DDoS est due à une augmentation substantielle des attaques des États-nations et à la prolifération continue des services DDoS à bas prix. Microsoft a atténué une moyenne de 1955 attaques par jour, soit une augmentation de 40 % par rapport à l'année précédente.

- **Les défis du marché cybernétique**

Le caractère connecté du risque cyber peut conduire à d'importantes pertes cumulées. Au rythme actuel de croissance du marché, il est attendu à atteindre les limites de ce que le marché de la réassurance peut financièrement supporter.

Pour continuer à soutenir la demande croissante d'assurance cybernétique, il faut créer de nouvelles capacités. L'accès à la capacité de risque des marchés de capitaux et/ou les programmes soutenus par les gouvernements pour les pires scénarios d'accumulation sont des options potentielles qui se trouvent dans les phases exploratoires initiales.

- **Le débat d'actualité : Quelle peut être la contribution du Cyber ILS au défi de la capacité**

Il est très important pour le secteur de répondre à la question de savoir comment nous pouvons appliquer au marché des cyber-risques un concept similaire à celui des Cat Bonds.

Le début de l'année 2023 a vu la première transaction commerciale qui pourrait être le signe d'un nouveau marché cyber ILS naissant et émergent. Beazley a obtenu une couverture de réassurance de 45 millions d'USD grâce à la première obligation catastrophe cyber dédiée et négociable du secteur.

L'un des principaux défis pour un tel marché est de définir précisément ce qui constitue un cyber-événement. Ce n'est qu'à cette condition qu'un indice approprié pourra être développé pour soutenir éventuellement des solutions paramétriques. En l'absence d'une telle définition, seuls les produits basés sur l'indemnisation ont des chances d'attirer les investisseurs.

Les cyber-risques, contrairement aux risques de catastrophes naturelles, ne sont pas limités à une région. En outre, le risque est de nature humaine, alors que les CAT NAT sont principalement dues à des forces physiques. Ces facteurs font qu'il est particulièrement difficile d'évaluer ou de modéliser les cyber-risques et de quantifier le risque de cyber-accumulation.

Il est donc nécessaire d'investir davantage dans la normalisation des données cybernétiques et dans le développement d'approches de modélisation robustes.

Pour rester au fait de l'évolution des cyber-risques, il est également très important que le secteur investisse dans le développement d'une cyber-expertise au sein de la profession, afin de combler la pénurie de cyber-talents.

VI. Les tendances Tarifaires

Alors que l'assurance cyber demeure le sous-secteur à la croissance la plus rapide du marché mondial de l'assurance, S&P souligne l'importance de la réassurance dans le développement d'un marché cyber durable et efficace.

Selon S&P, les assureurs primaires ont cédé environ 50% à 65% de leurs primes d'assurance cyber aux réassureurs en 2022, selon la région. Cela est significatif et met en évidence la forte dépendance à l'égard de la réassurance dans le secteur de l'assurance cyber.

S&P déclare que les réassureurs resteront un pilier important dans le développement d'un marché d'assurance cyber durable et efficace. Le marché de la réassurance et, éventuellement, le marché de la rétrocession seront donc extrêmement importants pour fournir des capitaux et des capacités afin de soutenir une croissance supplémentaire des primes brutes émises.

S&P indique que les primes d'assurance mondiales devraient augmenter d'environ 30 % par an pour atteindre environ 23 milliards de dollars d'ici 2025.

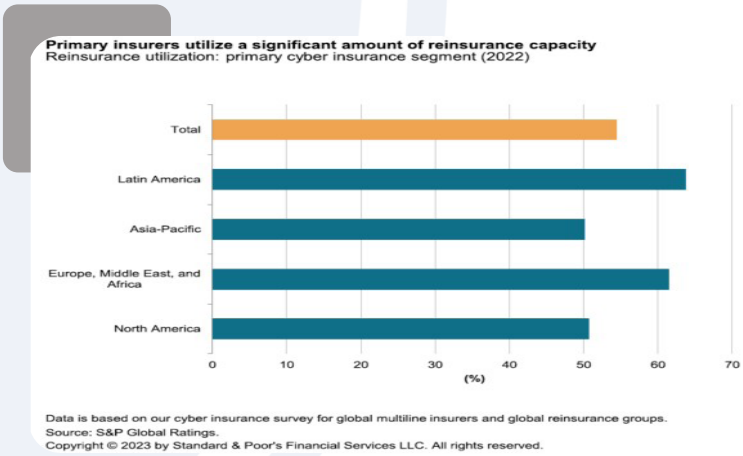
Pour atteindre cette croissance, S&P estime que le rôle des réassureurs est crucial, non seulement en raison de leur capacité, mais aussi de leur expertise en modélisation et en souscription, ce qui contribue également au développement du marché.

S&P explique que si l'assurance cyber doit répondre aux besoins des clients à l'avenir, il est plus important que jamais que l'industrie se concentre sur la différenciation des risques, une souscription solide et la fourniture de services d'assistance tels que des mesures de prévention, la gestion de crise et la récupération de données.

À mesure que les schémas de sinistres évoluent et que les menaces cyber continuent d'augmenter, associées à une vaste accumulation de risques, S&P souligne les opportunités que ces facteurs créent pour augmenter la capacité de réassurance. En fait, l'agence de notation note que le nombre de sociétés de réassurance offrant une couverture cyber est en augmentation en réponse aux dynamiques du marché.

De nombreux réassureurs approchent des limites de la quantité d'exposition cyber qu'ils peuvent et veulent gérer. Cependant, S&P n'attend pas à ce que le marché s'assouplisse comme cela a été le cas pour l'assurance cyber. Cela est évident grâce aux ajustements de taux plus élevés du segment de la réassurance jusqu'à présent en 2023. Les réassureurs doivent également retrouver une rentabilité en souscription dans leurs portefeuilles cyber.

Après une année 2022 difficile en raison de la faible rentabilité et même de pertes en souscription dans les portefeuilles cyber, S&P prévoit de voir davantage d'augmentations de tarifs pour les activités de réassurance cyber en 2023. Cependant, l'agence pense que les assureurs en cyber peuvent absorber les augmentations sans les transmettre aux assurés. Cela pourrait être essentiel dans le développement d'un marché d'assurance cyber durable



Même dans la récente enquête de Moody's, il a été révélé que les prix de la réassurance cyber commencent enfin à trouver une stabilité après des années d'augmentations significatives. Cette évolution survient alors que les assureurs se préparent à la possibilité de nouvelles hausses des coûts liés aux pertes cyber, incitant un nombre croissant d'entre eux à rechercher une protection de réassurance accrue. Ce changement de tendance est un indicateur solide de la croissance globale attendue dans le secteur de l'assurance cyber.

Selon l'enquête, 67 % des répondants prévoient que les prix de l'assurance cyber continueront d'augmenter en 2024, bien que à un rythme plus modéré par rapport aux années précédentes. Les 33 % restants prédisent que les prix resteront stables. À noter que des disparités régionales sont évidentes, avec une part significative

d'assureurs basés aux États-Unis prévoyant des augmentations de prix modérées, tandis que les assureurs des régions EMEA (Europe, Moyen-Orient et Afrique) et APAC (Asie-Pacifique) anticipent une croissance plus substantielle. Dans l'ensemble, environ un quart des répondants prévoient une augmentation des prix de la réassurance cyber allant de 2,5 % à 7,5 % l'année prochaine.

La modération des hausses de prix devrait résulter des récentes attaques de ransomwares et d'une réévaluation approfondie des risques cyber dans l'ensemble du secteur de l'assurance. De plus, les améliorations de performance observées en 2022 ont contribué à une augmentation de la capacité de réassurance. Cette augmentation de capacité est stimulée par des directives améliorées encourageant des pratiques de cybersécurité plus robustes et un meilleur partage d'informations au sein de l'industrie.

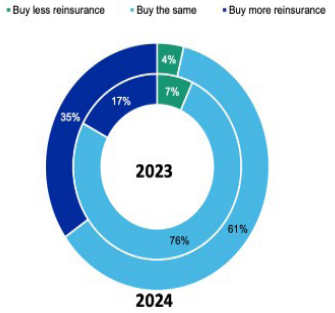
De plus, l'enquête révèle une augmentation significative de la demande de réassurance cyber. Contrairement à d'autres lignes d'assurance de biens et de responsabilité, 35 % des assureurs expriment leur intention d'acheter plus de protection cyber en 2024, marquant une augmentation substantielle par rapport aux 17 % signalés l'année précédente.

Cette hausse de la demande est en partie attribuée à la popularité croissante de la couverture d'assurance cyber autonome. Les experts estiment que la tendance à la hausse de la demande de réassurance cyber devrait se poursuivre à mesure que les prix se stabilisent. Les primes d'assurance cyber autonomes ont connu un remarquable taux de croissance de 30 % au cours des cinq dernières années. Munich Re prévoit que le volume total de l'assurance cyber atteindra un impressionnant 33 milliards de dollars d'ici 2027. La focalisation croissante des organismes gouvernementaux et réglementaires sur les risques cyber systémiques et l'impératif de partage d'informations devraient soutenir davantage la croissance de ce segment.

Exhibit 12

Cedants want to increase their reinsurance protection as demand grows

Question: Do you plan to buy more/the same/less reinsurance for cyber risks?



Proportions are based on 23 insures for this year's report and 29 for the previous period because not all survey respondents underwrite cyber risks.
Source: Moody's Reinsurance Buyer Survey 2024

Les clauses liées à la cyber-guerre :

La LMA a récemment effectué des mises à jour importantes sur ses clauses liées à la cyber-guerre, se concentrant particulièrement sur l'implication d'États et d'acteurs souverains dans les cyberattaques et autres opérations. Les modifications apportées concernent l'utilisation du terme «État souverain» et son application dans certaines exclusions.

La résilience cybernétique devient la solution optimale qui ne peut être réalisée qu'avec l'organisation de processus de souscription, l'amélioration des termes de la police et la différenciation des prix pour divers risques cybernétiques.

La définition de la couverture d'assurance cyber est primordiale, englobant des aspects tels que les coûts de violation de données, les violations de sécurité réseau, l'interruption d'activité, les responsabilités médiatiques, les frais juridiques et les dépenses liées à la confidentialité.

VII. Les marchés de réassurance et les nouvelles orientations des assureurs / réassureurs : Risk bonds et modélisation

Selon les analystes de Moody's, le soutien de la réassurance joue un rôle important sur le marché de l'assurance cyber, car les assureurs continuent de réassurer le risque cyber par le biais d'un traité en quote-part pour obtenir une expertise et une protection du capital. Les analystes notent que les prix de la réassurance pour la couverture cyber ont continué d'augmenter avec des points d'attache plus élevés et certaines réductions de limite de traité.

Ils soulignent que les réassureurs maintiennent des plafonds agrégés sur les contrats de réassurance en quote-part pour gérer leur risque d'accumulation. En raison des changements mis en œuvre par les assureurs primaires, les réassureurs ont lentement augmenté leur tolérance au risque cyber, et une certaine nouvelle capacité est arrivée sur le marché. Cependant, les réassureurs restent prudents en raison du potentiel de risque systémique, et une cyberattaque généralisée à l'échelle mondiale pourrait entraîner des paiements de sinistres potentiels de plusieurs milliards de dollars.

Moody's indique que le marché du capital alternatif a considérablement augmenté sa part sur le marché de la réassurance des catastrophes naturelles, mais en est encore aux tout premiers stades du transfert du risque cyber. Quelques transactions ont été conclues, comme les deux opérations distinctes annoncées par l'assureur londonien Lloyd's, Beazley, plus tôt cette année. En janvier 2023, la société a émis la première obligation de catastrophe couvrant ses polices d'assurance cyber. Cette obligation de catastrophe cyber de 45 millions de dollars peut être négociée en vertu de la revente de la règle 144A et fournit à Beazley une couverture d'indemnité contre tous les périls en cas d'événement catastrophique de plus de 300 millions de dollars. L'obligation était soutenue par des investisseurs institutionnels tiers, dont Fermat Capital Management, LLC, qui prennent en charge les réclamations potentielles d'assurance cyber au-dessus d'un certain niveau de pertes, moyennant un rendement généralement non corrélé aux marchés financiers.

En janvier également, Hannover Re a développé une couverture de rétrocession pour permettre aux marchés financiers de prendre en charge les risques cyber dans le portefeuille mondial de Hannover Re par le biais d'un traité en quote-part. Stone Ridge Asset Management, un gestionnaire d'actifs alternatif, a fourni 100 millions de dollars de capital d'investisseurs pour soutenir la transaction. Moody's note que Hannover Re a une longue histoire d'utilisation de titres adossés à des assurances pour transférer des risques pour ses clients et couvrir ses risques par le biais des marchés financiers.

Si les marchés financiers se montrent disposés à soutenir l'assurance cyber par le biais d'investissements dans des titres adossés à des assurances, cela pourrait créer une capacité supplémentaire sur le marché pour soutenir la croissance tout en permettant aux (ré) assureurs de gérer le risque résiduel, explique l'agence de notation. Cependant, l'incertitude autour de la modélisation du risque cyber et la standardisation limitée des libellés de police entre les transporteurs pourraient entraver le développement des titres adossés à l'assurance cyber.

VIII. L'industrie de l'assurance : un grand défi à relever

Dans le cas des cyberattaques,la crainte a conduit de nombreuses entreprises, organisations et gouvernements à renforcer leurs défenses.

La forte augmentation des cyberattaques ces dernières années a fait prendre conscience à la plupart des organisations et des entreprises qu'elles pouvaient devenir une cible aux conséquences graves. Cette prise de conscience, associée au fait que le coût d'une attaque pourrait être bien plus élevé que tout investissement dans des efforts d'atténuation préventifs et dans le cyber hygiène, les a incitées à agir.

Le secteur de l'assurance dispose d'une grande marge de manœuvre pour surmonter ses limites.

Dans cet environnement en pleine évolution, chaque acteur doit envisager de renforcer son rôle. Le secteur de l'assurance, en particulier, dispose d'un levier important pour accroître la cyber-résilience, soulignent les chercheurs du SRI. L'assurance joue un rôle clé, non seulement en transférant les risques, mais aussi en encourageant l'atténuation des cyber risques

pour obtenir une couverture cybernétique, les entreprises doivent prouver qu'elles ont mis en place un programme de cyber risques de qualité qui permet de surveiller les cyberattaques et d'y répondre.

Mais il ne faut pas ignorer le fait que les efforts entrepris contre les menaces cyber ne sont jamais suffisants. À mesure que la numérisation prolifère et que la technologie progresse, l'exposition aux menaces cyber s'accroît.

Un nouveau document du Swiss Re Institute (SRI) «Cyber : Extending insurability for a rapidly evolving risk», met l'accent sur le cœur du problème : Le rythme du changement technologique, la prise de conscience croissante du risque cybernétique et l'adoption de pratiques d'hygiène cybernétique pour assurer la sécurité des données et des réseaux ne sont pas synchronisés. En fait, les protocoles de sécurité et de systèmes informatiques hérités sont dépassés, et les cadres réglementaires suivent lentement les tendances technologiques. Ce retard en matière de cyberdéfense ouvre la porte aux acteurs malveillants qui cherchent à exploiter les vulnérabilités numériques à des fins financières, de données personnelles ou géopolitiques.

- **Le secteur de l'assurance doit montrer sa puissance dès maintenant**

Le secteur de l'assurance devrait démontrer sa force en ce moment, alors que l'assurabilité limitée restreint la capacité, malgré une demande croissante, et remet en question la durabilité du marché de l'assurance Cyber. Les chercheurs du SRI mettent en évidence trois domaines d'amélioration dans lesquels le secteur de l'assurance peut contribuer à gérer plus efficacement les cyber-risques et à accroître l'assurabilité.

Pour remédier à ces limitations, les chercheurs du SRI recommandent aux parties prenantes d'améliorer la résilience aux risques Cyber :

Standardiser les données et optimiser la modélisation, combler le manque de cyber compétences en investissant dans l'éducation, et investir dans de nouvelles sources de capitaux et dans la collaboration entre les secteurs public et privé. Cela permettra d'atténuer l'exposition globale, d'améliorer la compréhension du risque et de rendre la société plus résistante aux attaques ayant des conséquences dévastatrices et potentiellement systémiques. En même temps, elle souligne que la nature humaine et en réseau de la cybercriminalité signifie que le risque évoluera constamment et nécessitera une réponse coordonnée. Le renforcement de la résilience exigera une collaboration entre les entreprises, les assureurs et les gouvernements.

- **Trois axes de travail pour les réassureurs :**

Standardisation des clauses d'assurance : Les ambiguïtés dans les polices d'assurance cybernétique peuvent entraîner des litiges. Une normalisation des conditions générales est nécessaire pour favoriser la croissance en clarifiant les solutions.

Nouveaux modèles de coopération : Les titres liés à l'assurance cybernétique émergent comme solution pour les risques difficiles à évaluer. Les capitaux alternatifs pourraient compléter les fonds traditionnels, suscitant un intérêt croissant.

Pénurie de talents en cybersécurité : Les entreprises et réassureurs doivent constamment développer leur expertise. Des initiatives visent à remédier à la pénurie de compétences.

***Approche face à la menace : Plutôt que la appréhension, une réponse adaptée est nécessaire. Chaque secteur doit contribuer, en mettant l'accent sur la collecte des données, la modélisation, et l'investissement dans les talents.**

***Pour gérer les risques d'agrégation, un modèle de partenariat public-privé PPP pourrait pallier le manque de protection.**

***Les Entreprises du Monde Entier Confrontées à une Hausse des Violations de Données Coûteuses**

Selon la récente enquête mondiale de PwC intitulée «2024 Global Digital Trust Insights», le nombre d'entreprises subissant des violations de données coûtant plus d'un million de dollars a considérablement augmenté, passant de 27% à 36% en un an. Les organisations du secteur de la santé ont été particulièrement touchées, avec 47% signalant de telles violations coûteuses. Le coût moyen d'une cyberattaque dommageable atteignait 4,4 millions de dollars, atteignant même 5,3 millions de dollars dans le secteur de la santé. L'enquête met également en évidence la perception mitigée de l'IA générative, avec

des inquiétudes quant aux cyberattaques, mais aussi une reconnaissance de son potentiel pour développer de nouvelles lignes commerciales.

- **Les Risques Numériques et Technologiques Classés Comme Priorité Absolue pour les Dirigeants d'Entreprise en 2024**

Malgré des défis mondiaux tels que le changement climatique et la pandémie de COVID-19, les dirigeants d'entreprise ont classé les risques numériques et technologiques comme leur priorité absolue pour l'année à venir, selon l'enquête. Les menaces liées au cloud, les attaques sur les appareils connectés et les opérations de piratage et de fuite ont été identifiées comme les principales menaces cyber. Les organisations se concentrent sur des stratégies d'acquisition et de rétention des talents pour renforcer leur cybersécurité, soulignant l'importance croissante de mesures proactives face aux défis du paysage cyber actuel.

- **Les Cyberattaques contre les Entreprises en Hausse pour la Quatrième Année Consécutive :**

Une étude de Hiscox, basée sur le «Hiscox Cyber Readiness Report» et impliquant plus de 5 000 organisations mondiales, révèle une augmentation alarmante des cyberattaques pour la quatrième année consécutive. Plus de 53% des entreprises interrogées ont été touchées au cours de la dernière année, avec une augmentation significative pour les petites entreprises. Le rapport souligne la persistance des paiements de rançon et le compromis d'emails commerciaux comme principales menaces, incitant une augmentation significative des investissements en cybersécurité, en particulier chez les petites entreprises.

- **Les titres assurantiels liés à la cybernétique (ILS)**

Dans une collaboration avec CyberCube et Envelop Risk, Lockton Re met en avant le potentiel des titres assurantiels liés à la cybernétique (ILS) dans un rapport conjoint. Malgré les hésitations initiales des investisseurs, les conditions actuelles du marché créent un environnement propice à l'exploitation des ILS liés à la cybernétique, soutenu par une meilleure compréhension des périls, des données améliorées et un consensus croissant sur l'utilisation des modèles. Les modèles actuels fournissent une analyse statistique basée sur des techniques actuarielles, répondant efficacement aux expositions assurées. Le rapport souligne les efforts éducatifs pour sensibiliser les investisseurs non spécialistes aux risques cyber, et conclut en affirmant que la demande de réassurance et d'assurance cyber continuera de croître, renforcée par le succès potentiel des transactions ILS liées à la cybernétique.

- **Modélisation du cyber Risks**

Plusieurs acteurs sur le marché comme DeNexus, ont souligné l'importance de la modélisation cybernétique de deuxième génération pour la visibilité des risques dans le paysage en constante évolution des risques cybernétiques. DeNexus vise à renforcer la compréhension des risques cybernétiques au-delà des données historiques en offrant une vue précise des expositions et une surveillance en temps réel, potentiellement stimulant l'engagement du marché des capitaux. Par ailleurs, le groupe Russell affirme qu'il existe suffisamment de données pour assurer les risques cybernétiques, utilisant l'intelligence artificielle et l'analyse prédictive pour construire des modèles basés sur des scénarios réalistes. Moody's RMS a lancé son Cyber Industry Steering Group avec la participation de Munich Re, Gallagher Re et Bitsight, visant à résoudre les contraintes actuelles du marché de l'assurance cyber, anticipant une augmentation des investissements pour favoriser la croissance du marché.

IX. Cyber risks en Afrique

L'Afrique se trouve actuellement en position de vulnérabilité face aux cyberattaques, principalement en raison du manque d'attention accordé à la cybersécurité par la plupart des entreprises du continent. Les faiblesses en termes d'infrastructures, de compétences et de sensibilisation parmi les entreprises et les utilisateurs contribuent à cette vulnérabilité. Bien que des mesures juridiques aient été adoptées par les États africains pour réguler le cyberespace, les initiatives continentales telles que la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel ont suscité un faible enthousiasme.

Le besoin pressant pour les entreprises

d'améliorer leurs stratégies de cybersécurité est souligné afin de prévenir un potentiel chaos numérique en 2023. Aucune structure ou État n'est à l'abri des cyberattaques, mettant en évidence l'importance de s'entourer de professionnels compétents pour contrer ces menaces.

L'année 2022 a été marquée par une série d'attaques cybernétiques variées en Afrique, dépassant la moyenne mondiale en termes de nombre, avec environ 1 848 attaques par semaine. Les menaces cyber pour l'année 2023 semblent préoccupantes, illustrées par des incidents tels que le vol de données personnelles de l'armée ivoirienne et les fuites de données de la banque BOA au Mali.

Face à ces défis, les gouvernements et les entreprises africaines sont appelés à investir massivement dans la sécurité numérique pour protéger les données personnelles des individus, devenues une cible de choix pour les cyberattaques. Malgré une population africaine d'environ 500 millions d'utilisateurs d'Internet, représentant seulement 38 % de la population, la région est confrontée à une vulnérabilité accrue aux cyberattaques, exploitant les faiblesses des infrastructures, le manque de compétences et l'absence de sensibilisation. Renforcer la stratégie de cybersécurité des entreprises est crucial pour éviter un chaos numérique en 2023. Bien que de nombreux pays africains aient adopté des mesures juridiques pour réguler le cyberespace, les initiatives continentales de lutte contre la cybercriminalité ont rencontré peu d'engouement. Il est impératif que les États et les entreprises se protègent en s'entourant de professionnels compétents pour riposter aux attaques et prévenir les menaces.

- **Lancement du Cercle Africain de Cybersécurité : Renforcement de la Sécurité Numérique en Afrique**

Agissant en tant que «DO and THINK TANK», le CAC se distingue par son engagement actif dans des actions concrètes visant à contrer les menaces croissantes dans le paysage numérique africain.

Le CAC favorise la collaboration public-privé, réunissant une diversité d'acteurs, tels que des experts civils et militaires, ainsi que des juristes, pour adopter une approche multidisciplinaire.

Les objectifs du CAC à court et long terme incluent l'évaluation des besoins en cybersécurité, le renforcement des membres, la création de structures spécialisées, et la collaboration avec le Patronat Africain.

En mettant l'accent sur la coopération régionale, le CAC prévoit des initiatives de sensibilisation, La vision ambitieuse du CAC vise à établir des points focaux dans plusieurs pays africains pour faciliter la communication et la coordination. En résumé, le CAC joue un rôle clé dans la promotion d'un cybersécurité dynamique et efficace en Afrique, stimulant l'innovation et l'éducation pour renforcer la protection numérique sur le continent.

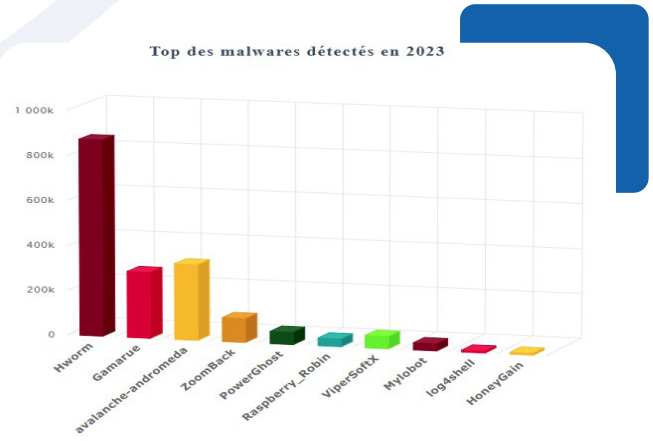
X. Indice Développement Cybersécurité de la Tunisie

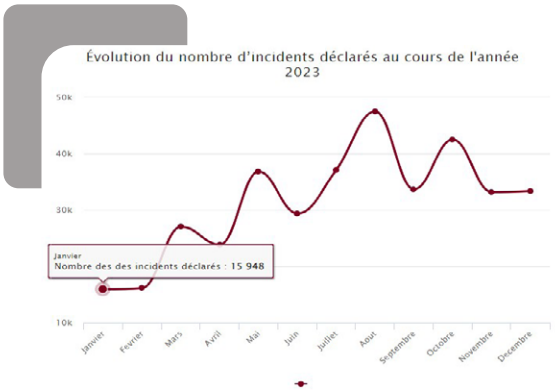
Classée 6ème dans la Région Arabe et 45 au GCI 2020, la Tunisie présente un bilan très élogieux et flatteur en matière de cybersécurité.

Le pays connaît depuis plus de 3 ans un nombre important d'attaques Cyber. Le nombre d'attaques cyber montre une croissance significative entre 2019 et 2023.

Selon les statistiques de l'Agence Nationale de Sécurité informatique, le nombre des attaques qui ont ciblé les institutions à intérêt vital montrent l'accroissement significative de ce risque en Tunisie.

Au cours du 1ère semestre 2023, la Tunisie a connu un nombre important d'événements cyber avec près de 149 134 incidents déclarés, soit en évolution de plus de 65% par rapport à la même période de l'année 2022.





D'après la dernière étude de Kaspersky, le leader mondial de la cybersécurité, portant sur la maturité des petites et moyennes entreprises (PME) tunisiennes en matière de cybersécurité, 80% d'entre elles estiment être immunisées contre le risque cyber. Cependant, l'étude révèle que la plupart des entreprises ne sont pas suffisamment formées sur les risques cyber et leurs conséquences, soulignant la nécessité d'une vigilance renforcée en matière de cybersécurité. Bien que la digitalisation des PME en Tunisie soit en croissance, l'étude indique que seulement 20% des PME interrogées estiment être exposées au risque cyber, malgré une augmentation des attaques détectées. Les experts soulignent le besoin d'une prise de conscience accrue et d'investissements dans des solutions de cybersécurité robustes pour protéger les PME contre les cybers menaces.

Alors que les nouvelles technologies offrent un environnement numérique interconnecté avec flexibilité, croissance rapide et bien-être des citoyens, ces avantages ne sont pas sans risques ; risques qui se cachent dans le cyberespace, en plus des menaces à l'intérieur des pays.

À travers sa stratégie nationale de cybersécurité 2020-2025, l'État tunisien vise à :

- Prévenir les cybers menaces.
- Résister aux cybers menace en s'appuyant sur ses capacités nationales.
- Diriger et gérer son cyberespace national.
- Soutenir la confiance numérique, en renforçant la coopération internationale et en atteignant le leadership dans le domaine numérique.

Quant au secteur des assurance, une nette évolution a été enregistrée ces dernières années que ce soit au niveau des capitaux assurés ou les primes nettes qui passent respectivement de 7 180 000 TND en 2019 à 47 230 461 TND en 2022 et de 45 650 TND en 2019 à 460 573 TND en Mai 2022.

Pour répondre aux besoins accrus du marché, plusieurs compagnies d'assurances commencent à commercialiser la couverture assurance Cyber dont nous pouvons citer STAR, GAT, CARTE.

Conclusion

Le marché du cyber assurance est à un tournant critique, montrant des signes positifs de croissance, mais confronté à des défis persistants liés à l'incertitude, à l'assurabilité et à la complexité des risques cyber. Pour favoriser la prospérité continue de ce marché et répondre aux besoins diversifiés des entreprises, il est impératif de trouver des solutions pour rendre la cyber assurance plus accessible, transparente et adaptable.

La cybersécurité demeure la première ligne de défense contre les menaces numériques, et la cyber assurance doit être considérée comme un complément essentiel face aux défis croissants du monde numérique. Dans un contexte d'interconnexion des systèmes d'information, où la sécurité informatique est intégrée au projet global de sécurité, il est crucial d'adopter une position offensive en préparant les entreprises à faire face aux cyberattaques.

Les risques et les modes de diffusion des cybers risques évoluent constamment, impactant particulièrement les PME et ETI. Les chiffres montrent la croissance incontestable des cyberattaques, rendant la cybersécurité plus cruciale que jamais. Ainsi, souscrire une assurance cyber devient une nécessité immédiate pour les chefs d'entreprise soucieux de protéger leurs biens.

Combler l'écart de protection en matière d'assurance cyber nécessite une approche multifacette, incluant des améliorations de la qualité des données, des mises à jour du langage des polices et des collaborations novatrices entre acteurs publics et privés. Ces mesures visent à renforcer la résilience face aux risques cyber et à promouvoir un marché de l'assurance cyber plus robuste.

Malgré l'augmentation rapide des attaques, la plupart des entités ne sont pas suffisamment assurées, les primes d'assurance ne couvrent qu'une fraction des pertes totales. Selon les estimations, il existe un écart de protection d'environ 90%. Comprendre et combler cette lacune nécessite une collaboration étroite entre les entreprises, l'industrie de l'assurance et les instances gouvernementales.

Ni l'assurance ni la réassurance ne peuvent absorber seules tous les risques, notamment ceux liés à des événements catastrophiques comme la cyber-guerre. Il est donc essentiel de renforcer la collaboration, en particulier pour faire face à des risques non modélisables, tels que la cyber-guerre, et pour combler ces lacunes potentielles.

Une collaboration étroite entre les secteurs public et privé est devenue indispensable pour relever tous ces défis à l'échelle mondiale.

Les Risques Politiques

RISQUES POLITIQUES

Les premières années de cette décennie ont été marquées par une série d'événements perturbateurs majeurs. La pandémie de COVID-19 a été un point de départ, suivi de près par le déclenchement de la guerre en Ukraine, ce qui a exacerbé les crises alimentaires et énergétiques. Le rapport sur les risques mondiaux 2023 souligne clairement les interconnexions entre les conflits géoéconomiques, la chaîne d'approvisionnement en énergie et en aliments, ainsi que les coûts de la vie en constante augmentation et l'endettement accru.

Ces défis exigent une réflexion et une action globales pour atténuer leurs effets. Dans ce contexte d'instabilité, le risque politique demeure toujours parmi les Top risques émergents de l'année 2023.

I. Les risques politiques

Le risque politique correspond à «l'ensemble des évènements ou décisions d'ordre politique ou administratif, nationales ou internationales pouvant entraîner des pertes économiques, commerciales ou financières pour l'entreprise, importatrice ou exportatrice, ou investissant à l'étranger».

Les risques politiques sont par nature difficiles à prévoir et les événements passés ne sont pas un indicateur fiable de ce qui se passera à l'avenir.

Le risque politique peut parfois être confondu avec le risque économique. Le risque économique correspond à la possibilité que des conditions macroéconomiques comme les taux de change ou l'inflation, et non des événements politiques, puissent affecter un investissement étranger.

Parmi les risques politiques majeurs susceptibles d'être couverts par une assurance :

1. La violence politique, qui comprend généralement les guerres civiles ou étrangères déclarées ou non, les coups d'État, les insurrections, les révolutions, le sabotage, les grèves et les émeutes, le terrorisme et les guerres qui causent des dommages matériels ou l'abandon d'actifs ou d'opérations, et la perte de revenus commerciaux qui en découle.
2. L'expropriation par le gouvernement d'actifs ou d'opérations, y compris empêcher la reprise de possession d'actifs par un créancier.
3. Les restrictions sur la conversion de fonds locaux en devises fortes, ou le transfert de fonds à l'étranger, dans le cadre du transfert de dividendes, du service de dette ou d'autres flux de trésorerie générés dans le pays vers un assuré.
4. L'inexécution d'une sentence arbitrale liée à une rupture de contrat par une entité gouvernementale.
5. Les risques de crédit els que le non-paiement par les entités souveraines.

II. L'assurance des Risques politiques

1. Evolution de l'assurance des risques politiques

L'assurance des risques politiques est une forme de couverture d'assurance conçue pour protéger les entreprises, les investisseurs et les prêteurs contre les pertes financières découlant de situations politiques imprévisibles.

La couverture peut varier en fonction des besoins spécifiques de l'assuré, mais elle peut inclure des indemnités en cas d'expropriation, de nationalisation, de troubles civils, de non-transfert de devises, de guerre, et d'autres risques politiques spécifiques.

Les souscripteurs de contrat d'assurance contre le risque politique sont généralement des multinationales, des entreprises d'import-export, des porteurs de projets, des institutions financières, des marchés de capitaux (les plus grands utilisateurs de ces contrats), des investisseurs étrangers et des entrepreneurs du secteur de la construction et de l'ingénierie.

Avant les attentats du 11 septembre 2001, les risques liés aux attentats, au terrorisme et au sabotage (A.T.S.) étaient généralement pris en charge par les assureurs et les réassureurs, mais il y avait des différences dans la manière dont ces risques étaient évalués, tarifés et couverts. En règle générale, de nombreux contrats d'assurance incluaient une couverture contre les actes de terrorisme, mais la définition précise de ces actes et les modalités de couverture pouvaient varier.

Après les événements de 2001, les compagnies d'assurance et de réassurance ont ajusté leurs approches pour mieux prendre en compte les risques politiques et les menaces terroristes. Cette adaptation a impliqué des modifications dans les polices d'assurance, notamment la limitation des risques liés au terrorisme, aux émeutes et aux mouvements populaires à un pourcentage déterminé des sommes assurées. Les traités proportionnels ont instauré des limites spécifiques par événement et par année d'assurance.

Parallèlement, les risques de terrorisme et de guerre sont de plus en plus transférés à des assureurs ou réassureurs spécialisés, suivant une tendance similaire à celle observée pour les risques liés à l'aviation, qui sont fractionnés entre risques standards et risques de guerre.

Une évolution significative s'est également produite sur le marché facultatif de la réassurance, où plus de 2,5 milliards de dollars de capacité étaient disponibles en 2013 pour couvrir les risques de terrorisme et de sabotage, selon les données de Guy Carpenter.

En parallèle, le contexte du printemps arabe a engendré une distinction entre les mouvements avec des revendications politiques et ceux sans revendications. Les premiers ont souvent été exclus des polices d'assurance classiques, tandis que les seconds ont été maintenus dans les couvertures d'assurance.

En effet l'émergence du printemps arabe a considérablement modifié les habitudes de commercialisation des risques politiques par les assureurs. Les grèves, émeutes et mouvements populaires étaient fréquemment associés sans surprime aux garanties incendie de base. Après la survenance des tumultes dans les sociétés arabes, les réassureurs ont systématiquement exigé une prime additionnelle pour la couverture des risques politiques dans les polices dommages IARD sans réelle modélisation. Le manque de données sur ce sujet ne permettant pas une tarification précise.

Enfin La guerre russo-ukrainienne qui s'est déclenchée au début de l'année 2022 a impacté considérablement le secteur d'assurance politiques. En effet, es polices d'assurances « Risques de guerre » qui ont été renouvelées après le déclenchement de la guerre, ont connu une hausse des primes qui avoisine les 150% et une baisse de l'agrégat général lié à la confiscation. On prévoit aussi pour les années à venir une hausse des primes pour les autres couvertures du fait du ralentissement du transport aérien, la perte de certains marchés et la diminution du nombre de passagers transportés.

Ces ajustements témoignent d'une adaptation stratégique de l'industrie de l'assurance pour mieux appréhender et gérer les risques politiques et les menaces, reflétant ainsi une volonté de personnaliser les approches en fonction de la nature spécifique de chaque risque.

2. L'assurance maritime et risques politiques

Avant 1967, les risques de guerre étaient inclus dans les polices d'assurance standard en tant que risques ordinaires. Cependant, au fil du temps, ils ont été progressivement retirés de ces polices pour être couverts par des polices spécifiques en raison de leur caractère exceptionnel. De nos jours, les polices d'assurance de base excluent généralement la couverture des risques politiques en raison de leur potentiel de causer d'énormes pertes, que ce soit aux marchandises transportées, dont la valeur ne cesse d'augmenter, ou au corps du navire lui-même.

Les polices de transport actuelles suivent souvent les clauses du marché de Londres, intégrant les conditions du Joint Excess Loss Committee. Cependant, il est courant d'ajouter des conventions spéciales et des clauses additionnelles pour prendre en compte des risques politiques spécifiques. Ces dispositions incluent fréquemment :

- Des conventions spéciales pour l'assurance des marchandises transportées et/ou du corps du navire contre la plupart des risques

politiques, assorties de garanties étendues. Ces conventions offrent des couvertures complémentaires aux conventions spéciales pour l'assurance des marchandises transportées et/ou du corps du navire.

- Des garanties Waterborne Agreement, qui sont des conventions spéciales pour l'assurance des marchandises transportées et/ou du corps du navire par voie maritime.

En incorporant ces conventions et garanties spéciales, les polices de transport maritime visent à fournir une protection étendue contre les risques politiques, reflétant ainsi la complexité et la diversité des défis liés à ces événements exceptionnels. Ces dispositions permettent aux assureurs de répondre de manière plus spécifique aux besoins des assurés et de gérer de manière proactive les conséquences financières potentiellement massives associées aux risques politiques dans le secteur maritime.

3. L'assurance-crédit et risques politiques

L'assurance-crédit et risques politiques est un outil financier qui permet de sécuriser des échanges commerciaux entre des entreprises, puis d'accélérer leur croissance. Elle est destinée spécifiquement aux entreprises qui ont des activités B2B, donc entre entreprises, et non entre entreprises et consommateurs.

L'assurance-crédit est une protection essentielle pour les entreprises, couvrant généralement deux catégories de risques distincts : le risque commercial et le risque politique.

1. Risque Commercial :

- Défaillance Financière : Cela concerne la probabilité que les clients ne puissent pas honorer leurs factures en raison de difficultés financières, telles que l'insolvabilité déclarée ou une défaillance prolongée.

2. Risque Politique :

- Événements Indépendants de la Volonté : Ce type de risque englobe le non-paiement résultant d'événements hors du contrôle de l'assuré ou de l'acheteur. Cela peut inclure des événements politiques tels que des guerres ou des révolutions, des catastrophes naturelles comme les tremblements de terre ou les ouragans, ainsi que des difficultés économiques, telles qu'une pénurie de devises entraînant l'incapacité de transférer des sommes dues d'un pays à un autre.

L'assurance-crédit à l'exportation offre une protection spécifique aux exportateurs, les libérant du danger potentiel de non-paiement par des acheteurs situés à l'étranger. Cette couverture permet aux assurés d'accorder un crédit en toute confiance à leurs clients étrangers, conférant ainsi un avantage concurrentiel significatif.

Cette forme d'assurance peut englober à la fois les risques commerciaux et politiques. La protection contre les risques politiques couvre un large éventail de scénarios, dont certains sont énumérés ci-dessous :

- Troubles Civils : Englobant les émeutes, les pillages, ou le blocus de ports perturbant les flux d'importation/exportation.
- Changements de Monnaie : Incluant l'incapacité de convertir une monnaie ou des fluctuations extrêmes de sa valeur.
- Douanes et Tarifs Douaniers : Les modifications inattendues dans les règles d'importation et d'exportation.
- Expropriation ou Confiscation : La prise de biens, d'argent, ou d'entreprises par un gouvernement.
- Révolution ou Coup d'État : Des changements de direction forcés, qu'ils soient violents ou pacifiques.
- Terrorisme ou Guerre : Rend le commerce avec un pays dangereux ou non viable.
- Restriction à l'Exportation/Importation: Des décisions ou mesures générales restreignant le commerce en raison d'embargos ou d'autres sanctions.
- Rupture de Contrat : L'annulation de contrats légalement conclus en raison de décisions gouvernementales qui empêchent le paiement ou l'exécution du contrat.

En résumé, l'assurance-crédit à l'exportation offre une couverture complète contre une gamme étendue de risques commerciaux et politiques, offrant ainsi une sécurité financière précieuse aux entreprises opérant sur le marché international.

III. Le Contexte International Actuel

Le monde traverse une période internationale complexe et tendue depuis l'agression russe contre l'Ukraine en février 2022. Depuis lors, les répercussions de cet événement se font ressentir sur plusieurs fronts, allant de l'économie à la politique, en passant par les relations internationales. La région de l'Europe de l'Est a été durement touchée, et les tensions entre la Chine et les États-Unis ont également augmenté. Parallèlement, les coûts élevés de l'énergie et les inquiétudes liées à la sécurité alimentaire, exacerbées par la guerre en Ukraine, ont créé un contexte global préoccupant.

Le Global Risks Report 2023, publié par le Forum économique mondial en partenariat avec Marsh McLennan, identifie quatre facteurs de risques croissants en 2023, représentant des menaces pour le commerce mondial, la sécurité et les investissements.

Ces facteurs comprennent une instabilité politique persistante, un repli économique, une compétition accrue pour les ressources stratégiques et une diversification de la chaîne d'approvisionnement.

L'instabilité politique constante représente un défi majeur pour de nombreux pays, influençant directement leur capacité à attirer et à utiliser efficacement les investissements directs étrangers. La stabilité politique est souvent un critère déterminant pour les investisseurs internationaux, qui cherchent un environnement prévisible et sûr pour leurs engagements financiers.

Par ailleurs, certaines économies émergentes pourraient se retrouver confrontées à des difficultés supplémentaires. L'augmentation de l'inflation et des coûts d'emprunt élevés pourrait agir comme un catalyseur, intensifiant l'instabilité politique et suscitant des troubles sociaux.

Ces défis économiques peuvent entraîner des mécontentements populaires, des manifestations et des tensions sociales, mettant en péril la stabilité politique déjà fragile dans certaines régions.

1. Indice mondial de la paix 2023

La 17éme édition du Global Peace Index (GPI), qui mesure la pacification dans le monde, indique que la paix mondiale continue de se détériorer pour la neuvième année consécutive. Parmi les 84 pays qui ont connu une amélioration, 79 ont vu leur situation se détériorer. Cela suggère que les détériorations sont plus nombreuses que les améliorations, en raison notamment des troubles civils et de l'instabilité politique persistants après la pandémie de COVID-19, ainsi que de l'accentuation des conflits régionaux et mondiaux. Ce rapport a mis l'accent sur les ponts suivants :

- Le nombre de décès liés aux conflits mondiaux a augmenté de 96%, atteignant 238 000 personnes.
- Soixante-dix-neuf pays ont connu une augmentation des niveaux de conflit, notamment l'Éthiopie, le Myanmar, l'Ukraine, Israël et l'Afrique du Sud.
- L'impact économique mondial de la violence a augmenté de 17% ou 1 billion de dollars, atteignant 17,5 billions de dollars en 2022, soit l'équivalent de 13% du PIB mondial.
- Malgré le conflit en Ukraine, 92 pays ont augmenté leurs dépenses militaires et 110 ont réduit leurs effectifs militaires.
- L'Ukraine a enregistré la plus grande détérioration, chutant de 14 places pour atteindre la 157ème position.
- L'impact économique de la violence a augmenté de 479%, soit 449 milliards de dollars, l'équivalent de 64% du PIB de l'Ukraine.
- Malgré le conflit, le taux d'incarcération en Russie, les manifestations violentes, l'impact du terrorisme et les taux d'homicides ont connu une amélioration au cours de la dernière année, avec le taux d'homicides au plus bas depuis 2008.
- 65% des hommes en Ukraine âgés de 20 à 24 ans ont fui le pays ou sont décédés dans le conflit.

La guerre entre la Russie et l'Ukraine, les tensions entre Israël et le Hamas et les troubles civils dans le monde entrainent une prise de conscience des risques associés. Dans certains territoires, dont la Russie, l'Ukraine, la Moldavie, la Biélorussie, Israël et Taïwan, les assureurs sont désormais incapables ou réticents à offrir une couverture en raison des sanctions et des restrictions imposées par les traités.

Plusieurs pays ont été le théâtre d'actes de violence politique, mettant en évidence la difficulté de prévoir de tels risques. Parmi ces événements, on peut citer :

- La France a fait face à des grèves nationales et à des manifestations à la suite d'un nouveau projet de loi sur les retraites augmentant l'âge de la retraite, ainsi qu'à des émeutes après la fusillade par la police d'un garçon d'origine algérienne.
- Les États-Unis ont connu une hausse du harcèlement, des agressions et des menaces violentes visant des fonctionnaires civiques et publics, ainsi qu'une augmentation des fusillades de masse.
- L'Iran a connu un mécontentement généralisé suite à la mort de Mahsa Amini, une femme irano-kurde.
- En Syrie, la guerre civile de 12 ans a coûté la vie à environ 300 000 civils et a contraint 22 millions de personnes à fuir leur domicile.
- Au Niger, des manifestations ont eu lieu après un coup d'État qui a vu le président Mohamed Bazoum pris en otage. Au Bangladesh, des manifestations se poursuivent contre la Première ministre en exercice, Sheikh Hasina, au milieu d'une crise économique.
- Au Pakistan, au moins 44 personnes ont été tuées lors d'une explosion lors d'un rassemblement organisé par un parti islamiste.
- Au Sri Lanka, des manifestations de masse ont eu lieu alors que le pays fait face à sa pire crise économique depuis son indépendance. L'insécurité énergétique et les coûts alimentaires restent élevés, tandis qu'il y a une pénurie critique de médicaments essentiels.
- En Équateur, des manifestations violentes ont éclaté à la suite de pénuries de carburant et d'aliments. Un état d'urgence et des couvre-feux nocturnes ont été imposés dans trois provinces côtières en juillet, au milieu d'une vague de violence.
- Au Brésil, les partisans de l'ancien dirigeant Jair Bolsonaro ont pris d'assaut des sites clés du pays en janvier, y compris le palais présidentiel.

2. Le secteur de l'assurance bouleversé par les événements de violence politique dans le monde

D'après le rapport de Marsh pour l'année 2023, les récents incidents de violence politique dans le monde ont engendré des modifications significatives sur le marché de l'assurance contre la violence politique, influençant les tarifs, les plafonds de couverture et les conditions générales.

En réponse à ces évolutions, les assureurs réévaluent les limites souscrites ainsi que l'étendue des termes et conditions de leurs polices d'assurance. En raison des restrictions imposées par les réassureurs lors des renouvellements de traités en 2023, les assureurs effectuent des examens approfondis des programmes et des données des clients, mettant un accent particulier sur des clauses spécifiques, notamment celles liées à l'interruption d'activité contingente. Les assureurs conduisent également des évaluations plus approfondies des indicateurs socio-économiques clés, tels que l'indice des prix alimentaires, le PIB et la disparité des richesses, qui influent sur la couverture et les conditions.

La couverture des traités pour les marchés de la violence politique et du terrorisme fait l'objet d'un examen approfondi accru en 2023. La couverture des traités de catastrophe immobilière subit une pression particulière en raison des conditions de marché difficiles, les réassureurs cherchant à réduire leur exposition aux risques de SRCC (Sabotage, Risque de grève, Conflit civil) et aux risques de guerre non modélisée.

Types des sinistres liés au risque politique

En 2023, malgré une année pleine de perturbations, certaines tendances dans les pertes liées au risque politique ont persisté par rapport aux années précédentes. Par exemple, le transfert de devises a été le principal responsable, suivi de près par les sanctions et la violence politique, qui ont augmenté en fréquence en raison du conflit en Ukraine. D'autre part, les pertes liées à l'expropriation et au défaut souverain ont été moins courantes.

Le conflit en Ukraine a également modifié la liste des pays où les entreprises ont subi des pertes liées au risque politique. La Russie a été en tête, avec sept entreprises sur 50 signalant des pertes directes, tandis que l'Ukraine était en septième position, avec quatre entreprises signalant des pertes.

Malgré ces changements, on a observé une certaine continuité dans les tendances des années précédentes. Ces dernières années, des pays à haut risque peu attractifs pour les investissements occidentaux dominaient la liste, mais récemment, des destinations d'investissement populaires comme l'Inde, la Chine et les États-Unis ont figuré en tête. En 2023, la liste comprenait tous les BRICS et, de manière surprenante, le Royaume-Uni (peut-être lié à des effets post-Brexit).

Cependant, une rupture notable dans le schéma des pertes liées au risque politique a été observée cette année. Alors que dans les années précédentes, on constatait une distribution en forme de U des pertes, avec des pertes très faibles étant fréquentes, des pertes moyennes rares, et des pertes très importantes à nouveau fréquentes, cette année a présenté un changement dans ce schéma.

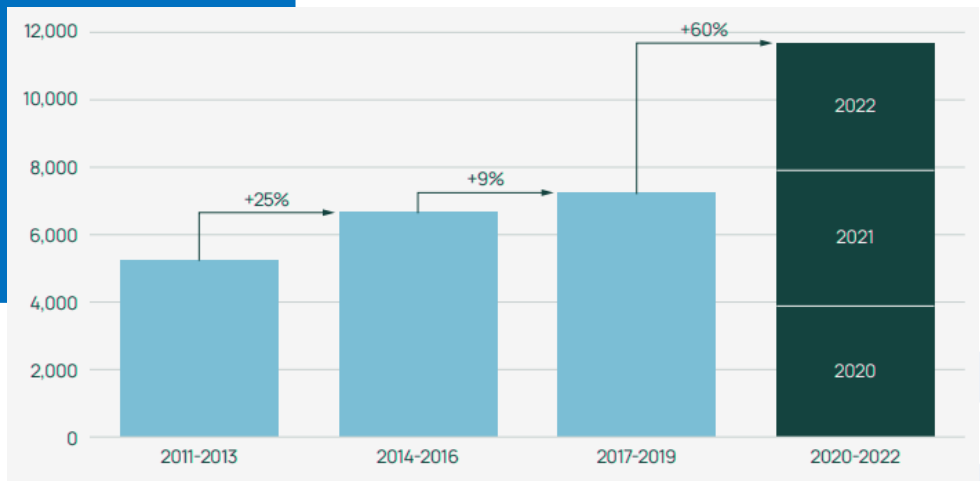
Fréquence et Gravité de la Couverture SRCC

L'augmentation des risques SRCC est le reflet de grandes tendances ainsi que de problèmes de longue date qui s'aggravent, comme la hausse du coût de la vie, l'insécurité alimentaire et énergétique, la baisse des revenus réels, le populisme/politisation, une gouvernance perçue comme défaillante et la corruption.

L'utilisation des médias sociaux rend la situation plus imprévisible, car leur portée et la rapidité avec laquelle ils diffusent l'information ont conduit à une propagation rapide des incidents, touchant plusieurs endroits plutôt que restant des risques localisés comme par le passé. Les médias sociaux peuvent inciter à l'agitation, impactant simultanément plusieurs villes/états ou même des pays (comme cela s'est produit avec le mouvement Black Lives Matter), exposant ainsi le marché PV à des pertes systémiques potentielles. Tout cela se produit alors que la demande de couvertures autonomes augmente rapidement, car de nombreux assureurs tous risques se retirent de l'espace SRCC.

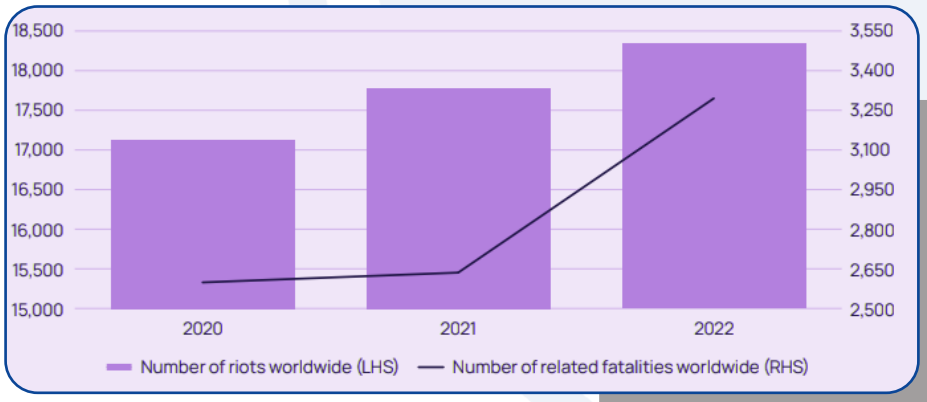
En utilisant les données du projet ACLED (Armed Conflict Location and Event Data Project), la Figure 2 montre le nombre d'émeutes enregistrées en Afrique au cours de la dernière décennie. Les épisodes croissants d'agitation observés ces dernières années, en particulier, reflètent des tendances similaires observées dans la plupart des autres régions. Entre 2020 et 2022, le nombre d'émeutes en Afrique a augmenté de 60% par rapport à la période triennale précédente, qui était déjà à un niveau historiquement élevé.

Nombre d'émeutes enregistrées en Afrique par période de 3 ans de 2011 à 20221(Source Analyse Howden utilisant les données ACLED)l'Ukraine par la Russie.



Source: Howden analysis using ACLED data, St. Louis Fed

La figure ci-dessous utilise les données de l'ACLED pour représenter le nombre quotidien de protestations et d'émeutes dans le monde lié à la hausse des prix des carburants en 2022 et leur corrélation avec les fluctuations des prix du pétrole à la suite de l'invasion de l'Ukraine par la Russie.



3. Impact de la guerre d'Ukraine sur l'assurance Maritime

La situation géopolitique tendue entre la Russie et l'Ukraine a eu un impact significatif sur le secteur de l'assurance maritime. Depuis le début du conflit, entre 200 et 300 navires se trouvent bloqués en zone de guerre, et au moins 10 navires marchands ont été endommagés par des missiles ou des mines, mettant ainsi le marché de l'assurance transport sous une pression considérable.

Le Joint Coordination Centre (JCC) a réagi immédiatement en considérant la mer Noire et la mer d'Azov comme des zones à risques accrus, exposées à des actes de destruction et de pillage des cargaisons. Les navires opérant dans les eaux territoriales ukrainiennes et russes font face à des risques exceptionnels, entraînant des surprimes pour assurer ces trajets périlleux.

Le Joint War Committee, un autre organisme spécialisé, a également classé, depuis le 24 février 2022, les eaux autour de la Russie et de l'Ukraine comme une zone à haut risque. En mars, cette classification a été étendue aux eaux des côtes roumaines et géorgiennes. Ces ajustements reflètent la dynamique changeante des risques géopolitiques et l'importance pour les assureurs maritimes de s'adapter rapidement pour garantir une protection adéquate.

En réponse à ces classifications, les assureurs et réassureurs internationaux ont résilié les contrats Risques de Guerre pour la Russie et l'Ukraine dans un délai de 48 heures.

Certains assureurs ont élargi la classification de l'Ukraine à une zone de 200 km autour du pays, touchant également certains pays voisins. Cette série de mesures a entraîné une augmentation des primes d'assurance et la mise en place de restrictions géographiques.

L'ensemble de ces ajustements témoigne de l'impact direct des événements géopolitiques sur le secteur de l'assurance maritime, avec des changements significatifs dans les couvertures et les primes pour faire face aux risques accrus dans les zones concernées. Cette situation souligne la nécessité pour l'industrie de

s'adapter rapidement aux évolutions géopolitiques pour assurer une gestion efficace des risques et maintenir la stabilité du secteur.

Cette situation a entraîné une augmentation des primes d'assurance et l'implémentation de restrictions géographiques.

Finalement, cette série de mesures témoigne de l'impact direct des événements géopolitiques sur le secteur de l'assurance maritime, avec des ajustements significatifs dans les couvertures et les primes pour faire face aux risques accrus dans les zones concernées.

4. Durcissement du marché de la réassurance

La réaction du marché de la violence politique continuera probablement pendant une bonne partie de cette année, les pressions étant aggravées par le durcissement considérable du secteur de la réassurance lors des renouvellements du 1 janvier 2023. Dans certains cas, les rétentions et les tarifs ont doublé et une grande partie de la couverture de réassurance a été perdue dans l'ensemble.

L'appétit pour les traités de réassurance dans cette branche a diminué au 1 janvier 2023, en particulier pour les transporteurs en amont qui ne veulent pas ou ne peuvent pas répondre aux attentes de tarification des traités futurs.

Ce changement est dû aux cinq principaux réassureurs de traités qui, après avoir récemment subi des pertes disproportionnées dans le cadre de polices autonomes et de polices tous risques, ont refusé de poursuivre dans les conditions antérieures non rentables.

Les définitions des événements et les termes et conditions se sont également resserrés au 1 janvier 2023, les réassureurs des traités ayant réduit les expositions, en particulier dans le domaine de la perte d'exploitation potentielle. Ces changements spectaculaires se sont répercutés en aval de la chaîne de valeur, obligeant les assureurs initiaux à répercuter sur les acheteurs les formulations restreintes, les coûts plus élevés et les franchises.

En plus, l'effet de ce changement varie selon les risques, les engagements de capacité diminuant pour les SRCC et les PV de 30 % et 60 % respectivement, et la tarification augmentant de manière significative dans tous les domaines.

5. Les projections pour l'année 2024

En 2024, l'escalade des conflits pourrait être observée dans trois points chauds vitaux, à savoir Israël, l'Ukraine et Taïwan. Si tel est le cas, les conséquences économiques, géopolitiques et sécuritaires pourraient être considérables.

Le rapport souligne : «Ces trois régions se trouvent à un carrefour géopolitique, où les grandes puissances ont des intérêts directs : le pétrole et les routes commerciales au Moyen-Orient, la stabilité et l'équilibre des pouvoirs en Europe de l'Est et les chaînes d'approvisionnement en technologies de pointe en Asie de l'Est. Chacun de ces points chauds pourrait conduire à une déstabilisation régionale plus large, en impliquant directement une ou plusieurs grandes puissances et en aggravant l'ampleur du conflit. Les trois impliquent aussi directement une ou des puissances dotées de capacités nucléaires».

En outre, des thèmes socio-économiques, idéologiques et environnementaux pourraient donner lieu à de nouvelles tensions, érodant davantage la stabilité économique et politique d'un certain nombre de pays. Un monde plus multipolaire pourrait également ouvrir la voie à une série de factions et de puissances plus petites, mais pertinentes au niveau régional, qui prendraient le contrôle. Chacune d'entre elles étant susceptible d'avoir ses propres objectifs, la résolution des conflits pourrait devenir de plus en plus difficile.

L'escalade des conflits entraîne également des crises humanitaires plus graves, ce qui alourdit le fardeau des autres pays qui se doivent d'apporter une aide sous peine de faire face à des critiques. Dans certains cas, comme avec les États-Unis, cela peut également s'accompagner d'un déploiement militaire supplémentaire.

La demande d'assurance contre les risques politiques pourrait connaître une hausse en 2024 en raison des élections prévues pour cette année.

La demande d'assurance contre les risques politiques devrait augmenter en 2024 en raison de l'augmentation du nombre d'élections dans le monde, un événement qui accroît généralement la valeur des économies et augmente simultanément le risque politique pour les entreprises opérant dans des pays confrontés à une incertitude politique, a déclaré Chaucer.

Selon les données des réassureurs, le nombre total d'élections nationales augmentera de 14% l'année prochaine, passant de 56 dans le monde en 2023 à 64 en 2024. Parmi celles-ci, les élections aux États-Unis et en Afrique du Sud revêtent une importance particulière.

Les élections suivantes en 2024 sont identifiées comme étant particulièrement cruciales du point de vue du risque politique :

14 février : Indonésie (législatives et présidentielles)

10 avril : Corée du Sud (législatives)

Mai-juin : Inde (législatives)

Mai-juin : Afrique du Sud (législatives)

2 juin : Mexique (législatives et présidentielles)

5 novembre : États-Unis (législatives et présidentielles)

Ces élections sont considérées comme ayant un impact potentiellement significatif sur le risque politique, et une attention particulière est recommandée.

Les pays ayant des élections en 2023 ont un PIB combiné de 9,89 billions de dollars. Cette somme augmentera de plus de quatre fois pour atteindre un PIB combiné de 40,79 billions de dollars en 2024. Cette augmentation du PIB combiné représente un bond de 9,8 % à 40,6 % du PIB mondial qui sera soumis au vote l'année prochaine.

L'augmentation du nombre d'élections et la taille des économies en jeu présentent un risque politique accru pour les entreprises opérant dans des pays confrontés à une incertitude politique. Lorsque les gouvernements ont du mal à payer leurs factures, cela peut accroître le risque que les entreprises voient soudainement annulés leurs contrats du secteur public ou restent impayés. Les entreprises ont de plus en plus souscrit une assurance contre le défaut de paiement des gouvernements en achetant une couverture de «frustration de contrat.

6. Cas de la Tunisie

La Tunisie, comme tout autre pays, peut être confrontée à divers risques politiques qui peuvent avoir des implications sur la stabilité économique et sociale. Parmi ces risques, on peut citer :

1. Stabilité Politique : Les changements fréquents de gouvernement ou les tensions politiques internes peuvent créer un climat d'instabilité, ce qui peut être préjudiciable à la confiance des investisseurs et à l'environnement des affaires.
2. Tensions Sociales : Les mouvements sociaux, les manifestations et les grèves peuvent perturber les activités économiques et créer des défis pour les entreprises.
3. Risques Électoraux : Les périodes électorales peuvent être associées à une certaine incertitude politique, en particulier si les résultats des élections sont contestés.
4. Sécurité : Les menaces liées au terrorisme et aux activités extrémistes peuvent poser des risques pour la sécurité nationale, affectant ainsi le climat des affaires.
5. Corruption : Les pratiques de corruption au sein du gouvernement ou dans le secteur privé peuvent créer des obstacles pour les entreprises et décourager les investisseurs.
6. Évolutions Législatives : Les changements fréquents dans la législation ou l'adoption de nouvelles lois peuvent avoir des répercussions sur les activités des entreprises, en particulier si elles ne sont pas bien anticipées.
7. Relations Internationales : Les tensions diplomatiques avec d'autres pays peuvent également influencer le climat des affaires, en particulier si elles conduisent à des sanctions ou à des restrictions commerciales.
8. Économie Mondiale : Les fluctuations économiques mondiales peuvent également

influencer la situation économique en Tunisie, en particulier en tant que pays dépendant des échanges internationaux.

Selon le Global Peace Index, un instrument de référence évaluant la sécurité et la stabilité des nations, la Tunisie se positionne modestement au 81ème rang parmi 163 pays évalués en 2023, enregistrant tout de même une avancée d'une place par rapport à l'année précédente, avec un indice de paix de 2.01.

La Tunisie est catégorisée comme étant de niveau «moyen». Elle se trouve ainsi entre les pays considérés comme «assez pacifiste» ou « très pacifistes» d'une part, et ceux répertoriés comme «peu pacifistes» ou «très peu pacifistes» de l'autre. Dans le contexte du monde arabe, la Tunisie se classe au sixième rang des pays les plus sûrs, tandis qu'à l'échelle africaine, elle occupe la douzième position.

Impact de la guerre d'Ukraine sur le marché tunisien

La Tunisie, bien qu'éloignée géographiquement du conflit entre la Russie et l'Ukraine, subit des conséquences économiques significatives en raison de sa forte dépendance aux importations de céréales et d'énergie, principalement en provenance de l'Ukraine et de la Russie.

L'incidence de la guerre russo-ukrainienne sur la Tunisie est estimée à une variation du taux de croissance de - 2,5% et de -2,2%, respectivement en 2022 et 2023, par rapport à une situation sans guerre, indique une étude réalisée par l'ONU Habitat et le bureau régional Afrique du nord de la Commission économique pour l'Afrique des Nations Unies.

Les importations de céréales, en particulier de blé, jouent un rôle crucial dans la sécurité alimentaire du pays, et une diminution des importations en provenance d'Ukraine pourrait avoir des répercussions sur l'approvisionnement alimentaire et les prix.

La Tunisie a importé en moyenne sur la période 2018-2021, 93% de sa consommation de blé tendre, 67% d'orge et 40% de blé dur.

En effet, la Tunisie est très dépendante des importations de céréales : En 2019, les importations de céréales provenant de l'Ukraine représentaient, près de 47,7% des importations tunisiennes en blé, celles de la Russie étaient de 3,97%.

L'augmentation des importations de diesel et de gasoil en provenance de Russie souligne également la vulnérabilité de la Tunisie aux fluctuations des marchés mondiaux de l'énergie, surtout en période de crise géopolitique. Les variations des prix du pétrole et les perturbations dans les approvisionnements pourraient impacter l'économie tunisienne, avec des répercussions sur les coûts de production et les prix à la consommation.

La Tunisie importe une bonne partie de ses besoins en énergie, notamment de la Russie près de 77 000 barils par jour (bpj) de gasoil et de diesel russes en février 2023, contre 25 000 bpj en décembre 2022.

La situation en matière d'assurance, avec l'exclusion des garanties liées aux risques de guerre dans le contexte du conflit russo-ukrainien, démontre comment les tensions internationales peuvent influencer le secteur financier d'un pays. Les assureurs tunisiens, confrontés à des incertitudes quant aux impacts à court, moyen et long terme de la guerre, doivent faire preuve de vigilance dans leurs opérations.

L'analyse des sanctions internationales met également en évidence les nuances dans leur impact sur l'économie russe. L'arrêt des exportations de technologies sensibles a des conséquences plus significatives que certaines restrictions dans le domaine des assurances. Cela souligne la complexité des réponses internationales et la nécessité pour les acteurs économiques de s'adapter rapidement à l'évolution de la situation géopolitique.

En résumé, la crise entre la Russie et l'Ukraine a des répercussions indirectes sur des pays tels que la Tunisie, mettant en lumière la manière dont les interconnexions économiques mondiales peuvent exposer des nations éloignées géographiquement à des vulnérabilités économiques en période de crise internationale.

Conclusion

En résumé, le marché de l'assurance des risques politiques s'est adapté aux changements mondiaux. Les entreprises cherchent de plus en plus à se protéger contre les risques liés à l'instabilité politique et aux conflits. Les assureurs ont développé des produits plus sophistiqués pour faire face à la complexité croissante des risques, y compris les cyber-risques.

Les tensions géopolitiques et les sanctions économiques ont également influencé les offres d'assurance. Les compagnies d'assurance innovent en proposant des solutions sur mesure pour les entreprises opérant dans des zones politiquement instables.

La réglementation a également joué un rôle, incitant les assureurs à s'adapter aux nouvelles exigences. En fin de compte, l'assurance des risques politiques évolue pour mieux répondre aux réalités changeantes des affaires et de la géopolitique, incitant les entreprises à revoir régulièrement leurs besoins d'assurance.

Les Risques Economiques

LE DÉFI DU RISQUE MACROÉCONOMIQUE DANS LE SECTEUR DE L'ASSURANCE : CONTEXTE DÉGRADÉ

L'année 2023 apparaît globalement la plus risquée depuis plus d'une décennie. L'environnement de risque de 2023 est le plus élevé du fait de la montée des risques macroéconomiques, stratégiques et opérationnels mis en évidence depuis le début de l'année 2022.

En 2023, parmi les risques émergents qui préoccupent le secteur, le risque macroéconomique se profile comme un élément majeur. L'incertitude quant aux politiques des banques centrales dans un contexte d'inflation persistante, de hausse des coûts de la main-d'œuvre et de perturbations de la chaîne d'approvisionnement ainsi que le spectre d'une possible récession mondiale à l'horizon.

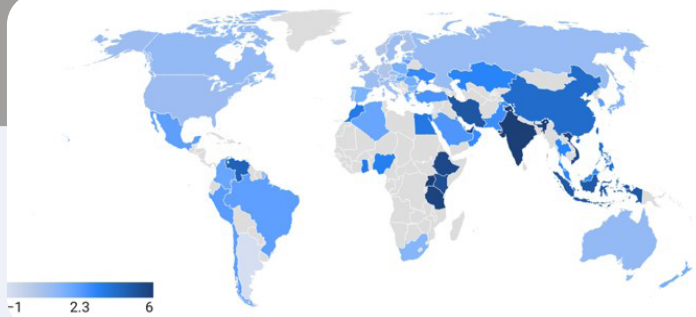
Section 1 : Risque Macroéconomique & Assurance

Le risque macroéconomique se réfère aux menaces qui découlent des fluctuations économiques à grande échelle, telles que les cycles économiques, l'inflation, le chômage et les crises financières. Ces éléments peuvent exercer une influence significative sur la stabilité financière des assureurs et sur leur capacité à gérer les sinistres et à maintenir des marges bénéficiaires.

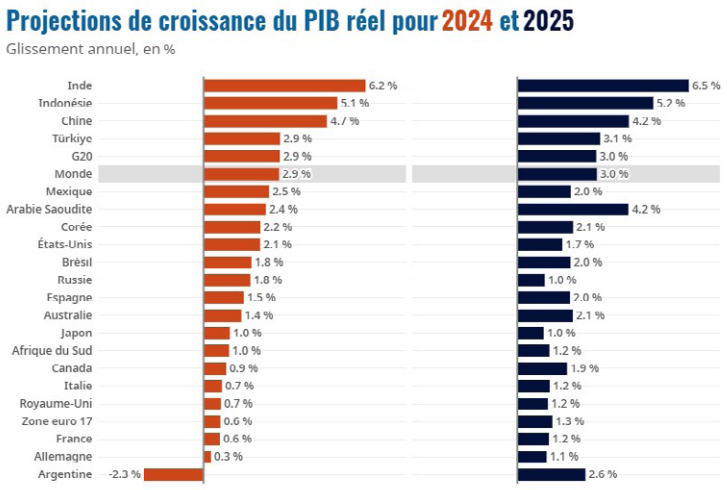
Selon l'OCDE la croissance économique mondiale, qui a augmenté d'environ 3,1% en 2023, devrait connaître une nouvelle décélération en 2024, avec une troisième année consécutive de ralentissement, avec un taux de croissance projeté à 2,9% puis remonter à 3,0% en 2025, influencée par des politiques monétaires restrictives, un durcissement des conditions financières, et une diminution notable des échanges commerciaux et des investissements. Les risques potentiels incluent une escalade des conflits au Moyen-Orient, des tensions financières croissantes, une persistance de l'inflation, la fragmentation des échanges commerciaux ainsi que des catastrophes climatiques.

Ces facteurs constituent autant de menaces à la baisse qui pèsent sur les perspectives de croissance à l'échelle mondiale.

La croissance réelle du PIB dans le monde en 2023 **(en %)**



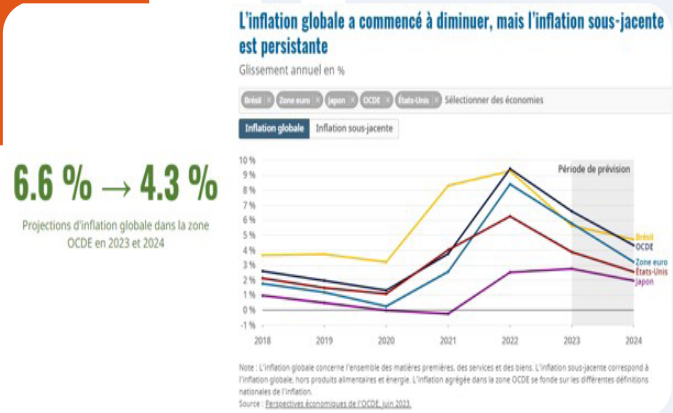
Les fluctuations des cycles économiques, caractérisées par des phases d'expansion et de contraction, représentent l'un des éléments majeurs contribuant à la dégradation de l'environnement économique. En 2023, les incertitudes entourant la reprise économique après la pandémie de COVID-19 intensifient ces variations. Ces fluctuations peuvent impacter la demande d'assurance, les taux de sinistralité et les exigences de capital, nécessitant une gestion agile des portefeuilles pour maintenir la stabilité financière des assureurs.



Source : Perspectives économiques de l'OCDE, Rapport intermédiaire, février 2024

1. Inflation et Pressions sur les Coûts

L'augmentation de l'inflation et les pressions sur les coûts représentent un défi croissant pour l'industrie de l'assurance.



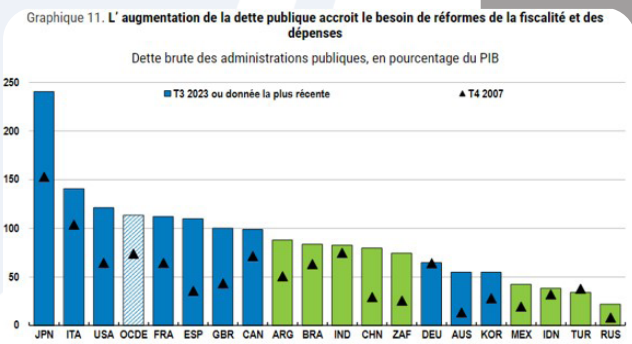
L'inflation peut entraîner une hausse des coûts de réparation et de remplacement, impactant directement les paiements de sinistres. Les assureurs sont confrontés à la nécessité de recalibrer leurs réserves et leurs tarifs pour faire face à ces pressions inflationnistes tout en maintenant leur compétitivité sur le marché.

2. Instabilité des Marchés Financiers

L'instabilité des marchés financiers, exacerbée par des événements géopolitiques et des incertitudes économiques, contribue à la dégradation de l'environnement économique. Les fluctuations des taux de change, les chocs boursiers, et les incertitudes entourant les politiques monétaires mondialisées représentent des risques importants pour les assureurs qui gèrent d'importants portefeuilles d'investissements.

3. Contraintes Budgétaires et Réduction des Dépenses

Les contraintes budgétaires au niveau individuel et gouvernemental, accentuées par des crises économiques, peuvent conduire à une réduction des dépenses consacrées aux assurances. Les consommateurs peuvent être amenés à réévaluer leurs priorités financières, affectant la demande pour certains types de polices d'assurance. Les assureurs doivent anticiper ces changements comportementaux et adapter leurs offres en conséquence.



4. Répercussions des Événements Extraordinaires

Les événements extraordinaires, tels que les catastrophes naturelles, les pandémies, et les crises sanitaires, exercent des pressions exceptionnelles sur l'environnement économique. Les assureurs sont confrontés à des défis multiples allant de l'évaluation des risques liés à ces événements à la gestion des conséquences financières. Les modèles traditionnels de tarification et de gestion des risques peuvent être remis en question, nécessitant une adaptation rapide.

Section 2 : Instabilité macroéconomique

Après la crise financière de 2008, les groupes à faibles revenus n'ont toujours pas retrouvé le chemin de la croissance et, pour beaucoup, le niveau de vie reste stagnant. Cette inégalité croissante aggrave l'instabilité des systèmes économiques et, sur le plan politique, ces facteurs alimentent la montée du populisme et une réaction contre les institutions multinationales, ce qui conduit au nationalisme et à une réglementation fragmentée.

La hausse récente et sans précédent des taux d'intérêt pour lutter contre une inflation élevée ralentira l'économie mondiale et augmentera le risque d'inflation ce qui pourrait conduire à une récession profonde. La viabilité financière des systèmes de sécurité sociale et des systèmes de retraite est plus que jamais menacée.

Les tensions entre les États-Unis et la Chine exercent une influence économique et politique croissante et déplacent le pouvoir économique mondial de l'Ouest vers l'Est, ce qui accroît la complexité et l'instabilité des équilibres mondiaux.

L'expansion des économies des BRICS (Brésil, Russie, Inde, Chine, Afrique du Sud) remet en question le système du pétrodollar.

La guerre en Ukraine a fait grimper l'inflation à des niveaux jamais atteints depuis des décennies, mondialisant la crise du coût de la vie et alimentant des troubles sociaux.

Le changement de politique monétaire marque la fin d'une ère économique définie par l'accès facile à une dette bon marché et aura de vastes répercussions sur l'économie mondiale.

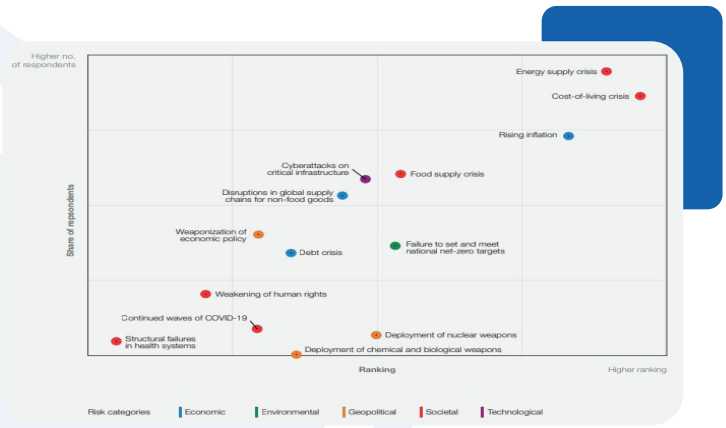
Deux événements majeurs, à savoir la pandémie du Covid-19 et la guerre Ukraine-Russie contribuent à la forte instabilité économique et financière de l'ensemble du marché. L'inflation est particulièrement redoutée du fait de l'érosion qu'elle impose à la marge de rentabilité des entreprises.

La tendance inflationniste devrait se poursuivre malgré les efforts des banques centrales et institutions financières pour la contenir, réduire les coûts de la vie et éviter la récession.

Selon Allianz Trade, les faillites d'entreprises devraient augmenter de manière significative (+19%) à l'échelle mondiale en 2023.

Aujourd'hui, le paysage mondial étant dominé par : la crise de l'approvisionnement en énergie, du coût de la vie, la hausse de l'inflation, etc.

On assiste à un retour des risques «plus anciens» qui sont compris historiquement mais que peu de générations actuelles de chefs d'entreprise et de décideurs publics ont connus.



1. Ralentissement économique

Aujourd'hui, les gouvernements et banques centrales - au premier rang desquels les marchés développés, notamment les États-Unis d'Amérique, la zone euro et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord – essayent de trouver l'équilibre entre la gestion de l'inflation et le maintien des taux d'intérêt sans déclencher une récession profonde ou prolongée afin de protéger les citoyens d'une crise du coût de la vie tout en assurant le service d'une dette historiquement élevée.

Les taux d'inflation ont dépassé plus de 80 % en Argentine et en Turquie, tandis que le Zimbabwe, la République bolivarienne du Venezuela, l'Inde et l'Indonésie ont été touchés par la crise. Le Liban, la République arabe syrienne et le Soudan ont connu une inflation à trois chiffres. L'inflation aux États-Unis d'Amérique a dépassé les 9 % en juin de l'année dernière et a atteint des records au Royaume-Uni et dans la zone euro en octobre avec respectivement 11,1 % et 10,6 % forçant les taux d'intérêt à augmenter

Les projections les plus récentes du FMI prévoient une baisse de l'inflation mondiale

qui passerait de près de 9 % en 2022 à 6,5 % cette année et à 4,1 % en 2024.

Même si les retombées économiques restent relativement limitées, la croissance mondiale devrait ralentir pour atteindre 2,7 % en 2023, avec un taux de chômage d'environ 1,5 % avec environ un tiers de l'économie mondiale confrontée à une récession technique.

Toutefois, pour les économies en développement, il existe un risque d'aggravation de la crise économique et d'un ralentissement de la croissance, des chocs de liquidité et de la crise de la dette à l'échelle mondiale en particulier ceux dont la dette est fortement libellée en USD.

2. Dette souveraine en défaut

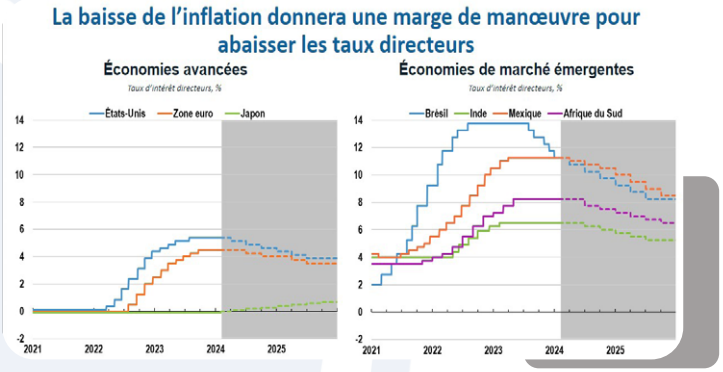
Pendant la pandémie de COVID-19, le volume de la dette souveraine intérieure détenue par les banques a considérablement augmenté dans les pays émergents, représentant en moyenne environ un cinquième des actifs du secteur bancaire et atteignant 200% des fonds propres réglementaires. Cette expansion des avoirs a renforcé les liens interdépendants entre les banques et les États.

À mesure que les conditions financières mondiales se durcissent et que les tensions géopolitiques s'intensifient, en particulier après l'invasion de l'Ukraine par la Russie, les pays émergents font face à des défis spécifiques. Depuis la pandémie, leurs perspectives de croissance se sont généralement détériorées par rapport aux pays avancés, leur espace budgétaire est plus restreint, et les risques de refinancement ont augmenté. Avec la dette publique atteignant des niveaux historiquement élevés et les perspectives des crédits souverains se détériorant dans de nombreux pays émergents, le renforcement des liens entre l'État et les banques pourrait mettre en péril la stabilité macro financière en cas de grave choc défavorable.

L'augmentation du coût de la dette peut remettre en question les finances publiques et exposer les vulnérabilités latentes des acteurs des marchés financiers qui se sont endettés dans un régime de taux d'intérêt à faible rendement et à faible volatilité.

Le poids élevé de la dette souveraine pourrait conduire à une réduction dans les infrastructures et les services publics, ce qui pourrait entraîner des infrastructures critiques et des services de santé détériorés.

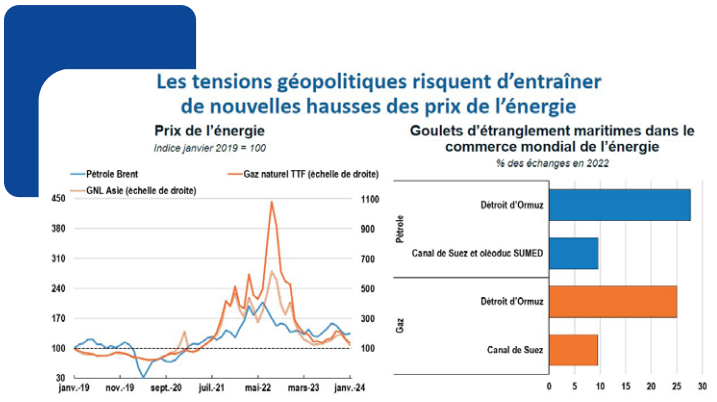
Une baisse des investissements publics axés sur la croissance pourrait conduire à une hausse du chômage, à une baisse de la productivité et, potentiellement, à des troubles sociaux. Ces derniers pourraient augmenter la demande des couvertures de crédit & de caution, dommages, d'interruption d'activité (BI) et de violence politique (PV).



En ce qui concerne la dette souveraine en devises fortes, bien que les titres à haut rendement aient récemment surperformé, il est conseillé de ne pas ajouter de risque excessif à ce stade. Les pays responsables de cette surperformance, tels que l'Ukraine, la Tunisie, le Ghana et la Zambie, pourraient s'avérer trop risqués pour un investissement actuel. Les titres souverains de bonne qualité restent une option solide dans un contexte de resserrement continu des conditions de crédit. Les pays à rendement élevé continuent de faire face à des coûts de financement élevés, mais des opportunités intéressantes existent, en particulier dans certaines obligations BB positives, comme celles de la Serbie, Oman, le Maroc et la République dominicaine. Le Sri Lanka, en restructurant sa dette, demeure également une option positive.

3. Crise énergétique

Sous-estimé les années précédentes, le risque énergétique fait son entrée à la 4ème place du classement 2023. Les perturbations et/ou interruptions d'approvisionnement ont entraîné une flambée des produits énergétiques (pétrole et gaz naturel).



Les impacts économiques ont été amortis par les pays qui en ont les moyens, mais de nombreux pays à faible revenu sont confrontés à des crises multiples : dette, changement climatique et sécurité alimentaire.

Au cours des dix prochaines années moins de pays auront la marge de manœuvre budgétaire nécessaire pour investir dans la croissance future, les technologies vertes, l'éducation, les soins et les systèmes de santé. La lente dégradation des infrastructures et des services publics dans les pays en développement et avancés peut-être relativement subtile, mais l'accumulation des impacts sera très corrosive. Alors que la volatilité dans de multiples domaines, le risque de polycrises s'accélère.

L'érosion de la coopération géopolitique aura des effets d'entraînement sur le paysage mondial des risques au cours des prochaines années autour des pénuries de nourriture, d'eau, de métaux et de minéraux qui pourraient déclencher une crise humanitaire et écologique.

Section 3 : La trajectoire jusqu'en 2025

L'évolution complexe et rapide du paysage mondial des risques était dominée par les risques sociaux et environnementaux induits par les tendances géopolitiques et économiques sous-jacentes.

Les coûts ont encore augmenté en 2022, principalement en raison des perturbations persistantes dans les flux d'énergie et de Russie et de l'Ukraine. Pour freiner les prix intérieurs, environ 30 pays ont introduit des restrictions, y compris des interdictions d'exportation sur les produits alimentaires et l'énergie, ce qui a accentué la hausse de l'inflation mondiale.

Selon les estimations, les prix de l'énergie 46 % plus élevés que la moyenne en 2023 par rapport aux projections de janvier 2025.

Les économies avancées continuent à mettre en place des mesures, dont la plupart ont une approche très large, allant de plafonds à la réduction des émissions de gaz à effet de serre, des remises sur les carburants et les factures d'électricité et des billets de transport public subventionnés pour les consommateurs, jusqu'aux contrôles des exportations de denrées alimentaires, des allègements fiscaux, des aides pour les entreprises concernées. La pression qui en résulte sur les équilibres budgétaires peuvent exacerber les problèmes de viabilité de la dette, laissant les pays émergents et en développement avec beaucoup moins de marge de manœuvre budgétaire pour protéger leurs populations à l'avenir.

L'année dernière, l'augmentation des prix des carburants a entraîné des manifestations dans 92 pays, dont certaines ont entraîné des bouleversements politiques et des morts ainsi que des grèves et des actions syndicales.

L'impact de l'insécurité continuera à se faire sentir pour les pays vulnérables notamment la Somalie, le Soudan, le Sud-Soudan et la République Arabe Syrienne - mais il pourrait aussi exacerber l'instabilité dans les pays confrontés à des crises comme la Tunisie, le Ghana, le Pakistan, l'Égypte et le Liban.

La combinaison d'événements climatiques extrêmes et d'un approvisionnement limité pourrait transformer la crise actuelle du coût de la vie en un scénario catastrophique de famine.

A cela s'ajoute l'effet décalé de la flambée des prix des engrais l'année dernière et l'impact des conditions météorologiques extrêmes sur la production alimentaire dans des régions clés. Les estimations suggèrent que plus de 800 000 hectares de terres agricoles ont été anéantis par les inondations au Pakistan, ce qui a entraîné une augmentation des prix des produits de base dans un pays qui était déjà aux prises avec une inflation record de 27%.

Les sécheresses et les pénuries d'eau prévues pourraient entraîner une baisse des récoltes et des décès de bétail dans toute l'Afrique de

l'Est, l'Afrique du Nord et l'Afrique australe.

Des chocs sont également inattendus en matière de production ou de transport dans les principaux pays exportateurs à cause des rivalités en matière de ressources, ce qui impactera les prix des produits de base.

Les effets catastrophiques de la famine et des pertes humaines peuvent également avoir des retombées plus lointaines, car le risque de violence généralisée s'accroît et les migrations involontaires augmentent.

Section 4 : Impact sur l'Industrie de l'Assurance

L'impact du risque économique sur l'industrie de l'assurance est significatif et multifacette, influençant divers aspects :

1. Demande d'Assurance et Comportement des Consommateurs :

En période économique difficile, les consommateurs peuvent réduire leurs dépenses discrétionnaires, y compris les primes d'assurance. La demande pour certaines polices, comme l'assurance vie ou les assurances haut de gamme, peut diminuer.

2. Exposition aux Risques et Sinistralité :

Les fluctuations économiques peuvent modifier la composition des portefeuilles d'assurance. De plus, les périodes de ralentissement économique peuvent influencer la fréquence et la gravité des sinistres. Par exemple, une économie en contraction peut entraîner une augmentation des sinistres liés aux accidents automobiles.

3. Réglementation et Exigences de Capital :

Les autorités de régulation peuvent ajuster leurs politiques en réponse aux défis économiques, affectant les exigences de capital et les règles de solvabilité des compagnies d'assurance. En plus, les périodes de crise économique peuvent inciter les régulateurs à renforcer la surveillance des compagnies d'assurance pour garantir leur stabilité financière.

4. Investissements et Gestion des Actifs :

Rendements d'Investissement : Les assureurs sont fortement exposés aux marchés financiers. Une détérioration économique peut entraîner des baisses de rendement sur les investissements, affectant la rentabilité globale des compagnies d'assurance.

Réévaluation des Portefeuilles : Les assureurs doivent constamment réévaluer et ajuster leurs portefeuilles d'actifs pour faire face aux changements des conditions économiques.

5. Tarification et Rentabilité :

Défis de Tarification : Les variations économiques peuvent rendre difficile la tarification des polices d'assurance, en particulier lorsqu'il y a des incertitudes autour des coûts futurs des sinistres.

Pressions sur la Rentabilité : Une économie dégradée peut mettre à rude épreuve la rentabilité des assureurs, les obligeant à rechercher des moyens novateurs de maintenir leurs marges.

6. Innovation et Adaptabilité :

Besoin d'Innovation Continue : Face aux défis économiques, les assureurs doivent innover pour répondre aux besoins changeants des clients et trouver des solutions adaptées.

Agilité Opérationnelle : L'agilité opérationnelle devient cruciale pour s'adapter rapidement aux changements économiques et aux nouvelles réalités du marché.

Section 5 : Impact de l'inflation sur les renouvellements de réassurance du 1/1

L'inflation était au premier plan des préoccupations des réassureurs européens lors des renouvellements du 1er janvier.

L'impact de l'inflation sur le coût de l'activité signifie que les pertes assurées seront plus coûteuses dans toutes les branches d'activité, ce qui conduit à une augmentation inévitable des franchises lors du renouvellement de la couverture.

Du point de vue des réassureurs, cela signifie une réduction du montant des affaires plus rentables qu'ils peuvent souscrire, ce qui faussera l'équilibre des portefeuilles en faveur de couvertures plus volatiles et plus lourdes.

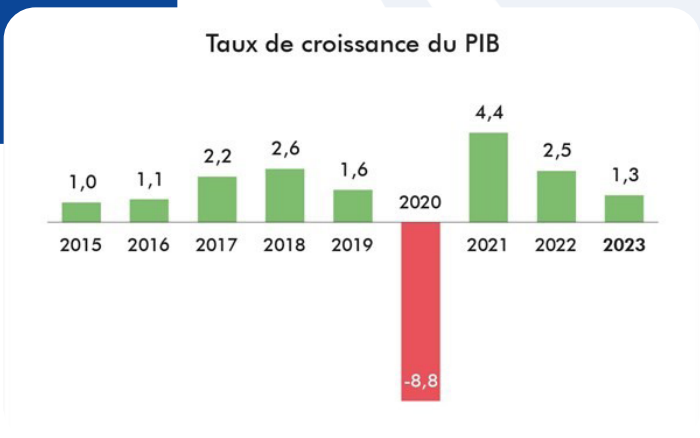
Pour les assureurs-vie, des taux d'intérêt plus élevés pourraient se traduire par une augmentation de la rentabilité des

investissements, tout en les aidant à rééquilibrer leurs portefeuilles. La hausse des taux peut également rendre les produits d'assurance-vie sensibles aux taux d'intérêt.

Dans ce contexte, il est attendu que les investisseurs continueront d'encourager l'acquisition de portefeuilles d'assurance-vie, à la fois par le biais de fusions et d'acquisitions et d'autres mécanismes similaires, ainsi que des structures de réassurance telles que les transferts de portefeuilles de sinistres.

Section 6 : La Tunisie entre crise politique et instabilité économique

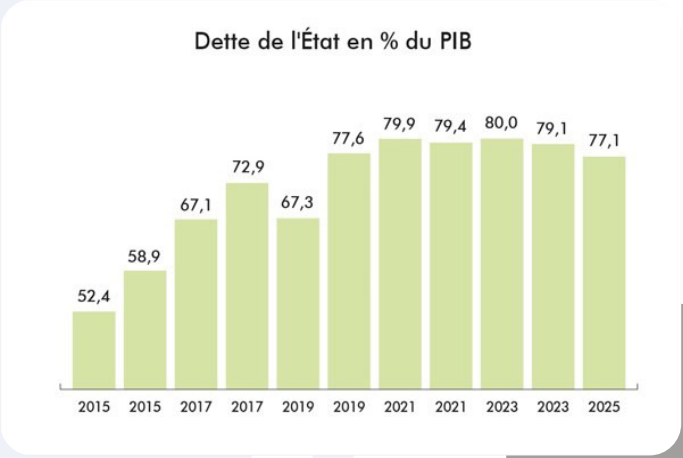
Une décennie après la révolution de 2011, la Tunisie souffre encore de nombreuses défaillances structurelles, en plus des retombées de l'instabilité politique. Le taux de croissance annuel moyen est passé de 4,3% pendant les années 2000 à 1,7% durant la décennie 2010, le déficit courant d'une fourchette de 2 à 6% du PIB à une fourchette de 8-11%. Le recul de la productivité et de l'investissement, passé de 25,4 à 17,8% du PIB entre 2010 et 2019, a affaibli le potentiel de croissance et la compétitivité de la Tunisie, fragilisant ses équilibres extérieurs.



Les conséquences de la guerre en Ukraine ont ébranlé la timide reprise post-crise sanitaire. Après -8,8% en 2020, +4,4% en 2021 et +2,5%, la croissance n'est plus prévue que de 1,3% (FMI) à 1,6% (loi de finance) pour 2023, contre 2,9% pour l'ensemble de la région MENA selon le FMI. La hausse des prix des hydrocarbures et des denrées alimentaires en 2022 a aggravé les tensions financières déjà élevées du pays. Leur évolution, en dépit d'une relative accalmie actuelle, reste une menace pour les approvisionnements du pays.

Les perspectives 2024 sont menacées par les conséquences dans le secteur agricole d'une sécheresse aigüe : rationnement de l'eau, effondrement déjà prévu de la récolte céréalière.

Les pressions inflationnistes affichent une tendance haussière jamais vue depuis les années 1990 tandis que les tensions sociales sont élevées : de 4,9% fin 2020, l'inflation est remontée à 10,3 % en mars 2023, alimentée principalement par la hausse en 2022 des



cours internationaux de l'énergie et de produits agricoles largement importés.

Les phénomènes de pénuries sur les hydrocarbures et produits alimentaires se sont multipliés en 2022 du fait de l'accumulation d'arriérés de l'Etat vis-à-vis de monopoles publics alors incapables de payer les fournisseurs, même si la situation s'est stabilisée depuis début 2023 sous l'effet de l'aide des partenaires (Algérie pour le gaz, banques multilatérales pour l'approvisionnement en céréales) et la régression des cours internationaux.

Les inquiétudes persistent sur les capacités de la Tunisie à financer son déficit courant et les risques pour les équilibres externes restent élevés : la perte d'attractivité du pays et l'absence de programme FMI freinent les entrées de capitaux - prêts étrangers et IDE. Les réserves en devises baissent régulièrement, depuis le pic de 162 jours d'importation fin 2020 à actuellement 93 jours (7,3 Md$).

Outre le risque inflationniste d'une telle monétisation indirecte de la dette, la hausse de l'exposition souveraine des banques met en risque leur bilan et la confiance qui leur est accordée. Sans conclusion d'un accord avec le FMI, la Tunisie encourt une situation financière tendue avec des remboursements relativement lourds de dette extérieure fin 2023.

Conclusion

En 2023, le risque macroéconomique se positionne comme l'un des défis émergents majeurs pour l'industrie de l'assurance. Les assureurs proactifs, armés d'analyses sophistiquées et de stratégies d'atténuation bien définies, seront mieux positionnés pour naviguer dans ce paysage en constante évolution.

Les équilibres géopolitiques apparaissent extrêmement fragiles. Face à la crainte croissante de conflits futurs, voire d'une guerre mondiale, les pays ont tendance à se replier sur eux-mêmes.

La coopération internationale et la mondialisation étant menacées, des vulnérabilités se profilent à l'horizon pour les systèmes économiques et financiers, avec des conséquences inévitables pour le secteur de l'assurance.

Les Risques Réglementaires

RISQUES RÉGLEMENTAIRES

Définition

La réglementation désigne l'ensemble des règles, normes, lois et directives émises par les autorités gouvernementales ou d'autres organismes compétents pour encadrer et guider le comportement des individus, des entreprises et d'autres entités au sein de la société.

La réglementation peut couvrir une vaste gamme de secteurs, tels que la finance, la santé, l'environnement, la sécurité alimentaire, les droits des travailleurs, les technologies de l'information.

Elle peut prendre différentes formes, allant de lois formelles adoptées par les législatures à des règlements émis par des organismes de réglementation spécifiques. Les sanctions en cas de non-respect de la réglementation peuvent varier, allant de simples avertissements à des amendes financières, des sanctions pénales, voire la fermeture d'entreprises. Il est donc essentiel pour les entreprises de comprendre et de respecter la réglementation qui s'applique à leur secteur d'activité afin d'éviter des conséquences négatives.

Les organismes gouvernementaux responsables de l'application de la réglementation jouent un rôle clé dans la surveillance et l'application des normes établies.

C'est dans ce contexte que cette partie traitera les différents aspects du risque règlementaire qui est classé aujourd'hui au baromètre des risques au cinquième rang.

En effet, parmi les risques auxquels doit faire face l'entreprise, on compte le risque réglementaire puisque le changement de loi ou de réglementation peut influer directement sur la rentabilité d'un secteur économique.

Le risque réglementaire fait référence à la possibilité que des changements dans les réglementations gouvernementales, les lois ou les politiques puissent avoir un impact négatif sur une entreprise, une industrie ou une activité. Ces changements peuvent provenir de diverses sources, notamment les autorités gouvernementales locales, nationales ou internationales.

Les entreprises opèrent dans un environnement réglementaire qui évolue constamment, et les changements dans les règles et les normes peuvent affecter divers aspects de leurs opérations, de la conformité aux normes environnementales à la protection des consommateurs, en passant par les exigences en matière de sécurité des produits et les pratiques commerciales. Les risques réglementaires peuvent se manifester sous différentes formes, telles que des sanctions financières, des litiges, des pertes de réputation, des coûts de conformité accrus, des limitations opérationnelles, ect.

Les entreprises doivent surveiller de près l'évolution du cadre réglementaire dans lequel elles opèrent, anticiper les changements potentiels et prendre des mesures proactives pour se conformer aux nouvelles réglementations.

Les secteurs fortement réglementés, tels que la finance, la santé et l'énergie, sont particulièrement sensibles aux risques réglementaires. Les équipes de gestion des

risques au sein des entreprises sont souvent responsables de l'identification, de l'évaluation et de la gestion de ces risques pour assurer la durabilité et la conformité à long terme de l'entreprise.

Aujourd'hui, les nouvelles réglementations peuvent amener les entreprises à revoir l'efficacité de leur gouvernance et de leurs processus. L'adoption continue de nouvelles réglementations ou de propositions de réglementations en matière de protection des données personnelles, de lutte anti-blanchiment, de protection de l'environnement peut entraîner des défis opérationnels liés aux obligations de déclaration, de reporting et de conformité.

En outre, la surrèglementation, la mauvaise réglementation, la non-réglementation et l'extraterritorialité de la réglementation ont été identifiées comme des risques dans plusieurs domaines d'activités.

Les enjeux des risques règlementaires au niveau du marché de l'assurance

Les risques réglementaires se réfèrent aux dangers et aux incertitudes auxquels une organisation est exposée en raison de changements dans les règles, les lois et les réglementations gouvernementales. Aujourd'hui, les compagnies font désormais face à une avalanche de mesures règlementaires qui s'abattent actuellement sur les entreprises.

Du règlement général sur la Protection des Données à la directive sur les marchés des instruments financiers (MIFID 2) en passant par IFRS17, la prolifération des nouveaux impératifs réglementaires est de nature à inquiéter les assureurs. Selon l'enquête annuelle réalisée par l'agence de notation Moody's. « L'ensemble de ces mesures augmentent les coûts réglementaires et introduisent de lourdes exigences de reporting ». Classant ce risque au premier rang des inquiétudes des assureurs européen, suivi par le risque de la volatilité des marchés, conséquence des fluctuations récentes dans les marchés financiers.

En effet, les risques réglementaires peuvent avoir un impact significatif sur le secteur de l'assurance. Les changements dans l'environnement réglementaire peuvent influencer divers aspects de l'industrie de l'assurance de plusieurs manières.

En effet, l'augmentation de la complexité des règlementations et du niveau des sanctions entraine un impact important sur les coûts de fonctionnement (sanctions ou mise en conformité).

Le Changement règlementaire qui traduit notamment un risque de surtransposition des directives avec effet parfois rétroactif, pourraient avoir des conséquences opérationnelles, comptables ou prudentielles, touchant les entreprises en termes de coûts avec en particulier l'affectation de ressources humaines en permanence sur des tâches auxiliaires, contraignant au regroupement des établissements les plus petits.

De nouvelles règlementations pourraient pénaliser le business model avec un risque de mise à l'arrêt de l'activité.

Des évolutions des normes comptables ou du référentiel prudentiel pourraient conduire à une illisibilité du bilan et accroître le risque financier.

1. La conformité

Compte tenu de la complexité de la réglementation, notamment en matière de fiscalité, de commerce, d'énergie, d'environnement, de cyber sécurité et de sécurité, la fonction conformité est souvent l'un des postes clés des entreprises qui permet de composer avec la difficulté du cadre réglementaire et à créer de la valeur pour l'entreprise.

En effet, la fonction de conformité est une entité chargée de veiller à ce que l'entreprise opère en conformité avec les lois, les réglementations, les normes éthiques et les pratiques internes établies. Cette dernière joue un rôle essentiel pour atténuer les risques juridiques, financiers et de réputation auxquels une entreprise pourrait être confrontée en raison du non-respect des normes éthiques ou des obligations légales et réglementaires.

Conformité réglementaire :

Les compagnies d'assurance doivent

constamment s'assurer qu'elles respectent les réglementations en vigueur. Les modifications des règles et des normes peuvent entraîner des coûts supplémentaires liés à la mise en conformité, tels que la mise à jour des systèmes informatiques, la formation du personnel et l'adaptation des processus opérationnels.

Ci-joint quelques **exemples** :

- Exigences en capital : Les régulateurs imposent souvent des exigences en matière de capital aux compagnies d'assurance pour garantir leur stabilité financière et protéger les assurés. Des changements dans ces exigences peuvent avoir un impact sur la rentabilité et les opérations des assureurs.
- Innovation et technologie : Les réglementations peuvent également influencer la manière dont les compagnies d'assurance adoptent et intègrent de nouvelles technologies. Par exemple, des règlements sur la protection des données peuvent affecter la façon dont les assureurs gèrent et stockent les informations clients.
- Tarification et souscription : Les réglementations peuvent également influencer les pratiques de tarification et de souscription. Des restrictions ou des exigences spécifiques peuvent être imposées, ce qui peut influencer les prix des polices d'assurance et les critères d'admissibilité.
- Gestion des risques : Les réglementations peuvent également influencer la manière dont les assureurs gèrent et évaluent les risques. Des exigences spécifiques peuvent être imposées en matière de reporting et de surveillance des risques, ce qui peut nécessiter des investissements importants dans les systèmes et les processus.
- Protection des consommateurs : Les réglementations visent souvent à protéger les droits des consommateurs. Cela peut inclure des exigences en matière de divulgation d'informations, de transparence dans les contrats d'assurance et de protection des consommateurs contre les pratiques commerciales déloyales.
- Sanctions et amendes : Les entreprises d'assurance qui ne respectent pas les réglementations peuvent faire face à des sanctions financières et à des amendes. Cela peut avoir un impact direct sur leur rentabilité et leur réputation.

L'ensemble de ces risques sont également susceptibles d'avoir un impact sur la souscription, la sinistralité, les fonds propres ou le ratio de solvabilité.

Comment la fonction conformité peut-elle être conçue pour détecter et atténuer les risques :

Pour détecter et atténuer les risques, la fonction conformité doit être conçue de manière à déployer des procédures préventives et à établir un cadre opérationnel capable de détecter les risques à travers les démarches suivantes :

- Elle doit être intégrée et liée à la protection de la réputation et à l'amélioration du rendement de l'entreprise.
- La fonction de conformité doit être sous la responsabilité d'un chef de la conformité possédant une expérience pertinente et capable de proposer des plans d'action en cas de lacunes importantes.
- Elle doit être intégrée à toutes les décisions d'affaires et alignée sur les valeurs de l'entreprise.
- Enfin, la fonction de conformité doit être soutenue par une solide culture de conformité initiée et appuyée par la haute direction et le conseil d'administration.

2. La protection des données personnelles :

De par la spécificité de l'activité des compagnies d'assurance et de réassurance qui sont amenées à recueillir d'importants volumes de données personnelles à travers les informations, qui proviennent aussi bien des formulaires remplis par les assurés eux-mêmes, que des acteurs rencontrés pendant le parcours client.

En effet, afin de mieux évaluer le risque et fixer les tarifs des contrats, lors de la souscription, les compagnies recueillent de nombreuses données personnelles (âge, sexe, domicile, profession, état de santé...) mais également des données nécessaires pour le règlement des sinistres.

Ainsi, les principales catégories de données traitées sont les suivantes :

- Les données d'identification : sont les données relatives à l'identification des personnes, parties intéressées ou intervenantes au contrat (Noms et prénoms, nationalité, numéros des pièces d'identités….).
- Les données relatives à la situation familiale: comprend notamment les éléments relatifs à la situation matrimoniale, le nombre d'enfant, l'âge, les héritiers.
- Les données relatives à la situation économique, patrimoniale et financière sont notamment les éléments relatifs aux : salaire, patrimoine mobilier et immobilier, autres revenus, crédits, identifiant fiscal, régime fiscal, statut fiscal, pays de résidence et imposition.
- Les données relatives à la situation professionnelle: La catégorie socioprofessionnelle, le secteur d'activité, les compétences et qualifications professionnelles.
- Les données de géolocalisation des personnes ou des biens en relation avec les risques assurés ou les services proposés: notamment les adresses postales, électroniques, les contacts téléphoniques.
- Les données relatives aux habitudes de vie et aux usages des biens en relation avec les risques assuré sont : les loisirs, activités sportives, trajets et kilométrages parcourus, présence d'animaux domestiques.
- Les données relatives à la détermination ou à l'évaluation des préjudices et des prestations : Il s'agit notamment des données liées au sinistre, les rapports d'expertise, les éléments afférents aux procédures administratives ou judiciaires éventuellement engagées; des données liées aux victimes : la nature et l'étendue des préjudices subis, le taux d'invalidité/ d'incapacité, les rentes, le capital décès, les montants des prestations.
- Les données sur les risques clients ou de la transaction: sont ceux relatives à la solvabilité, les jugements de faillite, l'implication ou la suspicion dans des actes et/ou transactions frauduleux, ceux liées aux déclarations et prestations sur sinistres d'assurance et données sur le risque d'impayé et le recouvrement des créances, à l'application des règles relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme et toutes informations liées aux contrôles requis par la législation en vigueur pour la gouvernance des risques (numéro de chèque, numéro de carte bancaire et sa date de fin de validité, les références bancaires).
- Les données sur les services demandés ou utilisés et comportement liés à ces services, notamment des données sur les services demandés, en cours d'utilisation ou utilisés dans le passé notamment les garanties incluses dans les contrats d'assurances et les sinistres déclarés, les canaux de distribution, les habitudes et aux préférences par rapports aux services offerts.
- Les données sur les interactions : Ce sont les données relatives aux interactions avec les intermédiaires en assurances, sur les sites internet, sur les applications et les courriers postaux et/ou électroniques et par tout autre moyen de communication, notamment pour demander un service ou une assistance, faire une réclamation ou en répondant à une enquête de satisfaction..
- Les données sensibles : doivent faire l'objet d'une attention toute particulière de la part des responsables de traitement.

Les données sensibles sont des données à caractère personnel qui contiennent des informations sensibles qui, si elles étaient révélées, pourraient avoir des incidences néfastes sur la vie privée des personnes concernées ou dont le traitement est susceptible de leur créer des risques.

Ces données étant confidentielles et parfois sensibles, leur utilisation est strictement encadrée, elles ne peuvent servir qu'à une finalité précise et pour une durée limitée, fixée par la loi.

Conscientes de ce défi majeur, les entreprises d'assurances et de réassurance ont lancé le tout premier guide pratique de protection des données personnelles dédié au secteur des assurances visant l'adoption des bonnes pratiques pour protéger les données des assurés telles que :

- La sensibilisation du personnel aux pratiques de gestion des données et de sécurisation des systèmes informatiques.
- La mise en place des processus internes inspirés de la loi sur la protection des données personnelles.
- Le respect des délais de conservation des données.
- La sécurisation des accès des personnels et de toutes les personnes intéressées par la mise en place d'un système d'authentification forte dans le cadre de l'accès aux systèmes d'information.
- Le stockage des données personnelles des assurés dans des serveurs sécurisés.
- La nomination d'un Data Protection Officer.

La protection des données personnelles dans le cadre de la lutte contre le blanchissement des capitaux et le financement du terrorisme :

Cette obligation est régie par les conventions FATCA, l'OCDE, le circulaires et décisions du CGA.

Il s'agit du traitement des données qui sont nécessaires à l'exercice des missions confiées aux autorités publiques dans le cadre de la sécurité publique ou de la défense nationale, ou qui s'avèrent nécessaires à la mise en œuvre des poursuites pénales ou à l'exécution des missions dont elles sont investies conformément aux lois et règlements en vigueur.

Pour le secteur des assurances et de réassurance, il s'agit des traitements des données personnelles des souscripteurs, assurés et bénéficiaires des contrats d'assurances dans le cadre de l'application de la législation et la réglementation en vigueur relative à la lutte contre le blanchiment d'argent et le financement du terrorisme.

Ainsi, il s'agit principalement des traitements afin de permettre :

1. La mise en œuvre des obligations de vigilance à l'égard de la clientèle conformément à l'approche par les risques.
2. La recherche des personnes qui doivent faire l'objet de mesures de vigilance complémentaires en tant que personnes politiquement exposées (PPE).
3. Le déclenchement des alertes et déclarations de soupçon.

4 - La mise sous surveillance de certains contrats ou clients sur la base de la classification des risques élaborée par la compagnie, ou d'opérations jugées complexes, d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite, ou d'une déclaration de soupçon n'ayant pas donné lieu à la résiliation de contrat.

5. L'analyse et la détermination du niveau de risque propre à chaque opération de maniement des fonds.

6 - La mise en place d'une surveillance adaptée visant à détecter les opérations portant sur des sommes dont elle sait, soupçonne ou a de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou participent au financement du terrorisme.

7. La garantie du respect des éventuelles mesures relatives aux sanctions financières nationales et internationales d'embargo et de gel des avoirs en vigueur.
8. Les vérifications complémentaires nécessaires.
9. L'application des mesures de gel des avoirs.

3 Promouvoir le cadre règlementaire du marché tunisien des assurances et l'adapter aux standards internationaux.

Le secteur des assurances en Tunisie est régi par un ensemble de dispositions législatives et réglementaires réunis dans un code des assurances promulgué par la loi n°92-24 du 9 mars 1992.

Ce code a pour objet de définir les règles et les principes qui encadrent l'activité des compagnies d'assurance, des intermédiaires d'assurance, et de protéger les intérêts des assurés.

Il est a souligné qu'un nouveau projet de loi sur le code des assurances sera prochainement

présenté au conseil des ministres, visant à adapter le cadre juridique du secteur des assurances aux standards internationaux afin de promouvoir la compétitivité des sociétés d'assurances compte tenu de leur rôle important dans la mobilisation de l'épargne nationale.

Un programme de réforme en profondeur est mis en œuvre après l'achèvement d'une étude actuarielle pour améliorer la compétitivité des entreprises et promouvoir leur productivité.

Ce programme s'articule autour de la modernisation de la législation et son adaptation aux normes internationales, le renforcement de l'assise financière des compagnies d'assurance à travers l'augmentation du capital minimum requis, l'instauration du principe de la spécialisation en assurance vie.

Toute une partie sera consacré aux normes prudentielles, il s'agit notamment :

- La solvabilité II :

désigne un projet de réforme de la réglementation prudentielle, le premier au niveau mondial dans le domaine des assurances. Ce concept dont les mesures auront des incidences sur les produits d'assurance et de réassurance.

Dans la lignée de Bâle III, cette réforme européenne de la réglementation prudentielle s'applique au secteur de l'assurance et doit lui permettre de garantir sa solvabilité.

Elle vise un renforcement des capacités des assureurs à respecter leurs engagements auprès de leurs clients, à savoir augmenter les fonds propres pour faire face aux évènements imprévus et maîtriser la gestion des risques. Cela se traduit par un relèvement du niveau des capitaux propres proportionnellement aux risques encourus sur les actifs détenus (immobilier, actions, obligations) : plus l'actif est risqué, plus l'exigence en matière de capitaux propres sera élevée.

Chaque assureur doit être capable d'évaluer les risques inhérents à son activité pour pouvoir allouer suffisamment de capital pour les couvrir.

Les exigences quantitatives en matière de gestion des risques doivent être accompagnées d'exigences qualitatives, c'est-à-dire une gouvernante solide capable de mettre en place un système de contrôle interne efficace.

Solvabilité II, régira le dispositif de surveillance des compagnies d'assurance. Les assureurs estiment que les nouvelles normes prudentielles fixant les exigences sur le niveau des fonds propres entraîneront une augmentation des primes de certains produits d'assurance. Exemple : entre 5% et 20% dans la couverture des risques en responsabilité civile et automobile. La charge de capital supplémentaire (entre 30% et 40%) incitera certains acteurs à délaisser des types de placement (actions), quitte à renoncer à leur rôle d'investisseurs à long terme dans les entreprises, quand il en obligera d'autres (ceux de petite ou moyenne taille) à fusionner, voire à déposer le bilan.

On voit déjà l'impact de la réforme sur l'assurance vie. Les assureurs investissent une grande partie des fonds confiés par les assurés sur les obligations d'Etat sans risque, mais à faible rendement.

- Les normes IFRS

Après les scandales financiers du début des années 2000 en Europe et aux États-Unis (Enron, Worldcom), les pouvoirs publics cherchent à renforcer la confiance du public à travers des textes renforçant la sécurité financière. Dans ce contexte, l'Europe souhaite harmoniser les documents financiers de ses états membres par le choix d'un référentiel comptable unique : les normes IFRS (International Financial Reporting Standards) reconnues sur le plan international.

En 1973, Sir Henry Benson (un associé de Coopers & Lybrand) créé l'organisation internationale privée, l'IASC (International Accounting Standard Committee), qui regroupe 10 pays fondateurs (l'Allemagne, l'Australie, le Canada, les États-Unis, la France, le Japon, le Mexique, les Pays-Bas, la Grande Bretagne et l'Irlande).

Les 3 objectifs majeurs de l'IASC à sa création sont :

- D'établir des normes comptables acceptables sur le plan international.

- De promouvoir l'utilisation et l'application rigoureuse de ces normes.

- De travailler pour harmoniser les réglementations comptables et la présentation des états financiers sur le plan international.

Les normes IFRS s'adressent avant tout aux investisseurs et aux analystes financiers. Elles doivent leur permettre de :

- Comprendre l'activité économique de l'entreprise à la simple lecture des documents comptables.

Prendre des décisions financières appropriées.

Dans ce sens, les normes IFRS cherchent à coller à la réalité économique du marché, à la loi de l'offre et de la demande.

Déployées dans plus de 160 pays, les normes IFRS concernent les entités ayant une obligation de rendre des comptes aux autorités (sociétés cotées et institutions financières).

Les normes évoluent normalement avec le temps. Certaines normes devenues obsolètes sont alors remplacées par d'autres pour répondre aux besoins d'un contexte économique, juridique et social spécifique. C'est le cas par exemple de la norme IFRS9 qui vient remplacer la norme «IAS 39 - Instruments financiers.

IFRS 15 : Cette norme est mise en place en janvier 2018 pour améliorer l'information relative au chiffre d'affaires.

IFRS 16 : Destinée aux contrats de location, la norme IFRS 16 s'applique depuis le 1ère janvier 2019.

IFRS 17 : remplace l'IFRS 4 qui autorise les entreprises à utiliser les règles comptables nationales.

IFRS 17 modifie le traitement comptable des contrats d'assurance et des contrats d'investissement chez les assureurs en prévoyant une comptabilisation plus homogène. Cette norme est entrée en vigueur le 1ère janvier 2023.

La norme IFRS 17 principes de base et objectifs

IFRS 17 est une nouvelle norme comptable internationale destinée au secteur de l'assurance, elle permet aux compagnies d'assurance d'harmoniser la présentation des états financiers à l'échelle internationale.

Compte tenu de la complexité de l'implémentation de cette norme et aux défis auxquels se sont heurté les compagnie d'assurance, la date d'entrée en vigueur de cette norme a été retardé plusieurs fois, pour enfin s'établir au 1 janvier 2023 à l'échelle Européen et retardée au 1ère janvier 2025 pour les autres pays émergents à l'instar de la Tunisie.

En effet, les demandes de report s'expliquent par les difficultés rencontrées sur ce projet et notamment par le niveau d'agrégation des contrats dit de « cohortes annuelles ». Le sujet comporte des implications assurantielles remettant en cause les équilibres liés à la mutualisation, mais aussi des enjeux de système d'information et de pilotage de résultat.

Les enjeux de la norme IFRS 17

La nouvelle norme modifie fortement la présentation du compte de résultat et aura des impacts en termes de communication financière. Le résultat en IFRS 17 dépend principalement de la classification des actifs et des modèles de valorisation des provisions techniques retenus pour l'évaluation du passif. IFRS 9 propose trois méthodes de valorisation des actifs.

La variation des actifs calculée par chacune de ces méthodes aura un impact différent sur le bilan et le compte de résultat.

Selon la nature des passifs et les méthodes de valorisation utilisées, les chocs techniques ou financiers sur les provisions techniques auront un impact différent sur le bilan et sur le compte de résultat. Ainsi, pour le modèle général, la CSM (marge de service contractuelle) est créditée des intérêts calculés sur la base de la courbe des taux à l'origine. Ensuite, elle est ajustée des écarts d'estimation des flux relatifs aux services futurs à l'exception des variations sur les conditions économiques et financières et des écarts d'estimation sur les sinistres survenus.

Le montant de la CSM est finalement alloué en résultat une fois la prise en compte des autres ajustements sur la CSM de début de période effectuée.

Le résultat en IFRS 17 sera plus délicat à appréhender et à anticiper du fait de la complexité de la norme et de la volatilité de certains mécanismes. Le délai supplémentaire accordé doit être utilisé pour tester différents scénarios et identifier ainsi les leviers de pilotage et assurer une communication financière transparente et maîtrisée.

Les leviers de pilotage devront faire l'objet de simulations pendant cette période complémentaire pour orienter les décisions structurantes avant l'entrée en vigueur de la norme.

Les nouveaux défis :

Une nouvelle maille de calcul : une des nouveautés de la norme IFRS 17 a porté sur le niveau de granularité utilisé ainsi que les enjeux liés à la volumétrie mais aussi à la nécessaire analyse des informations produites. Concernant les outils de modélisation, on anticipe que des ajustements des modifications variées seront nécessaires pour adapter les systèmes actuels à des délais de production des données bien plus restreints que ceux actuellement requis.

L'automatisation des processus de production des données devient ainsi incontournable pour gagner en rapidité et en sécurité. IFRS 17 joue dans ce domaine un rôle d'accélérateur.

Des équipes projet aux compétences transversales : La mise en œuvre d'IFRS 17 impose d'intégrer dans les équipes projet des compétences transversales. Les actuaires sont davantage associés aux travaux comptables: un dialogue entre les actuaires et les comptables est ainsi nécessaire, jusque dans la rédaction des schémas comptables.

Plus largement, IFRS 17 implique une proximité accrue entre les équipes finance et les équipes risques et actuariat. Le compte de résultat est emblématique de cette évolution, avec un chiffre d'affaires issu des systèmes de provisionnement et des charges d'assurances provenant du déversement des systèmes métier. Les systèmes d'information financière devront s'adapter à cette nouvelle donne.

En parallèle, IFRS 17 pose de nouveaux enjeux managériaux, tout spécialement au sein des équipes comptables dont le rôle va évoluer avec l'automatisation croissante des travaux de réconciliation. Par ailleurs, les attributions de chacun (actuariat, comptabilité, contrôle de gestion) seront probablement amenées à évoluer.

Dans la phase de préparation de la mise en œuvre, comprendre la philosophie de la norme, grâce à une formation ciblée, permettra de faire gagner du temps.

Une plus grande attention portée au bilan : L'impact d'IFRS 17 devrait être très important sur la communication financière et le pilotage du résultat même si les éventuels contrats «onéreux» pourraient poser moins de problème qu'initialement prévu. En revanche, les intervenants s'attendent à une plus grande attention portée au bilan.

Pour nos intervenants, IFRS 17 représente une opportunité de faire monter en compétence les équipes et de renforcer les outils d'analyse, notamment sur les marges et la rentabilité des contrats.

La norme IFRS 17 réclame un investissement majeur de la part de l'ensemble des acteurs. En effet, les enjeux de la première application sont clairement liés au niveau de la marge de service contractuelle qui sera calculée lors de l'entrée en vigueur, car il conditionne les résultats futurs et la capacité des assureurs à faire face à des déviations de sinistralité.

L'implantation progressive de la norme IFRS 17

Adoptée à fin juillet 2022 dans plus de 144 pays, la norme IFRS 17 est appliquée dans certains pays depuis janvier 2023. Certains groupes basés aux États-Unis continuent de publier leurs états financiers en US GAAP (Principes comptables américains).

En ce qui concerne le continent européen, les compagnies vie et non vie, se sont déjà alignés sur la nouvelle norme IFRS 17 lors de la présentation de leurs états financiers du premier trimestre et du premier semestre 2023.

Les grands groupes d'assurance du Moyen-Orient ont démontré un niveau de préparation élevé. Certaines compagnies comme GIG (Koweït) et QIC (Qatar) ont déjà publié des résultats trimestriels conformes à la nouvelle norme IFRS 17.

La banque centrale d'Arabie Saoudite (SAMA) ainsi que l'autorité du marché financier émirati ont également annoncé l'adoption officielle de la nouvelle norme.

Pour les pays de l'Afrique, on constate beaucoup de divergences entre le nord et le centre du continent, en effet, le Maroc et la Tunisie prévoient, l'adoption complète d'IFRS en 2025. En Côté d'Ivoire, les autorités financières ont exprimé leur intention d'adopter la norme sans pour autant préciser la date.

En Afrique du Sud, la version locale de la norme SAURS 17 est déjà en vigueur pour les compagnies d'assurance depuis le 1er janvier 2023.

La Responsabilité Sociétale de l'Entreprise :

La Responsabilité Sociale des Entreprises (RSE) est un concept qui fait référence à la prise en compte, par les entreprises, des impacts de leurs activités sur la société et l'environnement. La RSE englobe un ensemble de pratiques volontaires qui vont au-delà des obligations légales, visant à contribuer positivement au bien-être social, à la protection de l'environnement et au développement durable.

Les principales dimensions de la RSE incluent généralement :

1. La dimension économique : Il s'agit de la contribution de l'entreprise à la création de richesse, à la croissance économique et à la génération d'emploi. Cela englobe également la transparence financière et la gestion responsable des ressources.
2. La dimension sociale : La RSE implique une considération des droits des travailleurs, des conditions de travail équitables, de la diversité et de l'inclusion, de la santé et sécurité au travail, ainsi que des initiatives en faveur des communautés locales.
3. La dimension environnementale : Les entreprises engagées dans la RSE cherchent à minimiser leur impact environnemental en adoptant des pratiques respectueuses de l'environnement, en réduisant les émissions de gaz à effet de serre, en favorisant l'efficacité énergétique, etc.
4. La dimension éthique : implique également des pratiques commerciales éthiques, le respect des droits de l'homme, la lutte contre la corruption et la promotion d'une culture organisationnelle basée sur des valeurs éthiques.

Les entreprises adoptent la RSE pour diverses raisons, notamment pour renforcer leur réputation, attirer et fidéliser les clients et les employés, répondre aux attentes croissantes des parties prenantes et contribuer positivement à la société dans laquelle elles opèrent.

Il est important de noter que la RSE peut varier d'une entreprise à l'autre et peut être influencée par la nature de l'industrie, la taille de l'entreprise, et les spécificités régionales.

En Tunisie, depuis plusieurs années le secteur financier a adhéré à ce phénomène et a commencé à travailler activement pour pouvoir être un élément actif et apporter son soutien au tissu économique du pays.

Le cadre réglementaire de la responsabilité sociétale a été expressément introduit dans l'ordonnancement juridique à travers la loi n° 2018-35 du 11 juin 2018 qui en a fait une obligation à la charge des entreprises et autres institutions.

En effet, l'article 2 de la loi n° 2018-35 invite les entreprises publiques et privées et toute autre institution à consacrer des fonds au financement de projets permettant le développement de l'employabilité des jeunes et de l'économie verte ; l'article 4 crée des commissions régionales RSE en tant que structures de proposition d'idées de projets appropriés pour les régions et comités d'orientation et de gestion des projets RSE et l'article 6 (et dernier) institue un observatoire national RSE auprès de la présidence du gouvernement pour le suivi et la coordination des activités RSE dans le pays.

La démarche RSE en Tunisie est conforme aux engagements internationaux antérieurs du pays au titre :

- Du pacte mondial des Nations Unies (2000) (1), sachant qu'une cinquantaine d'entreprises publiques et privées sont partenaires du Pacte mondial RSE des Nations Unies, programme piloté par l'Institut de la responsabilité sociale de l'entreprise en Tunisie (IRSET) et que les premières assises nationales de la RSE ont été organisées en novembre 2017 afin de vulgariser le concept, mettre en valeur les « success stories » des entreprises tunisiennes partenaires du programme et donner l'opportunité à de nouvelles entreprises d'y adhérer.
- Des Objectifs du Développement Durable (ODD-2015-2030) pour la paix, l'humanité, la planète et la prospérité, adoptés en septembre 2015 par 193 États membres de l'Organisation des Nations Unies, sous la forme d'un Plan d'action à l'horizon 2030, nécessitant la mise en œuvre de partenariats multi-acteurs où chacun a vocation à faire sa part (gouvernements, secteur privé et société civile) ;
- Des Constitutions du 27 janvier 2014 et du 25 juillet 2022, qui ont consacré le droit à l'eau et à un environnement sain, de même qu'elles ont mis l'accent sur le devoir de l'État de contribuer à la sécurité climatique

L'article 1er de la loi n° 2018-35 du 11 mai 2018 sur la responsabilité sociétale des entreprises dispose d'ailleurs clairement que «La responsabilité sociétale des entreprises se fonde sur les principes consacrés par la Constitution et la communauté internationale, tels qu'énoncés par le Pacte des Nations Unies sur la responsabilité sociale, la Déclaration universelle des droits de l'homme, les conventions de l'OIT et la Déclaration de Rio sur l'environnement et le développement», sachant que le dernier alinéa du même article identifie la RSE comme « un principe adopté par les entreprises pour assumer les conséquences de l'impact de leurs activités sur la société et l'environnement, grâce à une démarche transparente entraînant des retombées communautaires positives au niveau local».

Afin de cerner l'importance de la responsabilité sociétale des entreprises et son potentiel pour les entreprises tunisiennes, il convient de rappeler qu'elle résulte des demandes de la société civile (associations écologiques et humanitaires) en vue d'une meilleure prise en compte des impacts environnementaux et sociaux des activités des entreprises.

Le lien entre l'objectif macroéconomique de la RSE (participation des entreprises à la réalisation du DD) et la satisfaction des parties prenantes de l'entreprise est toutefois assez complexe, d'autant que le développement durable ne dépend pas exclusivement des entreprises mais de tous les acteurs.

La RSE en tant que bonne gouvernance se traduit de différentes manières :

- La définition d'une éthique, formalisée dans une charte de l'entreprise,
- La mise en relation avec les parties prenantes de l'entreprise (tous les acteurs ayant des intérêts par rapport à la gestion de l'entreprise : clients, fournisseurs, employés, associations locales, collectivités territoriales, société civile représentée par les ONG),
- La mise en place de programmes de gestion des risques,
- Une surveillance accrue des principes de sécurité,
- Une veille, notamment environnementale, sociale, sociétale, et juridique,
- Des projets de gestion des connaissances en support à l'innovation qui impliquent également plusieurs types d'agents économiques : les acteurs publics territoriaux de l'enseignement et de la recherche (pôles de compétence).
- Des programmes d'assurance qualité, avec la mise en œuvre des nouvelles normes,
- La corrélation avec la nature du lien social et de la performance.
- Une communication interne et externe, incluant notamment des bilans sociaux et environnementaux.

L'approche RSE peut permettre de mettre en œuvre, entre autres, de nouvelles régulations et une meilleure gouvernance de l'entreprise, que l'entreprise soit grande, moyenne ou petite, dans les pays dits développés, comme dans les pays en développement. Son avantage réside en l'instauration d'une meilleure contextualisation des activités économiques des entreprises, une meilleure structuration des relations avec les parties prenantes et une meilleure gouvernance d'entreprise.

Plusieurs programmes en cours de réalisation en Tunisie vont dans le sens d'une introduction progressive de la responsabilité sociétale des entreprises et organisations (RSE/RSO), à travers des initiatives permettant de mettre en place des actions dans les trois domaines du développement durable.

Il s'agit souvent de programmes sectoriels (industrie, environnement, énergie...) pilotés par un ou plusieurs ministères, en collaboration avec diverses structures publiques et/ou privées.

Depuis 2005, 44 entreprises et organisations tunisiennes se sont engagées au titre du Pacte Mondial (dont 6 ONG, 2 universités et 1 institution publique) et plusieurs stratégies ont été développées, telles que la Stratégie nationale de développement durable (SNDD - 2012) ou la (Stratégie nationale pour une économie verte (SNEV - 2016).

Le Centre international des technologies de l'environnement de Tunis (CITET) a piloté plusieurs projets de ce type, notamment le programme de production propre ou l'Ecolabel tunisien, ainsi que le projet de Label RSE, en partenariat avec la Confédération des entreprises citoyennes de Tunisie (CONECT), qui a démarré en 2012, sur la base d'un appel à candidature des entreprises ayant un nombre de salariés inférieur à 500 personnes.

Les acteurs les plus reconnus en matière de RSE en Tunisie sont les suivants :

- Le centre international des technologies de l'environnement de Tunis (CITET) et la Confédération des entreprises citoyennes de Tunisie (CONECT) qui collaborent sur plusieurs projets pilotes en matière de RSE/RSO.
- L'institut national de la normalisation et de la propriété intellectuelle (INNORPI), qui contribue à la diffusion de la norme ISO 26 000
- L'institut de la responsabilité sociétale des entreprises en Tunisie (IRSET) qui sensibilise les entreprises aux bienfaits de la RSE/RSO et à la nécessité d'adhérer à un programme structuré, notamment le Pacte Mondial des Nations Unies...

Parmi les projets les plus significatifs figure le projet pilote pour la mise en place de l'ISO 26 000 dans certaines institutions publiques et privées.

Ce programme a permis d'introduire une certaine dynamique de RSE parmi les participants et a donné lieu à la formation d'une quinzaine d'experts et à l'animation d'une cinquantaine de séminaires.

Ce projet a aussi permis d'instaurer une dynamique concrétisée par la production du Référentiel national de la gouvernance (RNG), finalisé en 2016 et destiné à toutes les organisations publiques ou privées en tant que cadre visant à consolider l'intégrité et l'éthique professionnelles dans le cadre de la prévention de la corruption et de la décentralisation de la prise de décision.

Le secteur des assurances en Tunisie, un des piliers du tissu économique a fortement adhéré à ce projet et a commencé à travailler activement pour améliorer le climat des affaires et instaurer une culture de développement durable.

En effet, conscient des défis environnementaux et économiques, plusieurs projets ont été réalisés en collaboration avec les différents ministères et organisations à but non lucratif dans le but de soutenir et promouvoir les valeurs de la responsabilité sociétale.

En résumé, les risques réglementaires peuvent créer des défis pour les compagnies d'assurance, mais elles doivent également être perçues comme des opportunités d'adaptation et d'innovation afin de rester conformes et concurrentielles sur le marché.

Une gestion efficace des risques réglementaires est essentielle pour assurer la viabilité à long terme des entreprises d'assurance.

Il est essentiel pour les entreprises de mettre en place des processus de gestion des risques efficaces, y compris une veille réglementaire constante, pour anticiper, comprendre et atténuer les risques réglementaires potentiels. La conformité proactive permet non seulement d'éviter des sanctions, mais elle peut également renforcer la confiance des parties prenantes et contribuer à la durabilité à long terme de l'entreprise.

Conclusion

Au fil du temps, nous observons des fluctuations cycliques et des changements périodiques, dans le classement des risques émergents qui sont devenus un phénomène complexe qui caractérise la nature dynamique de l'environnement des affaires. Influencés par des facteurs tels que les évolutions économiques, les avancées technologiques et les tendances sociopolitiques. Cette dynamique instable nécessite une vigilance constante de la part des entreprises et des décideurs, les obligeant à ajuster régulièrement leurs stratégies de gestion des risques pour rester adaptés à un environnement dynamique. La compréhension des fluctuations cycliques dans le classement des risques émergents devient ainsi un élément essentiel pour anticiper, atténuer et réagir de manière proactive aux défis émergents.

Certes, dans ce paysage en constante évolution des risques émergents exige une réponse sophistiquée, le dilemme serait alors comment faire face à ces risques émergents qui nécessite une approche proactive et systématique. La gestion efficace de ces risques est devenue primordial dans le contexte actuel de changement technologique rapide, de perplexité politique et d'évolution des attentes des parties prenantes.

Chaque type de risques spécifiques nécessite une compréhension approfondie et des mesures ciblées. Des mesures de cybersécurité robustes, une prévoyance diplomatique, des pratiques durables et des stratégies économiques vigilantes sont identifiées comme des composants décisoires pour faire face aux menaces cybernétiques, à l'instabilité géopolitiques, aux événements climatiques et aux défis financiers.

Les organisations et les sociétés sont exhortées à rester vigilantes, à ajuster leurs stratégies et à s'engager dans des efforts collectifs pour construire les bases d'un avenir prospère au milieu des risques émergents.

La collaboration entre les secteurs est indispensable pour relever des défis tels que l'inflation, les guerres commerciales, les troubles sociaux et les pressions liées au changement climatique. Investir dans le talent en cybersécurité est souligné comme une priorité pour combler le fossé des compétences et naviguer dans cette décennie incertaine et turbulente.

L'intégration de l'assurance dans la stratégie globale de gestion des risques est soulignée comme un élément clé. L'assurance agit comme un filet de sécurité financier contre les pertes potentielles liées à divers risques, contribuant à la résilience globale. L'approche interconnectée reconnaît que l'atténuation implique à la fois la prévention et la préparation.

Les compagnies de (ré)assurance fournissent les principes clés et des conseils pratiques pour soutenir les équipes de gestion des risques d'entreprise dans l'évolution de leur approche face aux risques émergents. Le code de gouvernance d'entreprise souligne à juste titre l'importance de capturer les risques émergents, et malgré les défis, les fonctions de gestion des risques sophistiquées sont exhortées à établir des processus efficaces.

Alors que le monde fait face à un ensemble de risques familiers et nouveaux, Il est indispensable de capturer et à évaluer systématiquement les informations grâce à un processus défini, méthodique et structuré.

Cette approche renforce la capacité à identifier, prioriser et agir sur les risques et opportunités émergents, favorisant un avenir résilient, sécurisé et durable.

Bibliographie

- **Les Changements Climatiques**

– https://www.un.org/en/climatechange/science/mythbusters

– https://fr.wikipedia.org/wiki/Ouragan_Dorian#/media/Fichier:Dorian_2019-09-01_1002Z.jpg

– https://www.ledevoir.com/monde/etats-unis/785005/des-inondations-en-californie-font-deux-morts-et-des-milliers-d-evacues

– https://fr.wikipedia.org/wiki/Ouragan_Dorian#/media/Fichier:Dorian_2019-001_1002Z.jpg

- **Les Risques Cyber**

– Swiss Re Institute: about cyber insurance market

Amcs group: trends-in-cybersecurity-2023

Moodys cyber report

– Microsoft Digital Defense

– Hiscox :Cyber Readiness Report

– S&P Global Rating

– AON Cyber report

– www.insurancejournal.com

– www.reinsurancene.ws

– ancs Tunisie : statistics

- **Les Risques Politiques**

– The Global Risks Report 2023 18th edition

– Armed Conflict Location and Event Data (ACLED),

– https://beinsure.com/political-violence-insurance-market/#srcc-frequency-and-severity

– https://www.marsh.com/us/services/political-risk/insights/political-risk-report-2023.html

– https://www.chaucergroup.com/news/year-of-high-stakes-elections-lies-ahead-in-2024-increasing-the-appetite-for-political-risk-insurance

– https://www.howdengroup.com/sites/g/files/mwfley566/files/2023-04/howden-a-world-of-trouble.pdf

- **L'Instabilité Economique**

– https://www.conference-board.org/topics/global-economic-outlook#:~:text=Global%20real%20GDP%20is%20projected,remained%20resilient%20in%20Q3%202023

– https://www.imf.org/en/Publications/WEO/Issues/2024/01/30/world-economic-outlook-update-january-2024

– https://www.oecd.org/perspectives-economiques/fevrier-2024/

– https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

– https://read.oecd-ilibrary.org/view/?ref=1242_1242461-g2kb05p2g8&title=Perspectives-economiques-de-l-OCDE-Rapport-intermediaire-fevrier-2024

– https://read.oecd-ilibrary.org/view/?ref=1242_1242461-g2kb05p2g8&title=Perspectives-economiques-de-l-OCDE-Rapport-intermediaire-fevrier-2024

– https://www.ilboursa.com/marches/la-route-de-la-faillite-ou-la-voie-de-la-reforme-la-tunisie-a-la-croisee-des-chemins_42315

– https://channellife.com.au/story/australia-aims-to-become-global-cybersecurity-leader-by-2030

- **Les Risques Réglementaires**

– Axa future risks report (édition 2023)

– Management des risques/ Pascal Kleber

– Impact des IFRS sur les performances et les risques des compagnies d'assurances : Jean Michel Sahut & Naceur Souissi

– Guide de protection des données personnels/ FTUSA

– Vers une modification radicale du code des assurances

– https://www.ilboursa.com/marches/tunisie-vers-une-modification-radicale-du-code-des-assurances_14472

Tunis Re
...à la hauteur de vos risques

12 Avenue du Jappon. Montplaisir, Tunis - Tunisie
Email: Tunisre@tunisre.com.tn
Site web: www.tunisre.com.tn